eTravel EAC v1.0

MRTD EAC

Common Criteria / ISO 15408

Security Target – Public version

EAL4+

CONTENT

FIGURES

TABLES

1. ST INTRODUCTION

1.1 ST IDENTIFICATION

Title:	eTravel v1.0 MAÏA3 EAC Security Target
Version:	v0.9 issued 02 June 2009
ST reference:	ST_D1131803
Origin:	Gemalto
Author:	Antoine DE LAVERNETTE
Product identification:	eTravel v1.0
Security Controller:	IFX SLE66CLX800PE m1581 e13/a14
TOE identification:	eTravel v1.0
TOE documentation:	user guide [USR] and administration guide [ADM]

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.

CPLC field	Length	Value
IC Fabricator	2	IFX
IC Type	2	SLE66CLX800PE
Operating System Identifier	2	n.a.
Operating System release date	2	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 Eqiopment Identifier	4	n.a.
IC Personalizer	2	n.a.
IC Personalization Date	2	n.a.
IC Personalization Equipment Identifier	4	n.a.

Table 1-1. Card Production Life Cycle Data

IT Security Evaluation scheme:	Serma Technologies
IT Security Certification scheme:	Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)

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 [LDS] and [ASM].

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 CC CONFORMANCE

This security target claims conformance to:

- *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, August 2005, version 2.3, CCMB-2005-08-001 [CC-1],
- *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*, August 2005, version 2.3, CCMB-2005-08-002 [CC-2],
- *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements*, August 2005, version 2.3, CCMB-2005-08-003 [CC-3],

as follows:

- Part 2 extended,
- Part 3 conformant,
- Package conformant to EAL4 augmented with ADV_IMP.2, ALC_DVS.2, ALC_FLR.3, AVA_MSU.3 and AVA_VLA.4.

This security target claims conformance also to the Protection Profile *Machine Readable Travel Document with 'ICAO Application". Extended Access Control* [PP-MRTD-EAC].

The evaluation of the TOE uses the result of the CC evaluation of the IFX SLE66CLX800PE chip claiming conformance to the PP [PP-SC]. The hardware part of the composite evaluation is covered by the certification report [CR-IFX].

The minimum strength level for the TOE security functions is "SOF high" (Strength of functions high).

1.4 REFERENCES

1.4.1 External References

[ASM]	*Technical Guideline – Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC),* Version 1.0, 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
[CC-1]	*Common Criteria for Information Technology Security Evaluation* *Part 1: Introduction and general model,* CCMB-2005-08-001, version 2.3, August 2005
[CC-2]	*Common Criteria for Information Technology Security Evaluation* *Part 2: Security Functional Requirements* CCMB-2005-08-002, version 2.3, August 2005
[CC-3]	*Common Criteria for Information Technology security Evaluation* *Part 3: Security Assurance Requirements* CCMB-2005-08-003, version 2.3, August 2005
[CR-IFX]	*Certification Report, SLE66CLX800PE / m1581 - e13/a14* *BSI-DSZ-CC-0482-2008*
[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
[LDS]	*MRTD, Technical Report, Development of a Logical Data Structure - LDS for Optional Capacity Expansion Technologies* International Civil Aviation Organization LDS 1.7 -2004-05-18, Revision 1.7, May 18 2004
[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-MRTD-BAC]	*Common Criteria Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control* Bundesamt für Sicherheit in der Informationstechnik BSI-PP-0017, version 1.0, 18 August 2005
[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-0026, Version 1.2, 19th November 2007
[PP-SC]	*Smartcard IC Platform protection Profile* BSI-PP-0002, version 1.0, July 2001
[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
[ST-IFX]	*Security Target, IFX SLE66CLX800PEx and derivates* *Version 1.2 – 2008–01-09*
[TR-ECC]	*Elliptic Curve Cryptography according to ISO 15946,* Technical Guideline, TR-ECC, BSI, 2006

1.4.2 Internal References

[IGS]	**Installation, Generation and Start Up Procedures**
[ADM]	**Administrator Guidance**
[USR]	**User Guidance**

1.5 ACRONYMS AND GLOSSARY

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

	Application note [PP-MRTD-EAC]	Optional informative part of the PP containing additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
	Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
	Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
BAC	Basic Access Control	Security mechanism defined in [PKI] by which means the MTRD's chip proves and the inspection system 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 $K_{ENC)}$ and message authentication (key $K_{MAC)}$ of data transmitted between the MRTD's chip and the inspection system [PKI]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
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). [LDS]
	Issuing State	The Country issuing the MRTD. [LDS]
LDS	Logical Data Structure	The collection of groupings of Data Elements stored in the optional capacity expansion technology [LDS]. 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. [LDS]
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. [LDS]
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. [LDS]
	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 [LDS], - 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): 1. biographical data, 2. data of the machine-readable zone, 3. photographic image and 4. 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. [LDS]
	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.

2. TOE DESCRIPTION

2.1 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 [LDS] and [ASM] and providing:

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

Application note: Additionally to the [PP-MRTD-EAC] 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) IFX SLE66CLX800PE,*
- *the IC Dedicated Test Software,*
- *the IC Dedicated Support Software (Boot Rom Software, Mifare Operating System),*
- *the eTravel EAC v1.0 Embedded Software (ES),*
- *the NVM Embedded Software,*
- *part of the MRTD Logical Data Structure,*
- *the guidance documentation of the eTravel EAC v1.0 product:*
    - *the administrator's guide (assurance family AGD-ADM),*
    - *the user's guide (assurance family AGD-USR).*

The eTravel EAC v1.0 Embedded Software (eTravel EAC v1.0 ES) is implemented in the ROM of the chip. This eTravel EAC v1.0 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.

2.2 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 [LDS] 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 [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:
  - 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.

2.3 IT FEATURES OF THE TOE

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 additional biometrics as optional security measure in the ICAO Technical report [PKI]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently of the TOE by the TOE environment.

This ST addresses the protection of the logical MRTD

- in integrity by write-only-once access control and by physical means and
- in confidentiality by the Basic Access Control Mechanism and the Extended Access Control Mechanism.

The Basic Access Control is a security feature, which shall be supported by the TOE. The Basic Access Control mechanism checks that the inspection system has physical access to the MRTD's datapage. This is enforced by requiring the inspection system to derive the Document Basic Access keys K_{ENC} and K_{MAC} from the optically read MRZ (Machine Readable Zone). This protocol is also used to generate session keys KS_{ENC}

and KS_{MAC} that are used to protect the confidentiality and integrity of the transmitted data by means of secure messaging [PKI], Annex E, and [LDS]. The BAC protocol can be seen from the following picture.

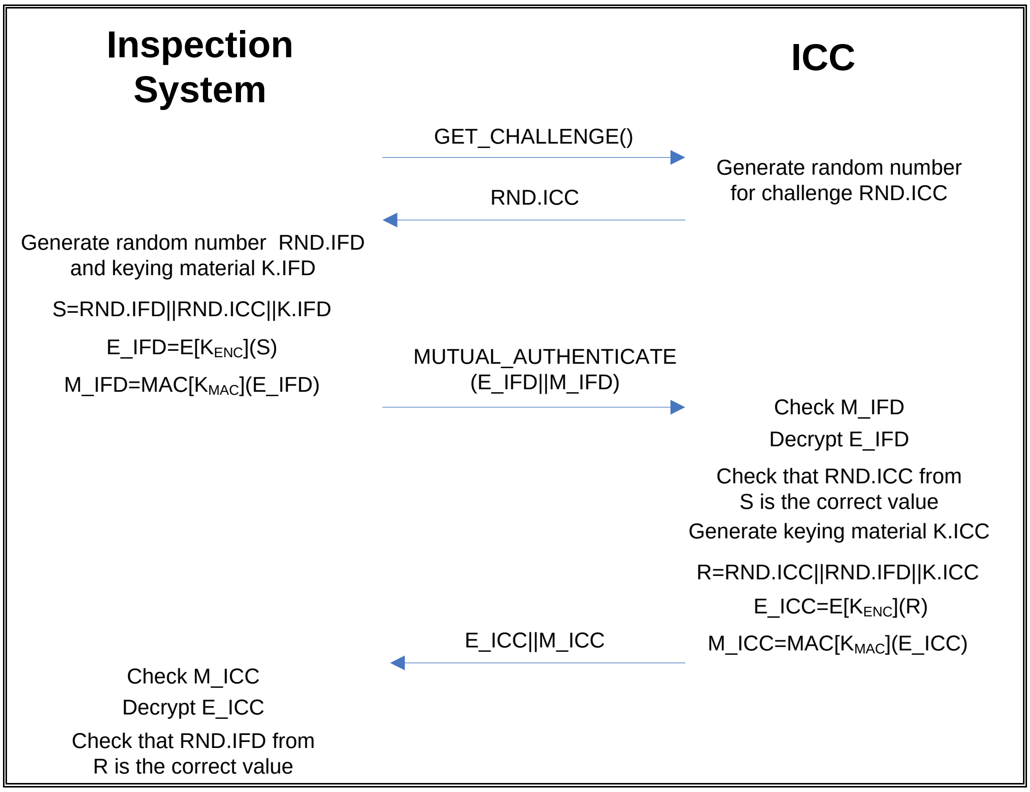


Figure 2-1. Basic Access Control Protocol

The ST requires the TOE to implement the Chip Authentication defined in [ASM]. The Chip Authentication provides evidence of the MRTD's chip authenticity and prevents data traces described in [PKI]. The Chip Authentication is provided by the following steps:

- the inspection system communicates by means of secure messaging established by Basic Access Control
- 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
- the inspection system generates a ephemeral key pair
- the TOE and the inspection system agree on two session keys for secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive
- 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. it could apply the Chip Authentication Private Key corresponding to the Chip Authentication Public Key for derivation of the session keys).

The Chip Authentication requires collaboration of the TOE environment.

The ST requires the TOE to implement the Extended Access Control as defined in [ASM]. The Extended Access Control consists of two parts:

- a Terminal Authentication Protocol to authenticate the inspection system as entity authorized by the Issuing State or Organization through the receiving state
- access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. It requires secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during transmission from the TOE to the inspection system. Therefore the Chip Authentication Mechanism must have been successfully executed before Terminal Authentication Protocol.

The CA and the TA protocols can be seen from the following figure and more detailed information can be found from [ASM]. When the Chip Authentication has been successfully performed secure messaging is restarted using new session keys $KS_{CA\ ENC}$ and $KS_{CA\ MAC}$ derived from K (see picture).

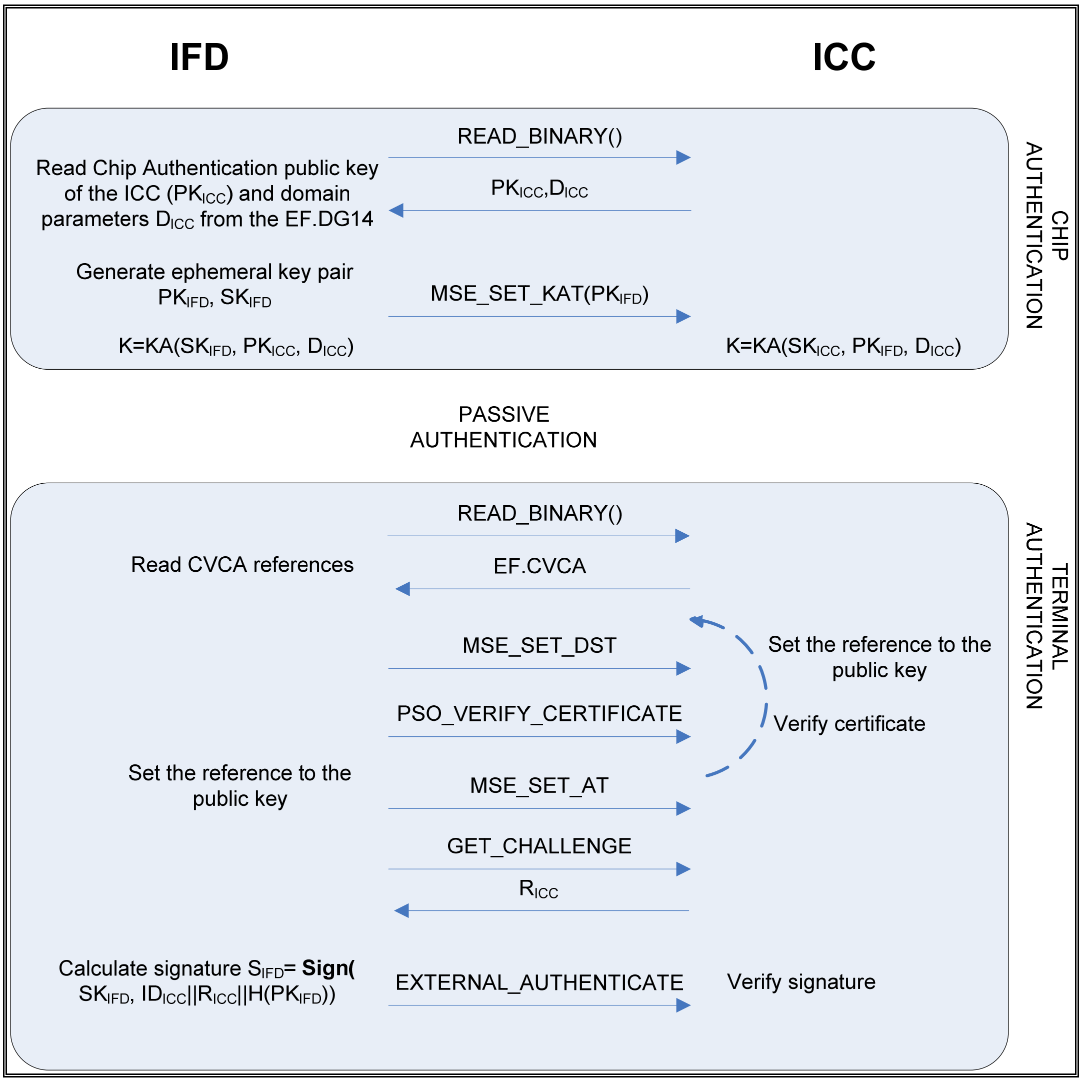


Figure 2-2. Extended Access Control Protocol

2.4 Scope of the TOE

2.4.1 Physical scope of the TOE

Figure 2-3 displays a picture of the eTravel EAC v1.0 product embedded in the datapage of a MRTD.

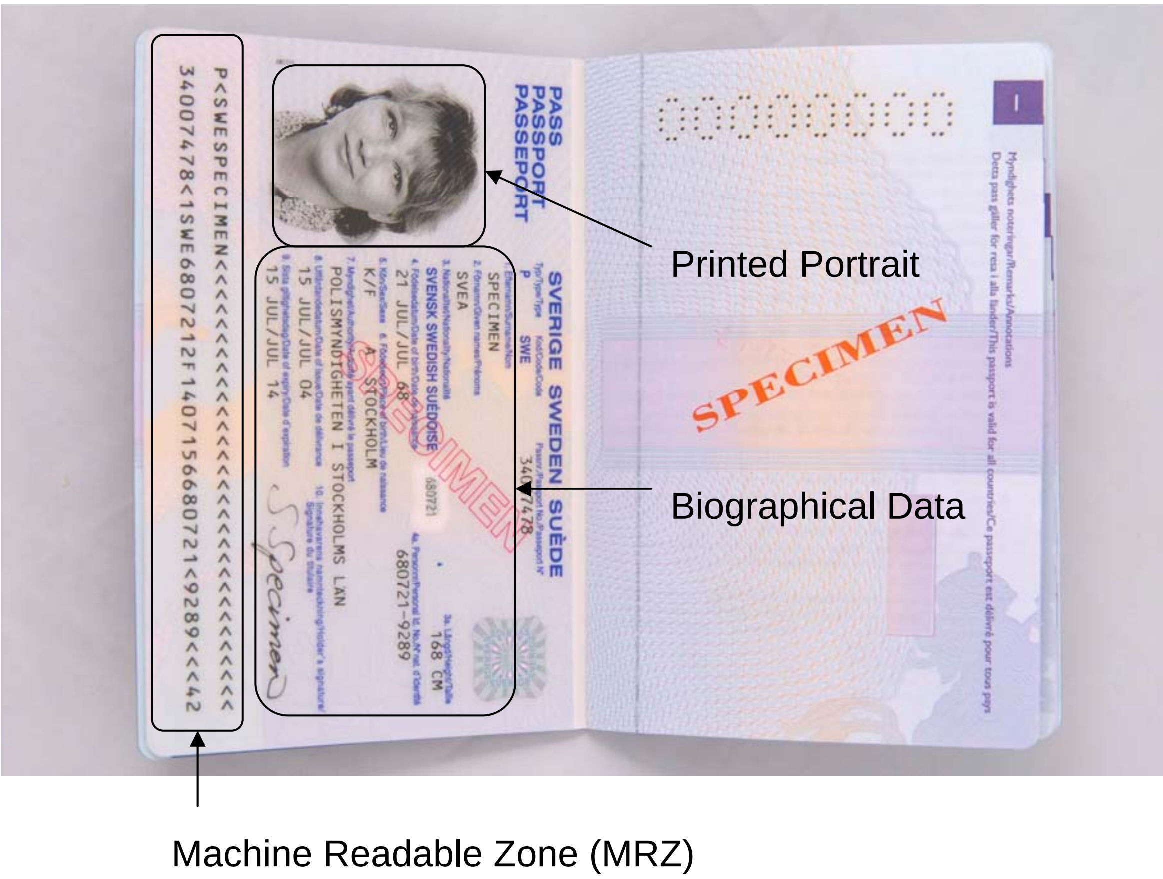


Figure 2-3. Physical aspect of the TOE embedded in the MRTD environment

The physical scope of the TOE is represented by the guidance documentation and the eTravel EAC v1.0 product (see Figure 2-4 below),.

The guidance documentation consists of user guide and administrator guide. The USER of the TOE is defined as the traveler and the inspection systems in the “Operational Use” phase. The administrator is defined as the passport Issuing State or Organization. So the personalization tasks and the TOE administration after personalisation are included in the administrator responsibilities. After issuance of the TOE to the passport holder, the TOE administrator could need to read traceability information of defect products.

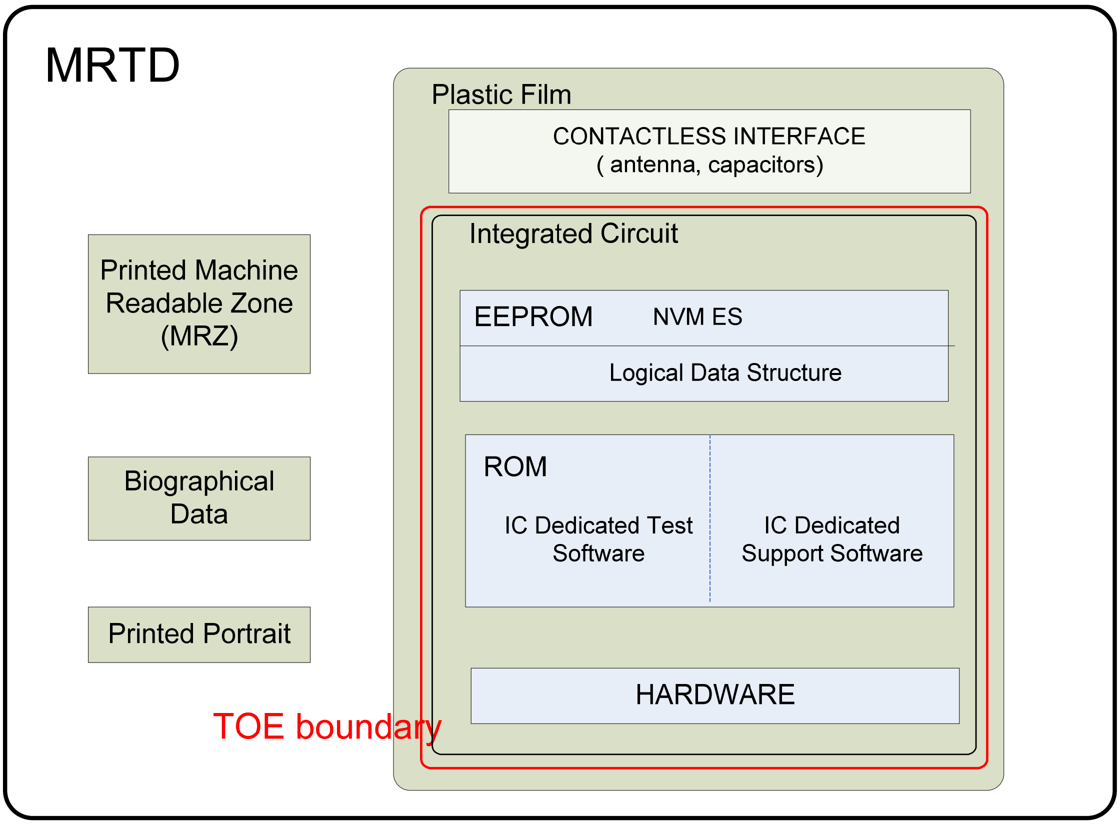


Figure 2-4. Physical structure of the TOE

2.4.2 Logical scope of the TOE

Figure 2-5 shows the logical file structure during operational use of the eTravel EAC v1.0 product.

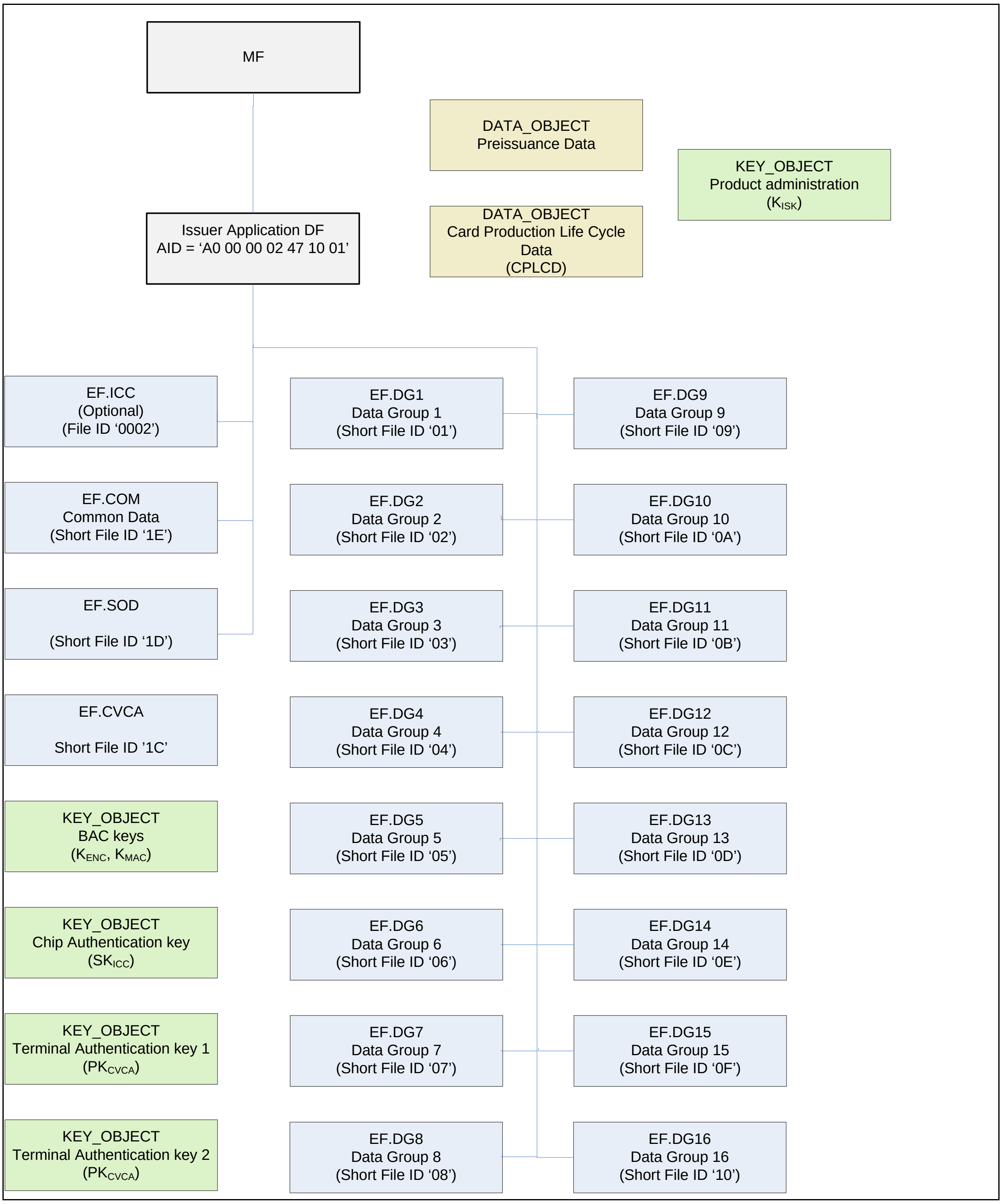


Figure 2-5. Logical data structure of the eTravel EAC v1.0 product

According to the issuing Organizations or States, some files are not mandatory (see Table 2-1 and [LDS]).

To allow confirmation of the authenticity and integrity of recorded details, an authenticity/Integrity object (Security Object Document) is recorded within a separate elementary file (EF.SOD). A *mandatory* Header and Data Group Presence Map are included within each implementation method, this information is stored in EF.COM.

Data Group	Mandatory (M) / Optional (O)	Data Item
Detail (s) Recorded in MRZ of the MRTD		
1	M	Machine Readable Zone (MRZ) Data
Machine Assisted Identity Confirmation Detail (s) – Encoded Identification Feature (s)		
2	M	Global Interchange feature – Encoded Face
3	O	Additional Feature – Encoded Finger (s)
4	O	Additional Feature – Encoded Iris (s)
Machine Assisted Identity Confirmation Detail (s) – Displayed Identification Feature (s)		
5	O	Displayed Portrait
6	O	Reserved for future use
7	O	Displayed Signature or Usual Mark
Machine Assisted Security Feature Verification – Encoded Security Feature (s)		
8	O	Data Feature (s)
9	O	Structure Feature (s)
10	O	Substance Feature (s)
Additional Personal Detail (s)		
11	O	Additional Personal Data Elements
Additional Document Detail (s)		
12	O	Additional Document Data Elements
Optional Detail (s)		
13	O	Discretionary Data Element(s) defined by issuing State or Organization
Reserved for Future Use		
14	O	Chip Authentication Public Key Info
15	O	Active Authentication Public Key Info
Person (s) to Notify		
16	O	Person (s) to Notify Data Element(s)

Table 2-1. Data Groups of the Issuer Application DF.

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. This implies that EF.DG14 is used.

2.5 TOE LIFE-CYCLE

2.5.1 Four phases

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

Phase 1 “Development”:

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

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

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

Phase 2 “Manufacturing”:

In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the nonvolatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as MRTD material during the IC manufacturing and the delivery process to the MRTD manufacturer. The IC is securely delivered from the IC manufacturer to the MRTD manufacturer.

The MRTD manufacturer has the following tasks:

- **Initialization:** adding the parts of the IC Embedded Software (NVM ES) to the EEPROM,
- **Pre-personalization:** creation of the MRTD application and equipping chip with Pre-personalization Data,

The following tasks are not part of the TOE manufacturing:

- **Inlay manufacturing:** packing the IC with hardware for the contactless interface.
- **Book manufacturing:** manufacturing the passport book.

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

Phase 3 “Personalization of the MRTD”:

The personalization of the MRTD includes:

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

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

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

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

Phase 4 “Operational Use”

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

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

2.5.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	IFX
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	IFX
Initializer	Gemalto or IFX
Pre-personalizer	Gemalto or IFX
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 2-2: Identification of the actors

2.5.3 Init on module at Gemalto site

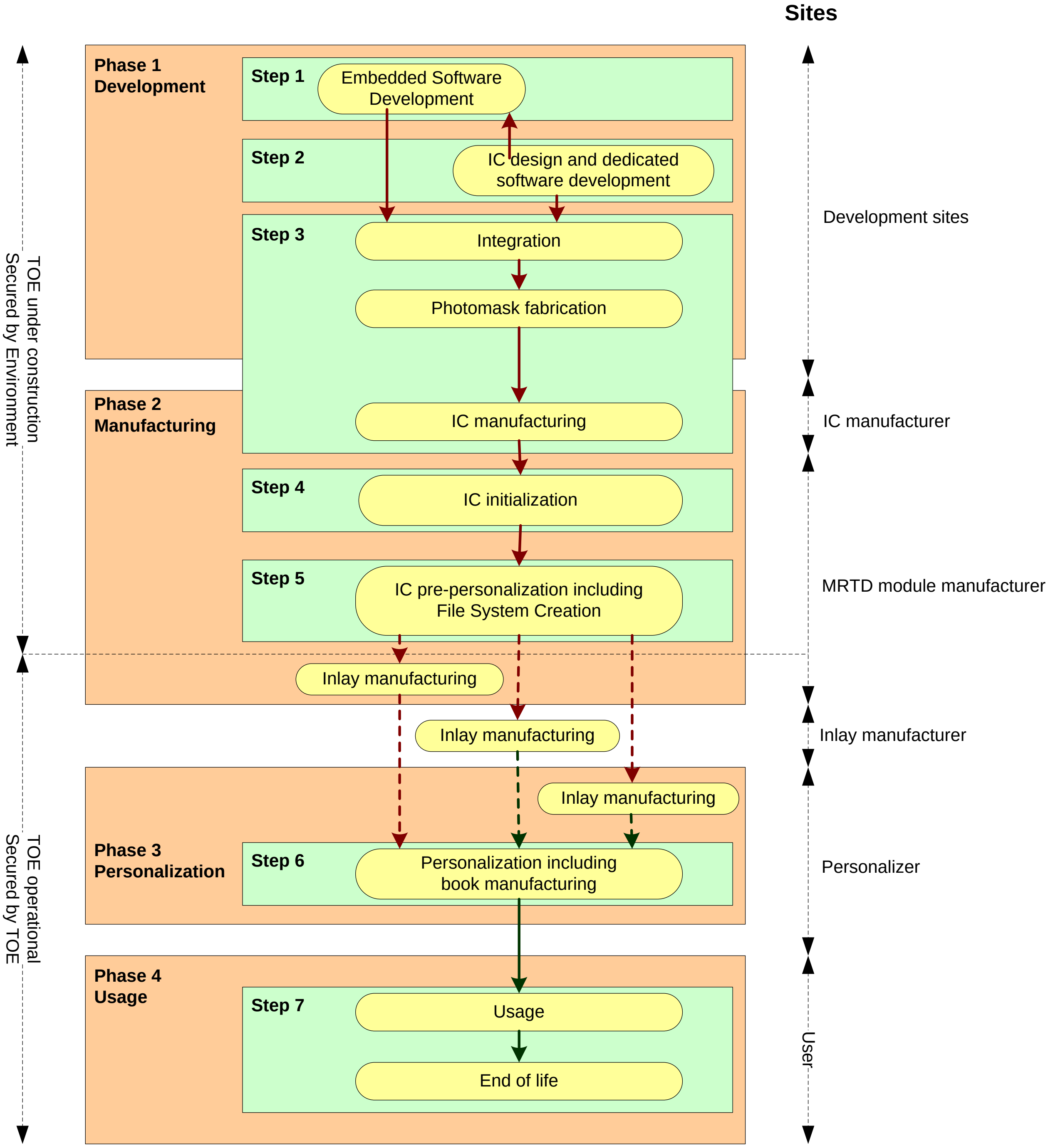


Figure 2-6. LC1: Init on module at Gemalto site

Figure 2-6. LC1: Init on module at Gemalto site describes the standard Life Cycle. The module is manufactured at the founder site. It is then shipped to Gemalto site where it is initialized and pre-personalized and then shipped to the Personalizer directly or after through the Inlay manufacturer.

During the shipment from Gemalto to the Personalizer, the module is protected by a diversified key.

2.5.4 Init on module at Founder site

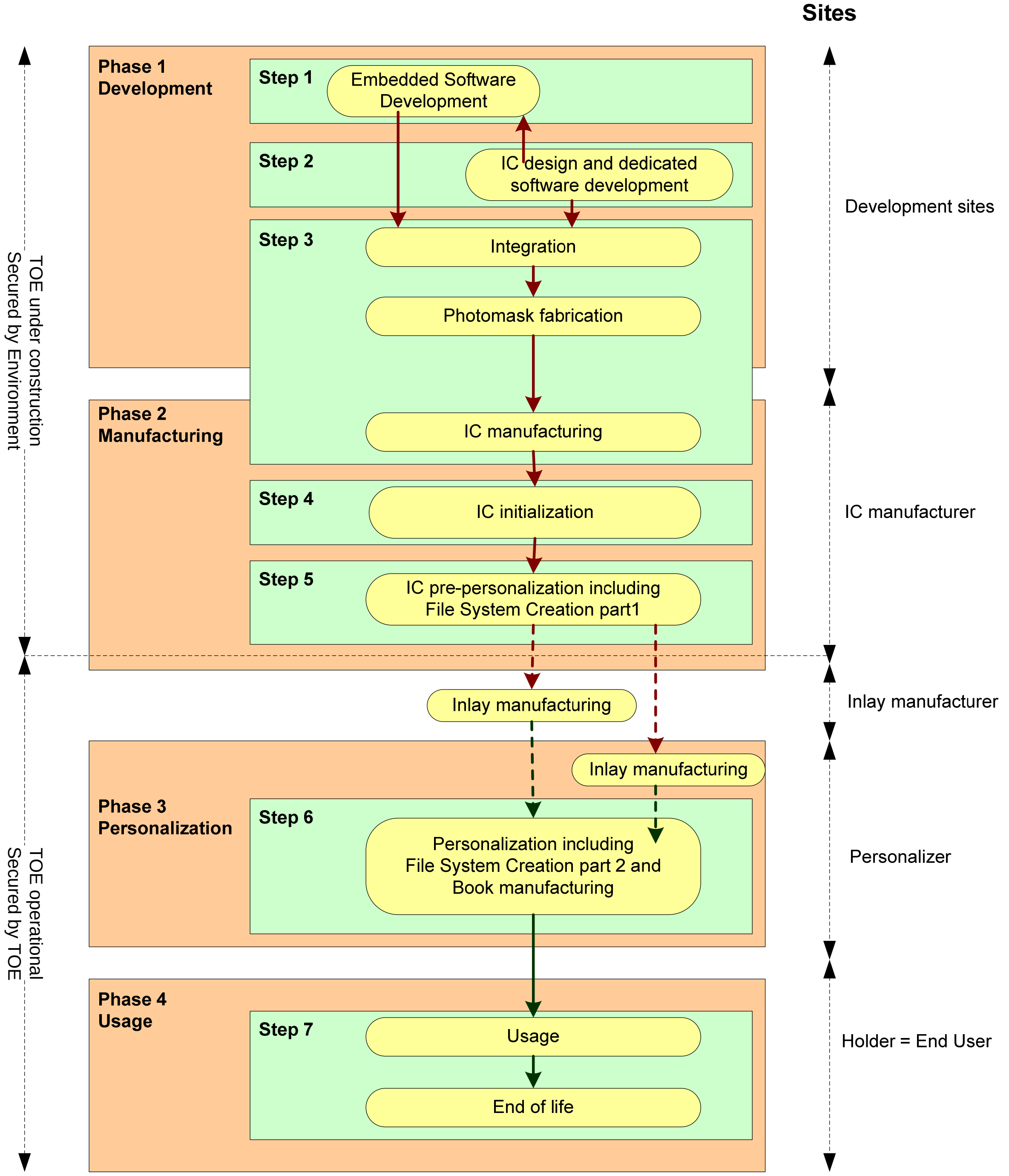


Figure 2-7. LC2 Init on module at Founder site

LC2 is an alternative to LC1. *Figure 2-7. LC2 Init on module at Founder site* describes the Life Cycle when the customer whishes to receive wafers directly from the founder. In this case, initialization and pre-personalization, which include sensitive operations such as the loading of patches, take 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.

2.5.5 Init on inlay at Gemalto site

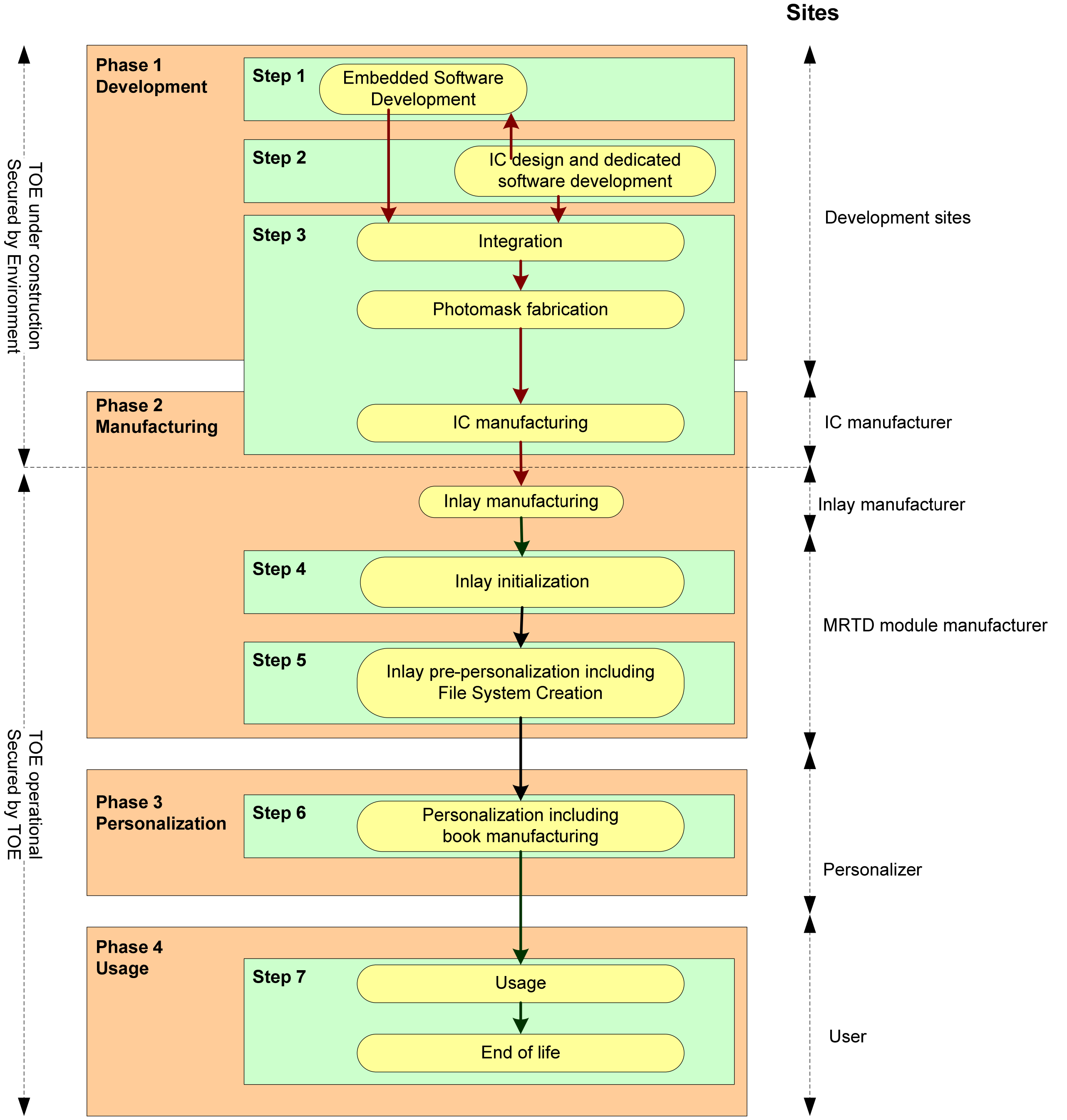


Figure 2-8. LC3: Init on inlay at Gemalto site

LC3 is another alternative to LC1. *Figure 2-8. LC3: Init on inlay at Gemalto site* describes the Life Cycle when the Gemalto whishes to receive inlays instead of 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 module is protected by a diversified key.

3. TOE SECURITY ENVIRONMENT

3.1 ASSETS

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

D.LDS : **Logical MRTD Data**

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different security needs) and the Document Security Object (EF.SOD) according to [LDS]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The data groups EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG14) is used by the inspection system for the Chip Authentication. The Active Authentication Public Key (EF.DG15) is used by the inspection system for the Active Authentication. The Document Security Object is used by the inspection system for Passive Authentication of the logical MRTD.

Even if all assets could be protected with a high security level (with the EAC mechanisms), some of them called later "standard data", have to be accessible through a mechanisms with a lower security level (BAC mechanisms). This is due to interoperability reasons as the ICAO Doc 9303 [5] specifies only the BAC mechanisms.

Assets are exhaustively detailed in the following way:

- keys used for product administration and MRTD application,
- data refined in less-sensitive data (protected by BAC)
- sensitive data (protected by EAC when enabled) as proposed in [ASM].

D.LDS. KEYS : Keys

Keys are protected in integrity and confidentiality and they are TSF data.

Key name	Key abbrev.	Function
Manufacturer Key	-	Product administration key
Document Basic Access Key for Encryption	K_{ENC}	Access Control to less-sensitive data of the MRTD application
Document Basic Access Key for MAC	K_{MAC}	
Document Basic Access Session Key for Encryption	KS_{ENC}	
Document Basic Access Session Key for MAC	KS_{MAC}	
Chip Authentication Private Key	SK_{ICC}	Key used by TOE in Chip Authentication to check authenticity of the MRTD chip
Chip Authentication Session Key for Encryption	KS_{CA_ENC}	Agreed keys as a result of Chip Authentication
Chip Authentication Session Key for MAC	KS_{CA_MAC}	
Country Verifying Certification Authority Public Key(s)	PK_{CVCA}	TOE starts certificate chain validation in Terminal Authentication by using this key

Table 3-1: Keys.

D.LDS.STANDARD_DATA : Standard Data

All the less-sensitive data are protected in integrity and confidentiality.

Data name	Data abbrev.	Location	Function
eTravel EAC v1.0 administration data			
Card Production Life Cycle Data	CPLCD	EEPROM Data Object and optionally EF.ICC	Unique identification of MRTD's chip (ES version, NVM ES version…)
MRTD applicative data			
Machine Readable Zone	MRZ	EF.DG1	Reflects the entire content of the MRZ
Encoded Face	-	EF.DG2	Represents the globally interoperable biometric for machine assisted identity confirmation
Security Object Document	SOD	EF.SOD	Contains the signatures used by the inspection system for Passive Authentication of the logical MRTD
Data Group Presence Map	DGPM	EF.COM	Contains the mandatory header and data group presence information
Data Groups 5-16	DG5, DG6, …, DG16	EF.DG5, EF.DG6, …, EF.DG16	See table 2-1

Table 3-2: Standard data.

Application note: As the CPLCD identifies uniquely the MRTD's chip, it is possible to trace the MRTD holder and realizing the threat T. CHIP_ID, thus access to CPLCD is protected.

D.LDS.SENS_DATA : Sensitive Data

All the sensitive data are protected in integrity and confidentiality.

Data name	Data abbrev.	Location	Function
eTravel V1 64K management data, TSF data			
Life cycle status	LCS	EEPROM	Life cycle status
Send Sequence Counter	SSC	RAM	Needed for secure messaging protocol
Current Date	CD	EEPROM	Needed for Terminal Authentication
Trusted Point	TP	EEPROM	Needed for Terminal Authentication
BAC authentication attempts counter	BACAC	EEPROM	Protects BAC keys
ISK authentication attempts counter	ISKAC	EEPROM	Protects Initial Supplier Key K_{ISK}
ISK authentication attempts status	ISKS	EEPROM	Protects Initial Supplier Key K_{ISK}
MRTD applicative data			

Data name	Data abbrev.	Location	Function
Fingerprint	DG3	EF.DG3	Additional biometric reference data
Encoded Iris	DG4	EF.DG4	Additional biometric reference data

Table 3-3: Sensitive data

An additional asset is the following more general one:

D.MRTD : **Authenticity of the MRTD's chip**

The authenticity of the MRTD's chip personalized by the issuing State or Organization for the MRTD's holder is used by the traveler to authenticate himself as possessing a genuine MRTD.

3.2 SUBJECTS

This security target considers the following subjects:

MANUFACTURER :

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

MRTD_HOLDER :

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

TRAVELER :

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

PERSONALIZATION_AGENT :

The agent is acting on the behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities:

- establishing the identity of the holder for the biographic data in the MRTD
- enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s)
- writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability
- writing the initial TSF data
- signing the Document Security Object defined in [LDS].

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) contains a terminal for the contactless communication with the MRTD's chip, implements the terminals part of the Basic Access Control Mechanism and gets the authorization to read the logical MRTD under the Basic Access Control by optical reading the printed data in the MRZ 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

- implements the Terminal Authentication Protocol

- 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.

TERMINAL :

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

ATTACKER :

A threat agent trying:

- to identify and to trace the movement of the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD)
- to read or to manipulate the logical MRTD without authorization,
- to forge a genuine MRTD.

COUNTRY VERIFYING CERTIFICATION AUTHORITY (CVCA):

The Country Verifying Certification Authority (CVCA) 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 and creates the Document Verifier Certificates within this PKI. The updates of the public key of the CVCA are distributed in form of Country Verifying CA Link-Certificates.

DOCUMENT VERIFIER (DV):

The Document Verifier (DV) 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 Document Verifier 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.

3.3 ASSUMPTIONS

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

A.PERS_AGENT : **Personalization of the MRTD's chip**

The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document 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 Public Key and the Document Signer Public Key of each issuing State or Organization [PKI].
ii. implements the terminal part of the Basic Access Control [PKI].

The Basic Inspection System reads the logical MRTD being under the 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 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). The CA

i. securely generates, stores and uses the Country Signing CA Key pair

ii. manages the MRTD's Chip Authentication Key Pairs.

The CA keeps the Country Signing CA Private Key secret and distributes 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

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 and distributes them 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 distributes the public key of their Country Verifying Certification Authority to their MRTD's chip.

3.4 THREATS

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

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

T.CHIP_ID: **Identification of MRTD's chip**

An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening a communication through the contactless communication interface. The attacker can not read optically and does not know in advance the physical MRTD data page.

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

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

T.READ_SENSITIVE_DATA: Read the sensitive biometric reference data

An attacker with high attack potential knowing the Document Basic Access Keys is trying 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 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 visual readable on the physical MRTD as well.

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

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

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim 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 MRTD's to create a new forged MRTD, e.g. the attacker write the digitized portrait and optional biometric reference data of finger read from the logical MRTD of a traveler into an other 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 in another contactless chip.

T.COUNTERFEIT: MRTD's chip

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.

T.ABUSE_FUNC: **Abuse of Functionality**

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

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

T.INFORMATION_LEAKAGE : **Information Leakage from MRTD's chip**

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

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

T.PHYS_TAMPER : **Physical Tampering**

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

MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) to modify User Data or (iv) to modify TSF data.

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

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

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

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

3.5 ORGANIZATIONAL SECURITY POLICIES

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

P.MANUFACT: **Manufacturing of the MRTD's chip**

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

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

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

P.PERSONAL_DATA: Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. Additional to the Basic Access Control Authentication defined by ICAO in [PKI] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip authentication.

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. 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.

4. SECURITY OBJECTIVES

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

OT.AC_PERS : **Access Control for Personalization of logical MRTD**

The TOE must ensure that the logical MRTD data groups EF.DG1 to EF.DG16, the Document Security Object according to [LDS] 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 can not be changed after its personalization. The Document Security Object can be updated by authorized Personalization Agents if data in the data groups EF.DG 3 to EF.DG16 are added.

Application note: This ST specify that in the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.

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.DATA_CONF : **Confidentiality of personal data**

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as (i) Personalization Agent or (ii) Basic Inspection System or (iii) Extended Inspection System. The TOE implements the Basic Access Control as defined by ICAO [PKI] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the 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 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 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". If the TOE is configured for use with Basic Inspection Terminals only in Phase 4 "Operational Use" the TOE shall identify themselves only to a successful authenticated Basic Inspection System or Personalization Agent.

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]. The authenticity proof provided by MRTD's chip shall be protected against attacks with high attack potential.

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

OT.PROT_ABUSE_FUNC : **Protection against Abuse of Functionality**

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

- to disclose critical User Data,
- to manipulate critical User Data of the Smartcard Embedded Software,
- to manipulate Soft-coded Smartcard Embedded Software,
- to 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.

Application note: The executable code (called NVM ES in this document for Non Volatile Memory Embedded Software) could be loaded to rectify potential problems in the eTravel EAC v1.0 ES and/or to add functionalities. After loading, a lock mechanism forbids any modification of the NVM ES.

OT.PROT_INF_LEAK : **Protection against Information Leakage**

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

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

OT.PROT_PHYS_TAMPER : **Protection against Physical Tampering**

The TOE must provide protection 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.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

4.2.1 Security Objectives for the Development and Manufacturing Environment

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

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

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

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

4.2.2 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.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 biographic data for the MRTD, (ii) enrol 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 Key Pair, (ii) ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity. The Issuing State or organization must (i) generate a cryptographic secure Document Signing 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 Signing 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 [LDS].

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.

Receiving State or organization

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

OE.EXAM_MRTD : **Examination of the MRTD passport book**

The inspection system of the receiving State must examine the MRTD presented by the traveler to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control [PKI]. 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 Public Key and the Document Signing Public Key maintaining their authenticity and availability in all inspection systems.

OE.PROT_LOGICAL_MRTD : **Protection of data of the logical MRTD**

The inspection system of the receiving State 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.

OE.EXT_INSP_SYSTEMS: Authorization of Extended Inspection Systems

The Document Verifier of receiving States or Organizations authorize 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. IT SECURITY REQUIREMENTS

5.1 EXTENDED COMPONENTS DEFINITION

This ST uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-SC], other components are defined in the protection profile [PP-MRTD-EAC].

5.1.1 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.

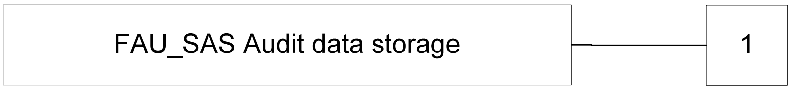
The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behaviour

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.
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.
Dependencies:	No dependencies.

5.1.2 Definition of the Family FCS_RND

To define the IT security functional requirements of the TOE an additional 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 as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

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

FCS_RND Generation of random numbers

Family behaviour

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

Component leveling:

FCS_RND Generation of random numbers — 1

FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1
	There are no management activities foreseen.
Audit:	FCS_RND.1
	There are no actions defined to be auditable.

FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].
Dependencies:	No dependencies.

5.1.3 Definition of the Family FIA_API

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

Application note: This security target uses this SFR for the TOE for the Chip Authentication mechanisms.

FIA_API Authentication Proof of Identity

Family behaviour

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 Authentication Proof of Identity — 1

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.

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

Dependencies: No dependencies.

5.1.4 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.

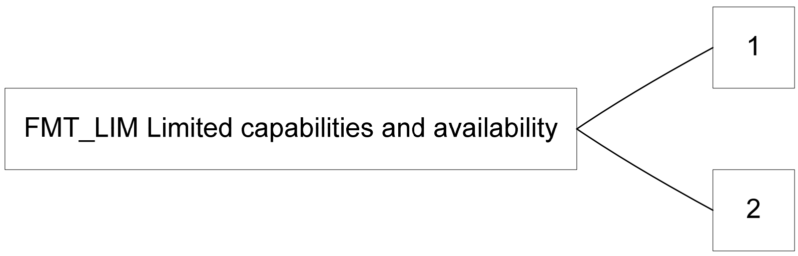
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

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 an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the

TOE show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

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

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: Limited capability and availability policy].
Dependencies:	FMT_LIM.2 Limited availability.

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

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited capability and availability policy].
Dependencies:	FMT_LIM.1 Limited capabilities.

5.1.5 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.

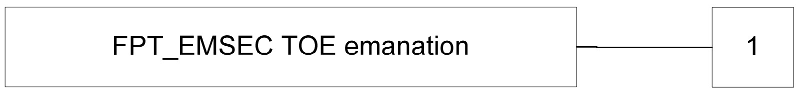
The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, 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 behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



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.
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].
Dependencies:	No other components.

5.2 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.

5.2.1 Class FAU Security Audit (FAU)

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

FAU_SAS.1 Audit storage

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

5.2.2 Class Cryptographic Support (FCS)

The Table below provides an overview on the cryptographic mechanisms used.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [PKI], Annex E, and [ASM]
Symmetric Authentication Mechanism for Initialization, Pre-personalization and Personalization	FCS_CKM.1.1/KDF_MRTD FCS_CKM.4.1/MRTD FCS_COP.1.1/SHA_MRTD-1 FCS_COP.1.1/TDES_MRTD FCS_COP.1.1/MAC_MRTD FCS_RND.1.1/MRTD	FCS_CKM.1.1/PKI FCS_CKM.1.1/KDF_BT FCS_CKM.4.1/BT FCS_COP.1.1/CERT_SIGN FCS_COP.1.1/SHA_BT FCS_COP.1.1/ENC_BT FCS_COP.1.1/MAC_BT FCS_RND.1.1/BT	Triple-DES, 112 bits keys, Retail-MAC, 112 bits keys SHA-1, BAC Key Derivation Mechanism
Basic Access Control Authentication Mechanism	FCS_CKM.1.1/KDF_MRTD FCS_CKM.4.1/MRTD FCS_COP.1.1/SHA_MRTD-1 FCS_COP.1.1/TDES_MRTD FCS_COP.1.1/MAC_MRTD FCS_RND.1.1/MRTD	FCS_CKM.1.1/PKI FCS_CKM.1.1/KDF_BT FCS_CKM.4.1/BT FCS_COP.1.1/CERT_SIGN FCS_COP.1.1/SHA_BT FCS_COP.1.1/ENC_BT FCS_COP.1.1/MAC_BT FCS_RND.1.1/BT	Triple-DES, 112 bits keys, Retail-MAC, 112 bits keys SHA-1, BAC Key Derivation Mechanism

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [PKI], Annex E, and [ASM]
Extented Access Control Authentication Mechanism	FCS_CKM.1.1/KDF_MRTD FCS_CKM.1.1/DH_MRTD-1 FCS_CKM.1.1/DH_MRTD-2 FCS_CKM.4.1/MRTD FCS_COP.1.1/SHA_MRTD-1 FCS_COP.1.1/SHA_MRTD-2 FCS_COP.1.1/SHA_MRTD-3 FCS_COP.1.1/SHA_MRTD-4 FCS_COP.1.1/TDES_MRTD FCS_COP.1.1/MAC_MRTD FCS_COP.1.1/SIG_VER-1 FCS_COP.1.1/SIG_VER-2 FCS_RND.1.1/MRTD	FCS_CKM.1.1/PKI FCS_CKM.1.1/KDF_BT FCS_CKM.4.1/BT FCS_COP.1.1/CERT_SIGN FCS_COP.1.1/SHA_BT FCS_COP.1.1/ENC_BT FCS_COP.1.1/MAC_BT FCS_RND.1.1/BT FCS_CKM.1.1/DH_GIS-1 FCS_CKM.1.1/DH_GIS-2 FCS_COP.1.1/SHA_GIS-1 FCS_COP.1.1/SHA_GIS-2 FCS_COP.1.1/SHA_GIS-3 FCS_COP.1.1/SHA_GIS-4 FCS_COP.1.1/SIG_SIGN_EIS	Triple-DES, 112 bits keys, Retail-MAC, 112 bits keys SHA-1, SHA-224, SHA-256, SHA-384 BAC Key Derivation Mechanism, RSA, 1536 and 2048 bits keys ECDSA, 192, 224, 256, 320 and 384 bits keys DH, 1536 and 2048 bits keys ECDH, 192 , 224, 256, 320 and 384 bits keys

Table 5-1. Cryptographic support

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below [CC-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/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

FCS_CKM.1.1/KDF_MRTD The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Control Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: [PKI].

FCS_CKM.1/DH_MRTD-1 Cryptographic key generation – Diffie-Hellman Keys by the MRTD

FCS_CKM.1.1/DH_MRTD-1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***DH Key Agreement Algorithm*** and specified cryptographic key sizes ***1536 and 2048 bits*** that meet the following: [ASM], Annex A.1.

FCS_CKM.1/DH_MRTD-2 Cryptographic key generation – Elliptic Curve Diffie-Hellman Keys by the MRTD

FCS_CKM.1.1/DH_MRTD-2 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***ECDH Key Agreement Algorithm*** and specified cryptographic key sizes ***192, 224, 256, 320 and 384 bits*** that meet the following: [ASM], Annex A.1.

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below [CC-2].

FCS_CKM.4/MRTD Cryptographic key destruction - MRTD

FCS_CKM.4.1/MRTD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[assignment: cryptographic key destruction method]* that meets the following: *[assignment: list of standards]*.

Refinement:

Key	Assignment: Cryptographic key destruction method	Assignment: List of standards
All session keys	Secure erasing of the value	None

Table 5-2. Cryptographic key destruction

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

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

FCS_COP.1.1/SHA_MRTD-1 The TSF shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-1*** and cryptographic key sizes none that meet the following: [FIPS180-2].

FCS_COP.1/SHA_MRTD-2 Cryptographic operation - Hash for Key Derivation by MRTD

FCS_COP.1.1/SHA_MRTD-2 The TSF shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-224*** and cryptographic key sizes none that meet the following: [FIPS180-2].

FCS_COP.1/SHA_MRTD-3 Cryptographic operation - Hash for Key Derivation by MRTD

FCS_COP.1.1/SHA_MRTD-3 The TSF shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-256*** and cryptographic key sizes none that meet the following: [FIPS180-2].

FCS_COP.1/SHA_MRTD-4 Cryptographic operation - Hash for Key Derivation by MRTD

FCS_COP.1.1/SHA_MRTD-4 The TSF shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-384*** and cryptographic key sizes none that meet the following: [FIPS180-2].

Application note: The TOE implements additional hash functions SHA-224, SHA-256 and SHA-384 for the Terminal Authentication Protocol.

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

FCS_COP.1.1/TDES_MRTD The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm Triple-DES in CBC mode and cryptographic key sizes 112 bits that meet the following: [FIPS46-3] and [PKI], Annex E.4.

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

FCS_COP.1.1/MAC_MRTD The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm Retail MAC and cryptographic key sizes 112 bits that meet the following: [ISO9797] (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2).

FCS_COP.1/SIG_VER-1 Cryptographic operation – Signature verification by MRTD

FCS_COP.1.1/SIG_VER-1 The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ***RSA*** and cryptographic key sizes ***1536 and 2048 bits*** that meet the following: ***[ISO9796-2]***.

FCS_COP.1/SIG_VER-2 Cryptographic operation – Signature verification by MRTD

FCS_COP.1.1/SIG_VER-2 The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm ***ECDSA*** and cryptographic key sizes ***192, 224, 256, 320 and 384 bits*** that meet the following: ***[ISO15946-2]***.

Application note:The minimum key size recommended in [ASM] for RSA algorithm is 1536 bits.

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/MRTD Quality metric for random numbers

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

5.2.3 Class Identification and Authentication (FIA)

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [PKI], Annex E, and [ASM]
Symmetric Authentication Mechanism for Personalization	FIA_UAU.4/MRTD	FIA_API.1/PT	Triple-DES with 112 bit keys
Basic Access Control Authentication Mechanism	FIA_AFL.1 FIA_UAU.4/MRTD FIA_UAU.6/MRTD	FIA_UAU.4/BT FIA_UAU.6/BT	Triple-DES, 112 bit keys, Retail-MAC, 112 bit keys
Chip Authentication Protocol	FIA_API.1/MRTD FIA_UAU.5/MRTD FIA_UAU.6/MRTD	FIA_UAU.4/GIS FIA_UAU.5/GIS FIA_UAU.6/GIS	DH or ECDH and Retail-MAC, 112 bit keys
Terminal Authentication Protocol	FIA_UAU.5/MRTD	FIA_API.1/EIS	RSASSA-PKCS1-v1_5 or EC-DSA with SHA

Table 5-3. Overview on authentication SFR.

Note the Chip Authentication Protocol include the asymmetric key agreement and 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.

Application note: The Table below lists additional authentication mechanisms supported by the TOE in comparison with the list of PP.

Name	SFR for the TOE	SFR for the TOE environment (terminal)	Algorithms and key sizes according to [PKI], Annex E, and [ASM]
Symmetric Authentication Mechanism for Personalization	FIA_UAU.4/MRTD	FIA_API.1/PT	Retail-MAC with112 bit keys
Terminal Authentication Protocol	FIA_UAU.5/MRTD	FIA_API.1/EIS	RSASSA-PSS with SHA-1 and SHA-256, EC-DSA with SHA-1, SHA-224, SHA-256 and SHA-384

Table 5-4. Additional overview on authentication SFR.

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below [CC-2].

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

1. <u>to establish the communication channel,</u>
2. <u>to read the Initialization Data if it not disabled by TSF according to FMT_MTD.1/INI_DIS</u>

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

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

Refinement:

Assignment: list of TSF-mediated actions	Refinement: Command
to read the Initialization Data in Phase 2 "Manufacturing"	READ_INFO and GET_DATA
to read the CPLC Data in Phase 3 "Personalization of the MRTD"	GET_DATA
to read the CPLC Data in Phase 4 "Operational Use"	GET_DATA

Table 5-5. Timing of identification

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below [CC-2].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

gemalto

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

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.

Refinement:

Assignment: list of TSF-mediated actions	Refinement: Command
to read the Initialization Data in Phase 2 “Manufacturing”	READ_INFO and GET_DATA
to read the CPLC Data in Phase 3 “Personalization of the MRTD”	GET_DATA
to read the CPLC Data in Phase 4 “Operational Use”	GET_DATA

Table 5-6. Timing of authentication

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

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

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

1. Basic Access Control Authentication Mechanism,

2. Terminal Authentication Protocol,

3. Authentication Mechanism based on Triple-DES.

Application note: The Authentication Mechanism based on Triple-DES is used for Personalization Agent authentication by means of the Personalization Terminal.

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

FIA_UAU.5/MRTD Multiple authentication mechanisms

FIA_UAU.5.1/MRTD The TSF shall provide

1. Basic Access Control Authentication Mechanism

2. Terminal Authentication Protocol

3. Secure Messaging in MAC-ENC mode

4. Symmetric Authentication Mechanism based on Triple-DES

to support user authentication.

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

1. the TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms:
   a) the Basic Access Control Authentication Mechanism with Personalization Agent Keys,
   b) the Symmetric Authentication Mechanism with the Personalization Agent Key,
   c) the Terminal Authentication Protocol with Personalization Agent Keys.
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with the key agreed upon with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.
4. After run of the Chip Authentication Mechanism 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.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism.

Application note: The TOE does not support authentication attempt as Personalization Agent by Terminal Authentication Protocol. The TOE is still compliant to the PP since the PP requires that the TOE accepts one mechanism from the list.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below [CC-2].

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

FIA_UAU.6.1/MRTD The TSF shall re-authenticate the user under the conditions

1. Each command sent to the TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.

2. 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 failure handling (FIA_AFL.1)" as specified below [CC-2].

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***a certain number of times (see table below)*** unsuccessful authentication attempts occur related to ***a certain authentication event (see table below)***.

Refinement:

Assignment: Number of unsuccessful authentication attempts	Assignment: Specified Authentication events	Assignment: Actions
3	Unsuccessful Mutual Authentication Command with Initial Supplier Key K_{ISK}	Initial Supplier Key blocked

Assignment: Number of unsuccessful authentication attempts	Assignment: Specified Authentication events	Assignment: Actions
1	Unsuccessful MAC verification after Basic Access Control Authentication	Basic Access Control session keys destroyed, authentication status reset
1	Unsuccessful MAC verification after Chip Authentication	Chip Authentication session keys destroyed, authentication status reset

Table 5-7. Authentication failure handling.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall perform ***actions specified in a following table.***

Refinement:

Assignment: Number of consecutive unsuccessful authentication attempts	Assignment: Specified Authentication events	Assignment: Actions
i	Unsuccessful Basic Access Control authentication attempt	Exponentially increasing time delay before new authentication attempt is possible

Table 5-8. BAC authentication failure handling.

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below ([CC-2] extended).

FIA_API.1/CAP Authentication Proof of Identity - MRTD

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

5.2.4 Class User Data Protection (FDP)

The TOE shall meet the requirement "Subset access control (FDP _ACC.1)" as specified below (Common Criteria Part 2). The instantiations of FDP_ACC.1 are caused by the TSF management according to FMT_MOF.1.

FDP_ACC.1 Subset access control

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

Application note: The data of the EF.ICC are user data. The EF.ICC data are readable under the control of the Basic Access Control SFP.

The TOE shall meet the requirement “Security attribute based access control (FDP_ACF.1)” as specified below [CC-2].

FDP_ACF.1 Security attribute based access control

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

1. Subjects:
    a) Personalization Agent,
    b) Basic Inspection System,
    c) Extended Inspection System,
    d) Terminal,
2. Objects:
    a) data in EF.DG1 to EF.DG16 of the logical MRTD,
    b) data in EF.COM,
    c) data in EF.SOD,
3. Security attributes
    a) Authentication status of terminals,
    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 Basic Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
3. the successfully authenticated Extended Inspection System is allowed to read the data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
4. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG3 according to the Terminal Authorization,
5. the successfully authenticated Extended Inspection System is allowed to read data in the EF.DG4 according to the Terminal Authorization.

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 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. The terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD.

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below [CC-2].

FDP_UCT.1/MRTD Basic data exchange confidentiality – MRTD

FDP_UCT.1.1/MRTD The TSF shall enforce the Access Control SFP to be able to transmit and receive objects 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 [CC-2].

FDP_UIT.1/MRTD Data exchange integrity – MRTD

FDP_UIT.1.1/MRTD The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication.

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

5.2.5 Class Security Management (FMT)

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below [CC-2].

FMT_SMF.1 Specification of Management Functions

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

1. Initialization
2. Personalization
3. Configuration

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

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifier Certification Authority,
4. Document Verifier,
5. Basic Inspection System,
6. Domestic Extended Inspection System,
7. Foreign Extended Inspection System.

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

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

FMT_LIM.1 Limited capabilities

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

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

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

FMT_LIM.2 Limited availability

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

- User Data to be disclosed or manipulated,
- TSF data to be disclosed or manipulated,

- software to be reconstructed and
- substantial information about construction of TSF to be gathered which may enable other attacks.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below [CC-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

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

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

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

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

FMT_MTD.1.1/CVCA_INI The TSF shall restrict the ability to write

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifier Certification Authority Certificate,
3. initial Current Date

to the Manufacturer and the Personalization Agent.

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

FMT_MTD.1.1/CVCA_UPD The TSF shall restrict the ability to update

1. Country Verifying Certification Authority Public Key,
2. Country Verifier Certification Authority Certificate

to the Country Verifier Certification Authority.

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

FMT_MTD.1.1/DATE The TSF shall restrict the ability to modify the Current Date to

1. Country Verifier Certification Authority,
2. Document Verifier,
3. domestic Extended Inspection System.

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

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

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

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to *[selection: create, load]* the Chip Authentication Private Key to *[assignment: the authorized identified roles]*.

Refinement:

Chip Authentication Private Key	Authorized roles
Key loading	Personalization Agent
Key creation	Personalization Agent

Table 5-9. Specification of management functions.

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

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read

1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. Personalization Agent Keys

to none.

FMT_MTD.3 Secure 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

gemalto

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 Authorization contained in the certificates of a valid certificate chain as a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

5.2.6 Class Protection of the Security Functions (FPT)

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMSEC.1 addresses the inherent leakage. With respect to the forced leakage they have to be considered in combination with the security functional requirements "Failure with preservation of secure state (FPT_FLS.1)" and "TSF testing (FPT_TST.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other. The SFR "Non-bypassability of the TSP (FPT_RVM.1)" and "TSF domain separation (FPT_SEP.1)" together with "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" and "Resistance to physical attack (FPT_PHP.3)" prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement "TOE Emanation (FPT_EMSEC.1)" as specified below [CC-2], extended:

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit ***electromagnetic and current emissions*** in excess of ***intelligible threshold*** enabling access to Personalization Agent Authentication Key and Chip Authentication Private Key and *[assignment: list of types of user data]*.

Refinement:

Assignment: List of types of user data
Data contents of EF.DG3
Data contents of EF.DG4

Table 5-10. User data which shall not emit electromagnetic or current emissions.

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 Authentication Key and Chip Authentication Private Key and *[assignment: list of types of user data]*.

Refinement:

Assignment: List of types of user data
Data contents of EF.DG3
Data contents of EF.DG4

Table 5-11. User data which shall be protected against access through smart card circuit contacts.

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

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below [CC-2].

FPT_FLS.1 Failure with preservation of secure state

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

1. exposure to 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 [CC-2].

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests *[selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]]* to demonstrate the correct operation of the TSF.

Refinement:

Selection and Assignment: Conditions under which self test should occur	Refinement: 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 5-12. TSF testing

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

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

The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below [CC-2].

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the TSP is not violated.

Refinement:

Application note: Related component FPT_PHP.3 information is provided in document [ST-IFX]. All the potential security violations managed by the component are included in the table below. Implemented software mechanisms provide protection against other security violations.

Assignment: Physical tampering scenarios	Assignment: List of TSF devices / elements
Physical manipulation and physical probing	Sensors
The external voltage supply is put out of range	Supply voltage sensors

Assignment: Physical tampering scenarios	Assignment: List of TSF devices / elements
The external clock signal is put out of range	Frequency sensors
The temperature is put out of range	Temperature sensors
Chip is exposed to light	Light sensors
Attempt to corrupt integrity of pointers	Redundant logic of PC, SP/SPE, PSWH
Attempts to corrupt the TDES computation	Triple-DES fault check
Attempts to run illegal instructions	Exception handling
Attempts to execute unauthorized system calls	Exception handling
Attempts to gain access to sensitive memory area	Exception handling
Attack which generates access collisions	Exception handling
Attempts to overflow the stack	Exception handling
Attempts to corrupt sensitive data writing	EEPROM writing check
Attempts to corrupt integrity of user data	Integrity check of user data
Attempts to corrupt integrity of TSF data (file headers, security attributes…)	Integrity check of TSF data
Attempts to corrupt the random number generator	Random number generator test
Attempts to corrupt the TDES computation	TDES verification
Attempts to corrupt the RSA computation	RSA verification
Attempts to disrupt the code execution	Software execution tracers

Table 5-13. Resistance to physical attack

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

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

FPT_RVM.1 Non-bypassability of the TSP

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

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

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by un-trusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.3 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

The security assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components: ADV_IMP.2, ALC_DVS.2, ALC_FLR.3, AVA_MSU.3 and AVA_VLA.4.

The minimum strength of function is SOF-high.

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

5.4 Security Requirements for the IT environment

This section describes the security functional requirements for the IT environment using components in [CC-2].

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

5.4.1 Passive Authentication

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

The Document Signer of the Issuing State or Organization shall meet the requirement “Basic data authentication (FDP_DAU.1)” as specified below [CC-2].

FDP_DAU.1 /DS Basic data authentication – Passive Authentication

FDP_DAU.1.1/DS The *Document Signer* shall provide a capability to generate evidence that can be used as a guarantee of the validity of logical data structure of the MRTD (EF.DG1 to EF.DG16) and the Document Security Object.

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

5.4.2 Extended Access Control PKI

The CVCA and the DV shall establish a Document Verification PKI by generating asymmetric key pairs and certificates for the CVCA, DV and IS which may be verified by the TOE.

FCS_CKM.1 /PKI-1 Cryptographic key generation – Document Verification PKI Keys -- RSA

FCS_CKM.1.1/PKI-1 The PKI shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***key generation algorithm for RSA keys*** and specified cryptographic key sizes ***1536 and 2048 bits*** that meet the following: [ASM], Annex A.

FCS_CKM.1 /PKI-2 Cryptographic key generation – Document Verification PKI Keys -- ECDSA

FCS_CKM.1.1/PKI-2 The PKI shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***key generation algorithm for ECDSA*** and specified cryptographic key sizes ***192, 224, 256, 320 and 384 bits*** that meet the following: [ASM], Annex A.

FCS_COP.1 /CERT_SIGN-1 Cryptographic operation – Certificate Signing -- RSA

FCS_COP.1.1/CERT_SIGN-1 The PKI shall perform digital signature creation in accordance with a specified cryptographic algorithm ***RSA*** and cryptographic key sizes ***1536 and 2048 bits*** that meet the following: ***[ASM], Annex A***.

FCS_COP.1 /CERT_SIGN-2 Cryptographic operation – Certificate Signing -- ECDSA

FCS_COP.1.1/CERT_SIGN-2 The PKI shall perform digital signature creation in accordance with a specified cryptographic algorithm ***ECDSA*** and cryptographic key sizes ***192, 224, 256, 320 and 384 bits*** that meet the following: ***[ASM], Annex A***.

5.4.3 Basic Terminal

This section describes common security functional requirements to the Basic Inspection Systems and the Personalization Agent if it uses the Basic Access Control Mechanism with the Personalization Agent Authentication Keys. Both are called "Basic Terminals" (BT) in this section.

The Basic Terminal shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below [CC-2].

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

FCS_CKM.1.1/KDF_BT The *Basic Terminal* shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm and specified cryptographic key sizes 112 bit that meet the following: ***[PKI]***.

The Basic Terminal shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below [CC-2].

FCS_CKM.4/BT Cryptographic key destruction - BT

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

The Basic Terminal shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below [CC-1]. The iterations are caused by different cryptographic algorithms to be implemented by the Basic Terminal.

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

FCS_COP.1.1/SHA_BT The Basic Terminal shall perform hashing in accordance with a specified cryptographic algorithm SHA-1 and cryptographic key sizes none that meet the following: FIPS180-2.

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

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

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

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

The Basic Terminal shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below [CC-2], extended).

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

FCS_RND.1.1/BT The Basic Terminal shall provide a mechanism to generate random numbers that meets ***K3-DRNG ([AIS20]) with seed entropy at least 112 bits and with strength of mechanism set to high.***

The Basic Terminal shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below [CC-2].

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

FIA_UAU.4.1/BT The Basic Terminal shall prevent reuse of authentication data related to Basic Access Control Authentication Mechanism.

The Basic Terminal shall meet the requirement "Re-authentication (FIA_UAU.6)" as specified below [CC-2].

FIA_UAU.6/BT Re-authentication - Basic Terminal

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

5.4.4 General Inspection System

The General Inspection System (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism. Therefore it has to fulfill all security requirements of the Basic Inspection System as described above.

The General Inspection System verifies the authenticity of the MRTD's by the Chip Authentication Mechanism during inspection and establishes new secure messaging with keys. The reference data for the Chip Authentication Mechanism is the Chip Authentication Public Key read form the logical MRTD data group EF.DG14 and verified by Passive Authentication (cf. to FDP_DAU.1/DS). Note, that the Chip Authentication Mechanism requires the General Inspection System to verify at least one message authentication code of a response sent by the MRTD to check the authenticity of the chip.

The General Inspection System shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below [CC-2].

FCS_CKM.1/DH_GIS-1 Cryptographic key generation – Diffie-Hellman Keys by the GIS

FCS_CKM.1.1/DH_GIS-1 The General Inspection System shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DH *Key Agreement Algorithm*** and specified cryptographic key sizes ***1536 and 2048 bits*** that meet the following: [ASM], Annex A.1.

FCS_CKM.1/DH_GIS-2 Cryptographic key generation – Elliptic Curve Diffie-Hellman Keys by the GIS

FCS_CKM.1.1/DH_GIS-2 The General Inspection System shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***ECDH Key Agreement Algorithm*** and specified cryptographic key sizes ***192, 224, 256, 320 and 384 bits*** that meet the following: [ASM], Annex A.1.

FCS_COP.1/SHA_GIS-1 Cryptographic operation – Hash for Key Derivation by GIS

FCS_COP.1.1/SHA_GIS-1 The General Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-1*** and cryptographic key sizes none that meet the following: [FIPS 180-2].

FCS_COP.1/SHA_GIS-2 Cryptographic operation – Hash for Key Derivation by GIS

FCS_COP.1.1/SHA_GIS-2 The General Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-224*** and cryptographic key sizes none that meet the following: [FIPS 180-2].

FCS_COP.1/SHA_GIS-3 Cryptographic operation – Hash for Key Derivation by GIS

FCS_COP.1.1/SHA_GIS-3 The General Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-256*** and cryptographic key sizes none that meet the following: [FIPS 180-2].

FCS_COP.1/SHA_GIS-4 Cryptographic operation – Hash for Key Derivation by GIS

FCS_COP.1.1/SHA_GIS-4 The General Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-384*** and cryptographic key sizes none that meet the following: [FIPS 180-2].

The General Inspection System shall meet the requirement “Single-use authentication mechanisms (FIA_UAU.4)” as specified below [CC-2].

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

FIA_UAU.4.1/GIS The General Inspection System shall prevent reuse of authentication data related to

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication Protocol.

The General Inspection System shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below [CC-2].

FIA_UAU.5/GIS Multiple authentication mechanisms – General Inspection System

FIA_UAU.5.1/GIS The General Inspection System shall provide

1. Basic Access Control Authentication Mechanism,
2. Chip Authentication

to support user authentication.

FIA_UAU.5.2/GIS The General Inspection System shall authenticate any user's claimed identity according to the following rules:

1. The General Inspection System accepts the authentication attempt as MRTD only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.

2. After successful authentication as MRTD and until the completion of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the authenticated MRTD by means of the Basic Access Control Authentication Mechanism.

3. After run of the Chip Authentication Mechanism the General Inspection System accepts only response codes with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.

The General Inspection System shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below [CC-2].

FIA_UAU.6/GIS Re-authenticating – Re-authenticating of Terminal by the General Inspection System

FIA_UAU.6.1/GIS The General Inspection System shall re-authenticate the user under the conditions

1. Each response sent to the General Inspection System after successful authentication of the MRTD with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall have a correct MAC created by means of secure messaging keys agreed upon by the Basic Access Control Authentication Mechanism.

2. Each response sent to the General Inspection System after successful run of the Chip Authentication Protocol shall have a correct MAC created by means of secure messaging keys generated by Chip Authentication Protocol.

The General Inspection System shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below [CC-2].

FDP_UCT.1/GIS Basic data exchange confidentiality - General Inspection System

FDP_UCT.1.1/GIS The General Inspection System shall enforce the Access Control SFP to be able to transmit and receive objects in a manner protected from unauthorized disclosure after Chip Authentication.

The General Inspection System shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below [CC-2].

FDP_UIT.1/GIS Data exchange integrity - General Inspection System

FDP_UIT.1.1/GIS The General Inspection System shall enforce the Basic Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors after Chip Authentication.

FDP_UIT.1.2/GIS The General Inspection System shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred after Chip Authentication.

5.4.5 Extended Inspection System

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.

FCS_COP.1/SIG_SIGN_EIS-1 Cryptographic operation – Signature creation by EIS -- RSA

FCS_COP.1.1/SIG_SIGN_EIS-1 The Extended Inspection System shall perform signature creation in accordance with a specified cryptographic algorithm ***RSA*** and cryptographic key sizes ***1536 and 2048 bits*** that meet the following: ***[ASM], Annex A.1***.

FCS_COP.1/SIG_SIGN_EIS-2 Cryptographic operation – Signature creation by EIS -- ECDSA

FCS_COP.1.1/SIG_SIGN_EIS-2 The Extended Inspection System shall perform signature creation in accordance with a specified cryptographic algorithm ***ECDSA*** and cryptographic key sizes ***192, 224, 256, 320 and 384 bits*** that meet the following: ***[ASM], Annex A.1***.

FCS_COP.1/SHA_EIS-1 Cryptographic operation – Hash for Key Derivation by EIS

FCS_COP.1.1/SHA_EIS-1 The Extended Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-1*** and cryptographic key sizes none that meet the following: FIPS 180-2.

FCS_COP.1/SHA_EIS-2 Cryptographic operation – Hash for Key Derivation by EIS

FCS_COP.1.1/SHA_EIS-2 The Extended Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-224*** and cryptographic key sizes none that meet the following: FIPS 180-2.

FCS_COP.1/SHA_EIS-3 Cryptographic operation – Hash for Key Derivation by EIS

FCS_COP.1.1/SHA_EIS-3 The Extended Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-256*** and cryptographic key sizes none that meet the following: FIPS 180-2.

FCS_COP.1/SHA_EIS-4 Cryptographic operation – Hash for Key Derivation by EIS

FCS_COP.1.1/SHA_EIS-4 The Extended Inspection System shall perform hashing in accordance with a specified cryptographic algorithm ***SHA-384*** and cryptographic key sizes none that meet the following: FIPS 180-2.

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below [CC-2], extended.

FIA_API.1/EIS Authentication Proof of Identity – Extended Inspection System

FIA_API.1.1/EIS The Extended Inspection System shall provide a Terminal Authentication Protocol according to [ASM] to prove the identity of the Extended Inspection system.

5.4.6 Personalization Terminals

The TOE supports different authentication and access control mechanisms which may be used for the Personalization Agent depending on the personalization scheme of the Issuing State or Organization:

1. The Basic Access Control Mechanism which may be used by the Personalization Terminal with a Personalization Agent Secret Key Pair. The Basic Access Control Mechanism establishes strong cryptographic keys for the secure messaging to ensure the confidentiality by Triple-DES and integrity by Retail-MAC of the transmitted data. This approach may be used in a personalization environment where the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.
2. The Personalization Terminal may use the Terminal Authentication Protocol like a Extended Inspection System but using the Personalization Agent Keys to authenticate themselves to the TOE. This approach may be used in a personalization environment where (i) the Personalization Agent want to authenticate the MRTD's chip and (ii) the communication between the MRTD's chip and the Personalization Terminal may be listened or manipulated.
3. In a centralized personalization scheme the major issue is high productivity of personalization in a high secure environment. In this case the personalization agent may wish to reduce the protocol to symmetric authentication of the terminal without secure messaging. Therefore the TOE and the Personalization Terminal support a simple the Symmetric Authentication Mechanism with Personalization Agent Key as requested by the SFR FIA_UAU.4/MRTD and FIA_API.1/SYM_PT.

The Personalization Terminal shall meet the requirement "Authentication Prove of Identity (FIA_API)" as specified below ([CC-2], extended) if it uses the Symmetric Authentication Mechanism with Personalization Agent Key.

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

FIA_API.1.1/SYM_PT The Personalization Terminal shall provide an Authentication Mechanism based on Triple-DES to prove the identity of the Personalization Agent.

6. TOE SUMMARY SPECIFICATION

6.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the eTravel EAC v1.0 embedded software (including the optional NVM ES) and by the chip.

6.1.1 TSFs provided by the eTravel EAC v1.0 Software

SF	**Description**	**SSF**	**SOF claim**
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	High
		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	High
		SF.TA_AUT.EXT_AUT	-

Table 6-1. Security Functions provided by the eTravel EAC v1.0 Software.

6.1.1.1 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 desynchronisation and/or random order treatments. This security function involve: random order processing mechanism, secured DES operation, secured RSA operation, secured ECC operation and software desynchronisation 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.

This function has no strength.

6.1.1.2 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 6-2. Correspondance 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).

This function has no strength.

6.1.1.3 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 is shown in the following picture.

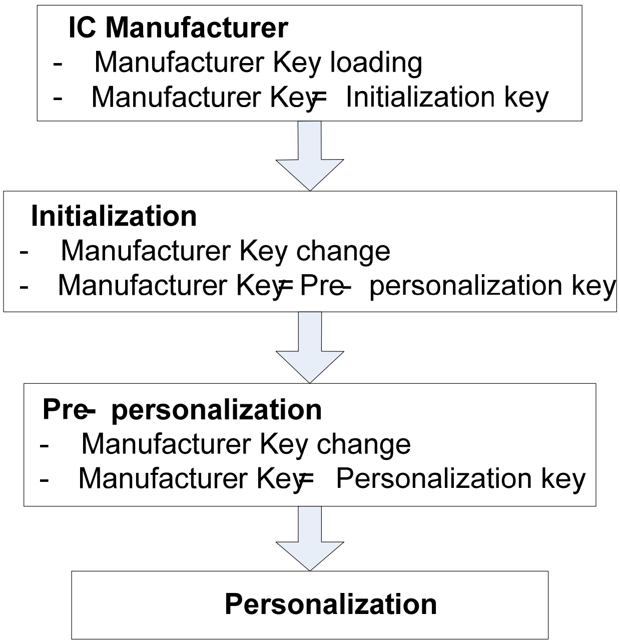


Figure 6-1. Manufacturer key

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.

The strength of function is high because the random number generation is based on probabilistic and/or permutational mechanisms.

6.1.1.4 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.

This function has no strength.

6.1.1.5 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 function has no strength.

6.1.1.6 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.

This function has no strength.

6.1.1.7 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.

The strength of function is high because the random number generation is based on probabilistic and/or permutational mechanisms.

6.1.2 TSFs provided by the Infineon SLE66CLX800PE chip

The evaluation is a composite evaluation and uses the results of the CC evaluation provided by [CR-IFX]. The IC and its primary embedded software have been evaluated at level EAL 5 with a minimum strength level for its security functions of SOF-high.

SF	Description
SEF.1	Operating state checking
SEF.2	Phase management with test mode lock-out
SEF.3	Protection against snooping
SEF.4	Data encryption and data disguising
SEF.5	Random number generation
SEF.6	TSF self test
SEF.7	Notification of physical attack
SEF.8	Memory Management Unit (MMU)
SEF.9	Cryptographic support

Table 6-3. Security Functions provided by the IFX SLE66CLX800PE chip.

These SF are described in [ST-IFX].

6.2 ASSURANCE MEASURES

Assurance Measure	Document title
AM_ASE	eTravel EAC V1 Security Target
AM_ADV_FSP	Functional Specifications eTravel EAC V1
AM_ALC	Class ALC eTravel EAC V1
AM_ACM	Class ACM eTravel EAC V1
AM_ADO	Class ADO eTravel EAC V1
AM_ADV_HLD	High Level Design eTravel EAC V1
AM_ADV_LLD	Low Level Design eTravel EAC V1
AM_AGD_ADM	Administrator Guidance eTravel EAC V1
AM_AGD_USR	User Guidance eTravel EAC V1
AM_ATE	Class ATE eTravel EAC V1
AM_AVA_MSU	Misuse eTravel EAC V1
AM_AVA_VLA_SOF	Vulnerability analysis – SOF eTravel EAC V1
AM_CODE	Source Code for eTravel EAC V1

Table 6-4. Assurance Measures.

The development team uses a configuration management system that supports the generation of the TOE. The configuration management system is well documented and identifies all different configuration items. The configuration management tracks the implementation representation, design documentation, test documentation, user documentation, administrator documentation. The security of the configuration management is described in detail in a separate document.

The delivery process of the TOE is well defined and follows strict procedures. Several measures prevent the modification of the TOE based on the developer's master copy and the user's version. The Administrator and the User are provided with necessary documentation for initialization and start-up of the TOE.

The implementation is based on an informal high-level and low-level design of the components of the TOE. The description is sufficient to generate the TOE without other design requirements.

The correspondence of the Security Functional Requirements (SFR) with less abstract representations will be demonstrated in a separate document. This addresses ADV_FSP, ADV_HLD, ADV_LLD. ADV_IMP and ADV_RCR.

The tools used in the development environment are appropriate to protect the confidentiality and integrity of the TOE design and implementation. The development is controlled by a life cycle model of the TOE. The development tools are well defined and documented.

The Gemalto R&E organization is equipped with organizational and personnel means that are necessary to develop the TOE.

As the evaluation is identified as a composite evaluation based on the CC evaluation of the hardware, the assurance measures related to the hardware (IC) will be provided by documents of the IC manufacturer.

7. PP CLAIMS

The eTravel EAC v1.0 security target is conformant with the Protection Profile "Machine Readable Travel Document with ICAO Application, Extended Access Control" BSI-PP-0026 version 1.2.