eTravel v1.1 with AA

EAC

Common Criteria / ISO 15408
Security Target – Public version
EAL4+

CONTENT

FIGURES

TABLES

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title:	eTravel EAC v1.1 with AA Maia4 EAC Security Target
Version:	v1.0 issued 25 October 2012
ST reference:	ST_D1276270
Origin:	Gemalto
Author:	Antoine DE LAVERNETTE
Product identification:	eTravel EAC v1.1 with AA (version 01 03)
Security Controllers:	NXP P5CD080
TOE identification:	eTravel EAC v1.1 with AA (version 01 03)
TOE documentation:	Operational User Guidance [OPE_MRTD] Preparative procedures [PRE_MRTD]

The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command.

The TOE is the whole eTravel EAC v1.1 with AA product.

CPLC field	Length	Value
IC Fabricator	2	NXP
IC Type	2	P5CD080
Operating System Identifier	3	n.a.
RFU	1	n.a.
Operating System release level	2	n.a.
IC Fabrication Date	2	n.a.
IC Serial Number	4	Unique identification of the chip written by the ICC Manufacturer
IC Batch Identifier	2	n.a.
IC Module Fabricator	2	n.a.
IC Module Packaging Date	2	n.a.
ICC Manufacturer	2	‘Gemalto’
IC Embedding Date	2	n.a.
IC Pre-personalizer	2	‘Gemalto’
IC Pre-personalization Date	2	n.a.
IC Pre-personalization Equipment Identifier	4	n.a.
IC Personalizer	2	n.a.

CPLC field	Length	Value
IC Personalization Date	2	n.a.
IC Personalization Equipment Identifier	4	n.a.

Table 1: Card Production Life Cycle Data

IT Security Evaluation scheme	Serma Technologies
IT Security Certification scheme	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

1.2 ST OVERVIEW

The ST is based on Protection Profile *Machine Readable Travel Document with "ICAO Application", Extended Access Control* [PP-MRTD-EAC].
The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) based on the requirements of the International Civil Aviation Organization (ICAO). More specifically the TOE consists of operating system of MRTD's chip with ICAO application. The TOE is programmed according to Logical Data Structure as defined in [ICAO-9303].
This Security Target defines the security requirements for the TOE. The main security objective is to provide the secure enforcing functions and mechanisms to maintain the integrity and confidentiality of the MRTD application and data during its life cycle.

The main objectives of this ST are:

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

1.3 REFERENCES

1.3.1 External References

[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2009-07-001, version 3.1 rev 3, July 2009
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CCMB-2009-07-002, version 3.1 rev 3, July 2009
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CCMB-2009-07-003, version 3.1 rev 3, July 2009
[CEM]	Common Methodology for Information Technology Security Evaluation Methodology CCMB-2009-07-004, version 3.1 rev 3, July 2009
[ST-IC]	[ST-NXP_80]
[ST- NXP_80]	Security Target, NXP P5CD080/ P5CN080/ P5CC080/P5CC073 V0B Version 2.3 – 05 August 2011
[CR-IC]	[CR-NXP_80]
[CR-NXP_80]	Certification Report, NXP P5CD080/ P5CN080/ P5CC080/P5CC073 V0B BSI-DSZ-CC-700-2011
[FIPS180-2]	*Federal Information Processing Standards Publication 180-2 SECURE HASH STANDARD (+Change Notice to include SHA-224),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2002 August 1
[FIPS46-3]	*Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES),* U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, Reaffirmed 1999 October 25
[ISO15946-1]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General,* 2002
[ISO15946-2]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures,* 2002
[ISO15946-3]	*ISO/IEC 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment,* 2002
[ISO7816]	*ISO 7816, Identification cards – Integrated circuit(s) cards with contacts, Part 4: Organization, security and commands for interchange*, FDIS2004
[ISO9796-2]	*ISO/IEC 9797: Information technology – Security techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms,* 2002
[ISO9797-1]	*ISO/IEC 9797: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,* 1999
[ICAO-9303]	9303 Part 3 Vol 2 – ICAO Machine Readable Travel Document Third edition 2008

[PKCS#3]	*PKCS #3: Diffie-Hellman Key-Agreement Standard,* An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993
[PKI]	*MRTD Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access* International Civil Aviation Organization Version 1.1, October 01 2004
[PP-IC-0002]	*Smartcard IC Platform protection Profile* BSI-PP-0002, version 1.0, July 2001
[PP-IC-0035]	*Smartcard IC Platform protection Profile* BSI-PP-0035
[PP-MRTD-EAC]	*Common Criteria Protection Profile – Machine Readable Travel Document with "ICAO Application", Extended Access Control* Bundesamt für Sicherheit in der Informationstechnik BSI-PP-0056, Version 1.10, 25th March 2009
[PP-MRTD-BAC]	*Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control* Bundesamt für Sicherheit in der Informationstechnik BSI-PP-0055, version 1.10, 25th March 2009
[PP-JCS-Open]	Java Card System Protection Profile – Open Configuration ANSSI-PP-2010/03, Version 2.6, April, 19th 2010
[SS]	*ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS*, *Excerpts from ICAO Doc 9303, Part 1* Machine Readable Passports, Fifth Edition – 2003
[TR-ECC]	*Technical Guideline TR-03111, Elliptic Curve Cryptography based on ISO 15946, v1.00* *Bundesamt für Sicherheit in der Informationstechnik*
[ASM-EAC]	*Technical Guideline – Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC),* *Version 1.11, TR-03110*
[BIO]	*BIOMETRICS DEPLOYMENT OF MACHINE READABLE TRAVEL DOCUMENTS,* *Technical Report, Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents,* *Version 2.0, ICAO TAG MRTD/NTWG, 21 May 2004*

1.3.2 Internal References

[ST-BAC]	D1239132 BAC Security Target – eTravel EAC v1.1 with AA Maia4
[PRE_MRTD]	D1191507 Preparative procedures - eTravel EAC v1.1 Maia4
[OPE_MRTD]	D1191508 Operational User Guidance - eTravel EAC v1.1 Maia4

1.4 ACRONYMS AND GLOSSARY

Acr.	Term	Definition
AA	Active Authentication	Security mechanism defined in [PKI] option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
	Application	Optional informative part of the PP containing additional supporting information that

	note [PP-MRTD-EAC]	is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
	Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
	Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
BAC	Basic Access Control	Security mechanism defined in [PKI] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
BIS	Basic Inspection System	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
	Biographical data (biodata)	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [SS]
	Biometric Reference Data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
	Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [SS]
CSCA	Country Signing Certification Authority	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
CPLCD	Card Production Life Cycle Data	The TOE identification is provided by the Card Production Life Cycle Data (CPLCD) of the TOE, located in OTP and in EEPROM. These data are available by executing a dedicated command
CVCA	Country Verifying Certification Authority	The Country Verifying Certification Authority enforces the privacy policy of the issuing Country or Organization with respect to the protection of sensitive biometric reference data stored in the MRTD. The CVCA represents the country specific root of the PKI of Inspection Systems.
DH	Diffie-Hellman Key Agreement Algorithm	Algorithm for Chip Authentication protocol
DV	Document Verifier	The Document Verifier enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The DV manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the Issuing State or Organization in form of the Document Verifier Certificates.
EC-DH	Elliptic Curve Diffie-Hellman Key Agreement Algorithm	Algorithm for Chip Authentication protocol
	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 MRTD's chip and the inspection system [PKI]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
SOD	Document Security Object	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [PKI]
	Eavesdropper	A threat agent with moderate attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
	Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [BIO]
EAC	Extended Access Control	Security mechanism identified in [PKI] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric

		reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
EIS	Extended Inspection System	The EIS in addition to the General Inspection System (GIS) (i) implements the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
	Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [SS]
GIS	General Inspection System	The GIS is a Basic Inspection System (BIS) which implements additional the Chip Authentication Mechanism.
	Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [BIO]
	IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
	IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
	Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [SS]
	Improperly	A person who travels, or attempts to travel with: (a) an expired travel
	Documented person	document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [BIO]
	Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).
	Inspection	The act of a State examining an MRTD presented to it by a traveler (the MRTD holder) and verifying its authenticity. [BIO]
IS	Inspection system	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
IC	Integrated circuit	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
	Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
	Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [ICAO-9303]
	Issuing State	The Country issuing the MRTD. [ICAO-9303]
LDS	Logical Data Structure	The collection of groupings of Data Elements stored in the optional capacity expansion technology [ICAO-9303]. The capacity expansion technology used is the MRTD's chip.
	Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure (LDS) as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTD holder (1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), (2) the digitized portraits (EF.DG2), (3) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and (4) the other data according to LDS (EF.DG5

		to EF.DG16).
	Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
MRTD	Machine readable travel document	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [ICAO-9303]
MRV	Machine readable visa	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [ICAO-9303]
MRZ	Machine Readable Zone	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [ICAO-9303]
	Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [SS]
	MRTD administrator	The Issuing State or Organization which is allowed to perform administrative commands (update data of the MRTD application, invalidation of the application) in the phase 4 Operational Use.
	MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes: -the file structure implementing the LDS [ICAO-9303], the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG14 and EF.DG16), - the TSF Data including the definition the authentication data but except the authentication data itself.
	MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
	MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
	MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and ICAOT, [10], p. 14. programmed according to the Logical Data Structure as specified by ICAOT, [10], p. 14.
	MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
	Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
	Passive authentication	verification of the digital signature of the Document Security Object comparison the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
	Personalization	The process by which the portrait, signature and biographical data are applied to the document. [SS]
	Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and

		(iii) writing these data on the physical and logical MRTD for the holder.
	Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
	Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and FIA_UAU.6/MRTD.
	Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to): biographical data, data of the machine-readable zone, photographic image and other data.
	Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
	Pre – personalized MRTD's chip	MRTD's chip equipped with pre-personalization data.
PIS	Primary Inspection System	A inspection system that contains a terminal for the contactless communication with the MRTD's chip and does not implement the terminals part of the Basic Access Control Mechanism.
	Receiving State	The Country to which the MRTD holder is applying for entry. [ICAO-9303]
	reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
	secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [SS]
	secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
	Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
	travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel. [BIO]
	traveler	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
	TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1 [1]).
	Unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD's chip.
	User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1 [1]).
	Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [BIO]
	verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

1.5 TOE OVERVIEW

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

1.5.1 TOE definition

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) [ICAO-9303] and providing the Basic Access Control and Extended Access Control according to the 'ICAO Doc 9303' [ICAO-9303] and BSI TR-03110 [ASM-EAC], respectively.
In addition to [PP-MRTD-EAC], the TOE supports the active authentication as defined in [ICAO-9303].

The TOE comprises of at least

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application and
- the associated guidance documentation.

1.5.2 TOE usage and security features for operational use

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents an MRTD to the inspection system to prove his or her identity. The MRTD in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the MRTD.
The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of

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

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

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

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

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

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

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

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-MRTD]. Due to the fact that [PP-BAC-MRTD] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has been evaluated and certified separately according to [ST-BAC], claiming [PP-BAC-MRTD].

For BAC, the inspection system (i) reads optically the MRTD, (ii) authenticates itself as inspection system by means of Document Basic Access Keys. After successful authentication of the inspection system the MRTD's chip provides read access to the logical MRTD by means of private communication (secure messaging) with this inspection system [ICAO-9303], normative appendix 5.

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

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

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

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

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

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

1.6 TOE BOUNDARIES

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

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

- the Basic Access Control (BAC) according to the ICAO document [PKI]
- the Active Authentication (AA) mechanism according to the ICAO document [ICAO-9303]
- the Extended Access Control according to the BSI document [ASM]

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

The TOE comprises of:

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system),
- the MRTD application, and
- the associated guidance documentation.

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

- *the Integrated Circuit (IC),*
- *the IC Dedicated Test Software,*
- *the IC Dedicated Support Software (Boot Rom Software, Mifare Operating System),*
- *the eTravel EAC v1.1 Embedded Software (ES),*
- *the NVM Embedded Software,*
- *part of the MRTD Logical Data Structure,*
- *the guidance documentation of the eTravel EAC v1.1 product:*
  - *the preparation guide (assurance family AGD-PRE),*
  - *the operational guide (assurance family AGD-OPE).*

The eTravel EAC v1.1 Embedded Software (ES) is mainly implemented in the ROM of the chip. Some features have been added in the EEPROM. This ES provides mechanisms to load executable code into the non-volatile-memory of the chip (EEPROM). These mechanisms are included in the TOE and are part of the evaluation.
The TOE is delivered to the Personalization Agent with data and guidance documentation in order to perform the personalization of the product. In addition the Personalization Key is delivered from the MRTD Manufacturer to the Personalization Agent or from the Personalization Agent to the MRTD Manufacturer.

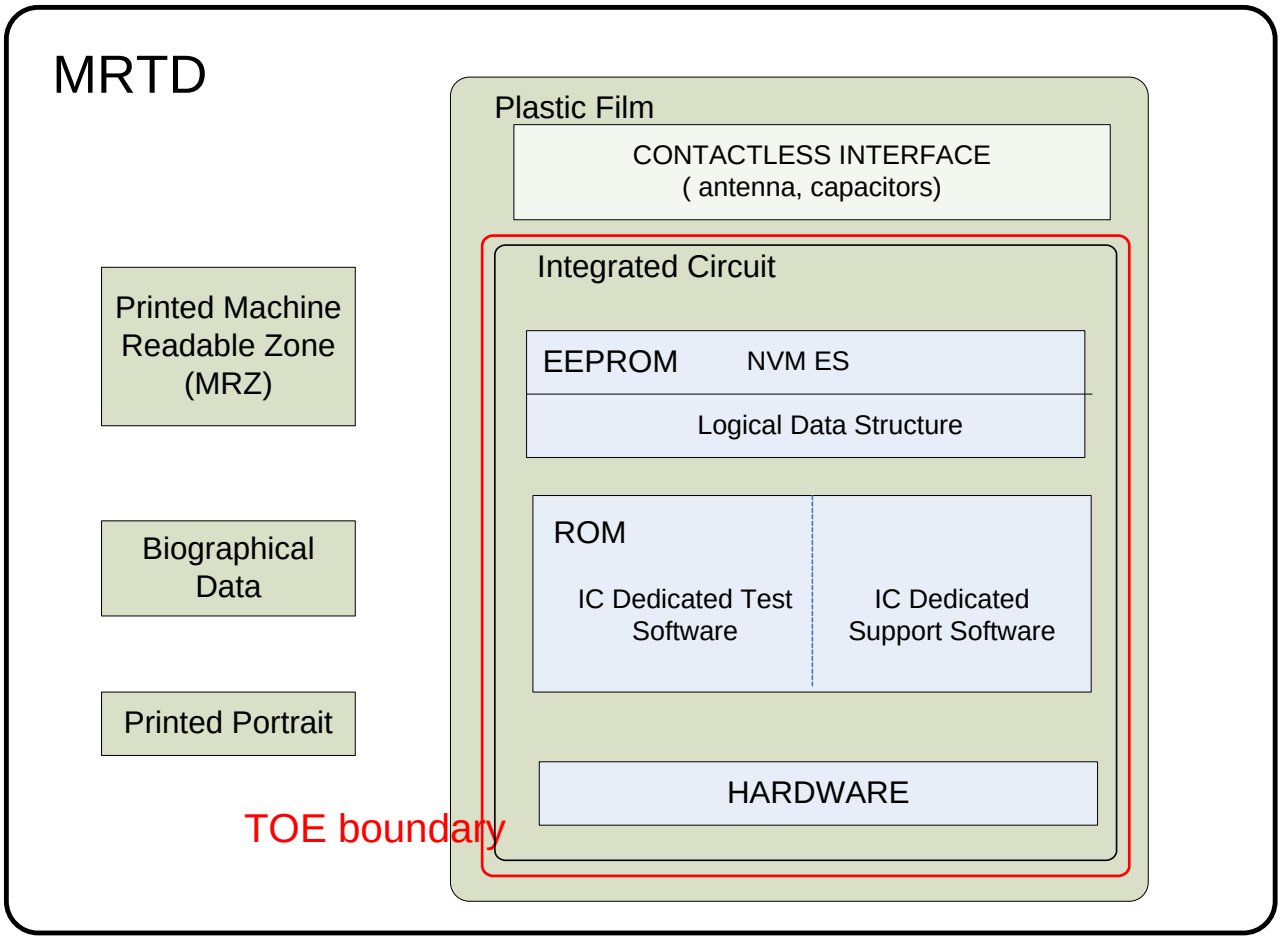


Figure 1: TOE Boundaries

1.7 TOE INTENDED USAGE

State or organization issues MRTD to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity.
The MRTD in context of this security target contains:

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

The authentication of the traveler is based on the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

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

- the **physical MRTD** as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder:
  - the biographical data on the biographical data page of the passport book,
  - the printed data in the Machine-Readable Zone (MRZ),
  - the printed portrait.
- the **logical MRTD** as data of the MRTD holder stored according to the Logical Data Structure [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:
  - the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

- the digitized portraits (EF.DG2),
- the optional biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both'
- the other data according to LDS (EF.DG5 to EF.DG16),
- the Document Security Object (SOD).

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the document number.
The physical MRTD is protected by physical security measures (e.g. watermark on paper, security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [SS]. These security measures include the binding of the MRTD's chip to the passport book.
This ST assumes that the issuing State or Organization uses EF.DG3 and/or EF.DG4 and protects these data by means of Extended Access Control.

1.8 TOE LIFE-CYCLE

1.8.1 Four phases

The TOE life cycle is described in terms of the four life cycle phases. (With respect to the [PP-IC-0035], the TOE life-cycle the life-cycle is additionally subdivided into 7 steps.)

Phase 1 “Development”:

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.
(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the MRTD application and the guidance documentation associated with these TOE components.
The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories (ROM) is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the MRTD application and the guidance documentation is securely delivered to the MRTD manufacturer.

Phase 2 “Manufacturing”:

(Step3) In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.
If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).
(Step4) The MRTD manufacturer combines the IC with hardware for the contactless interface in the passport book
(Step5) The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.
The pre-personalized MRTD together with the IC Identifier is securely delivered from the MRTD manufacturer to the Personalization Agent. The MRTD manufacturer also provides the relevant parts of the guidance documentation to the Personalization Agent.

Phase 3 “Personalization of the MRTD”:

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

The signing of the Document security object by the Document signer [5] finalizes the personalization of the genuine MRTD for the MRTD holder. The personalized MRTD (together with appropriate guidance for TOE use if necessary) is handed over to the MRTD holder for operational use.

Phase 4 “Operational Use”

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

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

1.8.2 Actors

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

Table 2: Identification of the actors

1.8.3 Pre-personalization on module at Gemalto site

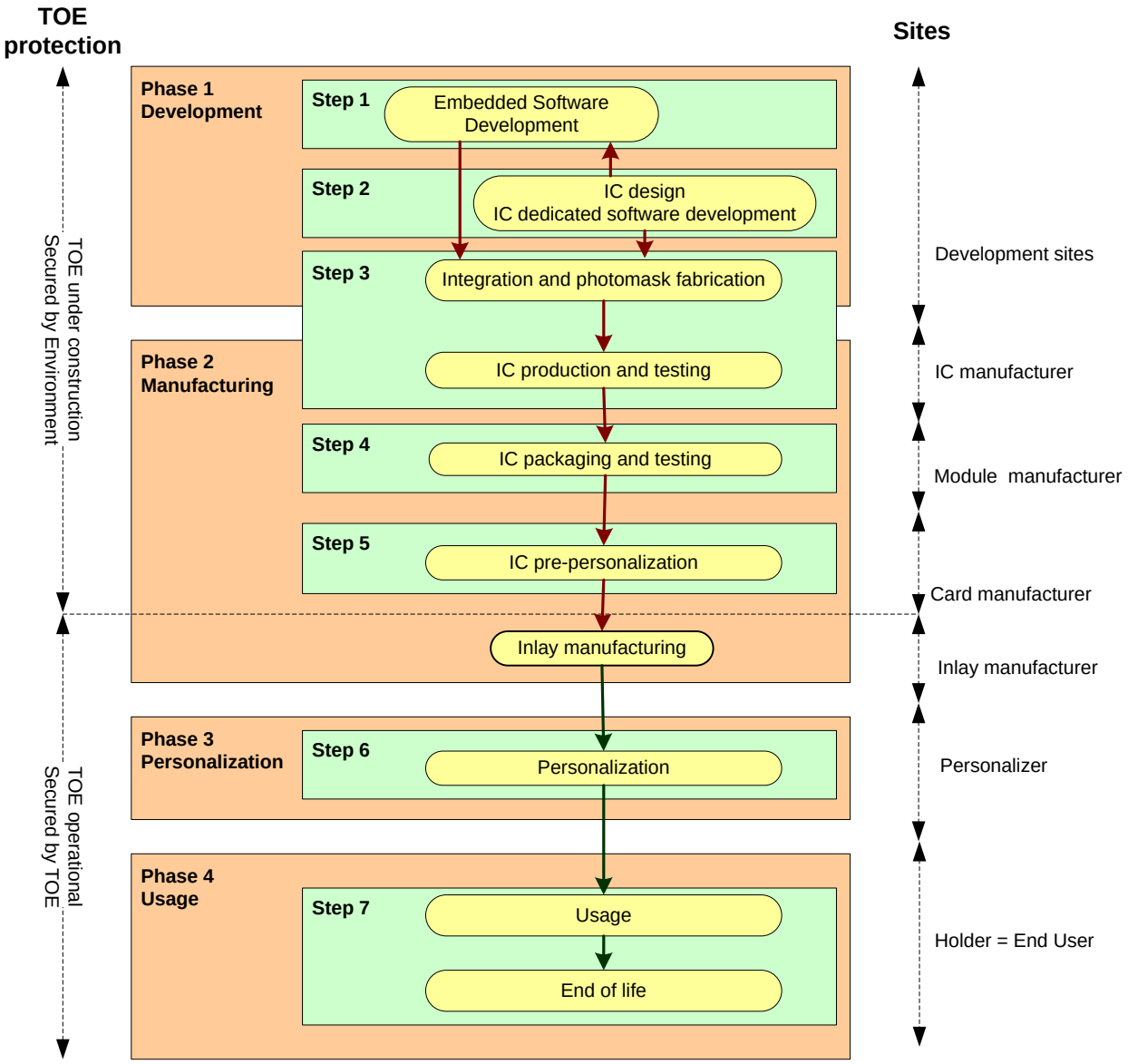


Figure 2: LC1: Pre-personalization on module at Gemalto site

Figure 2: LC1: Pre-personalization on module at Gemalto site describes the standard Life Cycle. The IC is manufactured at the founder site. It is then shipped to Gemalto site where it is pre-personalized. The transformation of wafers into modules can be performed either at the founder site or at Gemalto site. The modules are then shipped to the Personalizer or to the Inlay manufacturer. In the latter case, The Inlay manufacturer ships the inlays to the Personalizer
During the shipment from Gemalto to the Personalizer or the Inlay manufacturer, the module is protected by a diversified key.

1.8.4 Pre-personalization at Founder site

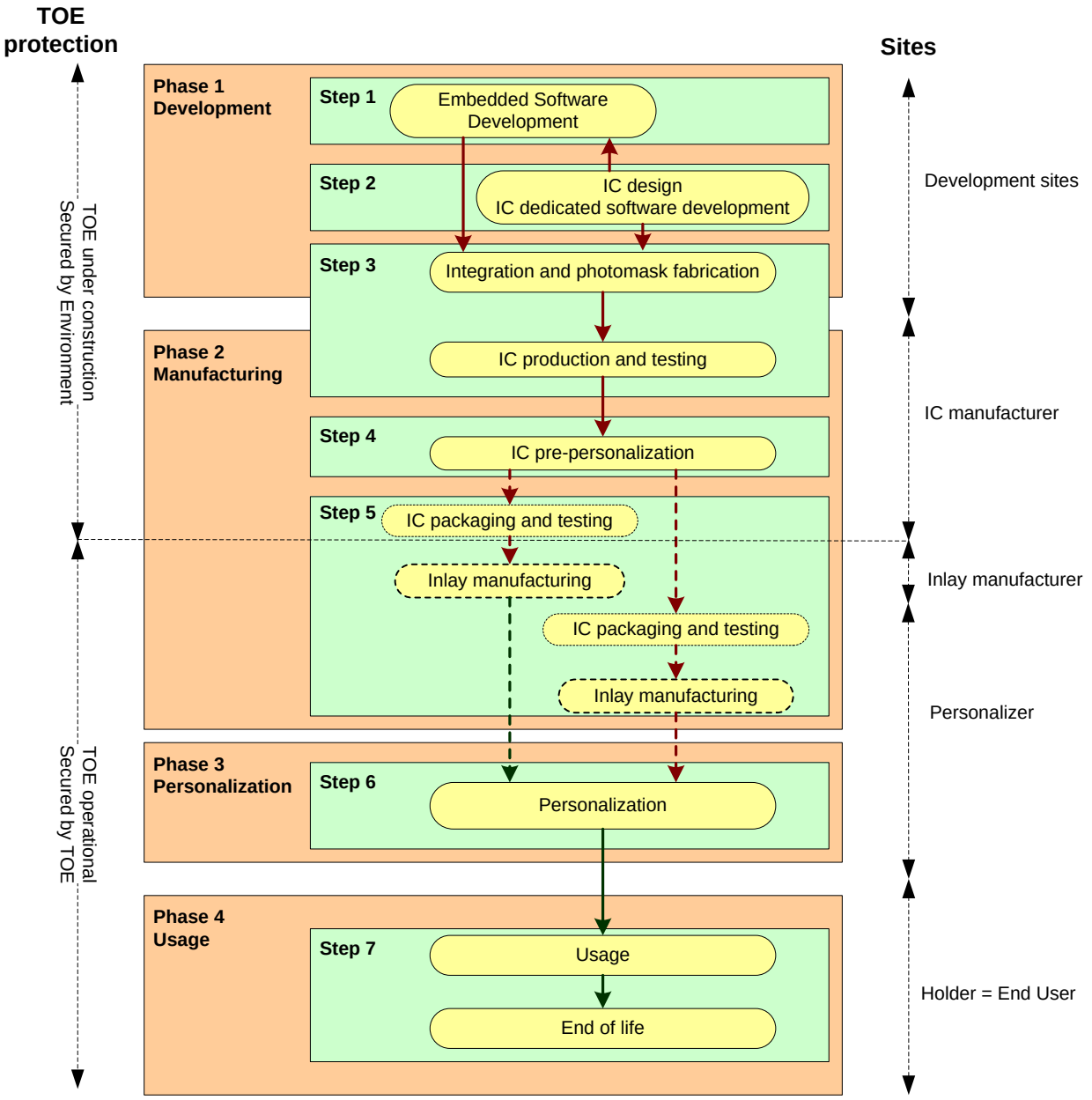


Figure 3: LC2 Pre-personalization at Founder site

LC2 is an alternative to LC1. *Figure 3: LC2 Pre-personalization at Founder site* describes the Life Cycle when the customer wishes to receive the IC directly from the founder. In this case, pre-personalization, which includes sensitive operations such as the loading of patches, takes place at the founder site. The creation of files is started by the founder and completed by the personalizer.
During the shipment from the founder to the Personalizer, the module is protected by a diversified key.

1.8.5 Pre-personalization on inlay at Gemalto site

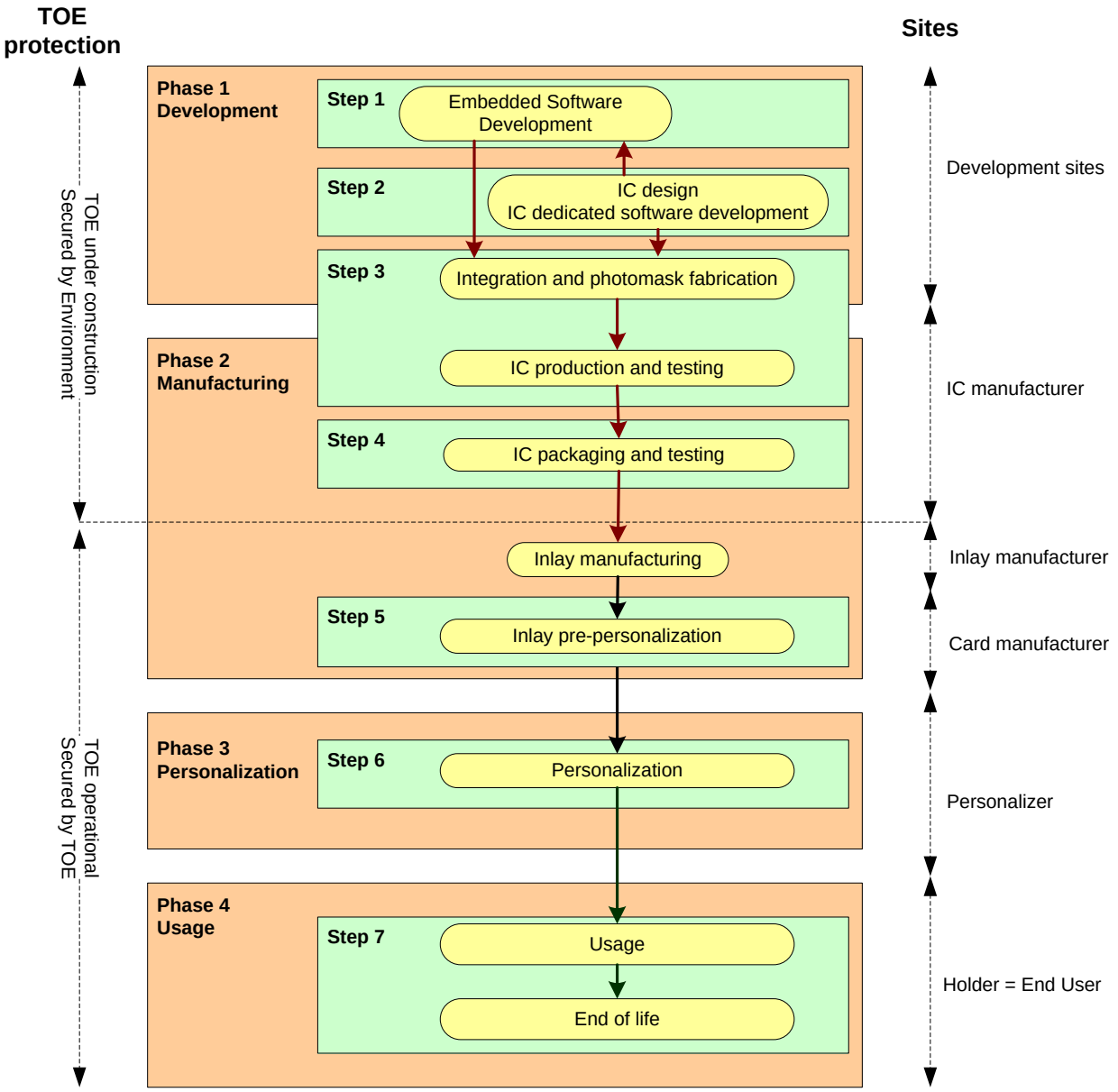


Figure 4: LC3: Pre-personalization on inlay at Gemalto site

LC3 is another alternative to LC1. *Figure 4: LC3: Pre-personalization on inlay at Gemalto site* describes the Life Cycle when the Gemalto wishes to receive inlays instead of IC or modules from the founder. In this case, the founder ships the module to the Inlay manufacturer.
During the shipment from the founder to Gemalto, the IC or module is protected by a diversified key.

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, rev 3, July 2009 [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, rev 3, July 2009 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, rev 3, July 2009 [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, rev 3, July 2009, [CEM] has to be taken into account.

2.2 PP CLAIM,

The eTravel EAC v1.1 - EAC security target claims strict conformance to the Protection Profile “Machine Readable Travel Document with ICAO Application, Extended Access Control” BSI-PP-0056 version 1.10 ([PP-MRTD-EAC]).
The eTravel EAC v1.1 EAC security target is a composite security target, including the IC security target [ST-IC]. However the security problem definition, the objectives, and the SFR of the IC are not described in this document.

The TOE also claims conformance to other Protection Profiles. This is described in another Security Target:

The ETravel v1.1 - BAC security target claims strict conformance to the Protection Profile “Machine Readable Travel Document with ICAO Application, Basic Access Control” BSI-PP-0055 version 1.10 ([PP-MRTD-BAC]).

2.3 PACKAGE CLAIM

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

2.4 CONFORMANCE STATEMENT

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

3. SECURITY PROBLEM DEFINITION

3.1 INTRODUCTION

3.1.1 Assets

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

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. As the BAC mechanisms may not resist attacks with high attack potential, security of other Data Groups of the logical MRTD are covered by another ST (cf. [ST-BAC]).

A sensitive asset is the following more general one.

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

3.1.2 Subjects

This security target considers the following subjects:

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.

Pre-personalization Agent
The pre-personalization agent is the Manufacturer, acting in step 5 pre-personalization. The pre-personalization agent loads pre-personalization data. He may also load executable code in NVM.

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 PP since this can only be averted by the BAC mechanism using the "weak" Document Basic Access Keys that is covered by [PP-MRTD-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.

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

3.2 ASSUMPTIONS

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

A.MRTD_Manufact MRTD manufacturing on steps 4 to 6
It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

A.MRTD_Delivery MRTD delivery during steps 4 to 6
Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

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

A.Pers_Agent Personalization of the MRTD's chip

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

A.Insp_Sys Inspection Systems for global interoperability
The Inspection System is used by the border control officer of the receiving State (i) examining 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 PKI for Passive Authentication
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 PKI for Inspection Systems
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.

3.3 THREATS

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

Application note: The threats T.Chip_ID and T.Skimming (cf. [PP-MRTD-BAC]) are averted by the mechanisms described in the BAC PP [PP-MRTD-BAC] (cf. P.BAC-PP) which cannot withstand an attack with high attack potential thus these are not addressed here. T.Chip_ID addresses the threat of tracing the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. T.Skimming addresses the threat of imitating the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE. Both attacks are conducted by an attacker who cannot read the MRZ or who does not know the physical MRTD in advance.

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

T.Read_Sensitive_Data Read the sensitive biometric reference data

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.
The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [PP-MRTD-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 Forgery of data on MRTD's chip

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

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

Asset: authenticity of logical MRTD data,

T.Counterfeit MRTD's chip

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,

The TOE shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

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 Information Leakage from MRTD's chip

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

T.Phys-Tamper Physical Tampering
Adverse action: An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data, or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data.
The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.
Threat agent: having 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 Malfunction due to Environmental Stress
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

3.4 ORGANIZATIONAL SECURITY POLICIES

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

P.BAC-PP Fulfillment of the Basic Access Control Protection Profile.
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 Doc 9303' [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-MRTD-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-MRTD-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-MRTD-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 security targets, which is assumed to result in technically separated evaluations (at least for classes ASE and VAN) and certificates.

P.Sensitive_Data Privacy of sensitive biometric reference data
The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the 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 Manufacturing of the MRTD's chip
The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

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

3.5 COMPATIBILITY BETWEEN SECURITY ENVIRONMENTS OF [ST-EAC] AND [ST-IC]

3.5.1 Compatibility between threats of [ST-EAC] and [ST-IC]

T.Read_Sensitive_Data, is included in T.Phys-Probing.
T.Forgery is included in T.Phys-Manipulation.
T.Counterfeit is specific to [ST-EAC] and it does not conflict with the threats of [ST-IC].
T.Abuse-Func of [ST-EAC] is included in T.Abuse-Func of [ST-IC].
T.Information_Leakage is included in T.Leak-Inherent and T.Leak-Forced.
T.Phys-Tamper is included in T.Phys-Manipulation
T.Malfunction of [ST-EAC] is included in T.Malfunction of [ST-IC].

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

3.5.2 Compatibility between OSP of [ST-EAC] and [ST-IC]

P.BAC-PP, P.Sensitive_Data, P.Manufact, and P.Personalization are specific to the MRTD and they do no conflict with the OSP of [ST-IC].

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

3.5.3 Compatibility between assumptions of [ST-EAC] and [ST-IC]

A.MRTD_Manufact and A.MRTD_Delivery are included in A.Process-Card

A.Pers_Agent, A.Insp_Sys, A.Signature_PKI, and A.Auth_PKI are assumptions specific to [ST-EAC] and they do no conflict with the assumptions of [ST-IC].

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

4. SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD
The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [ICAO-9303] and the TSF data can be written by authorized 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 Integrity of personal data
The TOE must ensure the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The TOE must ensure the integrity of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data
The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or 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 Identification and Authentication of the TOE
The TOE must provide means to store IC Identification and Pre-Personalization Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. The storage of the Pre-Personalization data includes writing of the Personalization Agent Key(s).

OT.Chip_Auth_Proof Proof of MRTD’s chip authenticity
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 [ASM-EAC]. 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.

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

OT.Activ_Auth_Proof Proof of MRTD's chip authenticity through AA
The TOE must support the General Inspection Systems to verify the identity and authenticity of the MRTD's chip as issued by the identified issuing State or Organization by means of the Active Authentication as defined in [ICAO-9303]. The authenticity proof through AA provided by MRTD's chip shall be protected against attacks with high attack potential.

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

OT.Prot_Inf_Leak Protection against Information Leakage
The TOE must provide protection against disclosure of confidential TSF data stored and/or processed in the MRTD's chip

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

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

OT.Prot_Phys-Tamper Protection against Physical Tampering
The TOE must provide protection of the confidentiality and integrity of the User Data, the TSF Data, and the MRTD's chip Embedded Software. This includes protection against attacks with 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 Protection against Malfunctions
The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency, or temperature.

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

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

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

OE.MRTD_ Delivery Protection of the MRTD delivery
Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

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

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

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

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature
The issuing State or Organization must (i) generate a cryptographic secure Country Signing CA Key Pair, (ii) ensure the secrecy of the Country Signing CA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing CA Public Key to receiving States and Organizations maintaining its authenticity and integrity.
The issuing State or Organization must (i) generate a cryptographic secure Document Signer Key Pair and ensure the secrecy of the Document Signer Private Keys, (ii) sign Document Security Objects of genuine MRTD in a secure operational environment only and (iii) distribute the Certificate of the Document Signer Public Key to receiving States and Organizations. The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [ICAO-9303].

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

OE.Auth_Key_MRTD MRTD Authentication Key
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 Authorization for Use of Sensitive Biometric Reference 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 Fulfillment of the Basic Access Control Protection Profile.
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-MRTD-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.

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

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

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

OE.Prot_Logical_MRTD Protection of data from the logical MRTD
The inspection system of the receiving State or Organization ensures the confidentiality and integrity of the data read from the logical MRTD. The 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: The figure 2.1 in [ASM-EAC] 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 less sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

OE.Ext_Insp_Systems Authorization of Extended Inspection 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.

5. EXTENDED COMPONENTS DEFINITION

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

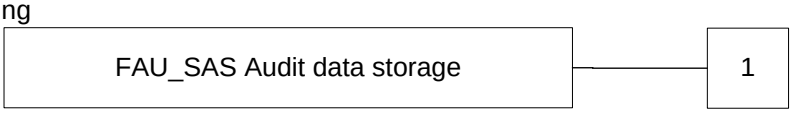
5.1 DEFINITION OF THE FAMILY FAU_SAS

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

FAU_SAS Audit data storage

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

Component leveling



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

Management: FAU_SAS.1
There are no management activities foreseen.

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

FAU_SAS.1 Audit storage

Hierarchical to: No other components
Dependencies: No dependencies

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

5.2 DEFINITION OF THE FAMILY FCS_RND

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

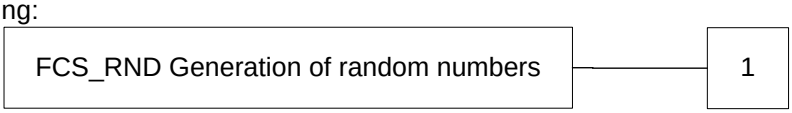
The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behavior

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

Component leveling:



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1
There are no management activities foreseen.

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

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components
Dependencies: No dependencies

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

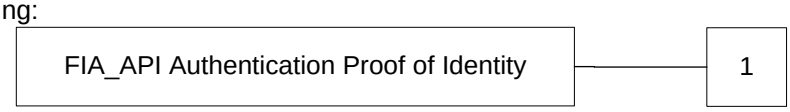
5.3 DEFINITION OF THE FAMILY FIA_API

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

FIA_API Authentication Proof of Identity

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

Component leveling:



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1
The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components
Dependencies: No dependencies

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

5.4 DEFINITION OF THE FAMILY FMT_LIM

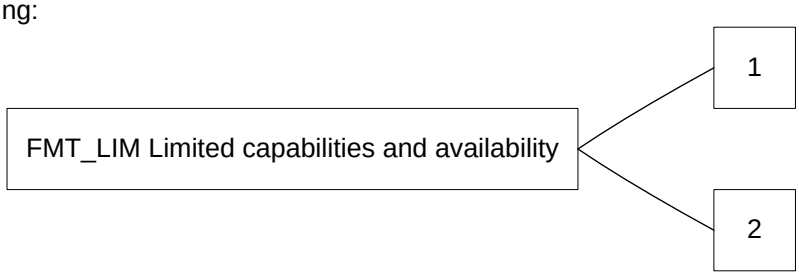
The family FMT_LIM describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class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

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

FMT_LIM Limited capabilities and availability

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

Component leveling:



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

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

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

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components
Dependencies: FMT_LIM.2 Limited availability.

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

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components
Dependencies: FMT_LIM.1 Limited capabilities.

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

Application note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

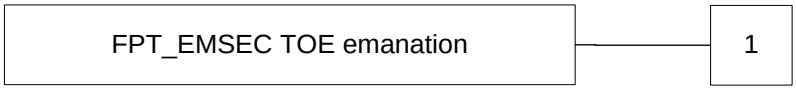
5.5 DEFINITION OF THE FAMILY FPT_EMSEC

The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC-2].

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

Family behavior
This family defines requirements to mitigate intelligible emanations.

Component leveling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1
There are no management activities foreseen.

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

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies.

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

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

6. SECURITY REQUIREMENTS

The definition of the subjects “Manufacturer”, “Pre-personalization Agent”, “Personalization Agent”, “Extended Inspection System”, “Country Verifying Certification Authority”, “Document Verifier” and “Terminal” used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC-2]. The operation “load” is synonymous to “import” used in [CC-2].

Definition of security attributes:

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

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

Name	Data
Country Verifying Certification Authority Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the

Name	Data
	most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (CCVCA)	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [ASM-EAC] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

Application note 20: The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From MRTD's point of view the domestic Document Verifier belongs to the issuing State or Organization.

6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

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

6.1.1 Class FAU Security Audit

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

FAU_SAS.1 Audit storage

Hierarchical to: No other components
Dependencies: No dependencies

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

6.1.2 Class Cryptographic Support (FCS)

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

FCS_CKM.1 /AA&CA Cryptographic key generation for AA and CA

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

FCS_CKM.1.1 /AA&CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

iteration	algorithm	Key size	standard
/RSA	**RSA CRT Key generation**	**1024, 1536 and 2048 bits**	**none (generation of random numbers and Miller- Rabin primality testing)**
/ECC	**ECC Key generation**	**160, 192, 224, 256, 320, 384, and 521 bits**	**None**

Table 3: FCS_CKM.1/AA&CA refinement

FCS_CKM.1 /Session Cryptographic key generation for Session keys

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

FCS_CKM.1.1 /Session The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: *based on the key Diffie-Hellman key derivation Protocol compliant to PKCS#3, ECDH compliant to ISO 15946*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [ASM-EAC] , Annex A.1.

iteration	algorithm	Key size
/TDESsession-Perso	**TDES ISK key derivation**	**112 bits**
/TDESsession-DH	**DH Key Agreement Algorithm - PKCS#3 – 1024, 1536 and 2048 bits**	**112 bits**
/TDESsession-ECDH	**ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256, 320, 384, and 521 bits**	**112 bits**

Table 4: FCS_CKM.1/Session refinement

Application Notes:
The BAC session keys generation is described in the BAC security target.

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

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

iteration	Key	When
/BAC	BAC session keys	– At power-up – When a MAC error is detected – After successful CA authentication
/DH	DH session keys	– At power-up – When a MAC error is detected
/ECDH	ECDH session keys	– At power-up – When a MAC error is detected

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

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

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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, SHA-512,** and cryptographic key sizes none

that meet the following: **FIPS 180-2**.

FCS_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SYM The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm **TDES CBC** and cryptographic key sizes **112 bits** that meet the following: 'TR-03110 ', [ASM-EAC].

FCS_COP.1/MAC Cryptographic operation – MAC

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/MAC The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm **TDES Retail MAC** and cryptographic key sizes **112 bits** that meet the following: 'TR-03110 ', [ASM-EAC].

FCS_COP.1/RSA_SIG_VER Cryptographic operation – RSA Signature verification by MRTD

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ SIG_VER The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024, 1536 and 2048 bits** that meet the following: **PKCS#1 v1.5 and PKCS#1-PSS**.

FCS_COP.1/ECDSA_SIG_VER Cryptographic operation – ECDSA Signature verification by MRTD

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ SIG_VER The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **160, 192, 224, 256, 320, 384, and 521 bits** that meet the following: : 'TR-03111 ', [TR-ECC].

FCS_COP.1/RSA_AA Cryptographic operation – RSA Active Authentication

Hierarchical to: No other components

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

FCS_COP.1.1/ RSA_AA The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **RSA CRT** and cryptographic key sizes **1024, 1536 and 2048 bits** that meet the following: **[ISO9796-2]**.

FCS_COP.1/ECDSA_AA Cryptographic operation – ECDSA Active Authentication

Hierarchical to: No other components
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ ECDSA_AA The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **160, 192, 224, 256 and 521 bits** that meet the following: **'TR-03111 ', [TR-ECC]**.

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

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components
Dependencies: No dependencies

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **K3-DRNG ([AIS20]) with seed entropy at least 112 bits**.

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

6.1.3 Class FIA Identification and Authentication

Application note: The Table 5 provides an overview on the authentication mechanisms used.

Name	SFR for the TOE
Symmetric Authentication Mechanism for Personalization Agents	FIA_UAU.4
Active Authentication Protocol	FIA_API.1, FIA_UAU.5, FIA_UAU.6
Chip Authentication Protocol	FIA_API.1, FIA_UAU.5, FIA_UAU.6
Terminal Authentication Protocol	FIA_UAU.5

Table 5: Overview on authentication SFR

Note the Chip Authentication Protocol as defined in this security target includes

- the BAC authentication protocol as defined in 'ICAO Doc 9303' [ICAO-9303] in order to gain access to the Chip Authentication Public Key in EF.DG14,
- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol,
- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The BAC mechanism does not provide a security function on their own. The Chip Authentication Protocol may be used independent of the Terminal Authentication Protocol. But if the Terminal Authentication Protocol is used the terminal shall use the same public key as presented during the Chip Authentication Protocol.

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow
1. to establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
3. to carry out the Active Authentication Protocol
4. 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.

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow

1. to establish the communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
3. to identify themselves by selection of the authentication key
4. to carry out the Active Authentication Protocol
5. 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.

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

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

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to
1. Terminal Authentication Protocol,
2. Authentication Mechanism based on **Triple-DES**.

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

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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide
1. Terminal Authentication Protocol,
2. Secure messaging in MAC-ENC mode,
3. Symmetric Authentication Mechanism based on **Triple-DES**

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules:
1. **TOE accepts the authentication attempt as Pre-personalization Agent by the Symmetric Authentication Mechanism with the Pre-personalization Agent Key.**
2. The TOE accepts the authentication attempt as Personalization Agent by **the Symmetric Authentication Mechanism with Personalization Agent Key**.
3. 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.
4. 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.

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

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

Hierarchical to: No other components
Dependencies: No dependencies

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

The TOE shall meet the requirement “Authentication Proof of Identity (FIA_API.1)” as specified below (Common Criteria Part 2 extended).

FIA_API.1 Authentication Proof of Identity – Chip Authentication

Hierarchical to: No other components
Dependencies: No dependencies

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

Application note: This SFR requires the TOE to implement the Chip Authentication Mechanism specified in [ASM-EAC]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (DH or EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO-9303], normative appendix 5, A5.1. The terminal verifies by means of secure messaging whether the MRTD’s chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_API.1 Authentication Proof of Identity – Active Authentication

Hierarchical to: No other components
Dependencies: No dependencies

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

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

6.1.4 Class FDP User Data Protection

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

FDP_ACC.1 Subset access control

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

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

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

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

1. Subjects:
    a. Personalization Agent,
    b. Extended Inspection System
    c. Terminal,
2. Objects:
    a. data EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD.
    b. data EF.DG3 and EF.DG4 of the logical MRTD
    c. data in EF.COM,
    d. data in EF.SOD,
3. Security attributes:
    a. authentication status of terminals,
    b. 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:

1. the successfully authenticated Personalization Agent is allowed to write and to read the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Extended Inspection System with the Read access to DG3 (Fingerprint) granted by the relative certificate holder authorization encoding is allowed to read the data in EF.DG3 of the logical MRTD.
3. the successfully authenticated Extended Inspection System with the Read access to DG4 (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 authorize 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:

1. A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. Any terminal is not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD,
6. 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.

Application note: Note the BAC mechanism controls the read access of the EF.COM, EF.SOD, EF.DG1, EF.DG2, and EF.DG5 to EF.DG16 of the logical MRTD. These security features of the MRTD are not subject of this ST.

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components
Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the Access Control SFP to transmit and receive user data in a manner protected from unauthorized disclosure after Chip Authentication.

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

FDP_UIT.1 Data exchange integrity

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

FDP_UIT.1.1 The TSF shall enforce the 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 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication.

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

6.1.5 Class FMT Security Management

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components
Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
1. Initialization ,
2. Pre-personalization,
3. Personalization.

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

FMT_SMR.1 Security roles

Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles
1. Manufacturer ,
2. **Pre-personalization Agent,**
3. Personalization Agent,
4. Country Verifying Certification Authority,
5. Document Verifier,
6. domestic Extended Inspection System
7. foreign Extended Inspection System.

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

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

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components
Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow,
1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components
Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow
1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

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

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

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

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

Application note: The pre-personalization Data includes but is not limited to the authentication reference data for the Personalization Agent which is the symmetric cryptographic Personalization Agent Key.

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

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

to **the Personalization Agent**.

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

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

to Country Verifying Certification Authority.

FMT_MTD.1/DATE Management of TSF data – Current date

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ DATE The TSF shall restrict the ability to modify the Current date to
1. Country Verifying Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System.

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

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

Application note: The Country Verifying Certification Authority Public Key is the TSF data for verification of the certificates of the Document Verifier and the Extended Inspection Systems including the access rights for the Extended Access Control.

FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

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

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

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

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to read the
1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. **Active Authentication Private Key**
4. Personalization Agent Keys

to none.

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

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components
Dependencies: FMT_MTD.1 Management of TSF data

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

Refinement: The certificate chain is valid if and only if

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

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

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

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

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

Application note 50: The Terminal Authentication is used for Extended Inspection System as required by FIA_UAU.4 and FIA_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1.

6.1.6 Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements “Failure with preservation of secure state (FPT_FLS.1)” and “TSF testing (FPT_TST.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other. The SFRs “Limited capabilities (FMT_LIM.1)”, “Limited availability (FMT_LIM.2)” and “Resistance to physical attack (FPT_PHP.3)” together with the SAR “Security architecture description” (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

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

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components
Dependencies: No dependencies.

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

FPT_EMSEC.1.2 The TSF shall ensure any 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 **Active Authentication Key, EF.DG3 and EF.DG4**.

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

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

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components
Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. Exposure to out-of-range operating conditions where therefore a malfunction could occur,
2. failure detected by TSF according to FPT_TST.1.

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

FPT_TST.1 TSF testing

Hierarchical to: No other components
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions see Table 6** 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.

Conditions under which self test should occur	Description of the self test
During initial start-up	**RNG live test, sensor test, FA detection, Integrity Check of NVM ES**
Periodically	**RNG monitoring, sensor test, FA detection**
After cryptographic computation	**FA detection**
Before any use or update of TSF data	**FA detection, Integrity Check of related TSF data**

Table 6: FPT_TST refinements

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components
Dependencies: No dependencies.

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

6.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5.

7. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the eTravel EAC v1.1 embedded software (including the optional NVM ES) and by the chip.

7.1.1 TSFs provided by the eTravel EAC v1.1 Software

SF	Description	SSF
SF.REL	Reliability	SF.REL.RNG_TEST
		SF.REL.SENSOR_TEST
		SF.REL.INTEGRITY
		SF.REL.CORR_EXEC
		SF.REL.PROT_SENS_DATA
		SF.REL.FAULT_REACTION
SF.AC	Access Control	SF.AC.LIFE_CYCLE
		SF.AC.STATE
		SF.AC.FILE_AC
SF.SYM_AUT	Symmetric Authentication Mechanisms	SF.SYM_AUT.RNG
		SF.SYM_AUT.MANUF
		SF.SYM_AUT.MANUF_PROT
		SF.SYM_AUT.MANUF_KEY_CHANGE
		SF.SYM_AUT.BAC
		SF.SYM_AUT.BAC_RESTR
SF.SM	Secure Messaging	
SF.CA	Chip Authentication	
SF.TA_CER	Validity of the Certificate Chain	SF.TA_CER.VERIFY
		SF.TA_CER.TRUST_UPDATE
		SF.TA_CER.TRUST_ATOMIC
		SF.TA_CER.CURRENT_DATE
SF.TA_AUT	Asymmetric Authentication Mechanism	SF.TA_AUT.RNG
		SF.TA_AUT.EXT_AUT
SF.AA	Active Authentication	

Table 7: Security Functions provided by the eTravel EAC v1.1 Software.

7.1.1.1 SF.REL : Reliability

The SF.REL security function is divided to the following SSFs:

1. SF.REL.RNG_TEST
2. SF.REL.SENSOR_TEST
3. SF.REL.INTEGRITY
4. SF.REL.CORR_EXEC
5. SF.REL.PROT_SENS_DATA
6. SF.REL.FAULT_REACTION.

SSFs SF.REL.RNG_TEST and SF.REL.SENSOR_TEST executes tests to insure that the TOE is in secure state. The SF.REL.RNG_TEST SSF tests random number generator and the SF.REL.SENSOR_TEST SSF tests environment sensors.

The SF.REL.INTEGRITY SSF checks the integrity of following assets:

- Keys
- application files (EF.DG1 to EF.DG16, EF.SOD, EF.COM)
- access rights flags
- NVM ES
- anti-tearing area
- life cycle status.

The SF.REL.CORR_EXEC consists of measures to detect Fault Attacks (FA), involving:

- performing twice and checking the consistency of the certain security critical operations,
- security tests near branching to protect a sensitive conditional branch against perturbation,
- step control to ensure that critical functional steps of a command are really executed and not skipped.

The SF.REL.PROT_SENS_DATA SSF provides several mechanisms ensuring the confidentiality of sensitive data during their manipulation. These mechanisms counter the exploitation of electrical or electromagnetic emissions which are generated during the treatment of data. They are mainly based on clock de-synchronization and/or random order treatments. This security function involve: random order processing mechanism, secured DES operation, secured RSA operation, secured ECC operation and software de-synchronization mechanism.

The SF.REL.FAULT_REACTION consists of detecting faults either by hardware reaction or by software detection based on the SF.REL.SENSOR_TEST, SF.REL.INTEGRITY and SF.REL.CORR_EXEC. When a fault is detected, the card goes to mute state, either immediately or after a delay.

7.1.1.2 SF.AC: Access Control

The SF.AC security function is divided to the following SSFs:

1. SF.AC.LIFE_CYCLE
2. SF.AC.STATE
3. SF.AC.FILE_AC

The TOE has four life cycle phases: development, manufacturing, personalization and operational. The TOE ES has the following life cycle states:

VIRGIN: the state in which chip is received from chip manufacturer

RE_INITIALIZATION: the state in which initialization can be repeated and conditionally erased all previously initialized or pre-personalized information

PRE_PERSONALIZATION: the state after (re-)initialization in which personalization commands are available, but where file access conditions do not apply

PERSONALIZATION: the state after (re-)initialization or pre-personalization in which personalization commands are available

OPERATIONAL: the state of normal usage after personalization in which the usage phase commands are available

TERMINATED: the state in which no commands are available.

The following table shows correspondence between life cycle states of the ES and lice cycle phases.

Life cycle state	Life cycle phase
VIRGIN	MANUFACTURING
RE_INITIALIZATION	MANUFACTURING
PRE_PERSONALIZATION	MANUFACTURING

PERSONALIZATION	PERSONALIZATION
OPERATIONAL	OPERATIONAL
TERMINATED	-

Table 8: Correspondence between TOE ES life cycle states and life cycle phases

During initial startup life cycle status is read. Each life cycle state has own set of available commands and particular command may have different behaviour depending on life cycle. The SF.AC.LIFE_CYCLE function manages the lifecycle status and ensures that the status is set in an irreversible way from the phase 2 “Manufacturing” to the phase 3 “Personalization of the MRTD” and from the phase 3 to the phase 4 “Operational Use”. The phases 2, 3 and 4 have dedicated commands. Life cycle status can be changed through END PERSO command. This command is used to finalize the pre-personalization or the personalization process. If the current life cycle status is PRE_PERSONALIZATION, the next state will be PERSONALIZATION or OPERATIONAL after execution of this command. If the current state is PERSONALIZATION, the next state will be OPERATIONAL after execution of this command. The chip becomes mute after END_PERSO command and initial startup is needed.

The SF.AC.LIFE_CYCLE function manages the high-level life cycle steps of the chip. The SF.AC.STATE function manages the run-time volatile states. The SF.AC.STATE controls the set of available commands through a state machine and the related state transitions. For each life cycle state there exist a specific and finite set of volatile states. A volatile state is characterized by the set of available commands and the available state transitions to other volatile states. The state transitions are implemented by the relevant commands.

The SF.AC.FILE_AC function ensures that the assets (keys, Data Groups, TSF data) can only be accessed under the control of the operating system and as defined by the access rights written during the personalization process. This SF controls the reading and writing access in personalization (Mutual Authenticate Access Control) and user phases (Basic Access Control and Extended Access Control).

7.1.1.3 SF.SYM_AUT: Symmetric Authentication Mechanisms

The SF.AC security function is divided to the following SSFs:

1. SF.SYM_AUT.RNG
2. SF.SYM_AUT.MANUF
3. SF.SYM_AUT.MANUF_PROT
4. SF.SYM_AUT.MANUF_KEY_CHANGE
5. SF.SYM_AUT.BAC
6. SF.SYM_AUT.BAC_RESTR

The SF.SYM_AUT.RNG SSF provides pseudo-random numbers.

The SF.SYM_AUT.MANUF SSF enforces mutual authentication with Manufacturer Key during manufacturing phase. The SF.SYM_AUT.MANUF_KEY_CHANGE manages the Manufacturer Key changes between the terminal and the TOE. The key can be changed in previous phase for next phase as shown in the following picture.

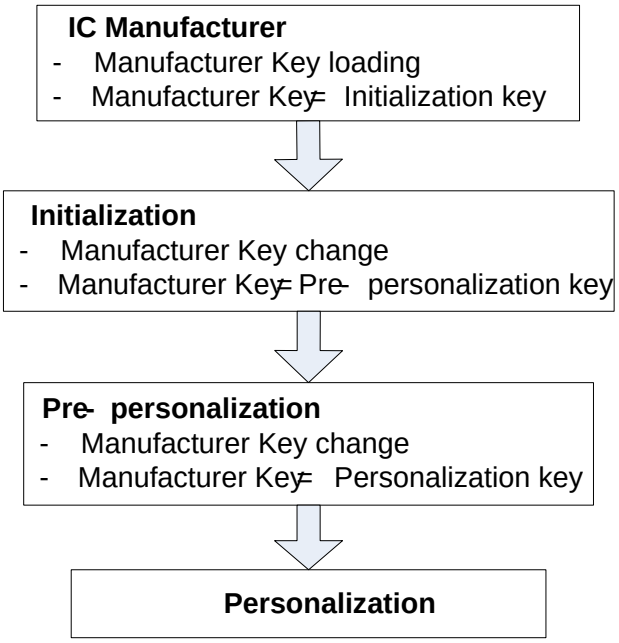


Figure 5: Manufacturer key

The SF.SYM_AUT.MANUF detects each unsuccessful authentication attempt. In such a case it warns the connected terminal. In case of successful termination of the protocol it stores appropriate keys for the secure messaging.
The SF.SYM_AUT.MANUF_PROT protects Manufacturer Key. After three consecutive false authentication attempts the key is locked.
SF.SYM_AUT.BAC enforces mutual authentication during Basic Access Control mechanism and manages the key exchanges between the terminal and the TOE. The SSF detects each unsuccessful authentication attempt. In such a case it warns the connected terminal. In case of successful termination of the protocol it stores appropriate keys for the secure messaging.
SF.SYM_AUT.BAC_RESTR restricts false Basic Access Control authentication attempts. After unsuccessful BAC authentication there is delay before next authentication attempt is possible. Every consecutive false attempt increases the delay until maximum value is reached.

7.1.1.4 SF.SM: Secure Messaging

The SF.SM function provides the management of the secure channel for the sensitive data exchange with the terminal. The integrity and authenticity of the communication is handled by using encryption and Message Authentication Codes. The authentication procedures differ between life cycles states, but once the session keys are generated, the SM processing is equal in all of them. If a SM error occurs, the session keys are cleared and the SM is aborted. Defined authentication status information is also cleared upon such event. A SM error may be due to not using SM, having too few or wrong SM fields, incorrect order of SM fields or having MAC or padding errors in SM fields.

7.1.1.5 SF.CA: Chip Authentication

SF.CA enforces Chip Authentication protocol. It is a Diffie-Hellman key agreement procedure. This function provides new session keys for secure messaging.

This SF also erases the BAC session keys upon successful completion of CA.

7.1.1.6 SF.TA_CER: Validity of the Certificate Chain

The SF.TA_CER security function is divided to the following SSFs:

1. SF.TA_CER.VERIFY
2. SF.TA_CER.TRUST_UPDATE
3. SF.TA_CER.TRUST_ATOMIC
4. SF.TA_CER.CURRENT_DATE

The SF.TA_CER.VERIFY enforces the Verify Certificate function during Terminal Authentication process through PSO: VERIFY CERTIFICATE command. The public key of the certification authority (PK_{CVCA}) to be used in the first verification process shall be present in the card (in EF.CVCA and in a key object) and is referenced with a prior MSE: SET DST command. This public key is called a *trustpoint*. At least two chained certificates are expected to be provided: C_{DV} and C_{IS}. Additionally, if there exists a newer trustpoint(s) and the corresponding link certificate(s) C_{CVCA} are stored in the terminal, there may be an indefinite number of trustpoint updates before the presentation of the certificate chain. The function SF.TA_CER.TRUST_UPDATE enforces management of the trust point. When receiving a new PK_{CVCA}, PSO VERIFY CERTIFICATE must perform the following operations:

- Search for an unused CVCA public key object (detected by checking if the object contains a key and if the key is listed in EF.CVCA).
- Write the new key into that key object (no backup management required as long as an interruption cannot corrupt the object).
- Update EF.CVCA to list the new key in the beginning of the file, and the younger one of the possible previous keys, unless it has expired (backup management required). This process practically disables the oldest key and any expired key.

The SF.TA_CER.TRUST_ATOMIC ensures that the operations for enabling or disabling a PK_{CVCA} public key (including key object manipulation and EF.CVCA modification) constitute one atomic operation.

SF.TA_CER.CURRENT_DATE manages Current Date. This information is updated in the case that the effective date of the received certificate (C_{CVCA}, C_{DV} or C_{IS}) is later than the Current Date, and the certificate has been signed by the CVCA or a domestic DV.

7.1.1.7 SF.TA_AUT: Asymmetric Authentication Mechanism

The SF.TA_CER security function is divided to the following SSFs:

1. SF.TA_AUT.RNG
2. SF.TA_AUT.EXT_AUT

The SF.TA_AUT.RNG provides pseudo-random numbers.

The SF.TA_AUT.EXT_AUT allows the authentication of a terminal by the mean of an external authentication using asymmetric keys. This SF completes the Terminal Authentication procedure. It detects each unsuccessful authentication attempt. In such a case it warns the connected terminal.

7.1.1.8 SF.AA: Active Authentication

The SF.AA function provides the active authentication mechanism. It also supports asymmetric key pair generation for the purpose of Active Authentication.

7.1.2 TSFs provided by the NXP P5CD080 chip

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

SF	Description
F.RNG	Random number generation
F.HW_DES	Triple-DES Co-processor
F.HW_AES	AES Co-processor
F.OPC	Control of Operating Conditions
F.PHY	Protection against physical manipulation
F.LOG	Logical protection
F.COMP	Protection of mode control
F.MEM_ACC	Memory Access Control
F.SFR_ACC	Special Function Register Access Control

Table 9: Security Functions provided by the NXP P5CD080 chip

These SF are described in [ST-IC].