	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

---

# Security Target Lite

## eTravel Essential 1.0

### EAC on BAC
















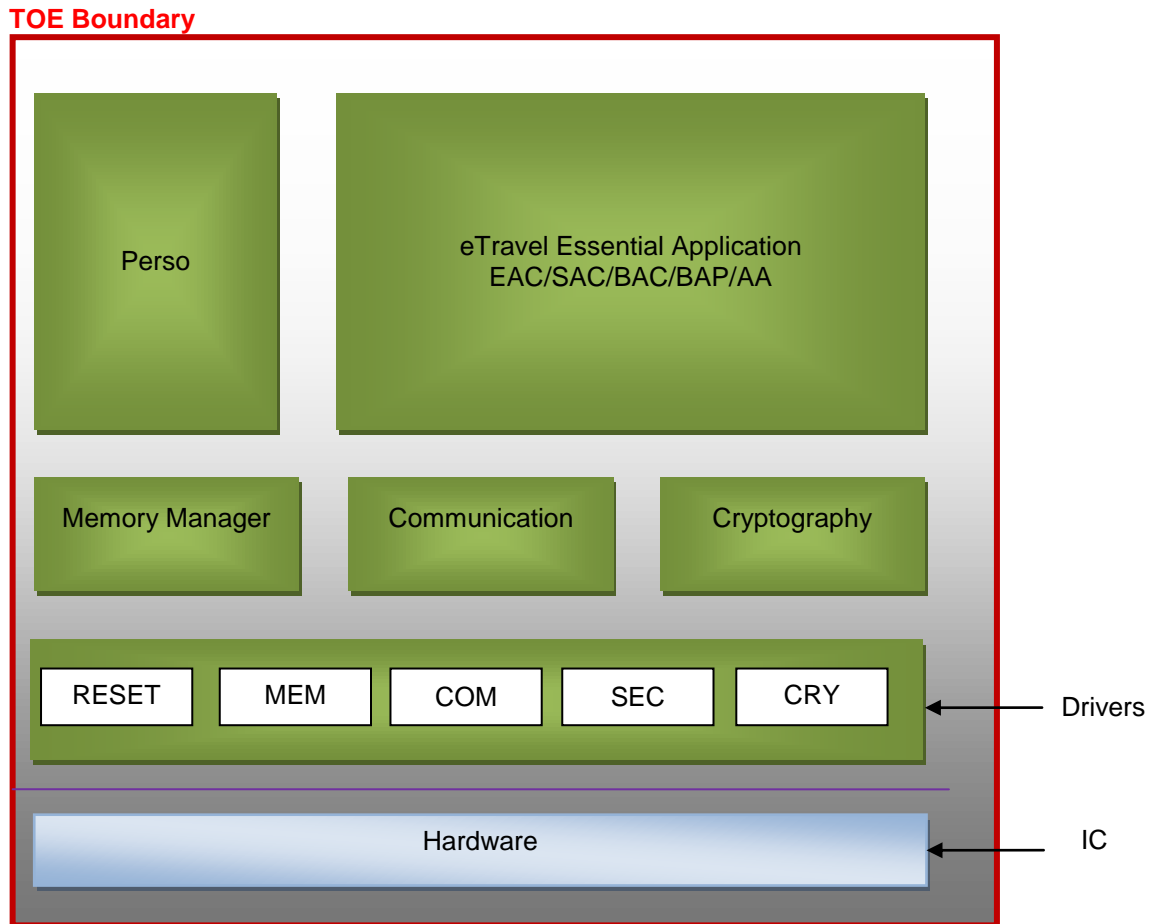


	Reference <b>D1315456</b>	Release <b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level <b>Public</b>	Pages <b>81</b>


- the guidance documentation of the eTravel Essential 1.0 product:
  - the preparation guide (assurance family AGD-PRE),
  - the operational guide (assurance family AGD-OPE).

The eTravel Essential 1.0 Embedded Software (ES) is implemented in the NVM memory (flash technology) of the chip.

The TOE is delivered to the Personalization Agent with data and guidance documentation in order to perform the personalization of the product. In addition the Personalization Key is delivered from the MRTD Manufacturer to the Personalization Agent or from the Personalization Agent to the MRTD Manufacturer.



**Figure 1: TOE Boundary**

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 1.4.3 TOE usage and security features for operational use

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

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

For this security target the MRTD is viewed as unit of

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

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


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

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

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

This security target addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This security target addresses the Chip Authentication Version 1 described in [TR-EAC-1] as an alternative to the Active Authentication stated in [ICAO-9303].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this ST as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

additionally to fulfil the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP-BAC-MRTD]. Due to the fact that [PP-BAC-MRTD] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA\_VAN.3) the MRTD has been evaluated and certified separately according to [ST-BAC], claiming [PP-BAC-MRTD].


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

The security target requires the TOE to implement the Chip Authentication defined in [TR-EAC-1]. The Chip Authentication prevents data traces described in [ICAO-9303], informative appendix 7, A7.3.3. The Chip Authentication is provided by the following steps: (i) the inspection system communicates by means of secure messaging established by Basic Access Control, (ii) the inspection system reads and verifies by means of the Passive Authentication the authenticity of the MRTD's Chip Authentication Public Key using the Document Security Object, (iii) the inspection system generates an ephemeral key pair, (iv) the TOE and the inspection system agree on two session keys for secure messaging in ENC\_MAC mode according to the Diffie-Hellman Primitive and (v) the inspection system verifies by means of received message authentication codes whether the MRTD's chip was able or not to run this protocol properly (i.e. the TOE proves to be in possession of the Chip Authentication Private Key corresponding to the Chip Authentication Public Key used for derivation of the session keys). The Chip Authentication requires collaboration of the TOE and the TOE environment.

The security target requires the TOE to implement the Extended Access Control as defined in [TR-EAC-1]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the MRTD's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organization through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organization authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates.

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

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 1.4.4 Toe Life-cycle

### 1.4.4.1 *Four phases*

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

#### Phase 1 “Development”:

(Step1)

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

(Step2)

The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the MRTD application and the guidance documentation associated.

#### Phase 2 “Manufacturing”:

(Step3)

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

If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

(Step4)

The MRTD manufacturer initializes the IC/inlay by loading the MRTD application in the IC flash memory.

(Step5)

The MRTD manufacturer (i) creates the MRTD application and (ii) equips MRTD’s chips with pre-personalization Data.


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

#### Phase 3 “Personalization of the MRTD”:

(Step6)

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

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

	Reference <b>D1315456</b>	Release <b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level <b>Public</b>	Pages <b>81</b>

Phase 4 “Operational Use”

(Step7)

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

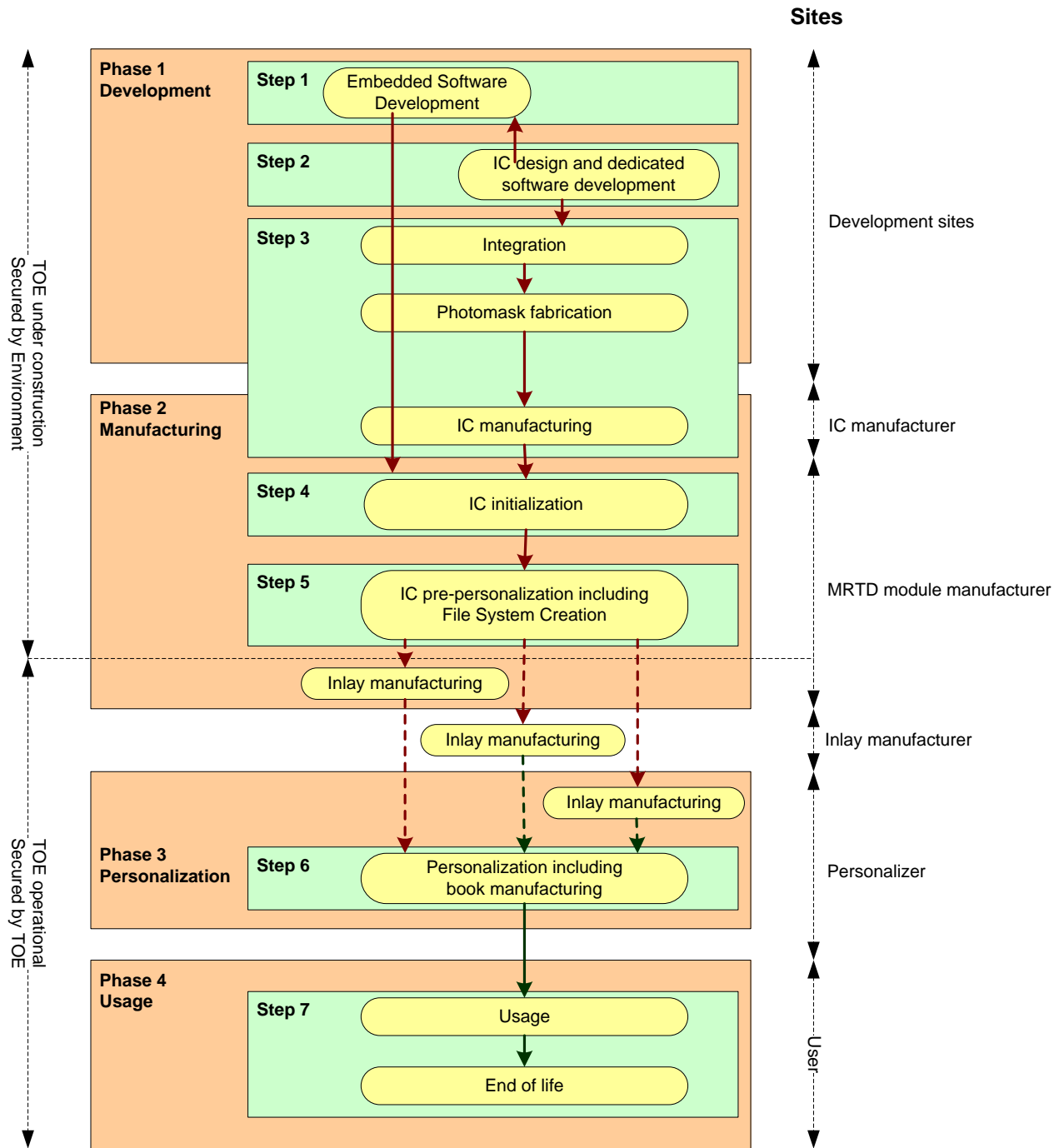
*Application note: In this ST, the role of the Personalization Agents is strictly limited to the phase 3 Personalization. In the phase 4 Operational Use updating and addition of the data groups of the MRTD application is forbidden.*

1.4.4.2 Actors

Actors	Identification
Integrated Circuit (IC) Developer	IFX
Embedded Software Developer	Gemalto
Integrated Circuit (IC) Manufacturer	IFX
Module manufacturer	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 1: Identification of the actors**

1.4.4.3 Init on module at Gemalto site

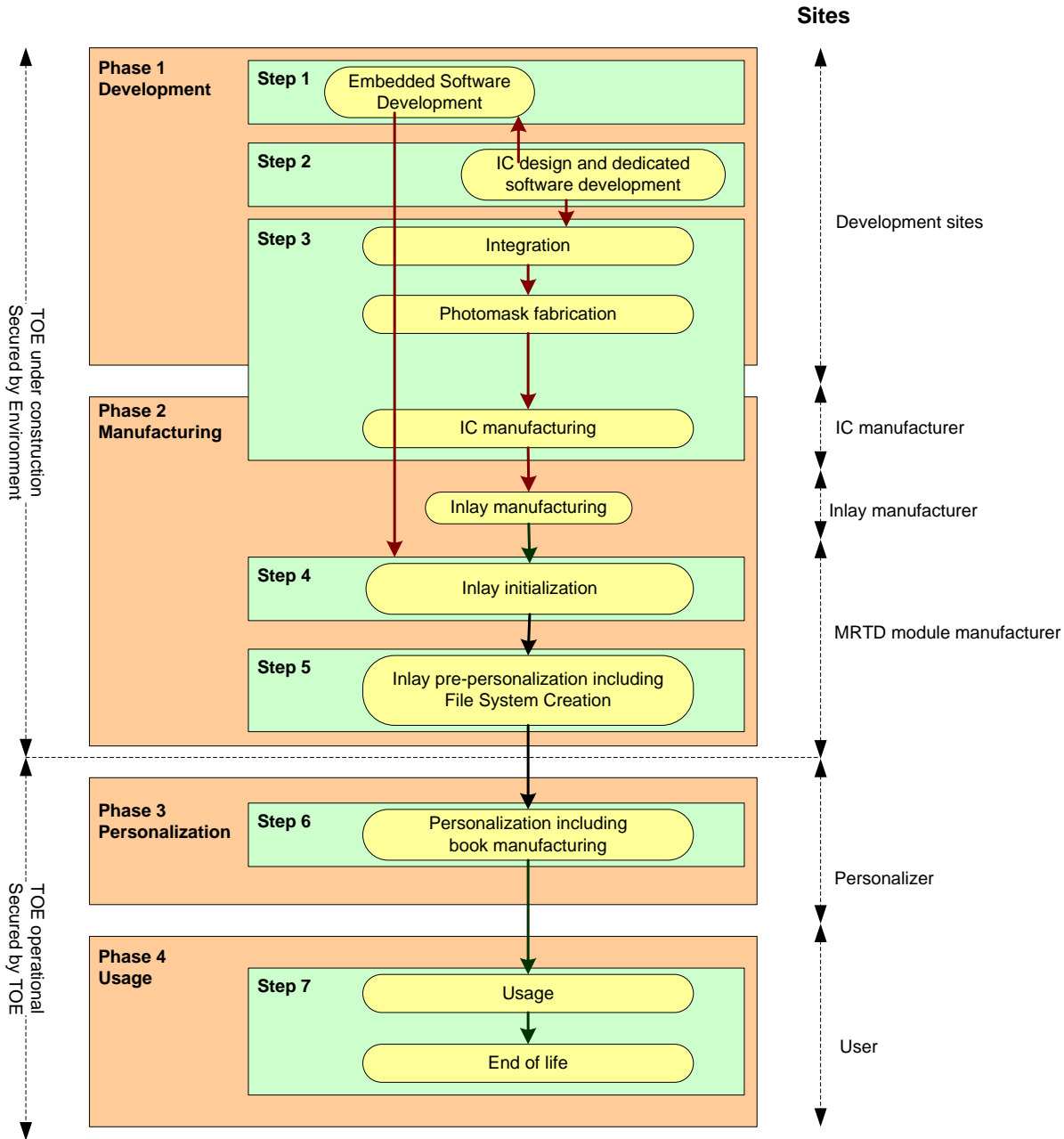


**Figure 2 : LC1: Init on module at Gemalto site**

LC1 describes the standard Life Cycle. The IC is manufactured at the founder site. It is then shipped to Gemalto site where it is initialized (OS loading) and pre-personalized. The transformation of wafers into modules can be performed either at the founder site or at Gemalto site. The modules are then shipped to the Personalizer or to the Inlay manufacturer. In the latter case, the Inlay manufacturer ships the inlays to the Personalizer

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

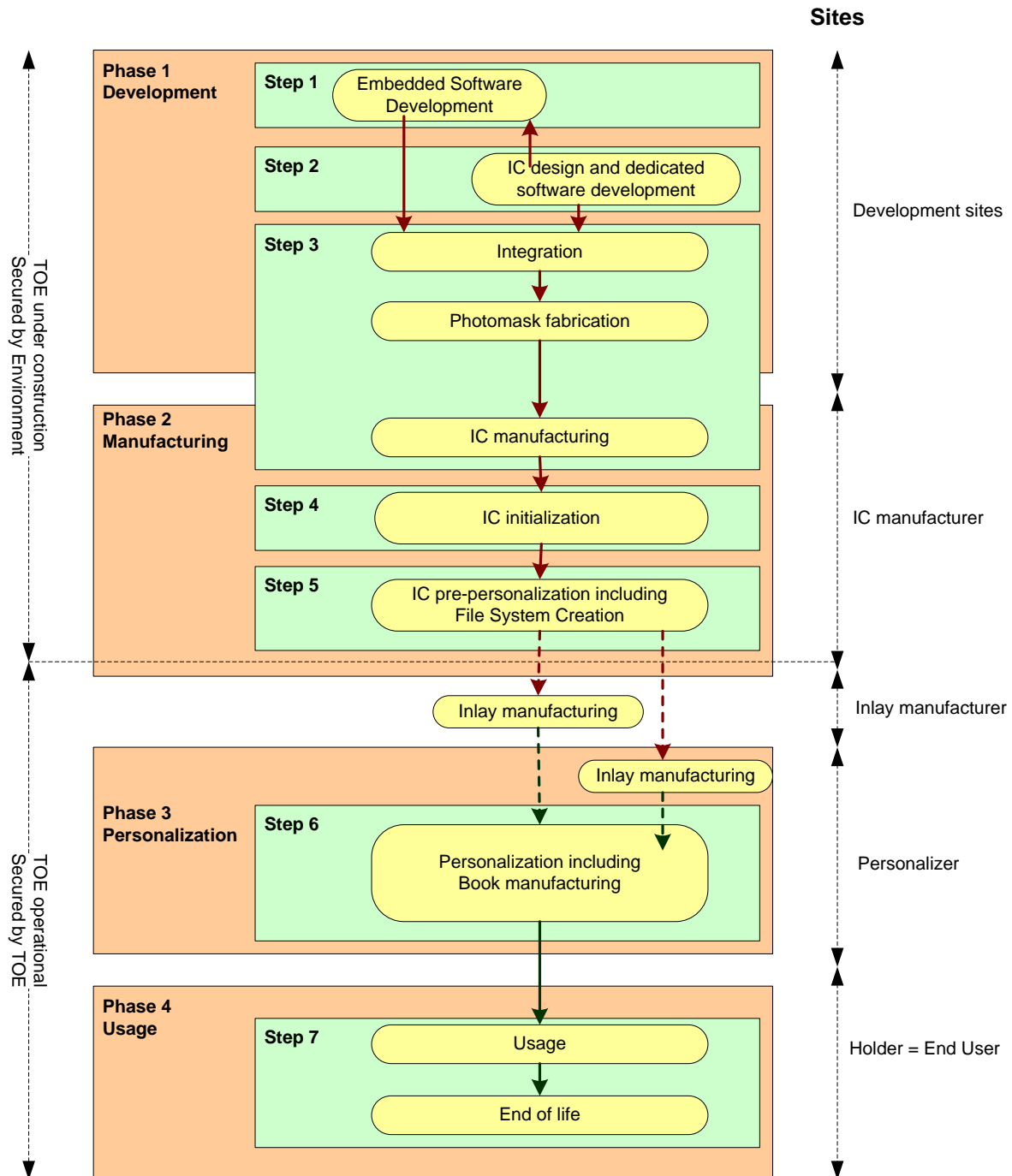
**1.4.4.4 *Init on inlay at Gemalto site***



**Figure 3: LC2: Init on inlay at Gemalto site**

LC2 is another alternative to LC1. LC2 describes the Life Cycle when Gemalto wishes to receive inlays instead of modules. In this case, the founder ships the module to the Inlay manufacturer.

1.4.4.5 Init on wafer (die) at founder site




**Figure 4: LC3 Init on wafer (die) at founder site**

LC3 is an alternative to LC1 and used when the wafers are directly shipped from the founder to the customer, module or inlay manufacturer.

This specific Life Cycle requires initialization(OS loading) and pre-personalization of the chip at the founder site. An initial pre-personalized file system is created and then completed by the personalizer (customer).

During the shipment from the founder to the Personalizer, each die is protected with a diversified key.




	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

---

#### **1.4.5 Non-TOE hardware/software/firmware required by the TOE**

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 2. CONFORMANCE CLAIMS

### 2.1 CC CONFORMANCE CLAIM

This security target claims conformance to

- [CC-1]
- [CC-2]
- [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant.

The

- [CEM] has to be taken into account.

### 2.2 PP CLAIM,

The eTravel Essential 1.0 EAC on BAC security target claims strict conformance to the Protection Profile [PP-MRTD-EAC].

The eTravel Essential 1.0 EAC on BAC security target is a composite security target, including the IC security target [ST-IC]. However the security problem definition, the objectives, and the SFR of the IC are not described in this document.

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

The eTravel Essential 1.0 SAC security target claims strict conformance to [PP-MRTD-SAC].


The eTravel Essential 1.0 BAC security target claims strict conformance to [PP-MRTD-BAC].

### 2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL5 augmented with ALC\_DVS.2 and AVA\_VAN.5 defined in CC part 3 [CC-3].

### 2.4 CONFORMANCE STATEMENT

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 3. SECURITY PROBLEM DEFINITION

#### 3.1 INTRODUCTION

##### 3.1.1 Assets

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

##### Logical MRTD sensitive User Data

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

Application note: Due to interoperability reasons the 'ICAO Doc 9303' [ICAO-9303] requires that Basic Inspection Systems must have access to logical MRTD data DG1, DG2, DG5 to DG16. As the BAC mechanisms may not resist attacks with high attack potential, security of other Data Groups of the logical MRTD are covered by another ST (cf. [ST-BAC]).

A sensitive asset is the following more general one.

##### Authenticity of the MRTD's chip

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

##### 3.1.2 Subjects

This protection profile 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.

##### Personalization Agent


The agent is acting on behalf of the issuing State or Organization to personalize the MRTD for the holder by some or all of the following activities: (i) establishing the identity of the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s), (iii) writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (v) signing the Document Security Object defined in [ICAO-9303].

##### Country Verifying Certification Authority

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

##### Document Verifier

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### Terminal

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

#### Inspection system (IS)

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

### MRTD Holder

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

### Traveler

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

### Attacker

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

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

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

## 3.2 ASSUMPTIONS

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


### A.MRTD\_Manufact MRTD manufacturing on steps 4 to 6

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

### A.MRTD\_Delivery MRTD delivery during steps 4 to 6

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

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

#### **A.Pers\_Agent Personalization of the MRTD's chip**

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

#### **A.Insp\_Sys Inspection Systems for global interoperability**

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


The General Inspection System in addition to the Basic Inspection System implements the Chip Authentication Mechanism. The General Inspection System verifies the authenticity of the MRTD's chip during inspection and establishes secure messaging with keys established by the Chip Authentication Mechanism. The Extended Inspection System in addition to the General Inspection System (i) supports the Terminal Authentication Protocol and (ii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.

#### **A.Signature\_PKI PKI for Passive Authentication**

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

#### **A.Auth\_PKI PKI for Inspection Systems**

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 3.3 THREATS

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

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

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

#### **T.Read\_Sensitive\_Data Read the sensitive biometric reference data**

Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.

The attack T.Read\_Sensitive\_Data is similar to the threat T.Skimming (cf. [PP-MRTD-BAC]) in respect of the attack path (communication interface) and the motivation (to get data stored on the MRTD's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing Document Basic Access Keys) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the MRTD's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical MRTD as well.

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

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


#### **T.Forgery Forgery of data on MRTD's chip**

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

This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip.

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

Asset: authenticity of logical MRTD data,

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### T.Counterfeit MRTD's chip

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine MRTD's chip to be used as part of a counterfeit MRTD. This violates the authenticity of the MRTD's chip used for authentication of a traveler by possession of a MRTD.

The attacker may generate a new data set or extract completely or partially the data from a genuine MRTD's chip and copy them on another appropriate chip to imitate this genuine MRTD's chip.

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

Asset: authenticity of logical MRTD data,

The TOE shall avert the threats as specified below.

### T.Abuse-Func Abuse of Functionality

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

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

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

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

### T.Information\_Leakage Information Leakage from MRTD's chip

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

Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.

This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA).

Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

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


Asset: confidentiality of logical MRTD and TSF data

### T.Phys-Tamper Physical Tampering

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

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

Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

Threat agent: having high attack potential, being in possession of a legitimate MRTD  
 Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

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

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

Threat agent: having high attack potential, being in possession of a legitimate MRTD  
 Asset: confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

**3.4 ORGANIZATIONAL SECURITY POLICIES**

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

**P.BAC-PP Fulfillment of the Basic Access Control Protection Profile.**

The issuing States or Organizations ensures that successfully authenticated Basic Inspection Systems have read access to logical MRTD data DG1, DG2, DG5 to DG16 the 'ICAO Doc 9303' [ICAO-9303] as well as to the data groups Common and Security Data. The MRTD is successfully evaluated and certified in accordance with the 'Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control' [PP-MRTD-BAC] in order to ensure the confidentiality of standard user data and preventing the traceability of the MRTD data.

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

**P.Sensitive\_Data Privacy of sensitive biometric reference data**

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

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

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

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

The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with














	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

Authentication Protocol. Note that reading the less sensitive data directly after Basic Access Control Mechanism is allowed and is not assumed as threat in this PP. But the TOE ensures that reading of sensitive data is possible after successful Chip Authentication and Terminal Authentication Protocol only.

**OE.Ext\_Insp\_Systems Authorization of Extended Inspection Systems**

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

**OE.Activ\_Auth\_Sign Active Authentication of logical MRTD by Signature**

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


**OE.Activ\_Auth\_Verif Verification by Active Authentication**

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







	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

The threats **T.Information\_Leakage** "Information Leakage from MRTD's chip", **T.Phys-Tamper** "Physical Tampering" and **T.Malfunction** "Malfunction due to Environmental Stress" are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives **OT.Prot\_Inf\_Leak** "Protection against Information Leakage", **OT.Prot\_Phys-Tamper** "Protection against Physical Tampering" and **OT.Prot\_Malfunction** "Protection against Malfunctions".

**OT.Active\_Auth\_Proof** "Proof of MRTD's chip authenticity through AA" using a authentication key pair to be generated by the issuing State or Organization. The Public Active Authentication Key has to be written into EF.DG15

The TOE environment will also detect partly forged logical MRTD data by means of digital signature which will be created according to **OE.Active\_Auth\_Sign** "Active Authentication of logical MRTD by Signature" and verified by the inspection system according to **OE.Active\_Auth\_Verif** "Verification by Active Authentication".

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


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

The assumption **A.Pers\_Agent** "Personalization of the MRTD's chip" is covered by the security objective for the TOE environment **OE.Personalization** "Personalization of logical MRTD" including the enrolment, the protection with digital signature and the storage of the MRTD holder personal data.

The examination of the MRTD passport book addressed by the assumption **A.Insp\_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam\_MRTD** "Examination of the MRTD passport book" which requires the inspection system to examine physically the MRTD, the Basic Inspection System to implement the Basic Access Control, and the General Inspection Systems and Extended Inspection Systems to implement and to perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip. The security objectives for the TOE environment **OE.Prot\_Logical\_MRTD** "Protection of data from the logical MRTD" require the Inspection System to protect the logical MRTD data during the transmission and the internal handling.

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

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 4.3.2 Compatibility between objectives of [ST-EAC] and [ST-IC]

### 4.3.2.1 Compatibility between objectives for the TOE

OT.Sens\_Data\_Conf, OT.Chip\_Auth\_Proof, OT.AC\_Pers, and OT.Activ\_Auth\_Proof are specific to [ST-EAC] and they do not conflict with the objectives of [ST-IC].

OT.Data\_Int is included in O.Phys-Manipulation.

OT.Identification is included in O.Identification.

OT.Prot\_Abuse-Func is included in O.Abuse-Func.

OT.Prot\_Inf\_Leak is included in O.Leak-Inherent and O.Leak-Forced

OT.Prot\_Phys-Tamper is included in O.Phys-Manipulation.

OT.Prot\_Malfunction is included in O.Malfunction.

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

### 4.3.2.2 Compatibility between objectives for the environment

OE.MRTD\_Manufact, OE.MRTD\_Delivery, OE.Personalization are included in OE.ProcessSec-IC.


OE.Auth\_Key\_MRTD, OE.Authoriz\_Sens\_Data, OE.BAC\_PP, OE.Exam\_MRTD, OE.Prot\_Logical\_MRTD, OE.Ext\_Insp\_Systems, OE.Pass\_Auth\_Sign, OE.Passive\_Auth\_Verif, OE.Activ\_Auth\_Sign, and OE.Activ\_Auth\_Verif, are specific to [ST-EAC] and they do not conflict with the objectives of [ST-IC].

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

## 4.3.3 Justifications for adding objectives on the environment

### 4.3.3.1 Additions to [PP-MRTD-EAC]

The only additional objectives on the environment are OE.Activ\_Auth\_Sign and OE.Activ\_Auth\_Verif. These objectives request the environment to support Active Authentication. AA is an operation outside [PP-MRTD-EAC]. Therefore the added objectives on the environment do not weaken the TOE.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 5. EXTENDED COMPONENTS DEFINITION

This security target uses components defined as extensions to CC part 2. Some of these components are defined in protection profile [PP-IC-0035]; others are defined in the protection profile [PP-MRTD-EAC].

### 5.1 DEFINITION OF THE FAMILY FAU\_SAS

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

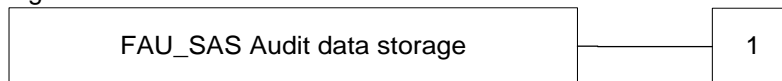
The family "Audit data storage (FAU\_SAS)" is specified as follows.

#### FAU\_SAS Audit data storage

Family behaviour

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

Component levelling



FAU\_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU\_SAS.1  
There are no management activities foreseen.


Audit: FAU\_SAS.1  
There are no actions defined to be auditable.

#### FAU\_SAS.1 Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 5.2 DEFINITION OF THE FAMILY FCS\_RND

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

The family “Generation of random numbers (FCS\_RND)” is specified as follows.

### FCS\_RND Generation of random numbers

#### Family behaviour

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

Component levelling:



FCS\_RND.1                      Generation of random numbers requires that random numbers meet a defined quality metric.

Management:                FCS\_RND.1  
                                    There are no management activities foreseen.


Audit:                         FCS\_RND.1  
                                    There are no actions defined to be auditable.

### FCS\_RND.1 Quality metric for random numbers

Hierarchical to:          No other components

Dependencies:            No dependencies

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 5.3 DEFINITION OF THE FAMILY FIA\_API

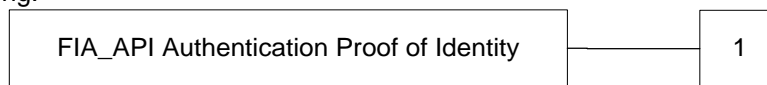
To describe the IT security functional requirements of the TOE a sensitive family (FIA\_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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

#### FIA\_API Authentication Proof of Identity

Family 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 levelling:



FIA\_API.1 Authentication Proof of Identity.


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

Audit: There are no actions defined to be auditable.

#### FIA\_API.1 Authentication Proof of Identity

Hierarchical to: No other components  
Dependencies: No dependencies

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

	Reference <b>D1315456</b>	Release <b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level <b>Public</b>	Pages <b>81</b>

## 5.4 DEFINITION OF THE FAMILY FMT\_LIM

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

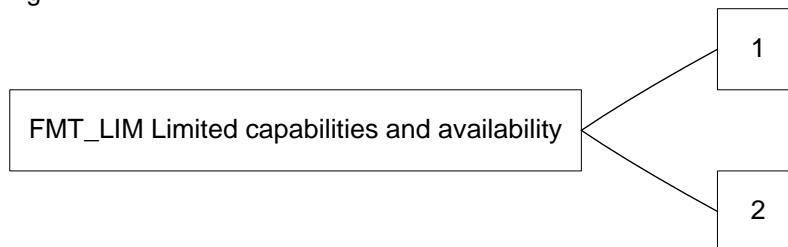
The family “Limited capabilities and availability (FMT\_LIM)” is specified as follows.

### FMT\_LIM Limited capabilities and availability

#### Family 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 levelling:



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

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

Management: FMT\_LIM.1, FMT\_LIM.2  
There are no management activities foreseen.

Audit: FMT\_LIM.1, FMT\_LIM.2  
There are no actions defined to be auditable.


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

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

### FMT\_LIM.1 Limited capabilities

Hierarchical to: No other components  
Dependencies: FMT\_LIM.2 Limited availability.

FMT\_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

with “Limited availability (FMT\_LIM.2)” the following policy is enforced [assignment: *Limited capability and availability policy*].

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

**FMT\_LIM.2 Limited availability**


Hierarchical to: No other components  
 Dependencies: FMT\_LIM.1 Limited capabilities.

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

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

- (i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced
- or conversely
- (ii) the TSF is designed with test and support functionality that is removed from, or disabled in, the product prior to the Operational Use Phase.

The combination of both requirements shall enforce the policy.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 5.5 DEFINITION OF THE FAMILY FPT\_EMS

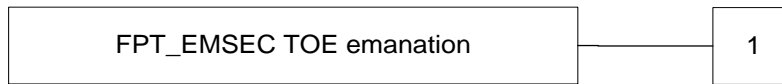
The sensitive family FPT\_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, 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\_EMS)" is specified as follows.

### Family behavior

This family defines requirements to mitigate intelligible emanations.

### Component leveling:



FPT\_EMS.1 TOE emanation has two constituents:

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

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

Management: FPT\_EMS.1  
There are no management activities foreseen.

Audit: FPT\_EMS.1  
There are no actions defined to be auditable.


### FPT\_EMS.1 TOE Emanation

Hierarchical to: No other components  
Dependencies: No dependencies.

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

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



	Reference <b>D1315456</b>	Release <b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level <b>Public</b>	Pages <b>81</b>

## 6. SECURITY REQUIREMENTS

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

Definition of security attributes:


security attribute	values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as domestic Document Verifier after successful CA and TA
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [TR-EAC-1], A.5.1); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [TR-EAC-1], A.5.1)
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR-EAC-1], A.5.1)
	DG3 (Iris) / DG4 (Fingerprint)	Read access to DG3 and DG4: (cf. [TR-EAC-1], A.5.1)

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

Name	Data
Country Verifying Certification Authority Private Key (SKCVCA)	The Country Verifying Certification Authority (CVCA) holds a private key (SKCVCA) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PKCVCA)	The TOE stores the Country Verifying Certification Authority Public Key (PKCVCA) as part of the TSF data to verify the Document Verifier Certificates. The PKCVCA has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying	The Country Verifying Certification Authority Certificate may be a self-

Name	Data
Certification Authority Certificate (CCVCA)	signed certificate or a link certificate (cf. [TR-EAC-1] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PKCVCA) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (CDV)	The Document Verifier Certificate CDV is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PKDV) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (CIS)	The Inspection System Certificate (CIS) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PKIS), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SKICC, PKICC) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 15946.
Chip Authentication Public Key (PKICC)	The Chip Authentication Public Key (PKICC) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Chip Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SKICC)	The Chip Authentication Private Key (SKICC) is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organization signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organization (e.g. a Basic Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organization signs the Document Security Object of the logical MRTD with the Document Signer Private Key and the signature will be verified by a Basic Inspection Systems of the receiving State or Organization with the Document Signer Public Key.
Document Basic Access Keys	The Document Basic Access Key is created by the Personalization Agent, loaded to the TOE, and used for mutual authentication and key agreement for secure messaging between the Basic Inspection System and the MRTD's chip.
BAC Session Keys	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a BIS in result of the Basic Access Control Authentication Protocol.
Chip Session Key	Secure messaging Triple-DES key and Retail-MAC key agreed between the TOE and a GIS in result of the Chip Authentication Protocol.

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE

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

Refinements in this section are in underline font when the SFR's refinement is already present in [PP-MRTD-EAC], and in bold font when the refinement is done in this ST. When the SFR is refined in the [PP-MRTD-EAC] and additionally refined in this ST then the font is bold and underline.

### 6.1.1 Class FAU Security Audit

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

#### FAU\_SAS.1 Audit storage

Hierarchical to: No other components  
 Dependencies: No dependencies

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

### 6.1.2 Class Cryptographic Support (FCS)


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

#### FCS\_CKM.1/CA Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys

Hierarchical to: No other components  
 Dependencies: [FCS\_CKM.2 Cryptographic key distribution or FCS\_COP.1 Cryptographic operation] ]: fulfilled by **FCS\_COP.1/CA\_MAC**  
 FCS\_CKM.4 Cryptographic key destruction: fulfilled by **FCS\_CKM.4**

FCS\_CKM.1.1 /CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [selection: based on the Diffie-Hellman key derivation protocol compliant to [PKCS#3] and [TR-EAC-1], based on an ECDH protocol compliant to [TR-ECC]].

iteration	algorithm	Key size
/TDESsession-DH	<b><u>DH Key Agreement Algorithm - PKCS#3 – 1024, 1280, 1536 and 2048 bits</u></b>	<b><u>112 bits</u></b>
/AESsession-DH	<b><u>DH Key Agreement Algorithm - PKCS#3 – 1024, 1280, 1536 and 2048 bits</u></b>	<b><u>128, 192, and 256 bits</u></b>
/TDESsession-ECDH	<b><u>ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256,</u></b>	<b><u>112 bits</u></b>

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

	<b>320, 384, 512 and 521 bits</b>	
/AESsession-ECDH	<b>ECDH Key Agreement Algorithm - ISO 15946 – 160, 192, 224, 256, 320, 384, 512 and 521 bits</b>	<b>128, 192, and 256 bits</b>

**Table 3: FCS\_CKM.1/CA refinement**

### FCS\_CKM.1/KeyPair Cryptographic key generation for AA and CA Key Pair

Hierarchical to: No other components  
 Dependencies: [FCS\_CKM.2 Cryptographic key distribution or FCS\_COP.1 Cryptographic operation]: fulfilled by **FCS\_COP.1/AA**, **FCS\_COP.1/CA\_MAC** and **FCS\_COP.1/SYM**  
 FCS\_CKM.4 Cryptographic key destruction: not fulfilled, see application note

FCS\_CKM.1.1 /KeyPair The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

iteration	algorithm	Key size	standard
/RSA	<b>RSA CRT Key generation</b>	<b>1024, 1280, 1536 and 2048 bits</b>	<b>none (generation of random numbers and Miller- Rabin primality testing)</b>
/ECC	<b>ECC Key generation</b>	<b>160, 192, 224, 256, 320, 384, 512 and 521 bits</b>	<b>FIPS 186-3 Appendix B.4.1</b>
CA/DH	<b>DH key generation</b>	<b>1024, 1280, 1536 and 2048 bits</b>	ANSI X9.42
CA/ECDH	<b>ECDH Key generation</b>	<b>160, 192, 224, 256, 320, 384, 512 and 521 bits</b>	[IEEE-P1363]

**Table 4: FCS\_CKM.1/AA&CA refinement**

Application notes:


- The dependency of FCS\_CKM1/KeyPair on FCS\_COP.1 is partly fulfilled by FCS\_COP.1/CA\_MAC and FCS\_COP.1/SYM. This dependence is not direct: FCS\_CKM1/KeyPair generates a static key which in turn generate session keys, via FCS\_CKM1/CA. These session keys then use FCS\_COP.1/CA\_MAC and FCS\_COP.1/SYM.
- The dependency of FCS\_CKM1/KeyPair on FCS\_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

### FCS\_CKM.1/PERSO Cryptographic key generation for Session keys

Hierarchical to: No other components  
 Dependencies: [FCS\_CKM.2 Cryptographic key distribution or FCS\_COP.1 Cryptographic operation]: fulfilled by **FCS\_COP.1/PERSO**  
**FCS\_CKM.4** Cryptographic key destruction]: fulfilled by **FCS\_CKM.4**

FCS\_CKM.1.1 /PERSO The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: [*assignment: list of standards*].

iteration	algorithm	Key size	standard
/TDES	<b>TDES ISK key derivation</b>	<b>112 bits</b>	<b>[ICAO-9303] normative appendix 5</b>
/AES	<b>AES ISK key derivation</b>	<b>256 bits</b>	<b>[ICAO-9303] normative appendix 5</b>

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

**Table 5: FCS\_CKM.1/PERSO refinement**

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

**FCS\_CKM.4 Cryptographic key destruction**

Hierarchical to: No other components  
 Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]: fulfilled by, **FCS\_CKM.1/CA**, and **FCS\_CKM.1/PERSO**.

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

Application note: Secure erasing of data is performed by overwriting the data with random numbers.

**FCS\_COP.1/SHA Cryptographic operation – Hash for Key Derivation by MRTD**

Hierarchical to: No other components.  
 Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation] FCS\_CKM.4 Cryptographic key destruction

FCS\_COP.1.1/ SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512** and cryptographic key sizes **none** that meet the following: **FIPS 180-2**.

**FCS\_COP.1/SYM Cryptographic operation – Symmetric Encryption / Decryption**

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]: fulfilled by **FCS\_CKM.1/CA** FCS\_CKM.4 Cryptographic key destruction: fulfilled by **FCS\_CKM.4**.


FCS\_COP.1.1 /SYM The TSF shall perform secure messaging – encryption and decryption in accordance with a specified cryptographic algorithm **Table 6: algorithm** and cryptographic key sizes **Table 6: Key size** that meet the following: **Table 6: list of standards**.

iteration	algorithm	Key size	List of standards
/ENC_TDES	<b>TDES in CBC mode</b>	<b>112 bits</b>	TR-03110
/ENC_AES	<b>AES in CBC mode</b>	<b>128, 192, 256</b>	<b><u>ISO 10116</u></b>

**Table 6: FCS\_COP.1/SYM refinements**

**FCS\_COP.1/SIG\_VER Cryptographic operation – Signature verification by MRTD**

Hierarchical to: No other components.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]: fulfilled by **FCS\_CKM.1/CA**  
FCS\_CKM.4 Cryptographic key destruction: fulfilled by **FCS\_CKM.4**.

FCS\_COP.1.1 /SIG\_VER The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm **Table 7: algorithm** and cryptographic key sizes **Table 7: Key size** that meet the following: **Table 7: list of standards**.

iteration	algorithm	Key size	List of standards
/RSA_VER	<b>RSA (STD)</b>	<b>1024, 1280, 1536, 2048</b>	<b>[ISO9796-2] RSA SHA PKCS#1 RSA SHA PKCS#1 PSS</b>
/ECC_VER	<b>ECC</b>	<b>160, 192, 224, 256, 320, 384, 512, 521</b>	<b>[TR-ECC] ECDSA SHA</b>

**Table 7: FCS\_COP.1/SIG\_VER refinements**

#### **FCS\_COP.1/CA\_MAC Cryptographic operation – MAC**

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]: fulfilled by **FCS\_CKM.1/CA**  
FCS\_CKM.4 Cryptographic key destruction: fulfilled by **FCS\_CKM.4**.

FCS\_COP.1.1 /CA\_MAC The TSF shall perform secure messaging – message authentication code in accordance with a specified cryptographic algorithm **Table 8 algorithm** and cryptographic key sizes **Table 8 Key size** that meet the following: **Table 8 list of standards**.

iteration	algorithm	Key size	List of standards
/MAC_TDES	<b>TDES Retail MAC</b>	<b>112 bits</b>	TR-03110
/MAC_AES	<b>AES CMAC</b>	<b>128, 192, 256</b>	<b>[NIST-800-38B]</b>


**Table 8: FCS\_COP.1/CA\_MAC refinements**

Remark: this SFR is renamed **FCS\_COP.1/CA\_MAC** instead of **FCS\_COP.1/MAC**

#### **FCS\_COP.1/PERSO Cryptographic operation – Symmetric encryption, decryption, and MAC during manufacturing**

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]: fulfilled by **FCS\_CKM.1/PERSO**.  
FCS\_CKM.4 Cryptographic key destruction: fulfilled by **FCS\_CKM.4**.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

FCS\_COP.1.1 /PERSO The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **Triple-DES, AES** and cryptographic key sizes **See table 9**

iteration	algorithm	Key size	List of standards
/ENC_TDES	<b>TDES encryption and decryption</b>	<b>112 bits</b>	<b>[SP 800-67]</b>
/ENC_AES	<b>AES encryption and decryption</b>	<b>128, 192, 256</b>	<b>[FIPS 197]</b>
/MAC_TDES	<b>TDES Retail MAC</b>	<b>112 bits</b>	<b>ISO 9797-1</b>
/MAC_AES	<b>AES CMAC</b>	<b>128, 192, 256</b>	<b>[NIST-800-38B]</b>

**Table 9: FCS\_COP.1/ PERSO refinements**

### FCS\_COP.1/AA Cryptographic operation – Active Authentication

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or FDP\_ITC.2 Import of user data with security attributes, or FCS\_CKM.1 Cryptographic key generation]: fulfilled by **FCS\_CKM.1/KeyPair**  
FCS\_CKM.4 Cryptographic key destruction: not fulfilled, see application note.

FCS\_COP.1.1 /AA The TSF shall perform **digital signature creation** in accordance with a specified cryptographic algorithm **Table 10 algorithm** and cryptographic key sizes **Table 10 Key size** that meet the following: **Table 10 List of standards**.

iteration	algorithm	Key size	List of standards
/AA_RSA	<b>RSA</b>	<b>1024, 1280, 1536, 2048 bits</b>	<b>ISO9796-2</b>
/AA_ECDSA	<b>ECDSA</b>	<b>160, 192, 224, 256, 320, 384, 512 and 521</b>	<b>[TR-ECC]</b>

**Table 10: FCS\_COP.1/AA refinements**

Application note:

- The dependency of FCS\_COP.1/AA on FCS\_CKM.4 is not fulfilled as these are permanent keys used on the card during its life-time.

### FCS\_RND.1 Quality metric for random numbers

Hierarchical to: No other components

Dependencies: No dependencies

FCS\_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet meet **RGS [RGS-B1] and [SP 800-90] with seed entropy at least 128 bits**.

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

### 6.1.3 Class FIA Identification and Authentication

Table 11 provides an overview on the authentication mechanisms used.

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

**Table 11 : Overview on authentication SFR**

Note the Chip Authentication Protocol as defined in this protection profile<sup>19</sup> includes

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

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

The TOE shall meet the requirement "Timing of identification (FIA\_UID.1/MRTD)" as specified below (Common Criteria Part 2).

#### **FIA\_AFL.1/PERSO Authentication failure handling during pre-personalization and personalization phases**

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1 Timing of authentication: fulfilled by **FIA\_UAU.1/PERSO**


FIA\_AFL.1.1 /Perso The TSF shall detect when [**Number in** ] unsuccessful authentication attempts occurs related to **authentication attempts using ISK key**.

FIA\_AFL.1.2 /Perso When the defined number of unsuccessful authentication attempts has been met, the TSF shall [**Actions in** ].

Auth type	Number	Actions
<b>ISK key</b>	<b>3</b>	<b>Block ISK Key.</b>

**Table 12: FIA\_AFL.1/PERSO refinements**



	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### FIA\_UID.1/PERSO Timing of identification

Hierarchical to: No other components.  
 Dependencies: No dependencies.

FIA\_UID.1.1 /PERSO The TSF shall allow  
**1. to establish a communication channel,**  
**2. to carry out the mutual authentication Protocol according to [GP]**  
 on behalf of the user to be performed before the user is identified.

FIA\_UID.1.2 /PERSO The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### FIA\_UID.1/MRTD Timing of identification

Hierarchical to: No other components.  
 Dependencies: No dependencies.

FIA\_UID.1.1/MRTD The TSF shall allow  
 1. to establish a communication channel,  
 2. to read the Initialization Data if it is not disabled by TSF according to FMT\_MTD.1/INI\_DIS  
 3. to carry out the Chip Authentication Protocol  
 on behalf of the user to be performed before the user is identified.

FIA\_UID.1.2//MRTD The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

The TOE shall meet the requirement “Timing of authentication (FIA\_UAU.1)” as specified below (Common Criteria Part 2).

### FIA\_UAU.1/PERSO Timing of authentication


Hierarchical to: No other components.  
 Dependencies: FIA\_UID.1 Timing of identification: fulfilled by **FIA\_UID.1/PERSO**

FIA\_UAU.1.1 /PERSO The TSF shall allow  
**1. to establish a communication channel,**  
**2. to carry out the mutual authentication Protocol according to [GP]**  
 on behalf of the user to be performed before the user is authenticated.


FIA\_UAU.1.2 /PERSO The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### Application note:

- FIA\_AFL.1/PERSO and FIA\_UID.1/PERSO are extensions to [PP-MRTD-EAC], in order to deal with identification and authentication in pre-personalisation and personalisation phases.

	Reference <b>D1315456</b>	Release <b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level <b>Public</b>	Pages <b>81</b>

---

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### FIA\_UAU.1/MRTD Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA\_UID.1 Timing of identification: fulfilled by **FIA\_UID.1/MRTD**

FIA\_UAU.1.1/MRTD TD The TSF shall allow

1. to establish a communication channel,
2. to read the Initialization Data if it is not disabled by TSF according to FMT\_MTD.1/INI\_DIS
3. to identify themselves by selection of the authentication key
4. to carry out the Chip Authentication Protocol

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

FIA\_UAU.1.2/MRTD TD The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

The TOE shall meet the requirements of “Single-use authentication mechanisms (FIA\_UAU.4)” as specified below (Common Criteria Part 2).

### FIA\_UAU.4 Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components

Dependencies: No dependencies

FIA\_UAU.4.1 The TSF shall prevent reuse of authentication data related to

1. Terminal authenticate protocol,
2. Authentication Mechanism based on Triple-DES, AES

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

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA\_UAU.5)” as specified below (Common Criteria Part 2).

### FIA\_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies


FIA\_UAU.5.1 The TSF shall provide

1. Terminal Authentication Protocol,
2. Secure messaging in MAC-ENC mode,
3. Symmetric Authentication Mechanism based on Triple-DES, AES

to support user authentication.

FIA\_UAU.5.2 The TSF shall authenticate any user’s claimed identity according to the following rules:

1. **TOE accepts the authentication attempt as Pre-personalization Agent by the**

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

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

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

#### **FIA\_UAU.6 Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to: No other components  
 Dependencies: No dependencies

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

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

#### **FIA\_API.1/CA Authentication Proof of Identity – Chip Authentication**

Hierarchical to: No other components  
 Dependencies: No dependencies

FIA\_API.1.1/CA The TSF shall provide a Chip Authentication Protocol v.1 according to [TR-EAC-1] to prove the identity of the TOE.


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

#### **FIA\_API.1/AA Authentication Proof of Identity – Active Authentication**

Hierarchical to: No other components  
 Dependencies: No dependencies

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

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 6.1.4 Class FDP User Data Protection

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

#### FDP\_ACC.1 Subset access control

Hierarchical to: No other components

Dependencies: FDP\_ACF.1 Security attribute based access control: fulfilled by **FDP\_ACF.1**

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

The TOE shall meet the requirement “Security attribute based access control (FDP\_ACF.1)” as specified below (Common Criteria Part 2).

#### FDP\_ACF.1 Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP\_ACC.1 Subset access control; fulfilled by **FDP\_ACC.1**, FMT\_MSA.3  
Static attribute initialization

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


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

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

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

FDP\_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP\_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

rules:

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

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

The TOE shall meet the requirement “Basic data exchange confidentiality (FDP\_UCT.1)” as specified below (Common Criteria Part 2).

**FDP\_UCT.1 Basic data exchange confidentiality**

Hierarchical to: No other components  
 Dependencies: [FTP\_ITC.1 Inter-TSF trusted channel, or  
 FTP\_TRP.1 Trusted path]

[FDP\_ACC.1 Subset access control, or  
 FDP\_IFC.1 Subset information flow control]

FDP\_UCT.1.1 The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure **after Chip Authentication..**

The TOE shall meet the requirement “Data exchange integrity (FDP\_UIT.1)” as specified below (Common Criteria Part 2).

**FDP\_UIT.1 Data exchange integrity**


Hierarchical to: No other components  
 Dependencies:

[FDP\_ACC.1 Subset access control, or  
 FDP\_IFC.1 Subset information flow control]

[FTP\_ITC.1 Inter-TSF trusted channel, or  
 FTP\_TRP.1 Trusted path]

FDP\_UIT.1.1 The TSF shall enforce the Access Control SFP to 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 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay has occurred **after Chip Authentication.**

	Reference <b>D1315456</b>	Release <b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level <b>Public</b>	Pages <b>81</b>

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

### 6.1.5 Class FMT Security Management

**Application note:** The SFR FMT\_SMF.1 and FMT\_SMR.1 provide basic requirements to the management of the TSF data.

The TOE shall meet the requirement “Specification of Management Functions (FMT\_SMF.1)” as specified below (Common Criteria Part 2).

#### FMT\_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT\_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-personalization,
3. Personalization.

The TOE shall meet the requirement “Security roles (FMT\_SMR.1)” as specified below (Common Criteria Part 2).

#### FMT\_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA\_UID.1 Timing of identification fulfilled by **FIA\_UID.1**

FMT\_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifying Certification Authority,
4. Document Verifier,
5. domestic Extended Inspection System,
6. foreign Extended Inspection System.


FMT\_SMR.1.2 The TSF shall be able to associate users with roles.

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

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

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

#### FMT\_LIM.1 Limited capabilities

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

Hierarchical to: No other components  
 Dependencies: FMT\_LIM.2 Limited capabilities: fulfilled by **FMT\_LIM.2**.

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

1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

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

**FMT\_LIM.2 Limited availability**

Hierarchical to: No other components  
 Dependencies: FMT\_LIM.1 Limited capabilities: fulfilled by **FMT\_LIM.1**.

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

1. User Data to be manipulated,
2. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed,
3. TSF data to be disclosed or manipulated
4. software to be reconstructed and
5. substantial information about construction of TSF to be gathered which may enable other attacks.

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

**Application note:** The following SFR are iterations of the component Management of TSF data (FMT\_MTD.1). The TSF data include but are not limited to those identified below.


The TOE shall meet the requirement “Management of TSF data (FMT\_MTD.1)” as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

**FMT\_MTD.1/INI\_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data**

Hierarchical to: No other components  
 Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
 FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**


FMT\_MTD.1.1/ INI\_ENA The TSF shall restrict the ability to write the Initialization Data and Pre-personalization Data to the Manufacturer.



	Reference <b>D1315456</b>	Release <b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level <b>Public</b>	Pages <b>81</b>

---

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### **FMT\_MTD.1/INI\_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data**

Hierarchical to: No other components  
 Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
 FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

FMT\_MTD.1.1/INI\_DIS The TSF shall restrict the ability to disable read access for users to the Initialization Data to the Personalization Agent.

### **FMT\_MTD.1/CVCA\_INI Management of TSF data – Initialization of CVCA Certificate and Current Date**

Hierarchical to: No other components  
 Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
 FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

FMT\_MTD.1.1/CVCA\_INI The TSF shall restrict the ability to write the  
 1. initial Country Verifying Certification Authority Public Key,  
 2. initial Country Verifying Certification Authority Certificate,  
 3. initial Current Date  
 to **the Personalization Agent.**

### **FMT\_MTD.1/CVCA\_UPD Management of TSF data – Country Verifying Certification Authority**


Hierarchical to: No other components  
 Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
 FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

FMT\_MTD.1.1/CVCA\_UPD The TSF shall restrict the ability to update the  
 1. Country Verifying Certification Authority Public Key,  
 2. Country Verifying Certification Authority Certificate  
 to Country Verifying Certification Authority.

### **FMT\_MTD.1/DATE Management of TSF data – Current date**

Hierarchical to: No other components  
 Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
 FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

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

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### FMT\_MTD.1/ KEY\_WRITE Management of TSF data – Key Write

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

FMT\_MTD.1.1 / KEY\_WRITE The TSF shall restrict the ability to write the Document Basic Access Keys to the Personalisation Agent.

### FMT\_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key

Hierarchical to: No other components

Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

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

### FMT\_MTD.1/AAK Management of TSF data – Active Authentication Private Key

Hierarchical to: No other components

Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

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

### FMT\_MTD.1/KEY\_READ Management of TSF data – Key Read

Hierarchical to: No other components

Dependencies: FMT\_SMF.1 Specification of management functions: fulfilled by **FMT\_SMF.1**  
FMT\_SMR.1 Security roles: fulfilled by **FMT\_SMR.1**

FMT\_MTD.1.1 / KEY\_READ The TSF shall restrict the ability to read the

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

to none.


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

### FMT\_MTD.3 Secure TSF data

Hierarchical to: No other components

Dependencies: FMT\_MTD.1 Management of TSF data: fulfilled by **FMT\_MTD.1/CVCA\_INI**,  
**FMT\_MTD.1/CVCA\_UPD**,

FMT\_MTD.3.1 The TSF shall ensure that only secure values of the certificate chain are accepted for TSF

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

data of the Terminal Authentication Protocol and the Access Control.


**Refinement: The certificate chain is valid if and only if**

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

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

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

**Application note:** The Terminal Authentication is used for Extended Inspection System as required by FIA\_UAU.4 and FIA\_UAU.5. The Terminal Authorization is used as TSF data for access control required by FDP\_ACF.1.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 6.1.6 Class FPT Protection of the Security Functions

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

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

#### FPT\_EMS.1 TOE Emanation

Hierarchical to: No other components  
 Dependencies: No dependencies.

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

FPT\_EMS.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to Personalization Agent Key(s) and Chip Authentication Private Key and Active Authentication Key, EF.DG3 and EF.DG4.

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

The TOE shall meet the requirement “Failure with preservation of secure state (FPT\_FLS.1)” as specified below (Common Criteria Part 2).

#### FPT\_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components  
 Dependencies: No dependencies.

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


1. Exposure out-of-range operating conditions where therefore a malfunction could occurs.
2. failure detected by TSF according to FPT\_TST.1.

The TOE shall meet the requirement “TSF testing (FPT\_TST.1)” as specified below (Common Criteria Part 2).

#### FPT\_TST.1 TSF testing

Hierarchical to: No other components  
 Dependencies: No dependencies.

FPT\_TST.1.1 The TSF shall run a suite of self tests **Conditions under which self test should occur** to demonstrate the correct operation of the TSF.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

FPT\_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT\_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

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

**Table 13: FPT\_TST refinements**

The TOE shall meet the requirement “Resistance to physical attack (FPT\_PHP.3)” as specified below (Common Criteria Part 2).

### **FPT\_PHP.3 Resistance to physical attack**

Hierarchical to: No other components

Dependencies: No dependencies.

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

**Application note:** The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

## **6.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE**

The SAR for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the following components: ALC\_DVS.2 and AVA\_VAN.5.

**Application note :** The TOE shall protect the assets against high attack potential under the assumption that 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.Prot\_Logical\_MRTD). Otherwise the confidentiality of the standard data shall be protected against attacker with at least Enhanced-Basic attack potential (AVA\_VAN.3).

### 6.3 SECURITY REQUIREMENTS RATIONALE

#### 6.3.1 Security Functional Requirements Rationale

The rationale in this paragraph comes from [PP-MRTD-EAC] §6.3.1. Additions due to Active Authentication and secure messaging in personalisation are shaded.

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunfion	OT.Activ_Auth_Proof
FAU_SAS.1				X						
FCS.CKM.1/CA	X	X	X		X					
FCS_CKM.1/KeyPair					X					X
FCS_CKM.1/PERSO		X	X							
FCS_CKM.4	X	X	X							
FCS_COP.1/SHA	X	X	X		X					
FCS_COP.1/SYM	X	X	X		X					
FCS_COP.1/SIG_VER	X		X							
FCS_COP.1/CA_MAC	X	X	X		X					
FCS_COP.1/PERSO		X	X							
FCS_COP.1/AA										X
FCS_RND.1	X		X							
FIA_AFL.1/PERSO		X	X							
FIA_UID.1/PERSO		X	X							
FIA_UAU.1/PERSO		X	X							
FIA_UID.1/MRTD	X	X	X							
FIA_UAU.1/MRTD	X	X	X							
FIA_UAU.4	X	X	X							
FIA_UAU.5	X	X	X							
FIA.UAU.6	X	X	X							
FIA_API.1/CA					X					
FIA_API.1/AA										X
FDP_ACC.1	X	X	X							
FDP_ACF.1	X	X	X							
FDP_UCT.1			X							
FDP_UIT.1		X								
FMT_SMF.1	X	X								
FMT_SMR.1	X	X								
FMT_LIM.1						X				
FMT_LIM.2						X				
FMT_MTD.1/INI_ENA				X						
FMT_MTD.1/INI_DIS				X						
FMT_MTD.1/CVCA_INI			X							
FMT_MTD.1/CVCA_UPD			X							
FMT_MTD.1/DATE			X							
FMT_MTD.1/ KEY_WRITE	X									

	OT.AC_Pers	OT.Data_Int	OT.Sens_Data_Conf	OT.Identification	OT.Chip_Auth_Proof	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunfunction	OT.Activ_Auth_Proof
FMT_MTD.1/AAK		X	X		X					
FMT_MTD.1/AAK										X
FMT_MTD.1/KEY_READ	X	X	X		X					X
FMT_MTD.3			X							
FPT_EMS.1	X						X			
FPT_FLS.1							X		X	
FPT_TST.1							X		X	
FPT_PHP.3							X	X		

**Table 14: Security functional requirement rationale**


The security objective **OT.AC\_Pers** “Access Control for Personalization of logical MRTD” addresses the access control of the writing the logical MRTD. The write access to the logical MRTD data are defined by the SFR FIA\_UID.1/MRTD, FIA\_UAU.1/MRTD, FDP\_ACC.1 and FDP\_ACF.1 in the same way: only the successfully authenticated Personalization Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical MRTD only once. The SFR FMT\_SMR.1 lists the roles (including Personalization Agent) and the SFR FMT\_SMF.1 lists the TSF management functions (including Personalization). The Personalization Agent handles the Document Basic Access Keys according to the SFR FMT\_MTD.1/KEY\_WRITE as authentication reference data for Basic Access Control.

The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA\_UAU.4 and FIA\_UAU.5. If the Personalization Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol (after Chip Authentication) with the Personalization Agent Keys the TOE will use TSF according to the FCS\_RND.1 (for the generation of the challenge), FCS\_CKM.1, FCS\_COP.1/SHA (for the derivation of the new session keys after Chip Authentication), and FCS\_COP.1/SYM and FCS\_COP.1/ CA\_MAC (for the ENC\_MAC\_Mode secure messaging), FCS\_COP.1/SIG\_VER (as part of the Terminal Authentication Protocol) and FIA\_UAU.6 (for the re-authentication). If the Personalization Terminal wants to authenticate itself to the TOE by means of the Symmetric Authentication Mechanism with Personalization Agent Key the TOE will use TSF according to the FCS\_RND.1 (for the generation of the challenge) and FCS\_COP.1/SYM (to verify the authentication attempt). The session keys are destroyed according to FCS\_CKM.4 after use.

The SFR FMT\_MTD.1/KEY\_READ prevents read access to the secret key of the Personalization Agent Keys and ensures together with the SFR FPT\_EMS.1 the confidentiality of these keys.

The security objective **OT.Data\_Int** “Integrity of personal data” requires the TOE to protect the integrity of the logical MRTD stored on the MRTD’s chip against physical manipulation and unauthorized writing. The write access to the logical MRTD data is defined by the SFR FDP\_ACC.1 and FDP\_ACF.1 in the same way: only the Personalization Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical MRTD (FDP\_ACF.1.2, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical MRTD (cf. FDP\_ACF.1.4). The Personalization Agent must identify and authenticate themselves according to FIA\_UID.1/MRTD and FIA\_UAU.1/MRTD



	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

before accessing these data. The SFR FMT\_SMR.1 lists the roles and the SFR FMT\_SMF.1 lists the TSF management functions.

The TOE supports the inspection system detect any modification of the transmitted logical MRTD data after Chip Authentication. The authentication of the terminal as Personalization Agent shall be performed by TSF according to SRF FIA\_UAU.4, FIA\_UAU.5 and FIA\_UAU.6. The SFR FIA\_UAU.6 and FDP\_UIT.1 requires the integrity protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS\_CKM.1 (for the generation of shared secret), FCS\_COP.1/SHA (for the derivation of the new session keys), and FCS\_COP.1/SYM and FCS\_COP.1/CA\_MAC for the ENC\_MAC\_Mode secure messaging. The session keys are destroyed according to FCS\_CKM.4 after use.

The SFR FMT\_MTD.1/CAPK and FMT\_MTD.1/KEY\_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

In pre-personalisation, the SFR FCS\_CKM.1/PERSO and FCS\_COP.1/PERSO ensure the authenticity of data transfers after successful authentication of the pre-personalisation agent according to FIA\_UID.1/PERSO and FIA\_UAU.1/PERSO, with the support of FIA\_AFL.1/PERSO.

The security objective **OT.Sense\_Data\_Conf** “Confidentiality of sensitive biometric reference data” is enforced by the Access Control SFP defined in FDP\_ACC.1 and FDP\_ACF.1 allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a validly verifiable certificate according FCS\_COP.1/SIG\_VER.

The SFR FIA\_UID.1/MRTD and FIA\_UAU.1/MRTD requires the identification and authentication of the inspection systems. The SFR FIA\_UAU.5 requires the successful Chip Authentication (CA) before any authentication attempt as Extended Inspection System. During the protected communication following the CA the reuse of authentication data is prevented by FIA\_UAU.4. The SFR FIA\_UAU.6 and FDP\_UCT.1 requires the confidentiality protection of the transmitted data after chip authentication by means of secure messaging implemented by the cryptographic functions according to FCS\_RND.1 (for the generation of the terminal authentication challenge), FCS\_CKM.1 (for the generation of shared secret), FCS\_COP.1/SHA (for the derivation of the new session keys), and FCS\_COP.1/SYM and FCS\_COP.1/CA\_MAC for the ENC\_MAC\_Mode secure messaging. The session keys are destroyed according to FCS\_CKM.4 after use. The SFR FMT\_MTD.1/CAPK and FMT\_MTD.1/KEY\_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.


In pre-personalisation, the SFR FCS\_CKM.1/PERSO and FCS\_COP.1/PERSO ensure the confidentiality of data transfers after successful authentication of the pre-personalisation agent according to FIA\_UID.1/PERSO and FIA\_UAU.1/PERSO, with the support of FIA\_AFL.1/PERSO.

To allow a verification of the certificate chain as in FMT\_MTD.3 the CVCA’s public key and certificate as well as the current date are written or update by authorized identified role as of FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD and FMT\_MTD.1/DATE.

The security objective **OT.Identification** “Identification and Authentication of the TOE” address the storage of the IC Identification Data uniquely identifying the MRTD’s chip in its non-volatile memory. This will be ensured by TSF according to SFR FAU\_SAS.1.

The SFR FMT\_MTD.1/INI\_ENA allows only the Manufacturer to write Initialization Data and Pre-personalization Data (including the Personalization Agent key). The SFR FMT\_MTD.1/INI\_DIS allows the Personalization Agent to disable Initialization Data if their usage in the phase 4 “Operational Use” violates the security objective OT.Identification.

The security objective **OT.Chip\_Auth\_Proof** “Proof of MRTD’s chip authenticity” is ensured by the Chip Authentication Protocol provided by FIA\_API.1 proving the identity of the TOE. The Chip Authentication Protocol defined by FCS\_CKM.1 is performed using a TOE internally stored confidential private key as required by FMT\_MTD.1/CAPK and FMT\_MTD.1/KEY\_READ. The Chip Authentication Protocol [26] requires additional TSF according to FCS\_COP.1/SHA (for the derivation

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

of the session keys), FCS\_COP.1/SYM and FCS\_COP.1/CA\_MAC (for the ENC\_MAC\_Mode secure messaging).

The security objective **OT.Prot\_Abuse-Func** “Protection against Abuse of Functionality” is ensured by the SFR FMT\_LIM.1 and FMT\_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.


The security objective **OT.Prot\_Inf\_Leak** “Protection against Information Leakage” requires the TOE to protect confidential TSF data stored and/or processed in the travel document’s chip against disclosure

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

The security objective **OT.Prot\_Phys-Tamper** “Protection against Physical Tampering” is covered by the SFR FPT\_PHP.3.

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


The security objective **OT.Activ\_Auth\_Proof** “Proof of MRTD’s chip authenticity through AA” is covered by FIA\_API.1/AA that proves the identity of the TOE. FCS\_COP.1/AA provides the signature. FMT\_MTD.1/AAK and FMT\_MTD.1/KEY\_READ participate to confidentiality of AA private key.

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

### 6.3.2 Dependency Rationale

The rationale in this paragraph comes from [PP-MRTD-EAC] §6.3.2. Additions due to Active Authentication are shaded.

SFR	Dependencies	Support of the dependencies
FAU_SAS.1	No dependencies	
FCS_CKM.1/CA	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_MAC, FCS_CKM.4
FCS_CKM.1/KeyPair	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/CA_MAC, Not fulfilled, see note 1
FCS_CKM.1/PERSO	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1/PERSO, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/CA, FCS_CKM.1/PERSO
FCS_COP.1/SHA	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	justification 2 for non-satisfied dependencies Fulfilled by FCS_CKM.4
FCS_COP.1/SYM	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA  FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA  FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/CA  FCS_CKM.4
FCS_COP.1/PERSO	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/PERSO  FCS_CKM.4
FCS_COP.1/AA	[FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/KeyPair  Not fulfilled: see note 1
FCS_RND.1	No dependencies	
FIA_AFL.1/PERSO	FIA_UAU.1	FIA_UAU.1/PERSO
FIA_UID.1/PERSO	No dependencies	
FIA_UAU.1/PERSO	FIA_UID.1	FIA_UID.1/PERSO
FIA_UID.1	No dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1/MRTD
FIA_UAU.4	No dependencies	
FIA_UAU.5	No dependencies	
FIA_UAU.6	No dependencies	
FIA_API.1/CA	No dependencies	
FIA_API.1/AA	No dependencies	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, Not fulfilled: see note 3

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

SFR	Dependencies	Support of the dependencies
FDP_UCT.1	[FTP_ITC.1, or FTP_TRP.1], [FDP_IFC.1 or FDP_ACC.1]	justification 4 for non-satisfied dependencies, FDP_ACC.1
FDP_UIT.1	[FTP_ITC.1, or FTP_TRP.1], [FDP_IFC.1 or FDP_ACC.1]	justification 4 for non-satisfied dependencies, FDP_ACC.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MTD.1/INI_ENA	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/INI_DIS	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/DATE	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/ KEY_WRITE	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AAK	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/AAK	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1/KEY_READ	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3	FMT_MTD.1	FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.3	No dependencies	

**Table 15: Security functional requirement dependencies**


Notes:

No. 1: The dependency between FCS\_COP.1/AA and FCS\_CKM.4 is not fulfilled because the key is permanently stored on the card.

No. 2: The hash algorithm required by the SFR FCS\_COP.1/SHA does not need any key material. Therefore neither a key generation (FCS\_CKM.1) nor an import (FDP\_ITC.1/2) is necessary

No. 3: The access control TSF according to FDP\_ACF.1 uses security attributes having been defined during the personalisation and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT\_MSA.1 and FMT\_MSA.3) is necessary here.

No. 4: The SFR FDP\_UCT.1 and FDP\_UIT.1 require the use secure messaging between the

	Reference <b>D1315456</b>	Release <b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level <b>Public</b>	Pages <b>81</b>

MRTD and the GIS. There is no need for the SFR FTP\_ITC.1, e.g. to require this communication channel to be logically distinct from other communication channels since there is only one channel. Since the TOE does not provide a direct human interface a trusted path as required by FTP\_TRP.1 is not applicable here.

### 6.3.3 Security Assurance Requirements Rationale

EAL5 was chosen because it provides a high level of independently assured security in a planned development. It requires a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

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

The selection of the component AVA\_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens\_Data\_Conf and OT.Chip\_Auth\_Proof.

For these additional assurance components, all dependencies are met or exceeded in the EAL5 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
TOE security assurance requirements (only additional to EAL5)		
ALC_DVS.2	no dependencies	-
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.5
	ADV_TDS.3	ADV_TDS.4
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.3

**Table 16: SAR Dependencies**

### 6.3.4 Security Requirements – Mutual support and internal consistency

Cf [PP-MRTD-EAC] §6.3.4

### 6.3.5 Compatibility between SFR of [ST-EAC] and [ST-IC]

**FAU\_SAS.1** of [ST-EAC] is included in FAU\_SAS.1 of [ST-IC].

**FCS\_RND.1**, **FCS\_CKM.1** and **FCS\_COP.1** of [ST-EAC] are supported by **FCS\_CKM.1**, **FCS\_COP.1** of [ST-IC].


**FPT\_EMS.1** and

**FPT\_PHP.3** of [ST-EAC] are included in **FPT\_PHP.3** of [ST-IC].


**FPT\_FLS.1** of [ST-EAC] is included in **FPT\_FLS.1** of [ST-IC].

**FCS\_CKM.4**, **FIA\_AFL.1**, **FIA\_UID.1**, **FIA\_UAU.1**, **FIA\_UAU.4**, **FIA\_UAU.5**, **FIA\_UAU.6**, **FIA\_API.1**, **FDP\_ACC.1**, **FDP\_ACC.1**, **FDP\_UCT.1**, **FDP\_UIT.1**, **FMT\_SMF.1**, **FMT\_SMR.1**, **FMT\_LIM.1**, **FMT\_LIM.2**, all **FMT\_MTD.1**, **FMT\_MTD.3**, **FPT\_TST.1** are specific to [ST-EAC] and they do not conflict with [ST-IC].

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

	Reference <b>D1315456</b>	Release <b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level <b>Public</b>	Pages <b>81</b>

---

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 7. TOE SUMMARY SPECIFICATION

### 7.1 TOE SECURITY FUNCTIONS

TOE Security Functions are provided by the eTravel Essential 1.0 software and by the chip.

#### 7.1.1 TSFs provided by the Etravel Essential 1.0 Software

SF	Description
SF.REL	Protection of data
SF.AC	Access control
SF.SYM_AUTH	Symmetric authentication
SF.SM	Secure messaging
SF.CA	Chip Authentication
SF.TA_CER	Validity of the Certificate Chain
SF.TA_AUT	Terminal Authentication Mechanism
SF.AA	Active Authentication

**Table 17: Security Functions provided by eTravel Essential 1.0 Software**

The SF.REL function provides the protection of data on the TOE. It encompasses: physical protection of the TOE as defined in

- **FPT\_PHP.3, FPT\_EMS.1, FPT\_FLS.1,**
- the test mechanisms as defined in **FPT\_TST.1,**
- protection against misuse of tests as defined in **FMT\_LIM.1** and **FMT\_LIM.2,**

The SF.AC function provides the access control of the TOE. It encompasses:

- the access control by the terminal as defined in **FDP\_ACC.1** and **FDP\_ACF.1,**
- the access control to specific data as defined in **FAU\_SAS.1, FMT\_MTD.1/INI\_ENA, FMT\_MTD.1/INI\_DIS, FMT\_MTD.1/CVCA\_INI, FMT\_MTD.1/CVCA\_UPD, FMT\_MTD.1/DATE, FMT\_MTD.1/KEY\_WRITE, FMT\_MTD.1/CAPK; FMT\_MTD.1/AAK** and **FMT\_MTD.1/KEY\_READ,**
- the role management as defined in **FMT\_SMR.1 ,**
- the management functions linked to the different states of the TOE as defined in **FMT\_SMF.1.**


The SF.SYM\_AUTH function provides the symmetric authentication functions to the TOE. It encompasses:

- the identification and authentication as defined in **FIA\_UID.1/MRTD, FIA\_UAU.1/MRTD FIA\_UAU.4, FIA\_UAU.5**
- the identification and authentication in personalisation phase as defined in **FIA\_AFL.1/PERSO, FIA\_UID.1/PERSO,** and **FIA\_UAU.1/PERSO,**  
The role authentication as requested by **FMT\_SMR.1 .**

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

the secure transfer of data through SM as defined in **FDP\_UCT.1** and

- **FDP\_UIT.1,**
- the cryptographic mechanisms used for the authentication and the SM, as defined in **FCS\_CKM.1/SYM, FCS\_CKM.1/PERSO, FCS\_COP.1/PERSO,** and **FCS\_RND.1.** Some cryptographic mechanisms are used for both authentication and secure messaging. For convenience, they are grouped in this function.
- the erasure of session keys as defined in **FCS\_CKM.4.**

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

The SF.CA function provides the chip Authentication. It encompasses:

- the CA authentication as defined in **FIA\_API.1/CA**, **FIA\_UAU.6**
- the CA cryptographic algorithm as defined in **FCS\_CKM.1/CA**, **FCS\_COP.1/SHA**, and **FCS\_COP.1/CA\_MAC**,
- the generation and input of CA keys, as defined in **FCS\_CKM.1/KeyPair** and **FMT\_MTD.1/CAPK**,
- The role authentication as requested by **FMT\_SMR.1**.

The SF.TA\_CER function provides the validity of the Certificate Chain. It encompasses:

- the initialisation and update of data used for the validation, as defined in **FMT\_MTD.1/CVCA\_INI**, **FMT\_MTD.1/CVCA\_UPD**, **FMT\_MTD.1/DATE**, and **FMT\_MTD.3**.

The SF.TA\_AUT function provides the TA Mechanism. It encompasses:

- the cryptographic mechanisms used for the authentication, as defined in **FCS\_COP.1/SIG\_VER** and **FCS\_COP.1/SHA**,
- The role authentication as requested by **FMT\_SMR.1**.

The SF.AA function provides the active authentication. It encompasses:

- the AA protocol itself as defined in **FIA\_API.1/AA**,
- the AA cryptographic algorithm as defined in **FCS\_COP.1/AA**,
- the generation and input of AA keys, as defined in **FCS\_CKM.1/KeyPair** and **FMT\_MTD.1/AAK**.

### 7.1.2 TSFs provided by the M7794 chip

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

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

**Table 18: Security Functions provided by the M7794 chip**

These SF are described in [ST-IC].



## 8. RATIONALES


### 8.1 TOE SUMMARY SPECIFICATION RATIONALE

#### 8.1.1 TOE security functions rationale

	SF.REL	SF.AC	SF.SYM_AUT	SF.SM	SF.CA	SF.TA_CER	SF.TA_AUT	SF.AA	SF.DPM	SF.PS	SF.PMA	SF.PLA	SF_CS
FAU_SAS.1		X							X				
FCS_CKM.1/CA					X								X
FCS_CKM.1/KeyPair					X		X						X
FCS_CKM.1/PERSO				X									X
FCS_CKM.4				X									
FCS_COP.1/SHA					X	X							
FCS_COP.1/SYM				X									
FCS_COP.1/SIG_VER						X							X
FCS_COP.1/CA_MAC					X								X
FCS_COP.1/PERSO				X									X
FCS_COP.1/AA							X						X
FCS_RND.1				X									X
FIA_AFL.1/PERSO			X										
FIA_UID.1/PERSO			X										
FIA_UAU.1/PERSO			X										
FIA_UID.1/MRTD			X										
FIA_UAU.1/MRTD			X										
FIA_UAU.4			X										
FIA_UAU.5			X										
FIA_UAU.6					X								
FIA_API.1/CA					X								
FIA_API.1/AA							X						
FDP_ACC.1		X											
FDP_ACF.1		X											
FDP_UCT.1				X									
FDP_UIT.1				X									
FMT_SMF.1		X											
FMT_SMR.1		X	X		X	X							
FMT_LIM.1	X								X				
FMT_LIM.2	X								X				
FMT_MTD.1/INI_ENA		X											
FMT_MTD.1/INI_DIS		X											
FMT_MTD.1/CVCA_INI		X				X							
FMT_MTD.1/CVCA_UPD		X				X							
FMT_MTD.1/DATE		X				X							

	SF.REL	SF.AC	SF.SYM_AUT	SF.SM	SF.CA	SF.TA_CER	SF.TA_AUT	SF.AA	SF.DPM	SF.PS	SF.PMA	SF.PLA	SF.CS
FMT_MTD.1/KEY_WRITE		X											
FMT_MTD.1/CAPK		X			X								
FMT_MTD.1/AAK		X					X						
FMT_MTD.1/KEY_READ		X											
FMT_MTD.3						X							
FPT_EMS.1	X									X			
FPT_TST.1	X										X		
FPT_FLS.1	X									X	X	X	
FPT_PHP.3	X									X	X	X	

**Table 19: Rationale table of functional requirements and security functions**

	Reference	<b>D1315456</b>	Release	<b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## 9. GLOSSARY AND ACRONYMS

### Glossary

Term	Definition
<i>Active Authentication</i>	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.
<i>Agreement</i>	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
<i>Application note</i>	Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the evaluation or use of the TOE.
<i>Audit records</i>	Write-only-once non-volatile memory area of the travel document's chip to store the Initialisation Data and Pre-personalisation Data.
<i>Authenticity</i>	Ability to confirm that the travel document itself and the data elements stored in were issued by the travel document Issuer
<i>Basic Access Control (BAC)</i>	Security mechanism defined in [PKI] by which means the travel document's chip proves and the basic inspection system (with BAC) protects their communication by means of secure messaging with Document Basic Access Keys (see there) based on MRZ information as key seed and access condition to data stored on travel document's chip according to LDS.
<i>Basic Inspection System with Basic Access Control protocol (BIS-BAC)</i>	A technical system being used by an official organisation <sup>1</sup> and operated by a governmental organisation and verifying correspondence between the stored and printed MRZ. BIS-BAC implements the terminal's part of the Basic Access Control protocol and authenticates itself to the travel document using the Document Basic Access Keys drawn from printed MRZ data for reading the less-sensitive data (travel document details data and biographical data) stored on the travel document. See also par. 1.2.5; also [PKI].
<i>Basic Inspection System with PACE protocol (BIS-PACE)</i>	A technical system being used by an inspecting authority <sup>2</sup> and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. A technical system being used by an inspecting authority and verifying the ePass presenter as the ePass holder (for ePassport: by comparing the real biometrical data (face) of the ePass presenter with the stored biometrical data (DG2) of the ePass holder). The Basic Inspection System with PACE is a PCT additionally supporting/applying the Passive Authentication protocol.
<i>Biographical data (biodata)</i>	The personalised details of the travel document holder appearing as text in the visual and machine readable zones of and electronically stored in the travel document. The biographical data are less-sensitive data.
<i>Biometric reference data</i>	Data stored for biometric authentication of the travel document holder in the travel document as (i) digital portrait and (ii) optional biometric reference data (e.g. finger and iris).


<sup>1</sup> an inspecting authority; concretely, by a control officer

<sup>2</sup> concretely, by a control officer


Term	Definition
<i>Card Access Number (CAN)</i>	A short password that is printed or displayed on the document. The CAN is a non-blocking password. The CAN may be static (printed on the Passport), semi-static (e.g. printed on a label on the Passport) or dynamic (randomly chosen by the electronic travel document and displayed by it using e.g. ePaper, OLED or similar technologies), see [ICAO-TR-SAC]
<i>Counterfeit</i>	An unauthorised copy or reproduction of a genuine security document made by whatever means [PKI].
<i>Country Signing Certificate (CCSCA)</i>	Certificate of the Country Signing Certification Authority Public Key (KPU CSCA) issued by Country Signing Certification Authority and stored in the rightful terminals.
<i>Country Signing Certification Authority (CSCA)</i>	An organisation enforcing the policy of the ePass Issuer with respect to confirming correctness of user and TSF data stored in the ePass. The CSCA represents the country specific root of the PKI for the ePass and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [PKI], 5.5.1.
<i>Document Basic Access Keys</i>	Pair of symmetric (two-key) Triple-DES keys used for secure messaging with encryption (key KBENC) and message authentication (key KBMAC) of data transmitted between the TOE and an inspection system using BAC [PKI]. They are derived from the MRZ and used within BAC to authenticate an entity able to read the printed MRZ of the passport book; see [PKI].
<i>Document Details Data</i>	Data printed on and electronically stored in the travel document representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
<i>Document Security Object (SOD)</i>	A RFC 3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups: A hash for each Data Group in use shall be stored in the Security Data. It is stored in the ePassport application (EF.SOD) of the travel document. It may carry the Document Signer Certificate (CDS); see [PKI], sec. A.10.4.
<i>Document Signer (DS)</i>	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the ePass for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (CDS)(CDS), see [PKI]. This role is usually delegated to a Personalisation Agent.
<i>Eavesdropper</i>	A threat agent reading the communication between the travel document and the terminal to gain the data on the travel document.
<i>Enrolment</i>	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity; see [PKI].
<i>ePassport application</i>	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [ICAO-TR-SAC].
<i>Forgery</i>	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or portrait; see [PKI].
<i>Global Interoperability</i>	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 utilise that data in inspection operations in their respective States. Global interoperability is a major objective of the standardised specifications for placement of both eye-readable and machine readable data in all travel documents; see [PKI].

Term	Definition
<i>IC Dedicated Software</i>	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life cycle phases.
<i>IC Embedded Software</i>	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life cycle phase and embedded into the IC in the manufacturing life cycle phase of the TOE.
<i>Impostor</i>	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; see [PKI].
<i>Improperly documented person</i>	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required; see [PKI].
<i>Initialisation Data</i>	Any data defined by the travel document manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer. These data are, for instance, used for traceability and for IC identification as travel document material (IC identification data).
<i>Inspection</i>	The act of an official organisation (inspection authority) examining an travel document presented to it by an travel document presenter and verifying its authenticity as the travel document holder. See also [PKI].
<i>Inspection system</i>	see BIS-PACE for this PP. see also BIS-BAC for general information
<i>Integrated circuit (IC)</i>	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
<i>Integrity</i>	Ability to confirm the travel document and its data elements stored upon have not been altered from that created by the travel document Issuer.
<i>Issuing Organisation</i>	Organisation authorised to issue an official travel document (e.g. the United Nations Organisation, issuer of the Laissez-passer); see [PKI].
<i>Issuing State</i>	The country issuing the travel document; see [PKI].
<i>Logical Data Structure (LDS)</i>	The collection of groupings of Data Elements stored in the optional capacity expansion technology [PKI]. The capacity expansion technology used is the travel document's chip.
<i>Machine readable zone (MRZ)</i>	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods; see [PKI]. The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for both PACE and BAC.
<i>Machine-verifiable biometrics feature</i>	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine; see [PKI].
<i>Manufacturer</i>	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life-cycle phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
<i>PACE password</i>	A password needed for PACE authentication, e.g. CAN or MRZ.
<i>PACE Terminal (PCT)</i>	A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the

Term	Definition
	travel document presenter. PCT implements the terminal's part of the PACE protocol and authenticates itself to the ePass using a shared password (CAN or MRZ).
<i>Passive authentication</i>	Security mechanism implementing (i) verification of the digital signature of the Card/Chip or Document Security Object and (ii) comparing the hash values of the read data fields with the hash values contained in the Card/Chip or Document Security Object. See [PKI].
<i>Passport (physical and electronic)</i>	An optically and electronically readable document in form of a paper/plastic cover and an integrated smart card. The Passport is used in order to verify that identity claimed by the Passport presenter is commensurate with the identity of the Passport holder stored on/in the card.
<i>Password Authenticated Connection Establishment (PACE)</i>	A communication establishment protocol defined in [ICAO-TR-SAC]. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the communication partners share the same value of a password $\pi$ ). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
<i>Personalisation</i>	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document.
<i>Personalisation Agent</i>	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [PKI], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [PKI] (in the role of DS).  Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
<i>Personalisation Data</i>	A set of data incl. (i) individual-related data (biographic and biometric data,) of the travel document holder, (ii) dedicated document details data and (iii) dedicated initial TSF data (incl. the Card/Chip Security Object, if installed, and the Document Security Object). Personalisation data are gathered and then written into the non-volatile memory of the TOE by the Personalisation Agent in the life cycle phase card issuing.
<i>Pre-personalisation Data</i>	Any data that is injected into the non-volatile memory of the TOE by the Manufacturer for traceability of the non-personalised travel document and/or to secure shipment within or between the life cycle phases manufacturing and card issuing.
<i>Pre-personalised travel document's chip</i>	travel document's chip equipped with a unique identifier and a unique Authentication Key Pair of the chip.
<i>Receiving State</i>	The Country to which the travel document holder is applying for entry; see [PKI].


	Reference <b>D1315456</b>	Release <b>1.2p</b> (Printed copy not controlled: verify the version before using)
	Classification Level <b>Public</b>	Pages <b>81</b>

Term	Definition
<i>Reference data</i>	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
<i>RF-terminal</i>	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443]
<i>Rightful equipment (rightful terminal or rightful Card)</i>	A technical device being expected and possessing a valid, certified key pair for its authentication, whereby the validity of the related certificate is verifiable up to the respective root CertA. A rightful terminal can be either BIS-PACE (see Inspection System).
<i>Secondary image</i>	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means; see [PKI].
<i>Secure messaging in combined mode</i>	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]
<i>Skimming</i>	Imitation of a rightful terminal to read the travel document or parts of it via the contactless/contact communication channel of the TOE without knowledge of the printed MRZ and CAN dataPACE password.
<i>Standard Inspection Procedure</i>	A specific order of authentication steps between an travel document and a terminal as required by [ICAO-TR-SAC], namely (i) PACE and (ii) Passive Authentication with SOD. SIP can generally be used by BIS-PACE and BIS-BAC.
<i>Supplemental Access Control</i>	A Technical Report which specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control.
<i>Terminal</i>	A Terminal is any technical system communicating with the TOE through a contactless / contact interface.
<i>TOE tracing data</i>	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document
<i>Travel document</i>	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [PKI] (there "Machine readable travel document").
<i>Travel document (electronic)</i>	The contactless/contact smart card integrated into the plastic or paper, optical readable cover and providing the following application: ePassport.
<i>Travel document holder</i>	A person for whom the ePass Issuer has personalised the travel document.
<i>Travel document Issuer (issuing authority)</i>	Organisation authorised to issue an electronic Passport to the travel document holder
<i>Travel document presenter</i>	A person presenting the travel document to a terminal and claiming the identity of the travel document holder.
<i>TSF data</i>	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC-1]).
<i>Unpersonalised travel document</i>	travel document material prepared to produce a personalised travel document containing an initialised and pre-personalised travel document's chip.
<i>User Data</i>	All data (being not authentication data) (i)stored in the context of the ePassport application of the travel document as defined in [PKI]and (ii)being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [ICAO-TR-SAC]).  CC give the following generic definitions for user data:

	Reference <b>D1315456</b>	Release <b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level <b>Public</b>	Pages <b>81</b>

Term	Definition
	Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC-1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC-2]).
<i>Verification data</i>	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.



	Reference	<b>D1315456</b>	Release	<b>1.2p</b> <small>(Printed copy not controlled: verify the version before using)</small>
	Classification Level	<b>Public</b>	Pages	<b>81</b>

## Acronyms

Acronym	Term
<i>AA</i>	Active Authentication
<i>BAC</i>	Basic Access Control
<i>BIS-BAC</i>	Basic Inspection System with BAC (equivalent to Basic Inspection System as used in [9])
<i>BIS-PACE</i>	Basic Inspection System with PACE
<i>CAN</i>	Card Access Number
<i>CC</i>	Common Criteria
<i>CertA</i>	Certification Authority
<i>MRZ</i>	Machine readable zone
<i>n.a.</i>	Not applicable
<i>OSP</i>	Organisational security policy
<i>PACE</i>	Password Authenticated Connection Establishment
<i>PCD</i>	Proximity Coupling Device
<i>PICC</i>	Proximity Integrated Circuit Chip
<i>PP</i>	Protection Profile
<i>RF</i>	Radio Frequency
<i>SAC</i>	Supplemental Access Control
<i>SAR</i>	Security assurance requirements
<i>SFR</i>	Security functional requirement
<i>SIP</i>	Standard Inspection Procedure, see [ICAO-TR-SAC]
<i>TOE</i>	Target of Evaluation
<i>TSF</i>	TOE security functionality
<i>TSP</i>	TOE Security Policy (defined by the current document)