Sagem Identification
SAFRAN Group

Security Target Lite

for the Sagem Identification EAC ePassport, version 1.2.1

a Product of

Sagem Identification bv

Certification ID: BSI-DSZ-CC-0704

Version: 1.0.0

Date: 2010-11-04

Document Revision History

Version	Date	Author	Description
1.0.0	2010-11-04	Sagem Identification	Public Release

Table of Contents

1 ST Introduction

The aim of this document is to describe the Security Target for the Machine Readable Travel Document (MRTD) chip with the ICAO application and Extended Access Control on the NXP JCOP operating system.

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

1.1 ST Reference

Title:	Security Target Lite for the Sagem Identification EAC ePassport 1.2.1
Version Number:	1.0.0
Document Reference:	8158-8101-107 Sagem Identification EAC ePassport 1.2.1 - ST-Lite v1.0.0.doc
CC version:	3.1
Provided by:	Sagem Identification bv
Evaluation assurance level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5

1.2 TOE Reference

TOE Name:	Sagem Identification EAC ePassport
TOE Version:	1.2.1
Developer:	Sagem Identification bv
TOE identification:	Sagem Identification EAC ePassport 1.2.1
Certification ID:	BSI-DSZ-CC-0704
Product type / platform	Machine Readable Travel Document (MRTD) with the ICAO application and Extended Access Control on the NXP J3A080 REV 2 Secure Smart Card Controller (BSI-DSZ-CC-0597-2010)
TOE hardware	NXP P5CD080V0B (certificate BSI-DSZ-CC-0410-2007) and the crypto libraries in the hardware have been certified by BSI (certificate BSI-DSZ-CC-0417-2008)

1.3 TOE Overview

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to the ICAO document [9303], Active Authentication according to the ICAO document [9303], and the Extended Access Control (Chip Authentication and Terminal Authentication) according to the technical report [TG_EAC].

The TOE [Sagem Identification EAC ePassport] comprises of

- the NXP J3A080 Revision 2 Secure Smartcard Controller (also named JCOP v2.4.1), comprising of
  - the circuitry of the MRTD's chip (the NXP P5CD080V0B integrated circuit, IC) with hardware for the contactless interface, e.g. antennae, capacitors;
  - the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
  - the IC Embedded Software (operating system): JCOP v2.4.1;
- the MRTD application: Sagem Identification EAC ePassport Applet version 06.07.0198 loaded in EEPROM
- the associated guidance documentation.

For this TOE, only one application will be present on the IC, namely the MRTD Application. The TOE utilises the evaluation of the underlying platform, which includes the NXP chip, the IC Dedicated Software, and the JCOP v2.4.1 (certification BSI-DSZ-CC-0597-2010).

The hardware platform NXP P5CD080V0B is certified by BSI (BSI-DSZ-CC-0410-2007) and the crypto libraries in the hardware are certified by BSI (BSI-DSZ-CC-0417-2008).

The State or organisation issues the MRTD to be used by the holder for international travel. The traveller presents its MRTD to the inspection system to prove his or her identity. The MRTD in the 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 the 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 genuine MRTD of issuing State or Organization.

The security functionality of the TOE respectively the Sagem Identification EAC ePassport applet will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

The following overview shows the security features of the composite TOE.

Authentication mechanisms

The different authentication mechanisms are supported by according APDU commands and parameters using the cryptographic functions provided by the platform.

Active Authentication of the MRTD's chip. The TOE can optionally demonstrate that the MRTD data is contained on the intended chip by using an RSA signature described in [9303].

Chip Authentication of the MRTD's chip. This protocol provides evidence of the MRTD's chip authenticity and prevents data traces described in [9303].

Extended Access Control uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system.

Authentication of the Personalization Agent using the according keys written to the TOE by the Manufacturer during pre-personalization.

Cryptographic functions support

3DES (112 bit keys) for en-/decryption (CBC and ECB) and signature (MAC) generation and verification, all provided by the platform.

SHA-1, SHA-224, and SHA-256 hash algorithm, provided by the platform.

ECDSA signature verification with key lengths 224 and 256 Bit, provided by the platform.

Diffie-Hellman key agreement with EC over GF(p) and cryptographic key sizes from 224 and 256 bit according to [ANSI X9.63], provided by the platform.

RSA digital signature generation for Active Authentication with key sizes of 1280, 1536 and 1792 Bit according to [ISO 9796-2] and [SHA-1 digest], provided by the platform

Destruction of cryptographic keys: A special javacard.security method of the JCOP platform is used. The transient keys will be reset by the JCOP platform if a deselect of the DF or a reset occurs in an authenticated phase of the TOE.

Random number generation according to class K3, SOF-high, of AIS 20 [AIS20], provided by the platform.

Protection against interference, logical tampering and bypass

The JCOP platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The JCOP platform will provide protection against physical attack and perform self tests.

Security domains are supported by the JavaCard platform used by the TOE underlying platform.

The Sagem Identification EAC Applet uses transient memory where a hardware reset should revert the Sagem Identification EAC ePassport Applet to an unauthenticated state.

Access control / Storage and protection of logical MRTD data

Security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

Authenticity and integrity of data are protected 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.

Write-only-once access control is set by the personalization agent and integrity protection by physical means is provided by the platform.

Confidentiality is ensured by the Basic Access Control Mechanism and the Extended Access Control Mechanism.

Keys: The Sagem Identification EAC Applet only stores keys in Java Card specified Key structures, which are protected by JCOP platform.

Secure Messaging

Secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive established by the Chip Authentication Mechanism.

Retail MAC is part of every APDU command/response when secure messaging is active for Basic Access Control. Re-authentication is performed by the mandatory MAC in secure messaging.

Security and life cycle management

Initialization and pre-personalisation functionality is supported by both the JCOP platform and the Sagem Identification EAC ePassport Applet .

Personalization and Configuration of the Sagem Identification EAC ePassport Applet is performed using the commands available in the personalization phase.

Management of TSF-Data can only be done after successful Terminal Authentication.

The **test features** of the JCOP platform are protected by ways described in JCOP platform.

The JCOP platform **protects the TOE against malfunctions** that are caused by exposure to operating conditions that may cause a malfunction.

The **Document Basic Access Keys, the Chip Authentication Private Key, and the Personalization Agent Keys** are protected from disclosure.

The JCOP platform **protects the TOE against malfunctions** that are caused by exposure to operating conditions that may cause a malfunction.

The **INSTALL for INSTALL** method of the JCOP platform will be used to store the chip identification data.

1.4 TOE Description

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS), providing the Basic Access Control and Active Authentication according to the ICAO document [9303], and the Extended Access Control (Chip Authentication and Terminal Authentication) according to the technical report [TG_EAC].

The TOE comprises of the following items:

- the circuitry of the MRTD's chip (the integrated circuit, IC) with hardware for the contactless interface, e.g. antenna, capacitors,
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the IC Embedded Software (operating system): JCOP v2.4.1,
- the MRTD application: Sagem Identification EAC ePassport Applet version 06.07.0198 loaded in EEPROM,
- the associated guidance documentation.

A schematic overview of the TOE is shown in Figure 1:

- The MRTD's chip circuitry and the IC dedicated software forming the Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- The IC embedded software running on the Smart Card Platform consists of
    - Java Card virtual machine, ensuring language-level security;
    - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
    - Java card API, providing access to card's resources for the Applet;
    - Global Platform Card Manager, responsible for management of Applets on the card. For this TOE post issuance loading or deletion of Applets is not allowed;
    - Native Mifare application, for this TOE the Mifare application is disabled
- The Applet Layer is the Sagem Identification EAC Applet.

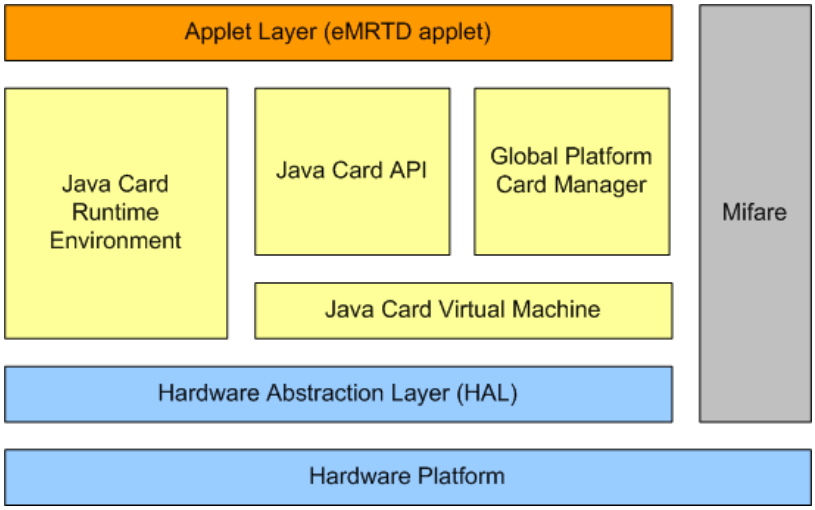


Figure 1: TOE

1.4.1 TOE usage and security features for operational use

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 as specified by ICAO in [9303], Volume 2, Section III, 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[1]
   (4) the other data according to LDS (EF.DG5 to EF.DG16) and
   (5) the Document security object.

[1] These additional biometric reference data are optional

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 organisational security measures (e.g. control of materials, personalization procedures) [SSMR]. 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 document [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 Basic Access Control Mechanism and the Extended Access Control Mechanism.

This ST addresses the Chip Authentication described in [TG_EAC] and Active Authentication stated in [9303].

1.4.2 TOE life cycle

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

1.4.2.1 Phase 1: "Development"

The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components. The IC developer also acts as the developer of the embedded software (operating system) which is the JCOP v.2.4.1platform.

The software developer uses the guidance documentation for relevant parts of the IC Embedded Software (operating system) and develops the MRTD application and the guidance documentation associated with this TOE component.

The MRTD application, the Sagem Identification EAC ePassport Applet run time code is securely delivered directly from the software developer (Sagem Identification development dept.) to the MRTD Manufacturer (Sagem Identification production dept.).

1.4.2.2 Phase 2 “Manufacturing”

Both IC manufacturer and MRTD manufacturer are involved in this life-cycle phase. In a first step the TOE integrated circuit is produced containing the MRTD’s chip Dedicated Software and the parts of the MRTD’s chip Embedded Software in the non-volatile nonprogrammable 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 manufacture to the MRTD manufacturer.

The MRTD manufacturer

i. adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM) if necessary,
ii. loads and creates the MRTD application,
iii. equips MRTD’s chips with pre-personalization data, and
iv. combines the IC with hardware for the contactless interface in the passport booklet or card.

The Sagem Identification EAC ePassport Applet is loaded into the EEPROM area of the NXP P5CD080V0B chip and activated in the MRTD manufacturing phase (creation of the MRTD application). Both the underlying platform and the Sagem Identification EAC ePassport Applet provide configuration and life-cycle management functions required for TOE preparation. TOE preparation steps are performed in manufacturing phase in accordance with the guidance documentation.

As final step in the TOE preparation the Personalization Agent Key Set is installed. The TOE is securely delivered to the Personalization Agent.

1.4.2.3 Phase 3 “Personalization of the MRTD”

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 the TOE User Data and TSF Data into the logical MRTD and
v. the writing the TSF Data into the logical MRTD and 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 digitised portrait (EF.DG2), and
iii. the document security object.

The signing of the Document security object by the Document signer [9303] 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.

This Security Target distinguishes between the Personalization Agent as entity known to the TOE and the Document Signer as entity in the TOE IT environment signing the Document security object as described in [9303]. This approach allows but does not enforce the separation of these roles.

The Personalization Agent authenticates by two 112 bit Triple-DES keys (MAC and ENC) that meet [FIPS46].

1.4.2.4 Phase 4 “Operational Use”

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

2 Conformance Claims

2.1 CC Conformance Claim

This security target claims to be conformant to the Common Criteria version 3.1, which comprises

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, September 2006 [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 2, September 2007 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 2, September 2007, [CC-3]

as follows:

- Part 2 extended with
  - FAU_SAS Audit data storage
  - FCS_RND Generation of random numbers
  - FIA_API Authentication proof of identity
  - FMT_LIM Limited capabilities and availability
  - FPT_EMSEC TOE emanation
- Part 3 conformant

The Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 2, September 2007 [CC-4]
has been taken into account.

2.2 PP Claim / Package Claim

This security target claims conformance to the

Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0026, version 1.2 [PP]

This ST is package conformant to EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

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 Data

The logical MRTD data consists of the EF.COM and the data groups DG1 to DG16 (with different security needs) and the Document security object EF.SOD according to LDS [9303]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1 to EF.DG13 and EF.DG16 contain personal data of the MRTD holder. The Active Authentication Public Key (EF.DG15) is used by the inspection system for Active Authentication of the chip (optional). The Chip Authentication Public Key (EF.DG14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD. The EF.CVCA is used for the Terminal Authentication.

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

Logical MRTD standard User Data

- Personal Data of the MRTD holder (EF.DG1, EF.DG2, EF.DG16)
- Active Authentication Public Key in EF.DG15
- Chip Authentication Public Key in EF.DG14
- Document Security Object (SOD) in EF.SOD
- Country Verifying Certification Authority Certificate's CAR value in EF.CVCA
- Common data in EF.COM

Logical MRTD sensitive User Data

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

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 traveller to proof his possession of a genuine MRTD.

3.1.2 Subjects

This security target considers the following subjects:

Manufacturer

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

Personalization Agent

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

i. establishing the identity the holder for the biographic data in the MRTD,
ii. enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s)
iii. writing these data on the physical and logical MRTD for the holder as defined for global, international and national interoperability,
iv. writing the initial TSF data and
v. signing the Document Security Object defined in [9303].

Country Verifying Certification Authority

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

Document Verifier

The Document Verifier (DV) enforces the privacy policy of the receiving Country with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits

provided by the issuing States or Organizations in form of the Document Verifier Certificates.

Terminal

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

Inspection system

A technical system used by the border control officer of the receiving State

i. examining an MRTD presented by the traveller and verifying its authenticity and

ii. verifying the traveller as MRTD holder..

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 **Active Authentication Basic Inspection System** (AABIS)[2] is a Basic Inspection System which implements additional the Active Authentication Mechanism,

The **General Inspection System** (GIS) is a Basic Inspection System which implements additional the Chip Authentication Mechanism.

The **Active Authentication General Inspection System** (AAGIS)[3] is a General Inspection System which implements additional the Active 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 **Active Authentication Extended Inspection System** (AAEIS)[4] is a Extended Inspection System which implements additional the Active Authentication Mechanism,

The security attributes of the EIS are defined of the Inspection System Certificates.

[2] added by the ST author

[3] added by the ST author

[4] added by the ST author

MRTD Holder

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

Traveller

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

Attacker

A threat agent trying

i. to identify and to trace the movement the MRTD's chip remotely (i.e. without knowing or optically reading the physical MRTD),

ii. to read or to manipulate the logical MRTD without authorization, or

iii. to forge a genuine MRTD.

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.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,

iv. the Active Authentication Public Key (EF.DG15) if stored on the MRTD's chip, and

v. 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 traveller and verifying its authenticity and

ii. verifying the traveller as MRTD holder.

The Basic Inspection System for global interoperability

i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

ii. implements the terminal part of the Basic Access Control [9303].

The Basic Inspection System reads the logical MRTD being 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 Active Authentication Inspection Systems (AABIS, AAGIS, and AAEIS) must be able to verify that the Active Authentication private key (stored on the MRTD IC) matches the Active Authentication public key contained in the logical MRTD using a challenge response mechanism in the TOE, [9303], Volume 2, Section IV, par. 7.2.2.

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 Organisations 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

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

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

The CA keeps the Country Signing CA Private Key secret and distributes the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer

i. generates the Document Signer Key Pair,

ii. hands over the Document Signer Public Key to the CA for certification,

iii. keeps the Document Signer Private Key secret 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 and distributes them to the receiving States and organizations.

A.Auth_PKI **PKI for Inspection Systems**

The issuing and receiving States or Organisations 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 Organisations 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 Organisations. The issuing States or Organizations distributes the public key of their Country Verifying Certification Authority to their MRTD's chip.

3.3 Threats

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

3.3.1 Threats to be averted by the TOE and its environment

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

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

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

T.Skimming **Skimming the logical MRTD**

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

T.Read_Sensitive_Data **Read the sensitive biometric reference data**

An attacker with high attack potential knowing the Document Basic Access Keys is trying to gain the sensitive biometric reference data through the communication interface of the MRTD's chip.

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

T.Forgery Forgery of data on MRTD's chip

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

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

T.Counterfeit MRTD's chip

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

The TOE shall avert the threat as specified below.

3.3.2 Threats to be averted by the TOE independently

The TOE independently shall avert the threats as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order

i. to manipulate User Data,

ii. to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or

iii. to disclose or to manipulate TSF Data.

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

T.Information_Leakage Information Leakage from MRTD's chip

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

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

T.Phys-Tamper Physical Tampering

An attacker may perform physical probing of the MRTD's chip in order

i. to disclose TSF Data, or

ii. to disclose/reconstruct the MRTD's chip Embedded Software.

An attacker may physically modify the MRTD's chip in order to

i. modify security features or functions of the MRTD's chip,

ii. modify security functions of the MRTD's chip Embedded Software,

iii. to modify User Data or

iv. to modify TSF data.

The physical tampering may be focused directly on the discloser 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.

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to

i. deactivate or modify security features or functions of the TOE or

ii. circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software.

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

3.4 Organisational Security Policies

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

P.Manufact Manufacturing of the MRTD's chip

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

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

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

P.Personal_Data Personal data protection policy

The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitised portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder i.e. if the MRTD is presented to an inspection system. Additional to the Basic Access Control Authentication defined by ICAO in [9303] the MRTD's chip shall protect the confidentiality and integrity of the personal data during transmission to the General Inspection System after Chip authentication.

P.Sensitive_Data Privacy of sensitive biometric reference data

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

OT.AC_Pers Access Control for Personalization of logical MRTD

The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [9303] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during personalization and cannot be changed afterwards.

OT.Data_Int Integrity of personal data

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

OT.Data_Conf Confidentiality of personal data

The TOE must ensure the confidentiality of the data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 and the Document Security Object of the logical MRTD by granting read access to terminals successfully authenticated by as

i. Personalization Agent or
ii. Basic Inspection System or
iii. Extended Inspection System.

The TOE implements the Basic Access Control as defined by [9303] and enforce Basic Inspection System to authenticate itself by means of the Basic Access Control based on knowledge of the Document Basic Access Key. The TOE must ensure the confidentiality of the logical MRTD data during their transmission to the General Inspection System after Chip Authentication.

OT.Sens_Data_Conf Confidentiality of sensitive biometric reference data

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

OT.Identification Identification and Authentication of the TOE

The TOE must provide means to store IC Identification Data in its non-volatile memory. The IC Identification Data must provide a unique identification of the IC during Phase 2 “Manufacturing” and Phase 3 “Personalization of the MRTD”. In Phase 4 “Operational Use”, the TOE shall identify itself only to a successful authenticated Basic Inspection System or Personalization Agent.

OT.Chip_Auth_Proof Proof of MRTD’S chip authenticity

The TOE must support the General Inspection Systems (and optionally support the Active Authentication Inspection Systems[5]) to verify the identity and authenticity of the MRTD’s chip as issued by the identified issuing State or Organization by means of the Chip Authentication as defined in [TG_EAC] or Active Authentication as defined in [9303][5]. The authenticity prove provided by MRTD’s chip shall be protected against attacks with high attack potential.

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

OT.Prot_Abuse-Func Protection against Abuse of Functionality

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

i. to disclose critical User Data,

ii. to manipulate critical User Data of the Smartcard Embedded Software,

iii. to manipulate Soft-coded Smartcard Embedded Software or

[5] This part of the objective is added to the PP to cover active authentication.

iv. bypass, deactivate, change or explore security features or functions of the TOE.

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

OT.Prot_Inf_Leak Protection against Information Leakage

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

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

OT.Prot_Phys-Tamper Protection against Physical Tampering

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

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security features, as well as
- controlled manipulation of memory contents (User Data, TSF Data)

with a prior

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

OT.Prot_Malfunction Protection against Malfunctions

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

4.2 Security Objectives for the Development and Manufacturing Environment

OD.Assurance Assurance Security Measures in Development and Manufacturing Environment

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

OD.Material Control over MRTD Material

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

4.3 Security Objectives for the Operational Environment

Issuing State or Organization

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

OE.Personalization Personalization of logical MRTD

The issuing State or Organization must ensure that the Personalization Agents acting on the behalf of the issuing State or Organisation

i. establish the correct identity of the holder and create biographic data for the MRTD,

ii. enrol the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) and/or the encoded iris image(s) and

iii. personalize the MRTD for the holder together with the defined physical and logical security measures to protect the confidentiality and integrity of these data.

OE.Pass_Auth_Sign Authentication of logical MRTD by Signature

The Issuing State or Organization must

i. generate a cryptographic secure Country Signing Key Pair,

ii. ensure the secrecy of the Country Signing Private Key and sign Document Signer Certificates in a secure operational environment, and

iii. distribute the Certificate of the Country Signing Public Key to receiving States and organizations maintaining its authenticity and integrity.

The Issuing State or organization must

i. generate a cryptographic secure Document Signing Key Pair and ensure the secrecy of the Document Signer Private Keys,

ii. sign Document Security Objects of genuine MRTD in a secure operational environment only and

iii. distribute the Certificate of the Document Signing Public Key to receiving States and organizations.

The digital signature in the Document Security Object relates to all data in the data in EF.DG1 to EF.DG16 if stored in the LDS according to [9303].

OE.Auth_Key_MRTD MRTD Authentication Key

The issuing State or Organization has to establish the necessary public key infrastructure in order to

i. generate the MRTD's Chip Authentication Key Pair and optionally the MRTD's Active Authentication Key Pair,

ii. store the Chip Authentication Private Key, and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14,

iii. store the Active Authentication Private Key, and store the Active Authentication Public Key in the Active Authentication Public Key data in EF.DG15 (if generated), and

iv. support inspection systems of receiving States or organizations to verify the authenticity of the MRTD's chip used for genuine MRTD by certification of the Chip and Active Authentication Public Key by means of the Document Security Object.

OE.Authoriz_Sens_Data Authorization for Use of Sensitive Biometric Reference Data

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

Receiving State or organization

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

OE.Exam_MRTD Examination of the MRTD passport book

The inspection system of the Receiving State must examine the MRTD presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical MRTD. The Basic Inspection System for global interoperability

i. includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and

ii. implements the terminal part of the Basic Access Control [9303].

Additionally General Inspection Systems and Extended Inspection Systems perform the Chip Authentication Protocol to verify the Authenticity of the presented MRTD's chip.

An Active Authentication (Basic, General or Extended) Inspection system performs all the functions of the Basic, General, respectively Extended Inspection System, and verifies the IC authenticity with an RSA signature generated by the MRTD (if available).

OE.Passive_Auth_Verif Verification by Passive Authentication

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

OE.Prot_Logical_MRTD Protection of data of the logical MRTD

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

OE.Ext_Insp_Systems Authorisation of Extended Inspection Systems

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

reference data with its private Terminal Authentication Key and its Inspection System Certificate.

5 Extended Components Definition

This ST uses the extended components defined by the PP [PP, 4]. That definition uses components defined as extensions to CC part 2. Some of these components are defined in [PP_IC], other components are defined in this Security Target.

5.1 Definition of the Family FAU_SAS

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

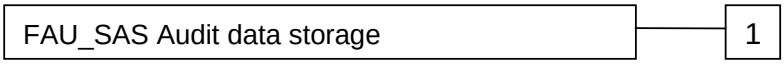
The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behaviour

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

Component leveling



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

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

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

Dependencies: No dependencies.

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 as the component FCS_CKM.1 is. The similar component FIA_SOS.2 is intended for non-cryptographic use.

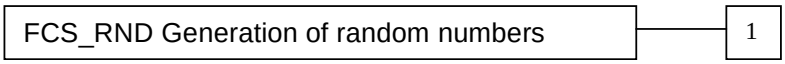
The family “Generation of random numbers (FCS_RND)” is specified as follows.

FCS_RND Generation of random numbers

Family behaviour

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

Component leveling:



FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	Quality metric for random numbers
Hierarchical to:	No other components.
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].
Dependencies:	No dependencies.

5.3 Definition of the Family FIA_API

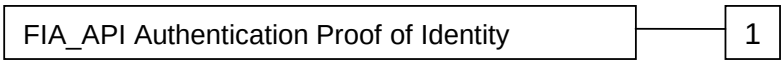
To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external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



FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT:

Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable .

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.4 Definition of the Family FMT_LIM

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

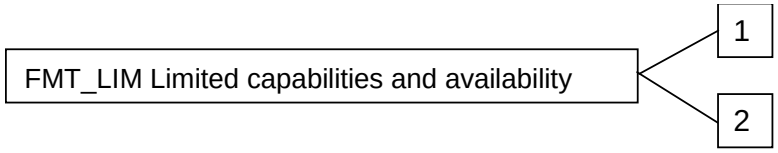
The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

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

Component leveling:



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

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

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

To define the IT security functional requirements of the TOE 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.

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

Dependencies: FMT_LIM.2 Limited availability.

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

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

Dependencies: FMT_LIM.1 Limited capabilities.

5.5 Definition of the Family FPT_EMSEC

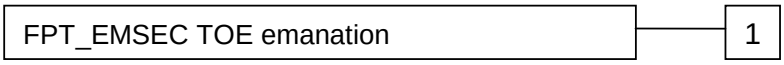
The sensitive family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena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

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

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

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

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

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

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

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

Dependencies: No other components.

6 Security Requirements

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of [CC-2]. Each of these operations is used in this security target.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements that add or change words are in **bold** text. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections filled in by the ST author appear as *slanted and underlined text*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear as *slanted and underlined text*.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

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

Name	Data
Country Verifying Certification Authority Private Key (SK_{CVCA})	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} 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 Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TG_EAC] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) 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.

Name	Data
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) 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
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (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 (SK_{ICC}, PK_{ICC}) 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 (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) 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 (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) 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.
Active Authentication Public Key	The optional Active Authentication Public Key is stored in the EF.DG15 Active Authentication Public Key of the TOE's logical MRTD and used by the inspection system for Active Authentication of the MRTD's chip. It is part of the user data provided by the TOE for the IT environment.
Active Authentication Private Key ()	The optional Active Authentication Private Key is used by the TOE to authenticate itself as authentic MRTD's chip. It is part of the TSF data.
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.

Name	Data
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.

Table 1: Keys and Certificates

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.

6.1.1 Class FAU Security Audit

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below For the extended components definition refer to [PP] chapter 4.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide the Manufacturer[6] with the capability to store the IC Identification Data[7] in the audit records.

Dependencies: No dependencies.

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 cryp-

6 [assignment: *authorized users*]

7 [assignment: *list of audit information*]

tographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD

Hierarchical to: No other components.

FCS_CKM.1.1/ KDF_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm Document Basic Access Key Derivation Algorithm[8] and specified cryptographic key sizes 112 bit[9] that meet the following: *[9303], Volume 2, Section IV, Appendix 5*[10].

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

Application note: The TOE uses this key derivation function as well to derive other session keys from shared secrets established by the Chip Authentication Protocol for the secure messaging required by FCS_COP.1/TDES_MRTD and FCS_COP.1/ MAC_MRTD. The algorithm uses the random number RND.ICC generated by TSF as required by FCS_RND.1/MRTD.

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

Hierarchical to: No other components.

FCS_CKM.1.1/ DH_MRTD	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH Key Agreement Algorithm over GF(p) and 3DES*[11] specified cryptographic key sizes of *224 or 256 bits, respectively 112 bits*[12] that meet the following: *[TG_EAC, Annex A.1]*[13]

8 [*assignment: cryptographic key generation algorithm*]

9 [*assignment: cryptographic key sizes*]

10 [*assignment*: *list of standards*]

11 [*assignment: cryptographic key generation algorithm*]

12 [*assignment: cryptographic key sizes*]

13 [*assignment*: *list of standards*]

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

Application note[14]: The TOE generates a shared secret value with the terminal secret value during the Chip Authentication Protocol (see TG_EAC] sec. 3.1 and Annex A.1, [ECCTR]) based on the ECDH protocol compliant to [BSI], Annex A.1. This protocol is based on the Diffie-Hellman-Protocol ECDH compliant to ISO 15946 (i.e. an elliptic curve cryptography algorithm) (cf. [TG_EAC], Annex A.1, [TG_ECC] and [ISO15946-3] for details). The shared secret value is used to derive the 112 bit Triple-DES key for encryption and the 112 bit Retail-MAC Chip Session Keys according to the Document Basic Access Key Derivation Algorithm [9303], Volume 2, Appendix 5 to Section IV, par. A5.1, for the TSF as required by FCS_COP.1/TDES_MRTD and FCS_COP.1/MAC_MRTD.

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 - MRTD

Hierarchical to: No other components.

FCS_CKM.4.1/ MRTD	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *physically overwriting the keys*[15] that meets the following: *none*[16].

14 Adapted to TOE

15 *[assignment: cryptographic key destruction method]*

16 *[assignment: list of standards]*

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

6.1.2.1 Cryptographic operation (FCS_COP.1)

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

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

Hierarchical to: No other components.

FCS_COP.1.1/ SHA_MRTD	The TSF shall perform hashing[17] in accordance with a specified cryptographic algorithm *SHA-1, SHA-224 or SHA-256*[18] and cryptographic key sizes none[19] that meet the following: FIPS 180-2[20].

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

Application note: The TOE implements the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism. The Chip Authentication Protocol may use SHA-1. The TOE implements the additional hash functions SHA-224 and SHA-256 for the Terminal Authentication Protocol (cf. [TG_EAC], Annex A.2.2 for details).

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

Hierarchical to: No other components.

[17] [*assignment: list of cryptographic operations*]

[18] *[assignment: cryptographic algforithm]*

[19] [assignment*: cryptographic key sizes*]

[20] [assignment: *list of standards*]

FCS_COP.1.1/ TDES_MRTD	The TSF shall perform secure messaging – encryption and decryption[21] in accordance with a specified cryptographic algorithm Triple-DES in CBC mode[22] and cryptographic key sizes 112 bit[23] that meet the following: FIPS 46-3 [FIPS46] and [9303], Volume 2, Appendix 5 to Section IV[24].

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

FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

Hierarchical to: No other components.

FCS_COP.1.1/ MAC_MRTD	The TSF shall perform secure messaging – message authentication code[25] in accordance with a specified cryptographic algorithm Retail MAC[26] and cryptographic key sizes 112 bit[27] that meet the following: ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)[28].

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

.

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

Hierarchical to: No other components.

[21] [assignment: *list of cryptographic operations*]

[22] [assignment: *cryptographic algorithm*]

[23] [assignment: *cryptographic key sizes*]

[24] [assignment: *list of standards*]

[25] [assignment: *list of cryptographic operations*]

[26] [assignment: *cryptographic algorithm*]

[27] [assignment: *cryptographic key sizes*]

[28] [assignment: *list of standards*]

FCS_COP.1.1/ SIG_VER	The TSF shall perform digital signature verification [29] in accordance with a specified cryptographic algorithm *ECDSA*[30] and cryptographic key sizes *224bit and 256bit*[31] that meet the following: *[ISO15946-2]*[32]

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

FCS_COP.1/RSA Cryptographic operation – RSA Signature

Hierarchical to: No other components.

FCS_COP.1.1/ RSA	The TSF shall perform *digital signature generation*[33] in accordance with a specified cryptographic algorithm *RSA*[34] and cryptographic key sizes *1280, 1536 and 1792 Bit*[35] that meet the following: *[ISO 9796-2] and [SHA-1 digest]*[36]

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

6.1.2.2 Random Number Generation (FCS_RND.1)

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

[29] [assignment: *list of cryptographic operations*]

[30] [assignment: *cryptographic algorithm*]

[31] [assignment*: cryptographic key sizes*]

[32] [assignment: *list of standards]*

[33] [assignment: *list of cryptographic operations*]

[34] [assignment: *cryptographic algorithm*]

[35] [assignment*: cryptographic key sizes*]

[36] [assignment: *list of standards]*

FCS_RND.1/MRTD Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1/ MRTD	The TSF shall provide a mechanism to generate random numbers that meet *class K3, of [AIS 20]*[37]

Dependencies: No dependencies.

6.1.3 Class FIA Identification and Authentication

Application note: The following table provides an overview on the authentication mechanisms used.

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

Table 2: Overview on authentication SFR

[37] [assignment: *a defined quality metric*]

Note the Chip Authentication Protocol include the asymmetric key agreement and the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

6.1.3.1 Timing of identification (FIA_UID.1)

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

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1	The TSF shall allow (1) to establish the communication channel, (2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS[38] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

6.1.3.2 Timing of authentication (FIA_UAU.1)

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

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

[38] [assignment: *list of TSF-mediated actions*]

FIA_UAU.1.1 The TSF shall allow

(1) to establish the communication channel,

(2) to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS

(3) to identify themselves by selection of the authentication key[39] on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification.

6.1.3.3 Single-use authentication mechanisms (FIA_UAU.4)

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

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

Hierarchical to: No other components.

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

1. Basic Access Control Authentication Mechanism,
2. Terminal Authentication Protocol,
3. Authentication Mechanism based on Triple-DES[40].

Dependencies: No dependencies.

6.1.3.4 Multiple authentication mechanisms (FIA_UAU.5)

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

[39] [assignment: *list of TSF-mediated actions*]

[40] [assignment: *identified authentication mechanism(*s)]

FIA_UAU.5/MRTD Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

1. Basic Access Control Authentication Mechanism,
2. Terminal Authentication Protocol,
3. Secure Messaging in MAC_ENC-mode,
4. Symmetric Authentication Mechanism based on Triple-DES[41]

to support user authentication.

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

1. The TOE accepts the authentication attempt as Personalization Agent by one of the following mechanisms
   (a) The Basic Access Control Authentication Mechanism with the Personalization Agent Keys,
   (b) The Symmetric Authentication Mechanism with the Personalization Agent Key,
   (c) The Terminal Authentication Protocol with Personalization Agent Keys
2. The TOE accepts the authentication attempt as Basic Inspection System only by means of the Basic Access Control Authentication Mechanism with the Document Basic Access Keys.
3. After successful authentication as Basic Inspection System and until the completion of the Chip Authentication Mechanism the TOE accepts only received command with correct message authentication code sent by means of secure messaging with key agreed with the authenticated terminal by means of the Basic Access Control Authentication Mechanism.
4. After run of the Chip Authentication Mechanism the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism.
5. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol only if the terminal uses secure messaging established by the Chip Authentication Mechanism[42].

Dependencies: No dependencies.

[41] [assignment: *list of multiple authentication mechanisms*]

[42] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

6.1.3.5 Re-authenticating (FIA_UAU.6)

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

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

Hierarchical to: No other components.

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

1. Each command sent to TOE after successful authentication of the terminal with Basic Access Control Authentication Mechanism and until the completion of the Chip Authentication Mechanism shall be verified as being sent by the authenticated BIS.
2. Each command sent to TOE after successful run of the Chip Authentication Protocol shall be verified as being sent by the GIS[43].

Dependencies: No dependencies.

6.1.3.6 Authentication Failure Handling (FIA_AFL.1)

The TOE shall meet the requirement “Authentication Failure Handling (FIA_AFL.1)” as specified below.

FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within one to 32767*[44] unsuccessful authentication attempts occur related to *BAC authentication*[45].

[43] [assignment: *list of conditions under which re-authentication is required*]

[44] *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*

[45] [assignment: *list of authentication events*]

FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *wait an administrator configurable time before the next authentication attempt can be performed*[46].

Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_API.1/CAP Authentication Proof of Identity - MRTD

Hierarchical to: No other components.

FIA_API/CAP	The TSF shall provide an Chip Authentication Protocol according to [TG_EAC][47] to prove the identity of the TOE[48].

Dependencies: No dependencies.

FIA_API.1/AA Authentication Proof of Identity - MRTD

Hierarchical to: No other components.

FIA_API/AA	The TSF shall provide an Active Authentication Protocol according to [9303][49] to prove the identity of the TOE[50].

[46] [assignment: *list of actions*]

[47] [assignment: *authentication mechanism*]

[48] [assignment: *authorized user or rule*]

[49] [assignment: *authentication mechanism*]

[50] [assignment: *authorized user or rule*]

Dependencies: No dependencies.

6.1.4 Class FDP User Data Protection

6.1.4.1 Subset access control (FDP_ACC.1)

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.

FDP_ACC.1.1	The TSF shall enforce the Access Control SFP[51] on terminals gaining write, read and modification access to the data in the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD[52].

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.4.2 Security attribute based access control (FDP_ACF.1)

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[53]

Hierarchical to: No other components.

[51] [assignment: *access control SFP*]

[52] [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*]

[53] The bold text below has been added to allow the use of active authentication.

FDP_ACF.1.1 The TSF shall enforce the Access Control SFP[54] to objects based on the following:

1. Subjects:
   a. Personalization Agent
   b. Basic Inspection System
   c. Extended Inspection System
   d. Terminal
2. Objects:
   a. data EF.DG1 to EF.DG16 of the logical MRTD
   b. data in EF.COM
   c. data in EF.SOD
3. Security attributes
   a. authentication status of terminals
   b. Terminal Authorization[55].

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 data and to read data of the data of the EF.COM, EF.SOD, EF.DG1 to EF.DG16 of the logical MRTD,
2. the successfully authenticated Basic Inspection System is allowed to read data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD, **and request active authentication**,
3. the successfully authenticated Extended Inspection System is allowed to read data in EF.COM, EF.SOD, EF.DG1, EF.DG2 and EF.DG5 to EF.DG16 of the logical MRTD,
4. the successfully authenticated Extended Inspection System is allowed to read data in EF.DG3 according to the Terminal Authorization,
5. the successfully authenticated Extended Inspection System is allowed to read data in EF.DG4 according to the Terminal Authorization[56].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following sensitive rules: none[57].

FDP_ACF.1.4

[54] [assignment: *access control SFP*]

[55] [assignment: *list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes*, *or named groups of SFP-relevant security attributes*]

[56] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[57] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

1. The TSF shall explicitly deny access of subjects to objects based on the rule: A terminal authenticated as CVCA is not allowed to read data in the EF.DG3,
2. A terminal authenticated as CVCA is not allowed to read data in the EF.DG4,
3. A terminal authenticated as DV is not allowed to read data in the EF.DG3,
4. A terminal authenticated as DV is not allowed to read data in the EF.DG4,
5. the Terminals are not allowed to modify any of the EF.DG1 to EF.DG16 of the logical MRTD[58].

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

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

FDP_ITC.1.1 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1	The TSF shall enforce the *Access Control SFP*[59] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *none*[60].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control],
FMT_MSA.3 Static attribute initialisation

FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

Hierarchical to: No other components.

[58] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[59] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[60] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

FDP_UCT.1.1/MRTD	The TSF shall enforce the Access Control SFP[61] to be able to transmit and receive[62] user data in a manner protected from unauthorized disclosure **after Chip Authentication**.

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

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

FDP_UIT.1/MRTD Data exchange integrity - MRTD

Hierarchical to: No other components.

FDP_UIT.1.1/MRTD	The TSF shall enforce the Access Control SFP[63] to be able to transmit and receive[64] user data in a manner protected from modification, deletion, insertion and replay[65] errors **after Chip Authentication**.
FDP_UIT.1.2/MRTD	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[66] has occurred **after Chip Authentication**.

[61] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[62] [selection*: transmit, receive*]

[63] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[64] [selection*: transmit, receive*]

[65] [selection: *modification, deletion, insertion, replay*]

[66] [selection: *modification*, *deletion, insertion, replay*]

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]

6.1.5 Class FMT Security Management

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.

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

1. Initialization,
2. Personalization
3. Configuration[67].

Dependencies: No Dependencies

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.

FMT_SMR.1.1 The TSF shall maintain the roles

1. Manufacturer,
2. Personalization Agent,
3. Country Verifier Certification Authority,
4. Document Verifier,
5. Basic Inspection System,
6. domestic Extended Inspection System
7. foreign Extended Inspection System[68].

[67] [assignment: *list of security management functions to be provided by the TSF*]

[68] [assignment: *the authorised identified roles*]

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

Hierarchical to: FIA_UID.1 Timing of identification.

The TOE shall meet the requirement “Limited capabilities (FMT_LIM.1)” as specified below. For the extended components definition refer to [PP] chapter 4.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their availability 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 disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[69].

Dependencies: FMT_LIM.2 Limited availability.

The TOE shall meet the requirement “Limited availability (FMT_LIM.2)” as specified below. For the extended components definition refer to [PP] chapter 4.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced:
Deploying Test Features after TOE Delivery does not allow
1. User Data to be disclosed or manipulated,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed and
4. substantial information about construction of TSF to be gathered which may enable other attacks[70].

[69] [assignment: *Limited capability and availability policy*]

[70] [assignment: *Limited capability and availability policy*]

Dependencies: FMT_LIM.1 Limited capabilities.

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.

FMT_MTD.1/INI_ENA	The TSF shall restrict the ability to write[71] the Initialization Data and Pre-personalization Data[72] to the Manufacturer[73].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/INI_DIS	The TSF shall restrict the ability to disable read access for users to[74] the Initialization Data[75] to the Personalization Agent[76].

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

[71] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[72] [assignment: *list of TSF data*]

[73] [assignment: *the authorized identified roles*]

[74] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[75] [assignment: *list of TSF data*]

[76] [assignment: *the authorized identified roles*]

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

Hierarchical to: No other components.

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 Verifier Certification Authority Certificate, 3. initial Current Date[77] to *the Personalization Agent*[78].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ CVCA_UPD	The TSF shall restrict the ability to update the 1. Country Verifier Certification Authority Public Key, 2. Country Verifier Certification Authority Certificate[79] to Country Verifier Certification Authority[80].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/ Date	The TSF shall restrict the ability to modify the Current Date[81]to 1. Country Verifier Certification Authority, 2. Document Verifier 3. domestic Extended Inspection System[82].

[77] [assignment: *list of TSF data*]

[78] [assignment: *the authorized identified roles*]

[79] [assignment: *list of TSF data*]

[80] [assignment: *the authorized identified roles*]

[81] [assignment: *list of TSF data*]

[82] [assignment: *the authorized identified roles*]

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

FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write[83]

Hierarchical to: No other components.

FMT_MTD.1.1/KEY_WRITE	The TSF shall restrict the ability to write[84] the Document Basic Access Keys **and the Active Authentication Keys**[85] to the Personalization Agent[86].

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

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

Hierarchical to: No other components.

FMT_MTD.1.1/CAPK	The TSF shall restrict the ability to *load*[87] the Chip Authentication Private Key to *the Personalization Agent*[88].

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

.

FMT_MTD.1/KEY_READ Management of TSF data – Key Read[89]

Hierarchical to: No other components.

[83] The bold text below has been added to allow the use of active authentication.

[84] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[85] [assignment: *list of TSF data*]

[86] [assignment: *the authorized identified roles*]

[87] [selection: *create, load*]

[88] [assignment: *the authorized identified roles*]

[89] The bold text below has been added to allow the use of active authentication.

FMT_MTD.1.1/KEY_READ The TSF shall restrict the ability to read[90] the

1. Document Basic Access Keys,
2. Chip Authentication Private Key,
3. **Active Authentication Private Key,**
4. Personalization Agent Keys[91]

to none[92].

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

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

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

Dependencies: ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

Refinement: The certificate chain is valid at the Current Date 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.

[90] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]

[91] [assignment: *list of TSF data*]

[92] [assignment: *the authorized identified roles*]

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.

6.1.6 Protection of the Security Functions

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

The TOE shall meet the requirement “TOE Emanation (FPT_EMSEC.1)” as specified below. For the extended components definition refer to [PP] chapter 4.

FPT_EMSEC.1 TOE Emanation[93]

Hierarchical to: No other components.

FPT_EMSEC.1.1	The TOE shall not emit *variations in power consumption or timing during command execution*[94] in excess of *non-useful information*[95] enabling access to Personalization Agent Authentication Key, **Active Authentication Private Key,** and Chip Authentication Private Keys [96] and *none*[97]

[93] The bold text below has been added to allow the use of active authentication.

[94] [*assignment: types of emissions*]

[95] [assignment: *specified limits*]

[96] [assignment: *list of types of TSF data*]

[97] [assignment: *list of types of user data*]

FPT_EMSEC.1.2	The TSF shall ensure any users[98] are unable to use the following interface smart card circuit contacts[99] to gain access to Personalization Agent Authentication Key, **Active Authentication Private Key,** and Chip Authentication Private Keys[100] and *none*[101].

Dependencies: No other components.

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.

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: (1) exposure to operating conditions where therefore a malfunction could occur, (2) failure detected by TSF according to FPT_TST.1[102].

Dependencies: ADV_SPM.1 Informal TOE security policy model

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.

FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up*[103] to demonstrate the correct operation of the TSF.

[98] [assignment: *type of users*]

[99] [assignment: *type of connection*]

[100] [assignment: *list of types of TSF data*]

[101] [assignment: *list of types of user data*]

[102] [assignment: *list of types of failures in the TSF*]

FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

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.

FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[104] to the TSF[105] by responding automatically such that the SFRs are always enforced.

Dependencies: No dependencies.

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

6.2 Security Assurance Requirements for the TOE

The security assurance requirements (SAR) for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) augmented by the following components ALC_DVS.2 and AVA_VAN.5.

The following table lists all SARs for the evaluation of the TOE:

Assurance class	Assurance component	Denotation
Development	ADV_ARC.1	Security architecture description

[103] *[selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions]*

[104] [assignment: *physical tampering scenarios*]

[105] [assignment: *list of TSF devices/elements*]

Assurance class	Assurance component	Denotation
	ADV_COMP.1	Design compliance with the platform certification report, guidance and [ETR_COMP]
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_COMP.1	Integration of the application into the underlying platform and Consistency check for delivery and acceptance procedures
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Tools and techniques – Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_COMP.1	Consistency of Security Target

Assurance class	Assurance component	Denotation
	ASE_ ECD.1	Extended components definition
	ASE_INT.1	Security objectives
	ASE_OBJ.2	PP claims
	ASE_REQ.2	IT security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COMP.1	Composite product functional testing
	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Depth – Testing:high-leve design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_COMP.1	Composite product vulnerability assessment
	AVA_VAN.5	Advanced methodical vulnerability analysis

Table 1: Security Assurance Requirements

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 the assurance that the TOE is shown to be highly resistant to penetration attacks to meet the security objectives OT.Prot_Inf_Leak, OT.Prot_Phys-Tamper and OT.Prot_Malfunction.

The Assurance Requirements for the selected level EAL 4 augmented are described in the Common Criteria for IT Security Evaluation documents. They are not listed in detail here.

7 TOE Summary Specification

As described in the TOE description (see chapt. 1.4) the TOE provides security features which can be associated into following groups:

- Identification and Authentication mechanisms
- Cryptographic functions support
- Access control /Storage and protection of logical MRTD data
- Secure messaging
- Security and Life-cycle management

Moreover the TOE will protect itself against interference, logical tampering and bypass.

The security functionality of the TOE respectively the Sagem Identification EAC ePassport applet will be externally available to the user by APDU commands according to the access conditions specified by the according policies considering the life cycle state, user role and security state.

The following overview shows how these features satisfy the security functional requirements specified in chapt. 6.1.

SF.I&A Identification and Authentication

include the mechanisms for

- Basic Access Control Authentication mechanism
- Chip Authentication
- Terminal Authentication Protocol
- Authentication of the Personalization Agent with the personalization key set

Authentication mechanisms The different authentication mechanisms are supported by according APDU commands and parameters using the cryptographic functions provided by the platform. The authentication mechanisms are enforced by protocols and APDU methods as specified in the functional specification.
1. Symmetric Basic Access Control Authentication Mechanism used by the Basic Inspection System knowing the Document Basic Access Keys (printed on the passport)
• FIA_UID.1 Timing of Identification • FIA_UAU.1 Timing of Authentication • FIA_AFL.1 Authentication Failure Handling • FIA_UAU.4/MRTD Single-use authentication of the Terminal by the TOE

• FIA_UAU.5/MRTD Multiple authentication mechanisms • FIA_UAU.6/MRTD Re-authenticating of Terminal by the TOE • FMT_SMR.1 Security Roles
2. Chip Authentication of the MRTD's chip. This protocol provides evidence of the MRTD's chip authenticity and prevents data traces described in [9303], Volume 2, Appendix 7 to Section IV, par. A7.3.3. It is used by a General Inspection System, an enhanced Basic Inspection System.
The implementation of Chip authentication contributes to • FIA_API.1/CAP Authentication Proof of Identity – MRTD • FIA_UAU.6/MRTD Re-authenticating of Terminal by the TOE • FMT_SMR.1 Security Roles
3. Terminal Authentication for Extended Access Control uses the secure messaging established by the Chip Authentication Mechanism to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Domestic and foreign Extended Inspection Systems have the certificates (provided by the Country Verifier Certification Authority and Document Verifier) to use Terminal Authentication.
• FIA_UAU.5/MRTD Multiple authentication mechanisms • FMT_MTD.3 Secure TSF data • FMT_SMR.1 Security Roles
4. Symmetric Authentication of the Personalization Agent using the according keys written to the TOE by the Manufacturer during pre-personalization.
• FIA_UAU.5/MRTD Multiple authentication mechanisms • FIA_UAU.4/MRTD Single-use authentication of the Terminal by the TOE • FMT_SMR.1 Security Roles
5. Active Authentication of the the MRTD's chip. This protocol provides evidence of the MRTD's chip authenticity as described in [9303]. It is used by a Active Authentication System, an enhanced Basic, Generic or Extended Inspection System.
• FIA_API.1/AA Authentication Proof of Identity – MRTD • FMT_SMR.1 Security Roles

SF.CF Cryptographic functions support

Following functionality is provided, mostly by the platform:

1. 3DES (112 bit keys) for en-/decryption (CBC and ECB) and signature (MAC) generation and verification, all provided by the platform.
• FCS_COP.1/TDES_MRTD Cryptographic operation – Encryption / Decryption Triple DES • FCS_COP.1/MAC_MRTD Cryptographic operation – Retail MAC

2. SHA-1, SHA-224, and SHA-256 hash algorithm, provided by the platform.
• FCS_COP.1/SHA_MRTD Cryptographic operation – Hash for Key Derivation by MRTD and according the application in paragraph 6.1.2.1 in this ST: • The TOE implements the hash function SHA-1 for the cryptographic primitive to derive the keys for secure messaging from the shared secrets of the Basic Access Control Authentication Mechanism (cf. [9303], Volume 2, Appendix 5 to Section IV. par. A5.1). • The Chip Authentication Protocol uses SHA-1 (cf. [TG_EAC], Annex A.1.1). • The TOE implements additional hash functions SHA-224, and SHA-256 for the Terminal Authentication Protocol (cf. [TG_EAC], Annex A.2.2 for details).
3. ECDSA digital signature verification according to [ISO 15946-2] with key lengths 224 and 256 bits, provided by the platform
• FCS_COP.1/SIG_VER Cryptographic operation – Signature verification by MRTD
4. Diffie-Hellman key agreement with EC over GF(p) and cryptographic key sizes from 224 and 256 bit according to [ANSI X9.63], provided by the platform
• FCS_CKM.1/DH_MRTD Cryptographic key generation – Diffie-Hellman Keys by the TOE
5. Destruction of cryptographic keys: A special javacard.security method of the JCOP platform is used. The transient keys will be reset by the JCOP platform if a deselect of the DF or a reset occurs in an authenticated phase of the TOE
• FCS_CKM.4/MRTD Cryptographic key destruction – MRTD The TOE will destroy the BAC Session Keys (i) after detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol. The TOE will destroy the Chip Authentication Session Keys after detection of an error in a received command by verification of the MAC. The TOE will clear the memory area of any session keys before starting the communication with the terminal in a new power-on-session.
6. Cryptographic key generation according to the Document Basic Access Key Derivation Algorithm and a key size of 112.
• FCS_CKM.1/KDF_MRTD Cryptographic key generation – Key Derivation Function by the MRTD
7. RSA digital signature generation for Active Authentication with key sizes of 1280, 1536 and 1792 Bit according to [ISO 9796-2] and [SHA-1 digest], provided by the platform
• FCS_COP.1/RSA Cryptographic operation – RSA Signature
8. Random number generation according to class K3, of AIS 20 [AIS20], provided by the platform

- FCS_RND.1/MRTD Quality metric for random numbers

SF.ILTB Protection against interference, logical tampering and bypass

1. Security domains are supported by the JavaCard platform used by the TOE underlying platform JCOP v. 2.4.1. The JCOP platform provides protection against physical attack and performs self tests as described in [JCOP_ST].

The JCOP platform protects the TOE against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

The Sagem Identification EAC ePassport Applet uses transient memory where a hardware reset should revert the Sagem Identification EAC ePassport Applet to an unauthenticated state.

- FPT_FLS.1 Failure with preservation of secure state
- FPT_TST.1 TSF testing
- FPT_PHP.3 Resistance to physical attack

SF.AC Access control / Storage and protection of logical MRTD data

Following functionality is provided including access control to MRTD data:

1. The TOE implements the subjects, objects, security attributes and rules according to the security attribute based access control. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification.

This functionality contributes to

- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_UIT.1/MRTD Data exchange integrity – MRTD
- FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD

SF.SM Secure Messaging

Following functionality is provided, mostly by the platform:

1. Secure messaging in ENC_MAC mode according to the Diffie-Hellman Primitive established by the Chip Authentication Mechanism. This functionality is based on SF.CF.

The functionality contributes to

- FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE
- FDP_UCT.1/MRTD Basic data exchange confidentiality - MRTD
- FDP_UIT.1/MRTD Data exchange integrity - MRTD

2. The Retail MAC is part of every APDU command/response when secure messaging is active for Basic Access Control. Re-authentication is performed by the mandatory MAC in secure messaging.
• FIA_UAU.6/MRTD Re-authenticating – Re-authenticating of Terminal by the TOE

SF.LCM Security and life cycle management

Following functionality is provided:

Management of phases and roles 1. The manufacturing phase is split up by the TOE into initialization and pre-personalization sub-phases. The initialization and pre-personalisation functionality is supported by both the JCOP platform and the Sagem Identification EAC ePassport Applet. Initialization and pre-personalization are part of the JCOP platform TOE preparation and will be performed according to the JCOP Administrator and User Guidance. Additional pre-personalisation steps are performed according to ALC_LCD of the Sagem Identification EAC ePassport.
• FMT_SMF.1 Specification of Management Functions (Initialization part) • FMT_SMR.1.1 Security roles (Manufacturer) • FMT_MTD.1/INI_ENA Management of TSF data – Writing of Initialization Data and Pre-personalization Data • FMT_MTD.1/INI_DIS Management of TSF data – Disabling of Read Access to Initialization Data and Pre-personalization Data
2. Personalization and Configuration of the Sagem Identification EAC ePassport Applet is performed using the commands available in the personalization phase. Writing of Initialization data of the JCOP platform is restricted to the Manufacturer by the Transport Key and the Pre-Personalization Key Set. Special APDU commands are used to write the initial Country Verifier Certification Authority Certificate's CAR, the Document Number, the initial Current Date, Active Authentication keys, Chip authentication keys and BAC keys to the TOE. These commands are only available for Authenticated Personalization Agent in the Personalization Phase.
• FMT_SMF.1 Specification of Management Functions (Personalization and Configuration part) • FMT_SMR.1.1 Security roles (Personalization Agent) • FMT_MTD.1/CVCA_INI Management of TSF data – Initialization of CVCA Certificate and Current Date • FMT_MTD.1/KEY_WRITE Management of TSF data – Key Write • FMT_MTD.1/CAPK Management of TSF data – Chip Authentication Private Key • FDP_ITC.1 Import of user data without security attributes
3. Management of TSF-Data can only be done after successful Terminal Authentication. Updating the

Country Verifier Certification Authority Public Key and Certificate is restricted to the *Country Verifier Certification Authority.* Modifying the Current Date is restricted to the *Country Verifier Certification Authority,* the *Document Verifier and* the *domestic Extended Inspection System.*
• FMT_SMF.1 Specification of Management Functions (Configuration part) • FMT_SMR.1 Security roles (Personalization Agent) • FMT_MTD.1/CVCA_UPD Management of TSF data – Country Verifier Certification Authority • FMT_MTD.1/DATE Current date
4. The test features of the JCOP platform are protected by ways described in JCOP platform. The Sagem Identification EAC ePassport Applet will not have any test features implemented.
The security management support functionality contributes to • FMT_LIM.1 Limited capabilities • FMT_LIM.2 Limited availability
6. The Document Basic Access Keys, the Chip Authentication Private Key, the Active Authentication Private Key, and the Personalization Agent Keys are protected from disclosure. The Sagem Identification EAC Applet only stores keys in Java Card specified Key structures, which are protected by JCOP platform.
• FMT_MTD.1/KEY_READ Management of TSF data – Key Read • FPT_EMSEC.1 TOE Emanation
7. Functionality provided by the JCOP platform will be used to store the chip identification data.
• FAU_SAS.1 Audit storage

8 Annex

8.1 Glossary

Term	Definition
Active Authentication	Security mechanism defined in [9303]. Option by which means the MTRD's chip proves and the inspection system verifies the identity and authenticity of the MTRD's chip as part of a genuine MRTD issued by a known State of organization.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE (cf. CC part 1, section B.2.7).
Audit records	Write-only-once non-volatile memory area of the MRTDs chip to store the Initialization Data and Pre-personalization Data.
Authenticity	Ability to confirm the MRTD and its data elements on the MRTD's chip were created by the issuing State or Organization
Basic Access Control	Security mechanism defined in [9303] by which means the MTRD's chip proves and the inspection system protect their communication by means of secure messaging with Basic Access Keys (see there).
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates themselves to the MRTD's chip using the Document Basic Access Keys drawn form printed MRZ data for reading the logical MRTD.
Biographical data (biodata).	The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book or on a travel card or visa. [0]
biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) digital portrait and (ii) optional biometric reference data.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [0]
Country Signing CA Certificate (C_{CSCA})	Self-signed certificate of the Country Signing CA Public Key (KPuCSCA) issued by CSCA stored in the inspection system.
Document Basic Access Keys	Pair of symmetric Triple-DES keys used for secure messaging with encryption (key KENC) and message authentication (key KMAC) of data transmitted between the MRTD's chip and the inspection system [9303]. It is drawn from the printed MRZ of the passport book to authenticate an entity able to read the printed MRZ of the passport book.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the MRTD's chip. It may carry the Document Signer Certificate (CDS). [9303]

Term	Definition
Eavesdropper	A threat agent with low attack potential reading the communication between the MRTD's chip and the inspection system to gain the data on the MRTD's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [9303]
Extended Access Control	Security mechanism identified in [9303] by which means the MTRD's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging. The Personalization Agent may use the same mechanism to authenticate themselves with Personalization Agent Authentication Private Key and to get write and read access to the logical MRTD and TSF data.
Extended Inspection System (EIS)	A role of a terminal as part of an inspection system which is in addition to Basic Inspection System authorized by the issuing State or Organization to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all MRTDs. [9303]
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document.
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [9303]
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as MRTD's material (IC identification data).

Term	Definition
Inspection	The act of a State examining an MRTD presented to it by a traveller (the MRTD holder) and verifying its authenticity. [9303]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an MRTD presented by the traveller and verifying its authenticity and (ii) verifying the traveller as MRTD holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The MRTD's chip is a integrated circuit.
Integrity	Ability to confirm the MRTD and its data elements on the MRTD's chip have not been altered from that created by the issuing State or Organization
Issuing Organization	Organization authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [9303]]
Issuing State	The Country issuing the MRTD. [9303]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [9303]. The capacity expansion technology used is the MRTD's chip.
Logical MRTD	Data of the MRTD holder stored according to the Logical Data Structure [9303] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) (1) personal data of the MRTD holder (2) the digital Machine Readable Zone Data (digital MRZ data, DG1), (3) the digitized portraits (DG2), (4) the biometric reference data of finger(s) (DG3) or iris image(s) (DG4) or both and (5) the other data according to LDS (DG5 to DG16).
Logical travel document	Data stored according to the Logical Data Structure as specified by ICAO in the contactless integrated circuit including (but not limited to) (1) data contained in the machine-readable zone (mandatory), (2) digitized photographic image (mandatory) and (3) fingerprint image(s) and/or iris image(s) (optional).
Machine readable travel document (MRTD)	Official document issued by a State or Organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [9303]
Machine readable visa (MRV):	A visa or, where appropriate, an entry clearance (hereinafter collectively referred to as visas) conforming to the specifications contained herein, formulated to improve facilitation and enhance security for the visa holder. Contains mandatory visual (eye readable) data and a separate mandatory data summary capable of being machine read. The MRV is normally a label which is attached to a visa page in a passport. [9303]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the MRTD or MRP Data Page or, in the case of the TD1, the back of the MRTD, containing mandatory and optional data for machine reading using OCR methods. [9303]

Term	Definition
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [0]
MRTD application	Non-executable data defining the functionality of the operating system on the IC as the MRTD's chip. It includes - the file structure implementing the LDS [9303] , - the definition of the User Data, but does not include the User Data itself (i.e. content of DG1 to DG13 and DG 16) and - the TSF Data including the definition the authentication data but except the authentication data itself.
MRTD Basic Access Control	Mutual authentication protocol followed by secure messaging between the inspection system and the MRTD's chip based on MRZ information as key seed and access condition to data stored on MRTD's chip according to LDS.
MRTD holder	The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.
MRTD's Chip	A contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO, [9303].
MRTD's chip Embedded Software	Software embedded in a MRTD's chip and not being developed by the IC Designer. The MRTD's chip Embedded Software is designed in Phase 1 and embedded into the MRTD's chip in Phase 2 of the TOE life-cycle.
Optional biometric reference data	Data stored for biometric authentication of the MRTD holder in the MRTD's chip as (i) encoded finger image(s) (DG3) or (ii) encoded iris image(s) (DG4) or (iii) both. Note that the European commission decided to use only finger print and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Personalization	The process by which the portrait, signature and biographical data are applied to the document.
Personalization Agent	The agent acting on the behalf of the issuing State or organisation to personalize the MRTD for the holder by (i) establishing the identity the holder for the biographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e. the portrait, the encoded finger image(s) or (ii) the encoded iris image(s) and (iii) writing these data on the physical and logical MRTD for the holder.
Personalization Agent Authentication Information	TSF data used for authentication proof and verification of the Personalization Agent.
Personalization Agent Authentication Key	Symmetric cryptographic key used (i) by the Personalization Agent to prove their identity and get access to the logical MRTD according to the SFR FIA_UAU.4/BT FIA_UAU.6/BT and FIA_API.1/SYM_PT and (ii) by the MRTD's chip to verify the authentication attempt of a terminal as Personalization Agent according to the SFR FIA_UAU.4/MRTD, FIA_UAU.5/MRTD and

Term	Definition
	FIA_UAU.6/MRTD.
Physical travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) (1) biographical data, (2) data of the machine-readable zone, (3) photographic image and (4) other data.
Pre-personalization Data	Any data that is injected into the non-volatile memory of the TOE by the MRTD Manufacturer (Phase 2) for traceability of non-personalized MRTD's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalization Agent Key Pair.
Receiving State	The Country to which the MRTD holder is applying for entry. [9303]
reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [0]
secure messaging in encrypted mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4
Skimming	Imitation of the inspection system to read the logical MRTD or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Terminal Authorization	Intersection of the Certificate Holder Authorizations of the Inspection System Certificate, the Document Verifier Certificate and Country Verifier Certification Authority which shall be valid for the Current Date.
Travel document	A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel. [9303]
Traveller	Person presenting the MRTD to the inspection system and claiming the identity of the MRTD holder.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (CC part 1).
Unpersonalized MRTD	MRTD material prepared to produce an personalized MRTD containing an initialised and pre-personalized MRTD's chip.
User data	Data created by and for the user, that does not affect the operation of the TSF (CC part 1).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. [9303]

Term	Definition
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.
Country Verifying Certification Authority	The country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. It enforces the Privacy policy of the issuing Country or Organization in respect to the protection of sensitive biometric reference data stored in the MRTD. It is
Document Verifier	Certification authority creating the Inspection System Certificates and managing the authorization of the Extended Inspection Systems for the sensitive data of the MRTD in the limits provided by the issuing States or Organizations
General Inspection System	A Basic Inspection System which implements sensitively the Chip Authentication Mechanism.
Extended Inspection System	A General Inspection System which (i) implements the Chip Authentication Mechanism, (ii) implements the Terminal Authentication Protocol and (iii) is authorized by the issuing State or Organization through the Document Verifier of the receiving State to read the sensitive biometric reference data.
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
Certificate chain	Hierarchical sequence of Inspection System Certificate (lowest level), Document Verifier Certificate and Country Verifying Certification Authority Certificates (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level. The Country Verifying Certification Authority Certificate is signed with the private key corresponding to the public key it contains (self-signed certificate).

8.2 Abbreviations

CC	Common Criteria, see [CC]
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
SEF	Security Enforcing Functions
SOF	Strength Of Function
TOE	Target of Evaluation
TSF	TOE Security Functions

8.3 References

[PP] Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0026, Version 1.2, 19 November 2007

[CC-1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, September 2006, CCMB-2006-09-001

[CC-2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 2, September 2007, CCMB-2007-09-002

[CC-3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 2, September 2007, CCMB-2007-09-003

[CC-4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCMB-2007-09-004

[9303] ICAO Doc 9303, Part 1, “Machine Readable Passports”, sixth edition, 2006, and Part 3, “Machine Readable Official Travel Documents”, third edition, 2008

[SSMR] Annex to Section III Security Standards for Machine Readable Travel Documents, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[PP_IC] PP conformant to Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[FIPS46] Federal Information Processing Standards Publication FIPS PUB 46-3, Data Encryption Standard (DES), Reaffirmed 1999 October 25, U.S. department of Commerce/National Institute of Standards and Technology

[TG_EAC] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[TG_ECC] Technical Guideline: Elliptic Curve Cryptography according to ISO 15946.TR-ECC, BSI 2006.

[ISO15946-1] ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2002.

[ISO15946-2] ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.

[ISO15946-3] ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002

[ISO 9796-2] ISO/IEC 9796-2: 2002, Information Technology — Security Techniques — Digital Signature Schemes giving message recovery — Part 2: Integer factorization based mechanisms.

[SHA-1 digest] FIPS PUB 180-1, „Secure Hash Standard”, Federal Information Processing Standards Publication, 17 April 1995.

[ANSI X9.63] ANSI X9.62:2005, “Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 7 January 1999.

[AIII] ANNEX to Section III SECURITY STANDARDS FOR MACHINE READABLE TRAVEL DOCUMENTS, Excerpts from ICAO Doc 9303, Part 1 - Machine Readable Passports, Fifth Edition – 2003

[JCOP_ST] NXP J3A080 v2.4.1 Secure Smart Card Controller Security Target

[AIS20] Application Notes and Interpretation of the Scheme (AIS) AIS 20, Version 1, Date: 2 December, 1999, Status: Mandatory, Subject: Functionality classes and evaluation methodology for, deterministic random number generators, Publisher: Certification body of the BSI, Section II 2, as part of the certification scheme

[ETR_COMP] ETR for Composition, V8: NXP J3A080 and J2A080 Secure Smart Card Controller Revision 2, 27.10.2010, TÜVIT GmbH