# XSmart ePassport V1.0

# Security Target Lite V1.0

| | |
|---|---|
| Doc ID | C1-UID-ST-ENG-0808-20.doc |
| Data | 2008.08.08 |
| Auth | Dong-Go Jang |

# [ Contents ]

# [ List of Table ]

# [ List of Figure]

# 1. SecurityTarget Introduction

This chapter describes the information of Security Target.

## 1.1. SecurityTarget Identification

| | |
|---|---|
| Title | XSmart ePassport V1.0 SecurityTarget V1.4 (2008.08.08) |
| Author | LG CNS |
| Evaluation Standard | Common Criteria Version V2.3 |
| Evaluation Assurance Level | EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) |
| Protection Profile | ePassport Protection Profile V1.0 (KECS-PP-0084-2008) |
| Product | XSmart V2.0 (2008.01.18) |
| TOE | XSmart ePassport V1.0 (2008.01.18) |
| IC Chip | SLE66CLX800PE |
| Keywords | ePassport, MRTD, ICAO, Smart Card, Java Card, GlobalPlatform |

## 1.2. SecurityTarget Overview

The aim of this document is to describe the Security Target for XSmart ePassport V1.0 for Passport Booklet IC. XSmart V2.0 is intended to be used to identify and verify the traveler as Passport Booklet IC.

TOE of XSmart V2.0 consists of the ePassport application and the operating system ('Open Platform') excluding the underlying IC chip.

Operating system fulfils the requirements specified in Java Card 2.2.1 Runtime Environment Specification [JCRE], Java Card 2.2.1 Virtual Machine Specification [JCVM], Java Card 2.2.1 Application Programming Interfaces [JCAPI] (hereinafter referred to as "Java Spec"), GlobalPlatform Card Specification 2.1.1[GPCS] (hereinafter referred to as "GP Spec") and Visa GlobalPlatform 2.1.1 Card Implementation Requirements [VGP] - Configuration 2 (hereinafter referred to as "VGP Spec").

ePassport application is the java applet programmed according to the ICAO Machine Readable Travel Documents, Doc 9303 Part 1 Volume 2[MRTD] and providing Extended Access Control according to Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.1 [EAC].

TOE is implemented on the Infineon Technology SLE66CLX800PE which is certified according to CC EAL5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4).

TOE provides SCP02 Security Mechanism required in [GPCS] for protecting ePassport user data in personalization phase and BAC Security Mechanism and EAC Security Mechanism in Usage phase.
Also, This TOE may provide Active Authentication as defined [MRTD] for detecting cloning of ePassport.

This SecurityTarget considers TOE Security Environment, Security Objects and Security Requirement contained in ePassport Protection Profile V1.0 (ePassport Protection Profile V1.0) and Security Function and Security Assurance Requirements fulfilled Security Requirement and TOE description.

## 1.3. Conformance Claim

This SecurityTarget claims conformance to.

- ePassport Protection Profile V1.0 (KECS-PP-0084-2008)
  EAL4+ Assurance Level (ADV_IMP.2, ATE_DPT.2, AVA_VLA.3)

This SecurityTarget claims conformance to

- Common Criteria for Information Technology Security Evaluation, part 2 : Security functional requirements, Version 2.3, Aug. 2005, CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation, part 3 : Security assurance requirements, Version 2.3, Aug. 2005, CCMB-2005-08-003
- Package Conformant to EAL4 augmented with ADV_IMP2, ATE_DPT2 and AVA_VLA.3

This Security Function has the level of strength SOF-high.

## 1.4. Conventions

The notation, formatting and conventions used in this Protection Profile are consistent with the Common Criteria for Information Technology Security Evaluation (hereafter referred to as "CC").
The CC allows several operations to be performed on functional requirements; assignment, iteration, refinement and selection. Each of these operations is used in this SecurityTarget.

**Assignment**
It is used to assign specific values to unspecified parameters (e.g. : password length). The result of assignment is indicated in square brackets, i.e., [ assignment_Value ].

**Iteration**
It is used when a component is repeated with varying operations. The result of iteration is marked by iteration number in parenthesis following the component identifier, i.e., (Iteration No.).

**Refinement**
It is used to add detail to a requirement, and thus further restricts a requirement. The result of refinement is shown in **bold text.**

**Selection**
It is used to select one or more options provided by the CC in stating a requirement. The result of selection is shown as *underlined and italicized.*

## 1.5. SecurityTarget Organization

Section 1 provides the introductory material for SecurityTarget.

Section 2 defines TOE and describes the IT environment on which the TOE depends.

Section 3 describes the TOE Security Environment and includes security problems of the TOE and its IT Environment from such as Assumptions, Threats, and

Organizational Security Policies.

Section 4 defines the Security Objects for the TOE and its IT environment to counter to identified threats and support the assumptions and organizational security policies.

Section 5 contains the IT Security Requirement including the functional and assurance requirement intended to satisfy security objectives.

Section 6 describes TOE Summary including the functional and assurance requirement intended to satisfy TOE Security Requirements.

Section 7 describes SecurityTarget compliant with Protection Profile

Section 8 provides a rationale to demonstrate that the security objectives for the TOE and its IT environment address the defined security problems appropriately and the IT security requirements are adequate and complete to satisfy the security objectives.

# 2. TOE Description

This chapter describes a description of TOE, TOE Operational Environment and TOE Scope

## 2.1. TOE Overview

XSmart V2.0 is ePassport IC chip which consists of the ePassport application and the operating system implemented on the Infineon Technology SLE66CLX800PE which is certified according to CC EAL5+. XSmart V2.0 is intended to be used to identify and verify the traveler as Passport Booklet IC.

TOE of XSmart V2.0 consists of the ePassport application and the operating system ('Open Platform') excluding the underlying IC chip.
TOE manages ePassport application data ( encryption key for authentication and secure message ) and user identification data ( personal data and biometric data ) and TOE authenticates Personalization Agent and Inspection System for access control ePassport user data.

## 2.2. TOE Operational Environment

### 2.2.1. IC Chip

IC chip of TOE is certified according to CC EAL5+ and consists of IC chip hardware, firmware and crypto library.

### 2.2.2. ePassport

XSmart V2.0 is the passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO).

This standard is comprised of physical part which defines visual printing(personal information, portrait, passport number, MRZ) examined by naked eye and OCR(Optical Character Recognition) and logical part which defines logical data structure using IC chip.

The contactless IC chip used in the ePassport is referred to as MRTD chip. The MRTD chip is loaded with the MRTD application and IC chip operating system(COS) to support IT and information security technology for electronic storage, processing and handling of the ePassport identity data.

The ePassport IC chip elements consist of CPU, co-processor, I/O port, memory (RAM, ROM, EEPROM) and contactless interface, etc.

Figure1 shows the physical configuration of the ePassport.

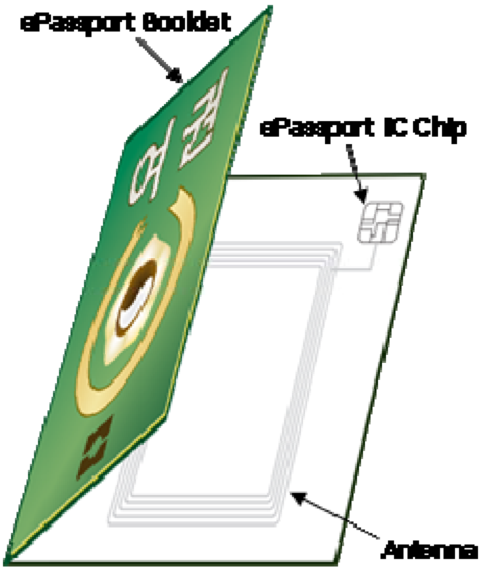


**Figure1 Physical Configuration of the ePassport**

The MRTD consists of the user data, such as passport holder information, portrait, fingerprint and iris and the TSF data required in the security mechanism.

### 2.2.3. ePassport System

The ePassport holder requests for issuing of the ePassport and receives the ePassport issued according to the Issuing Policy of the ePassport. The ePassport holder presents the ePassport to an immigration officer so that the ePassport is inspected at immigration control. For immigration control, the ePassport is verified by an immigration officer or an automatic Inspection System according to the ePassport immigration control policy for each country.

The Reception organization collects personal and biometric data of the ePassport holder, checks identity of the ePassport holder through cooperation with the related organizations, such as National Police Agency, and sends to the personalization agent for issuing of the ePassport with these data collected.

The Personalization agent generates document security object ('SOD' hereinafter) by digital signature on the user data (identity and authentication data) and records it in the MRTD chip with the ePassport identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the personalization agent is manufactures and issues the ePassport embedded the MRTD chip to the passport.
Details of data recorded in the ePassport will be described in [Table 3] of 2.2.3 Logical Scope of the TOE.

The Personalization agent generates digital signature key for verifying of forgery and corruption of the user data stored in the MRTD chip. Then, in accordance with the Certification Practice Statement (CPS) of the ePassport PKI System the personalization agent generates, issues and manages CSCA certificate and DS certificate. According to the Issuing Policy of the ePassport, the personalization agent generates digital signature key to verifying access-rights to the biometric data of the ePassport holder in case of supporting EAC security mechanism. Then, the personalization agent generates, issues and manages CVCA certificate, CVCA link certificate and DV certificate. For details related to of the ePassport PKI System and certification practice, such as certification server, key generation devices and the physical procedural security measures, etc., it depends on the Issuing Policy of the ePassport.

The Document verifier generates IS certificate by using CVCA and DV certificates, and then provides these certificates to Inspection System.

Figure2 shows the overall configuration of the ePassport system.

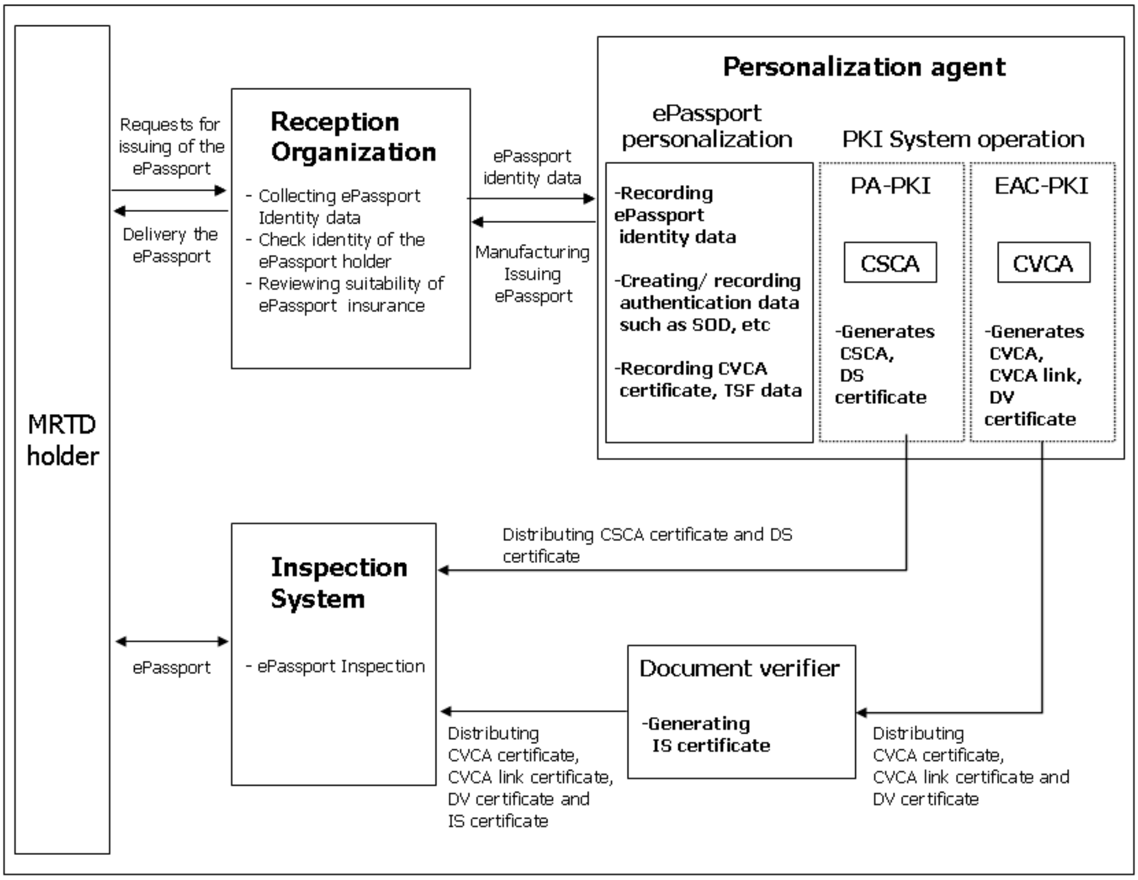

MRTD holder
Requests for issuing of the ePassport
Delivery the ePassport
Reception Organization
- Collecting ePassport Identity data
- Check identity of the ePassport holder
- Reviewing suitability of ePassport insurance
ePassport identity data
Manufacturing Issuing ePassport
Personalization agent
ePassport personalization
PKI System operation
-Recording ePassport identity data
-Creating/ recording authentication data such as SOD, etc
-Recording CVCA certificate, TSF data
PA-PKI
CSCA
-Generates CSCA, DS certificate
EAC-PKI
CVCA
-Generates CVCA, CVCA link, DV certificate
Distributing CSCA certificate and DS certificate
Inspection System
- ePassport Inspection
ePassport
Document verifier
-Generating IS certificate
Distributing CVCA certificate, CVCA link certificate, DV certificate and IS certificate
Distributing CVCA certificate, CVCA link certificate and DV certificate

Figure2 Overall Configuration of the ePassport System

Types of certificates used in the ePassport system are as shown in Table 1 below.

Table 1 Types of Certificates

| Usage | ePassport PKI System | Subject | Certificate |
|---|---|---|---|
| To verify forgery and Corruption of the user data | PA-PKI | CSCA | CSCA certificate |
| | | Personalization agent | DS certificate |
| To verify the access-right of the biometric data of the ePassport holder | EAC-PKI | CVCA | CVCA certificate |
| | | | CVCA link certificate |
| | | Document Verifier | DV certificate |
| | | EAC supporting Inspection System | IS certificate |

Figure3 shows the operational environment of the TOE in the phases of the ePassport Personalization and Operational Use through the relationship with major security functions of TOE and external entities (the Personalization agent, the Inspection System) that interact with TOE.

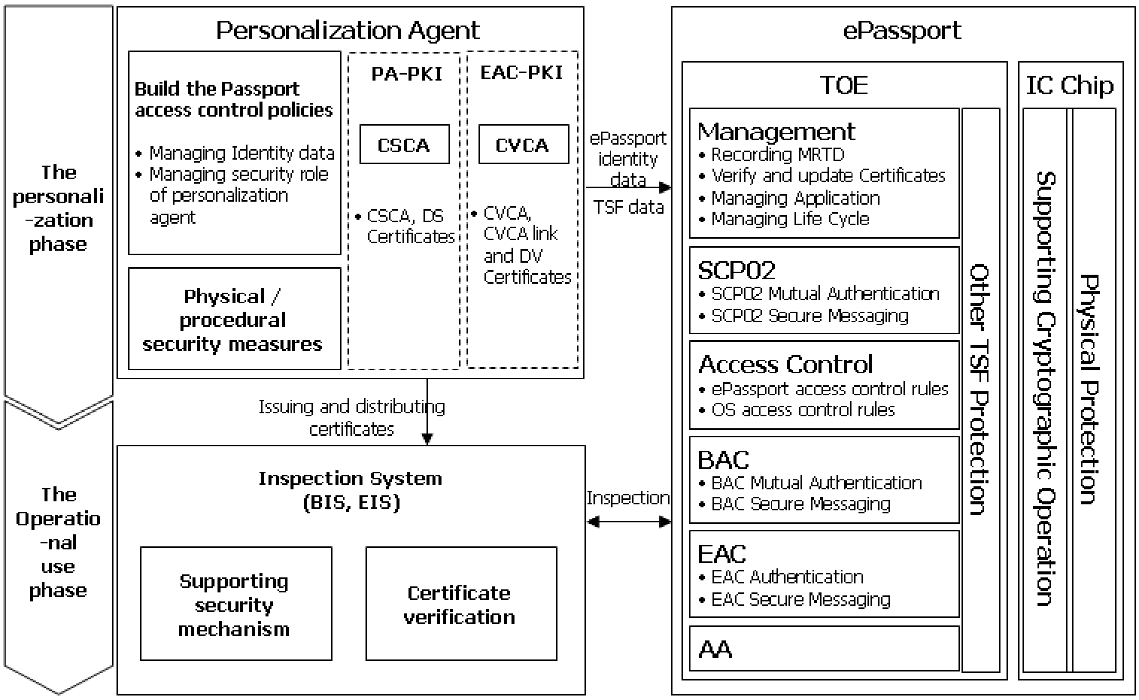

The personali -zation phase
The Operatio -nal use phase
Personalization Agent
Build the Passport access control policies
• Managing Identity data
• Managing security role of personalization agent
Physical / procedural security measures
PA-PKI
CSCA
• CSCA, DS Certificates
EAC-PKI
CVCA
• CVCA, CVCA link and DV Certificates
Issuing and distributing certificates
ePassport identity data
TSF data
Inspection
Inspection System (BIS, EIS)
Supporting security mechanism
Certificate verification
ePassport
TOE
Management
• Recording MRTD
• Verify and update Certificates
• Managing Application
• Managing Life Cycle
SCP02
• SCP02 Mutual Authentication
• SCP02 Secure Messaging
Access Control
• ePassport access control rules
• OS access control rules
BAC
• BAC Mutual Authentication
• BAC Secure Messaging
EAC
• EAC Authentication
• EAC Secure Messaging
AA
Other TSF Protection
IC Chip
Supporting Cryptographic Operation
Physical Protection

**Figure3 TOE Operation Environment**

## 2.3. TOE Scope

This Security Target defines the life cycle of the TOE, such as development, manufacturing, personalization and operational use of the ePassport and defines the TOE environment and physical/ logical scope of the TOE as of the following.

### 2.3.1. Life Cycle and Environment of the TOE

[Table 2] shows the life cycle of the MRTD chip and the TOE. The transmission process in [Table 2] has been omitted. In the life cycle shown in [Table 2], TOE development process corresponds to phase 1 (Development) and phase 2 (Manufacturing), while TOE operational environment corresponds to phase 3 (Personalization) and phase 4 (Operational Use).

**Table 2 Life Cycle of the MRTD Chip and the TOE**

| Phase | Life Cycle of the MRTD Chip | Life Cycle of the TOE |
|---|---|---|
| Phase 1 (Development) | ① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W | |
| | | ② The S/W developer to develop the TOE (COS, MRTD application) by using the IC chip and the Dedicated S/W |
| Phase 2 (Manufacturing) | ③ The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier and | |

| Phase | Life Cycle of the MRTD Chip | Life Cycle of the TOE |
|---|---|---|
| | to produce the IC chip | |
| | | ④ The ePassport manufacturer to create user data storage space according to the LDS format or the ICAO document and to record it in EEPROM<br>⑤ The ePassport manufacturer to record identification and authentication information of the ePassport Personalization agent in the EEPROM<br>⑥ The ePassport manufacturer to embed the IC chip in the passport book |
| Phase 3 (personalization) | | ⑦ The Personalization agent to write the Identification and Authentication information of the Personalization agent at Operating System<br>⑧ The Personalization agent to create SOD by a digital signature on the ePassport identity data<br>⑨ The Personalization agent to record the ePassport identity data, the authentication data (including SOD) and the TSF data in the TOE |
| Phase 4 (Operational Use) | | ⑩ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE |
| Phase 5 (Termination) | | ⑪ The Personalization agent changes state that ePassport is no more use. |

### 2.3.2. Physical Scope of the TOE

The ePassport refers to the passport book and the MRTD chip and the antenna embedded in the cover of the passport book. XSmart V2.0 includes the IC chip operating system, the MRTD application, the MRTD application data and the IC chip elements (IC chip hardware, firmware, ECC crypto library).

Figure4 shows the scope of the TOE.

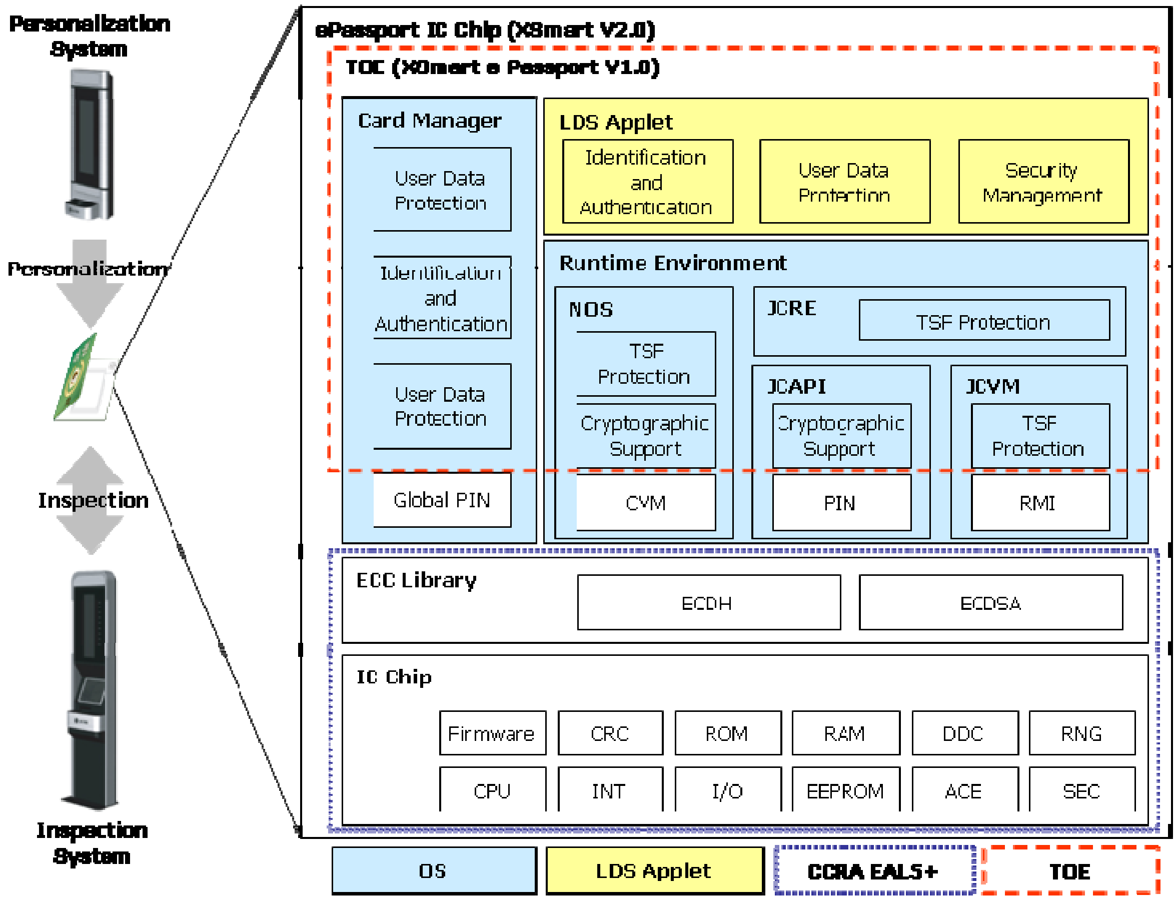


Figure4 Scope of the TOE

**ePassport Applet (LDS Applet)**

The MRTD application is javacard application that implements the function to store and process the ePassport identity data according to LDS (Logical Data Structure) format defined in the ICAO document and security mechanism to securely protect the function. Also, the MRTD application is added the EAC security mechanism by the EAC specifications, because the biometric data of the ePassport holder is included in the ePassport identity data.

The MRTD application data consists of the user data, such as the ePassport identity data, etc., and the TSF data required in the security mechanism.

**Card Manager**

Card Manager implements the function to manage Operating system fulfilled the requirements specified in "GP Spec" and "VGP Spec".

**Runtime Environment**

Runtime Environment consists of the functions of JCRE, JCVM and JCAPI as javacard platform elements defined in "Java Spec". Also, Runtime Environment implements Native OS.

**ECC Library**

ECC library certified CC EAL5+ is not included the scope of TOE, but it is a part of IT environment of TOE as a part of IC chip elements

**IC Chip**

IC chip certified CC EAL5+ consists of IC chip hardware and firmware. Thus, it is a part of IT environment of TOE.

### 2.3.3. Logical Scope of the TOE

The TOE communicates with the Inspection System according to the transmission protocol defined in ISO/IEC 14443-4. The TOE implements the security mechanism defined in the ICAO document and the EAC specifications and provides access control and security management functions. Also, the TOE provides functions of the TSF self-protection, such as the TSF self-testing, preservation of a secure state and domain separation, etc.

Figure5 shows the scope of the TOE.

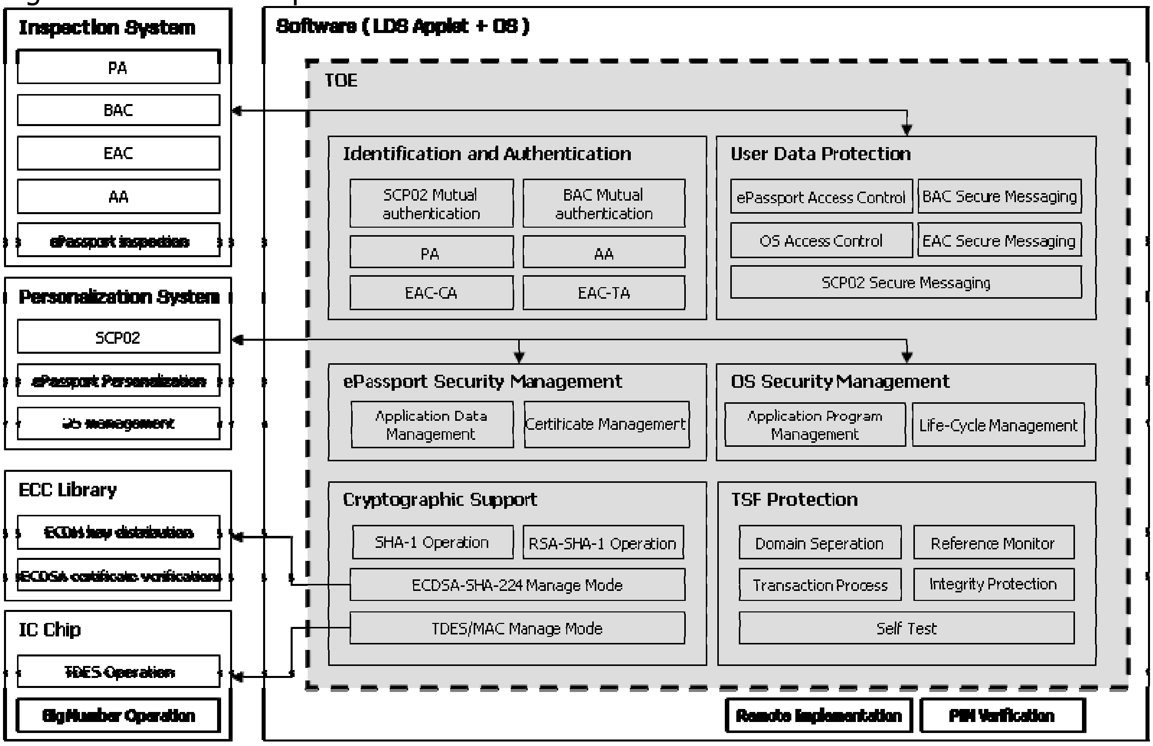


**Figure5 The logical scope of the TOE**

### Asset

In order to protect the TOE assets of [Table 3], the TOE provides security functions, such as the confidentiality, the integrity, the authentication and the access control, etc.

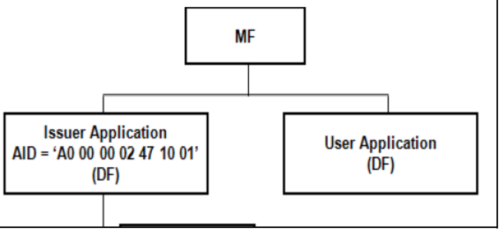
**Table 3 TOE Assets**

| Category | | | Description | Storage Space |
|---|---|---|---|---|
| ePassport User Data | ePassport Identity Data | Personal Data of the ePassport holder | Data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13 and EF.DG16 | EF file |
| | | Biometric Data of the ePassport holder | Data stored in EF.DG3 and EF.DG4 | |
| | ePassport Authentication Data | | SOD, EAC chip authentication public key(EF.DG14), AA chip authentication public key(EF.DG15) and etc. | |

| | | | |
|---|---|---|---|
| | EF.CVCA | In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System | |
| | EF.COM | LDS version info., tag list of DG used, etc. | |
| ePassport TSF Data | EAC Chip Authentication Private Key | In EAC-CA, Chip Private key used by the TOE to demonstrate Not forged MRTD chip | Secure memory |
| | CVCA Certificate | In personalization phase, Root CA Certificate issued in EAC-PKI | |
| | CVCA Digital Signature Verification Key | After personalization phase, CVCA certificate Public key newly created by certificate update | |
| | Current Date | In personalization phase, Date of issuing the ePassport is recorded. However, In operational use phase, the TOE internally updates it as the latest date among issuing dates of CVCA link certificate, DV certificate or Issuing State IS certificate. | |
| | BAC Authentication Key | BAC authentication encryption key, BAC authentication MAC key | |
| | BAC Session Key | BAC session encryption key, BAC session MAC key | Temporary memory |
| | EAC Session Key | EAC session encryption key, EAC session MAC key | |
| OS User Data | Personalization agent Basic Information | Identification Information, Serial Number, Issuing Date of Personalization agent | OS Memory |
| | Personalization agent Authentication Information | SCP02 Mutual Authentication Security Key | |
| | Execution File | Application Execution File Code loaded in the OS | |
| | Application Program | Application Instance installed in the OS | |
| OS TSF Data | GP Registry | Management of OS Data is Installed Application ID, Application Life Cycle State, Application authority | |
| | OS Life Cycle | Life Cycle State Value of OS | |
| | SCP02 Session Key | SCP02 Session Cryptographic Key and MAC Key | Temporary memory |

The LDS in which the user data are stored defines MF, DF and EF file structure. Table 4 shows the content of EF.DG1~EF.DG16 in which parts of the user data are stored.

**Table 4 Content of the LDS in which the User Data are Stored**

| Category | DG | Content | LDS Structure |
|---|---|---|---|
| Detail(s) in MRZ | DG1 | Document(Passport) Type |  |
| | | Issuing State | |
| | | Name (of Holder) | |
| | | Document Number | |
| | | Check Digit(of Doc Number) | |
| | | Nationality | |

| | | | |
|---|---|---|---|
| | | Date of Birth | |
| | | Check Digit(of DOB) | |
| | | Sex | |
| | | Data of Expiry of Valid Until Date | |
| | | Check Digit (of DOE) | |
| | | Composite Check Digit | |
| Biometric Data | DG2 | Encoded face info | |
| | DG3 | Encoded fingerprint info | |
| | DG4 | Encoded iris info (optional) | |
| Others | DG5 | Display Portrait | |
| | DG6 | - | |
| | DG7 | Displayed Signature | |
| | DG8 | - | |
| | DG9 | - | |
| | DG10 | - | |
| | DG11 | Additional Personal Detail(s) | |
| | DG12 | Additional Document Detail(s) | |
| | DG13 | - | |
| | DG14 | EAC Chip Authentication Public Key | |
| | DG15 | AA Chip Authentication Public Key | |
| | DG16 | Person(s) to Notify | |

**Security Mechanism**

The TOE provides security functions such as the confidentiality, the integrity, the access control and the authentication, in order to protect the TSF data and the user data of the ePassport identity data and the ePassport authentication data, etc. These security functions are implemented with the BAC mechanism of the ICAO document and the EAC mechanism of the EAC specifications. Table 5 summarized the ePassport security mechanisms.

**Table 5 ePassport Security Mechanism**

| ePassport Security Mechanism | | | |
|---|---|---|---|
| Security Mechanism | Function | Cryptography | Cryptographic Key/ Certificate Type |
| PA | ePassport User Data Authentication | N/A | N/A |
| BAC | BAC Mutual Authentication | Symmetric key-based entity authentication protocol<br>TDES-CBC<br>SHA-1<br>Retail MAC | BAC Authentication Key (Encryption Key, MAC Key) |

| | | | |
|---|---|---|---|
| | BAC Key Distribution | Symmetric key-based key distribution protocol<br>TDES-CBC<br>SHA-1<br>Retail MAC | BAC Session Key (Encryption Key, MAC Key) |
| | BAC Secure Messaging | ISO Secure Messaging | BAC Session Key (Encryption Key, MAC Key) |
| EAC | EAC-CA | ECDH Key Distribution Protocol | EAC Chip Authentication Public Key<br>EAC Chip Authentication Private Key |
| | EAC Secure Messaging | ISO Secure Messaging | EAC Session Key (Encryption Key, MAC Key) |
| | EAC-TA | ECDSA-SHA-1<br>ECDSA-SHA-224 | CVCA Certificate<br>CVCA Link Certificate<br>DV Certificate<br>IS Certificate |
| AA | ePassport Illegal Copy Verification | ECDSA-SHA-1 | AA Chip Authentication Public Key<br>AA Chip Authentication Private Key |
| SCP02 | SCP02 Mutual Authentication | Secure Channel Protocol 02<br>Full Triple DES MAC<br>TDES-CBC<br>Retail MAC | Personalization Agent Authentication Data<br>SCP02 Session Key |
| | SCP02 Secure Messaging | SCP02 Secure Messaging<br>TDES-CBC<br>Retail MAC | SCP02 Session Key |

**Security Function**

TOE provides the security functions of Identification and Authentication, User Data Protection, Security Management, TSF Protection, and Cryptographic Support.

Identification and Authentication

TOE provides SCP02 Mutual Authentication, BAC Mutual Authentication, EAC-CA, EAC-TA, PA and AA by means of Identification and Authentication.

User Data Protection

TOE provides ePassport/Operating System Access Control and SCP02/BAC/EAC secured communication channel for User Data Protection.

Security Management

TOE restricts only authorized Personalization Agent to manage user of application and operating system, secure properties of ser data and TSF data (session key, authentication key, and GP registry) and define the security management functions.
This Security Function provides security management functions of ePassport and Operating System such as management of application, lifecycle and ePassport data.

TSF Protection

TOE provides the functions for TSF Protection, such as firewall, atomic transaction, clearing sensitive information and reference monitor.

Cryptographic Support

TOE provides the cryptographic support such as Random number generation, Hash generation, Encryption and Decryption, Digital signature key ration, and Digital signature verification.

TOE assures that the external entity can not find out and exploit the cryptographic-related data from physical phenomena (change of current, voltage and electromagnetic, etc.) occurred when the TSF performs cryptographic operations. The TSF provides the means to verify the integrity of encryption key.

# 3. TOE Security Environment

The **TOE** security environment defines assumptions, threats and organizational security policies in order to determine the scope of the expected operation environment of the **TOE**.

## 3.1. Assumptions

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

**A.CERTIFICATE VERIFICATION**

The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically.

The EIS shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA link certificate, the DV certificate and the IS certificate in the EAC-TA.

Application Notes :

The Inspection System shall periodically download CSCA certificate from ICAO-PKD for the Inspection System to verify the certificate chain for the PA

**A.IC Chip**

The IC chip, the underlying platform of the TOE, provides the random number generation and cryptographic operation to support security functions of the TOE. It also detects the TOE's malfunction outside the normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using the probing and reverse engineering analysis.

Application Notes :

To ensure the secure TOE environment, the IC chip shall be SLE66CLX800PE which is a certified product of CCRA EAL5+(SOF-high). The cryptographic operation supported by the IC chip may be provided in the co-processor of the IC chip or cryptographic libraries loaded in the IC chip.

**A.INSPECTION SYSTEM**

The Inspection System shall implement security mechanisms of the PA, the BAC, the EAC, and the AA according to the ICAO document and EAC specifications on the basis of the verifying policy of the ePassport for the ePassport holder.

Also, after session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the BAC session key, the EAC session key and session information, etc.

Application Notes :

The TOE denies the request to access EF.SOD by the Inspection System that failed the BAC mutual authentication.

As the BIS supports the BAC and PA security mechanisms, it obtains the read-rights for the personal and authentication data of the ePassport holder if the BAC mutual authentication using the BAC authentication key succeeds. Then, by establishing the BAC secure messaging with the BAC session key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the BAC. Then, by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder.

As the EIS supports the BAC, EAC and PA security mechanisms, it obtains the read-rights for the personal, authentication and biometric data of the ePassport holder. The EIS, when the BAC mutual authentication and secure messaging succeed, executes the EAC-CA by using the EAC chip authentication public key read in the BAC to verify the genuine TOE. Then, it executes the PA in order to verify the EAC chip authentication public key. When the EAC-CA is succeeded, the BAC secure messaging is ended and the EAC secure messaging with the EAC session key is started, and the EAC-TA that the TOE authenticates the Inspection System is executed. When the EAC-TA is succeeded, the EIS obtains the read-rights for the biometric data of the ePassport holder. Therefore, the EIS is provided the biometric data of the ePassport holder from the TOE

**A.MRZ ENTROPY**
The BAC authentication key seed takes the MRZ entropy to ensure the secure BAC authentication key.

Application Notes :
In order to resistant to the moderate-level threat agent, the entropy for the passport number, date of birth, data of expiry or valid until date and check digit used as BAC authentication key seed among the MRZ in the current technological level shall be at least 56bit.

## 3.2. Threats

The ePassport is used by possession of individuals without physically controlled devices, therefore both logical and physical threats is occurred. The threat agent is an external entity that attempts illegal access to assets protected by the TOE, by using the physical or logical method outside the TOE.

In this protection profile, the IC chip provides functions of physical protection in order to protect the TOE according to the A. IC Chip. Therefore, the physical threat of the IC chip itself by the high-level threat agent is not considered.

Therefore, the threat agent to the TOE has the moderate level of expertise, resources and motivation.

<Threats to the TOE in the Personalization phase>

**T.APPLICATION PROGRAM INTERFERENCE**
The threat agent may attempt access to the user and TSF data by exploiting other application programs loaded in the MRTD chip and may deactivate or bypass security functions of the TOE.

**T.Reuse Issuer Certification**
The threat agent may intercept and reuse transmitting data between TOE and Issuer in the initial process of SCP02 mutual authentication which is issuer certification

mechanism and may bypass SCP02 mutual authentication of the TOE.

Application Notes :
If TOE reuse same SCP02 session key and certification information of issuer each session, they may be vulnerable to ciphertext only attack.

**T.TSF DATA MODIFICATION**
The threat agent may modify the transmitted TSF data when the Personalization agent records TSF data or attempt access to the stored TSF data by using the external interface through the Inspection System.

<BAC-related Threats in the Operational Use phase>

**T.BAC AUTHENTICATION KEY DISCLOSE**
In order to find out the personal data of the ePassport holder, the threat agent may obtain the read-rights of the BAC authentication key located inside the TOE and disclose.

Application Notes :
The BAC authentication key may be generated by Personalization_agent in the Personalization phase or by the TOE in the Operational Use phase.

**T.BAC REPLAY ATTACK**
The threat agent may bypass the BAC mutual authentication by replay after intercepting data transmitted by the TOE and the Inspection System in the initial phase of the BAC mutual authentication.

Application Notes :
The TOE delivers the random number of plaintext to Inspection_System according to 'get_challenge' instruction of the Inspection System in the BAC. Therefore, the threat agent can bypass the BAC mutual authentication by intercepting the random number and response value of the Inspection System and re-transmitting the response value of the Inspection System to the next session. Also, the threat agent may find the transmission data as threat agent can generate the BAC session key after obtaining the BAC authentication key by T. BAC Authentication Key Disclose.

**T.Eavesdropping**
In order to find out the personal data of the ePassport holder, the threat agent may eavesdrop the transmitted data by using the terminal capable of the RF communication.

**T.FORGERY AND CORRIPTION OF PERSONAL DATA**
In order to forge and corrupt the personal data of the ePassport holder stored in the MRTD chip, the threat agent may attempt access to read the user data by using the unauthorized Inspection System.

<EAC-related Threats in the Operational Use phase>

**T.Damage to Biometric Data**
The threat agent may disclose, forge and corrupt the biometric data of the ePassport holder by using terminal capable of the unauthorized RF communication, etc.

Application Notes :
Only the EIS that succeeded the EAC-TA can access the read-rights_the biometric data

of the ePassport holder. Therefore, the threat agent may attempt to obtain the biometric data by using the unauthorized Inspection System and BIS, etc.

**T.EAC-CA BYPASS**

The threat agent may bypass the authentication of the Inspection System so that to go through EAC-CA by using the threat agent generated EAC chip authentication public key.

**T.IS CERTIFICATE FORGERY**

In order to obtain the access-rights the biometric data of the ePassport holder, the threat agent may attempt to bypass the EAC-TA by forging the CVCA link certificate, DV certificate and IS certificate and requesting verification of the certificates to the TOE.

<BAC and EAC-related Threats in the Operational Use phase>

**T.SESSION DATA REUSE**

In order to find out the transmitted data through the secure messaging, the threat agent may derive session keys from a number of cryptographic communication texts collected by using the terminal capable of wide-ranging RF communication.

Application Notes :

When the TOE and Inspection System use the BAC authentication key as the BAC session key, they are vulnerable to ciphertext only attack as the same session key is used in each BAC session. When the BAC session key is generated with the same random number used in the BAC mutual authentication, critical information necessary in deriving the session key may be provided to an attacker as the first random number of the TOE is transmitted as plaintext. In case the EIS transmits temporary public key in the EAC-CA and random number in the EAC-TA to other sessions in the same way and the TOE continues to use them, they may be vulnerable to ciphertext only attack.

**T.Skimming**

The threat agent may read information stored in the IC chip by communicating with the MRTD Chip through the unauthorized RF communication terminal without the ePassport holder realizing it.

<Threats related to IC Chip Support>

**T.MALFUNCTION**

In order to bypass security functions or to damage the TOE executable code and TSF data stored in the TOE, threat agent may occur malfunction of the TOE in the environmental stress outside the normal operating conditions.

<Other Threats in the Operational Use phase>

**T.ePassport Reproduction**

The threat agent may masquerade as the ePassport holder by reproduction the MRTD application data stored in the TOE and forgery identity information page of the ePassport.

**T.Leakage to cryptographic key information**

By using electric power and wave analysis devices, the threat agent may obtain key information used in cryptographic technique applied to the ePassport security mechanism by analyzing information of electric power and wave emitted in the course of the TOE operation.

**T.Residual Information**
The threat agent may disclose to critical information by using residual information remaining while the TSF data, such as BAC authentication key, BAC session key, SCP02 session key, DV certificate and IS certificate, etc., are recorded and used in temporary memory.

## 3.3. Organizational Security Policies

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

**P.APPLICATION PROGRAM LOADING**
The Personalization agent shall approve application program loading after checking that application programs loaded in the MRTD chip does not affect the secure TOE.

Application Notes :
The application program loading can only be done by organizations holding the same authority as the Personalization agent.

**P.ePassport ACCESS CONTROL**
The Personalization agent and TOE shall build the ePassport access control policies in order to protect the MRTD application data. Also, the TOE shall regulate the roles of user.

Application Notes :
The TOE shall build access control policies as of the following according to the ICAO document and EAC specifications.

**Table 6 Passport Access Control Policies**

| | | List of Objects | Objects | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Personal data of the ePassport holder | | Biometric data of the ePassport holder | | ePassport Authentication Data | | EF.CVCA | | EF.COM | |
| List of Subjects | | Security Attributes<br>Security Attributes | Read-Rights | Write-Rights | Read-Rights | Write-Rights | Read-Rights | Write-Rights | Read-Rights | Write-Rights | Read-Rights | Write-Rights |
| Subjects | IS | BAC Authorization | allow | deny | deny | deny | allow | deny | allow | deny | allow | deny |
| | | EAC Authorization | allow | deny | allow | deny | allow | deny | allow | deny | allow | deny |
| | Personalization agent | Personalization Authorization | deny | allow | deny | allow | deny | allow | deny | allow | deny | allow |

**P.INTERNATIONAL COMPATIBILITY**
The Personalization agent shall ensure compatibility between security mechanisms of the ePassport and security mechanism of the Inspection System for immigration.

Application Notes :
The international compatibility shall be ensured according to the_ICAO document and EAC specifications.

**P.PERSONALIZATION AGENT**

The personalization agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational Use phase after verifying that the data inside MRTD chip are operating normally after issuing. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase. The Personalization agent shall build the access control policies for manage of Operating System.

Application Notes :

The security mechanism for verifying personalization agent shall be the SCP02 security mechanism for "GP Standard".

**P.PKI**

The Issuing State of the ePassport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to the CPS by implementing the PA-PKI and EAC-PKI according to the ePassport PKI System. Also, The Issuing State of the ePassport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System. When the EAC-TA provides the TOE with CVCA link certificate, DV certificate and IS certificate after the Inspection System obtaining information from EF.CVCA stored in the TOE, the TOE shall internally update certificates by verifying validity of the certificates.

**P.Range of RF Communication**

The RF communication distance between the MRTD chip and Inspection System shall be less than 5cm and the RF communication channel shall not be established if the page of the ePassport attached with IC chip is not opened.

**P.Security Mechanism Application Procedures**

The TOE shall ensure the order of security mechanism application according to the type of the Inspection System so that not to violate the ePassport access control policies of the Personalization agent.

Application Notes :

The operation flow of the TOE differs according to the type of_security mechanisms supported by the Inspection System. The basic operation flow depends on 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specifications.

# 4. Security Objects

This Security Target defines security objectives by categorizing them into the TOE and the environment. The security objectives for the TOE are directly handled by the TOE. The security objectives for the environment are handled in relation to IT fields or by non-technical/process-related means.

## 4.1. TOE Security Objects

The followings are security objectives to be directly handled by the TOE.

**O.AA**
The TOE shall implement AA security mechanism for verifying illegal copy of The TOE.

**O.Access Control**
The TOE shall provide the external IT entities that were authorized by The Issuer ePassport access control policy and The Issuer Operating System Access Control Policy with The Access Control Function that permit to approach the ePassport Application Data.

Application Notes :
Only the authorized Personalization agent in the Personalization_phase can record the MRTD application data. Also, access control policies for the read-rights according to the type of the Inspection System shall be built in the Operational Use phase.

**O.BAC**
The TOE executes the BAC mutual authentication of the Inspection System with the TOE by implementing the BAC security mechanism in order to allow the read-rights for the personal data of the ePassport holder only to the authorized Inspection System. Also, the TOE generates the BAC session key to be used for the BAC secure messaging.

**O.CERTIFACATE VERIFICATION**
The TOE shall automatically update the certificate and current date by checking valid date on the basis of the CVCA link certificate provided by the Inspection System.

**O.DELETING Residual Information**
When allocating resources, the TOE shall provide means to ensure that previous security-related information (Ex.: BAC session key, EAC session key, etc.) is not included.

**O.domain separation**
The TOE shall provide means to prevent interference and tampering of the TSF and TSF data by the external IT entities.

Application Notes :
The TSF data used inside the TOE shall be stored in secure memory_controlled by the COS so that not to be accessed through external interface. Also, the TOE shall separate execution domains between the MRTD application loaded in the MRTD chip and other application programs.

**O.EAC**

The TOE authenticates the Inspection System by implementing the EAC security mechanism (EAC-CA and EAC-TA) in order to allow the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System. Also, the TOE generates the EAC session key to be used for the EAC secure messaging.

**O.MANAGEMENT**

The TOE shall provide the means to manage the MRTD application data in the Personalization phase to the authorized Personalization agent.

Application Notes :

In the Personalization phase, the Personalization agent shall_deactivate the writing function after recording the MRTD application data.

**O.REPLAY PREVENTION**

The TOE shall ensure generation and use of different random number per session for the secure cryptographic-related information used in security mechanisms.

Application Notes :

The TOE shall generate the transmitted data to the Inspection System in the SCP02 mutual authentication, BAC mutual authentication and EAC-TA to be different per session and shall not use the BAC authentication key as the BAC session key. Also, the TOE shall not provide critical information necessary in deriving session key by generate the BAC session key with the same random number used in the BAC mutual authentication.

**O.SCP02**

The TOE implements the SCP02 security mechanism for providing management means of the ePassport Application Data, performs SCP02 mutual authentication of the TOE and the Inspection System and generates the SCP02 session key for the SCP02 process.

**O.Security Mechanism Application Procedures**

The TOE shall ensure instruction flow according to ePassport inspection procedures of the EAC specifications.

Application Notes :

The TOE shall ensure that the application order of PA, BAC and EAC_security mechanisms conforms to 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specifications and shall not allow requests from the Inspection System that do not correspond to the security mechanism application order. In case of implementation different from procedures of the EAC specifications, the ST author shall ensure reliability and secure operation that conforms to the EAC specifications.

**O.SELF-PROTECTION**

The TOE shall protect itself so that to preserve secure state from attempt of bypassing and modification of TSF executable code and data at start-up.

Application Notes:

The ePassport application program shall not be deleted during issuing state and using state.

**O.SECURE MESSAGING**

The TOE shall ensure confidentiality and integrity to protect the transmitted user and

TSF data.

**O.SESSION TERMINATION**
The TOE shall terminate the session in case of failure of the SCP02 mutual authentication, the BAC mutual authentication, failure of the EAC-TA or detecting modification in the transmitted TSF data.

## 4.2. Security Objectives for the Environment

The following are security objectives handled in relation to IT fields or by non-technical/procedure-related means.

**OE.APPLICATION PROGRAM LOADING**
The Personalization agent shall approve application program loading after checking that application programs loaded in the MRTD chip does not affect the secure TOE.

**OE.CERTIFACATE VERIFICATION**
The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically. The EIS shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA link certificate, the DV certificate and the IS certificate in the EAC-TA.

**OE.Handling Information Leakage**
The IC chip, the underlying platform of the TOE and ECC Cryptographic operation Library, implements a countermeasure to prevent misusing the leakage Information during the Cryptographic operation for TSF.

Application Notes :
The Cryptographic operation process of IC chip and the ECC Cryptographic Library loaded in the IC chip, implements a countermeasure to prevent misusing the leakage Information during the TDES operation and the ECDSA operation.

**OE.IC Chip**
The IC chip, the underlying platform of the TOE, provides the random number generation and cryptographic operation to support security functions of the TOE. It also detects the TOE's malfunction outside the normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using the probing and reverse engineering analysis.

**OE.INSPECTION SYSTEM**
The Inspection System shall implement security mechanisms according to the type of the Inspection System so that not to violate the ePassport access control policies of the Personalization agent and to ensure the order of application. Also, the Inspection System shall securely destroy all information used in communication with the TOE after the session termination.

**OE.MRZ ENTROPY**
Personalization agent shall ensure the MRZ entropy to ensure the secure BAC authentication key.

**OE.PASSPORT BOOK MANUFACTURING SECURITY**
Physical security measures (security printing, etc.) for the ePassport shall be prepared to detect reproduction of the MRTD chip and attack attempt of the Grandmaster chess, replacement of the portrait and modification of the MRZ data, etc.

**OE.PERSONALIZATION AGENT**
The personalization agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational Use phase after verifying the normal operation and compatibility of the ePassport. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.

**OE.PKI**
The Issuing State of the ePassport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to the CPS by implementing the PA-PKI and EAC-PKI according to the ePassport PKI System. Also, The Issuing State of the ePassport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System.

**OE.PROCEDURES OF ePassport HOLDER CHECK**
The Immigration officer shall prepare for procedures to check identity of the ePassport holder against the printed identity information page of the ePassport.

**OE.RANGE OF RF COMMUNICATION**
The RF communication distance between the MRTD chip and Inspection System shall be less than 5cm and the RF communication channel shall not be established if the page of the ePassport attached with the IC chip is not opened.

# 5. IT Security Requirements

IT security requirements specify security functional and assurance requirements that must be satisfied by the TOE for this Security Target.

## 5.1. TOE Security Functional Requirements

The security functional requirements for this Security Target consist of the following components from Part2 of the CC. Following [Table 7 shows Security Functional Requirements Component for this Security Target to satisfy TOE Security Objects identified in the previous chapter.

This TOE security functional requirements claims conformance to TOE security functional requirements of ePassport Protection Profile V1.0 (KECS-PP-0084-2008) and define additional security requirements.

The strength of function (SOF) for security functional requirements of FCS_CKM.1, FCS_COP.1(1), FCS_COP.1(2), FIA_UAU.4, FMT_MTD.3 in this ST is "SOF-high".

Table 7 TOE Security Functional Requirements

| Security Function Class | Security Function Component | |
|---|---|---|
| Cryptographic Support (FCS) | FCS_CKM.1(1) | Cryptographic key generation (Key Derivation Mechanism) |
| | FCS_CKM.1(2) | Cryptographic key generation (SCP02 Session key Generation) |
| | FCS_CKM.2(1) | Cryptographic key distribution (KDF Seed Distribution for BAC session key generation) |
| | FCS_CKM.4 | Cryptographic key destruction |
| | FCS_COP.1(1) | Cryptographic operation (Symmetric Key Cryptographic Operation) |
| User Data Protection (FDP) | FDP_ACC.1(1) | Subset access control (ePassport) |
| | FDP_ACC.1(2) | Subset access control (Operating System) |
| | FDP_ACF.1(1) | Security attribute based access control (ePassport) |
| | FDP_ACF.1(2) | Security attribute based access control (Operating System) |
| | FDP_DAU.1 | Basic Data Authentication |
| | FDP_RIP.1 | Subset residual information protection |
| | FDP_UCT.1 | Basic data exchange confidentiality |
| | FDP_UIT.1 | Data exchange integrity |
| Identification and Authentication (FIA) | FIA_AFL.1(1) | Authentication failure handling (User session termination) |
| | FIA_AFL.1(2) | Authentication failure handling (Replay prevention) |
| | FIA_UAU.1(1) | Timing of authentication (BAC mutual authentication) |
| | FIA_UAU.1(2) | Timing of authentication (EAC-TA) |
| | FIA_UAU.1(3) | Timing of authentication (SCP02 mutual authentication) |
| | FIA_UAU.4 | Single-use authentication mechanisms |
| | FIA_UAU.5 | Multiple authentication mechanisms |
| | FIA_UID.1 | Timing of identification |
| Security Management (FMT) | FMT_MOF.1(1) | Management of security functions behaviour (writing ePassport) |
| | FMT_MOF.1(2) | Management of security functions behaviour (changing lifecycle of operating system) |
| | FMT_MSA.1 | Management of security attributes |
| | FMT_MSA.3 | Static attribute initialization |
| | FMT_MTD.1(1) | Management of TSF data (Certificate Verification Info.) |
| | FMT_MTD.1(2) | Management of TSF data (SSC INITIALISATION) |
| | FMT_MTD.1(3) | Management of TSF data (Management Operating System) |
| | FMT_MTD.3 | Secure TSF data |
| | FMT_SMF.1 | Specification of management functions |
| | FMT_SMR.1 | Security roles |
| TSF Protection (FPT) | FPT_FLS.1 | Failure with preservation of secure state |
| | FPT_ITI.1 | Inter-TSF detection of modification |
| | FPT_RVM.1 | Non-bypassability of the TSP |
| | FPT_SEP.1 | TSF domain separation |
| | FPT_TST.1 | TSF Testing |

### 5.1.1. Cryptographic Support

**FCS_CKM.1(1) Cryptographic key generation (KEY DERIVATION MECHANISM)**

Hierarchical to : No other components.
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

FCS_CKM.1.1 The TSF shall generate **encryption keys and MAC keys** in accordance with a specified cryptographic key generation algorithm [ Appendix 5.1 Key Derivation Mechanism ] and specified cryptographic key sizes [ 112bit ] that meet the following: [ the ICAO document ].

Application Notes :
The TOE generates the BAC authentication key, BAC session key and EAC session key by using key derivation mechanism. If the Personalization agent generates BAC authentication key and records it in TOE in the Personalization phase according to the Issuing policy of the ePassport or it does not provide BAC authentication key, TOE records the BAC authentication key in secure memory by generating it TOE's own.

**FCS_CKM.1(2) Cryptographic key generation (SCP02 SESSION KEY GENERATION)**

Hierarchical to : No other components.
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

FCS_CKM.1.1 The TSF shall generate **session** keys in accordance with a specified cryptographic key generation algorithm [ Appendix E.4.1 DES Session Keys ] and specified cryptographic key sizes [ 112 bit ] that meet the following: [ GP standard ].

**FCS_CKM.2(1) Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)**

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

FCS_CKM.2.1 The TSF shall distribute **KDF Seed for the BAC session key generation** in accordance with a specified cryptographic key distribution method [ *key Establishment mechanism 6* ] that meets the following : [ *ISO/IEC 11770-2* ].

**FCS_CKM.4 Cryptographic key destruction**

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

FCS_CKM.4.1 The TSF shall destroy **encryption keys and MAC keys** in accordance with a specified cryptographic key destruction method [ resetting 'zero'] that meets the following: [ None ].

**FCS_COP.1(1) Cryptographic operation (Symmetric Key Cryptographic Operation)**
Hierarchical to : No other components.
Dependencies : [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1.1 The TSF shall perform [ hash operation ] in accordance with a specified cryptographic algorithm [ *SHA-1* ] and cryptographic key sizes [ None ] that meet the following: [ *ISO/IEC 10118-3* ].

Application Notes :
The TOE uses the SHA-1 hash function for generating session key used for BAC or EAC secure communication channel in the key derivation mechanism of the ICAO document.

### 5.1.2. User Data Protection

**FDP_ACC.1(1) Subset access control (ePassport)**
Hierarchical to : No other components.
Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [ the ePassport access control policy ] on [
a) Subjects
   (1) Personalization agent
   **(2) Inspection System**
   (3) [ None ]
b) Objects
   (1) Personal data of the ePassport holder
       : EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16
   (2) The biometric data of the ePassport holder
       : EF.DG3, EF.DG4
   (3) ePassport authentication data
       : EF.DG14, EF.DG15, EF.SOD
   (4) EF.CVCA
   (5) EF.COM
   (6) [ None ]
c) Operations
   (1) Read
   (2) Write
   (3) [ None ]
]

**FDP_ACC.1(2) Subset access control (Operating System)**
Hierarchical to : No other components.
Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [ the operating system access control policy ] on [

a) Subjects
   (1) Personalization agent
b) Objects
   (1) Executable File
   (2) Application program
   (3) Basic information of Personalization agent
   (4) Authentication information of Personalization agent
c) Operations
   (1) Load
   (2) Install
   (3) Delete
   (4) Read
   (5) Write
   (6) Modify
   (7) Select

]

Application Notes :
The basic information of Personalization agent includes Issuer Identification Number, Card Image Number, Card Recognition Data defined in 'GP standard' and Card Production Life Cycle, Key Derivation Data defined in 'VGP standard'. It may include information defined by the issuer additionally.

The authentication information of Personalization agent means the authentication key of Personalization agent used for SCP02 mutual authentication and generating SCP02 session key. It includes three 112-bit DES keys to generate SCP02 session key for cryptographic operation, MAC, cryptographic operation for secret information.

**FDP_ACF.1(1) Security attribute based access control (ePassport)**
Hierarchical to : No other components.
Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [ the ePassport access control policy ] to objects based on the following: [ Table 8, Table 9, [ None ] ].

**Table 8 Subject-relevant Security Attributes**

| Subjects | Security attributes |
|---|---|
| Inspection System | BAC authorization, EAC authorization |
| Personalization agent | Personalization agent issuing authorization |

**Table 9 Object-relevant Security Attributes**

| Objects | Security attributes | |
|---|---|---|
| | Security attributes of object's operation | Security attributes of object's access-rights |
| Personal data of the ePassport holder | Read-rights | BAC authorization, EAC authorization |
| | Write-rights | Personalization agent issuing authorization |
| Biometric data of the ePassport holder | Read-rights | EAC authorization |
| | Write-rights | Personalization agent issuing authorization |
| ePassport | Read-rights | BAC authorization, EAC authorization |

| | | |
|---|---|---|
| authentication data | Write-rights | Personalization agent issuing authorization |
| EF.CVCA | Read-rights | BAC authorization, EAC authorization |
| | Write-rights | Personalization agent issuing authorization |
| EF.COM | Read-rights | BAC authorization, EAC authorization |
| | Write-rights | Personalization agent issuing authorization |

Application Notes :
The BAC authorization is the right given to the user identified with the Inspection System that supports the MRTD application by FIA_UID.1 when the BAC mutual authentication succeeds.

The EAC authorization is the right given when the Inspection System with the BAC authorization succeeds in the EAC-CA and the EAC-TA and the read-rights of the biometric data is included in all of CVCA certificate, DV certificate and IS certificate held by that Inspection System. Even when the EAC-CA and the EAC-TA succeed, the Inspection System has only the BAC authorization if the certificates do not include the read-rights.

The Personalization agent issuing authorization is the right given when the Personalization agent is successfully authenticated in the Personalization phase by FIA_UID.1.

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

a) Execution of the operation is allowed only when security attributes of subjects are included in security attributes of the object's access-rights and operations corresponds to security attributes of the object's operation.
b) [ None ].

]

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [ following rules ].

a) Explicitly deny access of subjects to objects if instructions order of the inspection system is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specifications
b) Explicitly deny read of subjects to biometric data if there is no the read-rights of biometric data in IS certificate of the **IS** that has the EAC authorization
c) Explicitly deny access(read, write, etc.) of the unauthorized Inspection System to all objects
d) [ None ]

**FDP_ACF.1(2) Security attribute based access control (Operating System)**
Hierarchical to : No other components.
Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [ the operating system access control policy ] to objects based on the following: [ Table 10, Table 11 ].

**Table 10 Subject-relevant Security Attributes**

| Subjects | Security attributes |
|---|---|
| Personalization agent | Personalization authorization, Administraing authorization |

**Table 11 Object-relevant Security Attributes**

| Objects | Security attributes | |
|---|---|---|
| | Security attributes of object's operation | Security attributes of object's access-rights |
| Executable File | Load-Rights | Administrating authorization |
| | Delete-Rights | Administrating authorization |
| Application Program | Install-Rights | Administrating authorization |
| | Delete-Rights | Administrating authorization |
| | Select-Rights | Using authorization |
| Basic information of Personalization agent | Read-Rights | Using authorization, Administrating authorization |
| | Write-Rights | Administrating authorization |
| | Modify-Rights | Administrating authorization |
| Authentication information of Personalization agent | Write-Rights | Administrating authorization |
| | Modify-Rights | Administrating authorization |

Application Notes :
The using authorization is the right given to the user identified with the Personalization agent that requests to use card manager in the personalization and operation phase by FIA_UID.1.

The administrating authorization is the right given when the Personalization agent that has using authorization succeeds Personalization agent authentication.

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

a) Execution of the operation is allowed only when security attributes of subjects are included in security attributes of the object's access-rights and operations corresponds to security attributes of the object's operation.

]

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [ following rules ].

a) Deny all operations except read operation to basic information of Personalization agent in the termination phase
b) Deny delete operation to ePassport application program
c) Deny select operation to uninstalled application program

**FDP_DAU.1 Basic Data Authentication**
Hierarchical to : No other components.
Dependencies : No dependencies.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [ ePassport user data ].

FDP_DAU.1.2 The TSF shall provide [ Inspection System ] with the ability to verify evidence of the validity of the indicated information.

Application Notes :
When receiving AA request from BIS or EIS to ensure the validity of ePassport user data, TOE generates digital signature on random number received in AA request process with AA chip authentication private key in secure memory and provides inspection system with it. Inspection system verifies whether TOE is illegally copied with AA chip authentication public key from EF.DG15. In the case of EAC-CA request from EIS, EIS performs ECDH operation by using temporary public key generated using EAC-CA chip authentication public key information and EAC-CA chip authentication private key in secure memory. So EIS verifies illegal copy of TOE depending on the success of EAC-CA.

**FDP_RIP.1 Subset residual information protection**
Hierarchical to : No other components.
Dependencies : No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to, deallocation of the resource from* the following objects: [

a) BAC session key
b) EAC session key
c) BAC authentication key
d) [ SCP02 session key, random value ]

].

Application Notes :
After a session termination, the TSF shall not remain the BAC session key, the EAC session key and random numbers, etc. in temporary memory. The BAC session key, the EAC session key and the BAC authentication key, etc. can be ensured unavailable by destroying them with the method defined in FCS_CKM.4.

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

FDP_UCT.1.1 The TSF shall enforce the [ ePassport access control policy ] to be able to *transmit, receive* objects in a manner protected from unauthorized disclosure.

Application Notes :

When the Inspection System successfully completes the BAC mutual authentication, the TSF protects from disclosure by using the BAC session encryption key. When the EAC-CA is successfully executed, data transmitted thereafter are protected from disclosure by using the EAC session encryption key.

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

FDP_UIT.1.1 The TSF shall enforce the [ ePassport access control policy ] to be able to *transmit, receive* user data in a manner protected from *modification, deletion, insertion, replay* errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, replay* has occurred.

Application Notes :
The TSF protects integrity of the transmitted data by using the MAC key for BAC session or EAC session. This provides the method of protection against modification, deletion and insertion of user data. This also provides the method of protection against replay by using SSC.

### 5.1.3. Identification and Authentication

**FIA_AFL.1(1) Authentication failure handling (USER SESSION TERMINATION)**
Hierarchical to : No other components.
Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [ *1* ] unsuccessful authentication attempts occur related to [

a) BAC mutual authentication
b) [ SCP02 mutual authentication ]

].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [ user session termination ].

**FIA_AFL.1(2) Authentication failure handling (REPLAY PREVENTION)**
Hierarchical to : No other components.
Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [ *1* ] unsuccessful authentication attempts occur related to [ EAC-TA ].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [ EAC-TA replay prohibition ].

Application Notes :

In the case of a failure of the EAC-TA, while maintaining EAC secure communication channel, additional EAC-TA on the same EAC secure communication channel is not permitted.

**FIA_UAU.1(1) Timing of authentication (BAC Mutual authentication)**
Hierarchical to : No other components.
Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [

a) indication that support the BAC mechanism
b) [ None ]

] 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 except actions specified in FIA_UAU.1.1.

**FIA_UAU.1(2) Timing of authentication(EAC-TA)**
Hierarchical to : No other components.
Dependencies : FIA_UAU.1(1) Timing of authentication (BAC mutual authentication)

FIA_UAU.1.1 The TSF shall allow [

a) to perform the EAC-CA
b) to read user data except the biometric data of the ePassport holder
c) [assignment: list of other TSF mediated actions]

] 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 except actions specified in FIA_UAU.1.1.

**FIA_UAU.1(3) Timing of authentication(SCP02 mutual authentication)**
Hierarchical to : No other components.
Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [ reading of basic information of Personalization agent ] 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 except actions specified in FIA_UAU.1.1.

**FIA_UAU.4 Single-use authentication mechanisms**
Hierarchical to : No other components.
Dependencies : No dependencies.

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

a) BAC mutual authentication
b) EAC-TA
c) [ SCP02 mutual authentication ]

].

**FIA_UAU.5 Multiple authentication mechanisms**
Hierarchical to : No other components.
Dependencies : No dependencies.

FIA_UAU.5.1 The TSF shall provide [
a) BAC mutual authentication
b) EAC-TA
c) [ SCP02 mutual authentication ]
] to support user authentication.

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

a) The BIS or EIS shall succeed the BAC mutual authentication in order to have the BAC authorization.
b) The EIS, in order to have the EAC authorization, shall succeed the BAC mutual authentication, EAC-CA and EAC-TA and include the read-rights of biometric data in all of the CVCA certificate, DV certificate and IS certificate. For this, the TSF shall provide the EAC-CA.
c) [ The Personalization agent, in order to have the personalization or administration authorization, shall succeed SCP02 mutual authentication ]

].

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

FIA_UID.1.1 The TSF shall allow [

a) to establish the communication channel based on ISO/IEC 14443-4

] 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 except actions specified in FIA_UAU.1.1.

Application Notes :
When external entities communicated with the TOE request of the MRTD application in the Personalization phase, the TOE identifies it with the Personalization agent and when external entities communicated with the TOE request of the MRTD application in the Operational Use phase, the TOE identifies it with the Inspection System. When they request to use Card Manager in the Personalization or Operational use phase, the TOE identifies it with the Personalization agent.

### 5.1.4. Security Management

**FMT_MOF.1(1) Management of security functions behaviour(WRITING ePassport)**
Hierarchical to : No other components.
Dependencies : FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *disable* the functions [ writing function ]
to [ Personalization agent in the Personalization phase ].

Application Notes :
The Personalization agent delivers the ePassport to the Operational Use phase by deactivating writing function after recording the MRTD application data in the Personalization phase.

**FMT_MOF.1(2) Management of security functions behaviour (CHANGING LIFECYCLE OF Operating System)**
Hierarchical to : No other components.
Dependencies : FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *decide actions* the functions [ application program changing the life cycle of operating system ] to [ Personalization agent ].

Application Notes :
The Personalization agent determines if application program to be installed has authorization to change operating system life cycle when it install application program. Application program can change life cycle of operating system to CARD_LOCKED or TERMINATED state only.

**FMT_MSA.1 Management of security attributes**
Hierarchical to : No other components.
Dependencies : [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [ ePassport access control policy**, operating system access control policy** ] to restrict the ability to [ *initialization* ] the security attributes [ security attributes of subjects defined in FDP_ACF.1(1) **and FDP_ACF.1(2)** ] to [ TSF ].

Application Notes :
As an action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1, the TSF shall reset security attributes of subjects defined in FDP_ACF.1(1) and FDP_ACF.1(2).

**FMT_MSA.3 Static attribute initialization**
Hierarchical to : No other components.
Dependencies : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [ ePassport access control policy**, operating system access control policy** ] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [ **None** ] to specify alternative initial values to override the default values when an object or information is created.

Application Notes :
Security attributes of object's operation and object's access-rights of the ePassport access control policy and the operating system access control policy are determined to

implementation logic of the TOE and modifying their default values is not permitted according to [Table 11] of FDP_ACF.1(1) , [Table 13] of FDP_ACF.1.(2).

**FMT_MTD.1(1) Management of TSF data (Certificate Verification Info.)**
Hierarchical to : No other components.
Dependencies : FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to [ *write in secure memory* ] the [

a) EAC chip authentication private key
b) initial current date
c) initial CVCA certificate
d) initial CVCA digital signature verification key
e) [ AA chip authentication private key ]

] to [ Personalization agent in the Personalization phase ].

**FMT_MTD.1(2) Management of TSF data (SSC Initialization)**
Hierarchical to : No other components.
Dependencies : FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* the [ SSC(Send Sequence Counter) ] to [ TSF ].

Application Notes :
The TSF shall initialize SSC as '0' in order to terminate the BAC secure messaging before establishing the EAC secure messaging after generating the EAC session key.

**FMT_MTD.1(3) Management of TSF data (Management Operating System)**
Hierarchical to : No other components.
Dependencies : FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* the [ GP Registry ] to [ Personalization agent ].

**FMT_MTD.3 Secure TSF Data**
Hierarchical to : No other components.
Dependencies : ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

Application Notes :
The TSF shall use only secure value safe as random numbers against replay attack so that to satisfy the SOF-high. The TSF shall preserve secure values by verifying valid data of the CVCA link certificate, DV certificate and IS certificate provided by the EIS when executing the EAC-TA and internally updating the CVCA certificate, CVCA digital signature verification key, current date and EF.CVCA if necessary.

**FMT_SMF.1 Specification of management functions**
Hierarchical to : No other components.
Dependencies : No dependencies.

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

a) Function to write user data and TSF data in the Personalization phase

b) Function to verify and update the CVCA certificate, CVCA digital signature verification key and current data in the Operational Use phase

c) [

A. Loading, installation, deletion of executable file and application program in the Personalization phase or Operational Use phase

B. Writing, modifying basic information of Personalization agent, authentication information of Personalization agent, GP registry in the Personalization phase or Operational Use phase

C. Application program changing the life cycle of operating system in the Personalization phase or Operational Use phase

]

].

**FMT_SMR.1 Security roles**
Hierarchical to : No other components.
Dependencies : FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

a) Personalization agent

b) [ None ].

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

Application Notes :
The Personalization agent is defined as the role to execute a)security management function of FMT_SMF.1. The TSF executes security management functions to FMT_MTD.1(2) and b) of FMT_SMF.1. However, the TSF is not defined as the role since it is not a user.

### 5.1.5. TSF Protection

**FPT_FLS.1 Failure with preservation of secure state**
Hierarchical to : No other components.
Dependencies : ADV_SPM.1 Informal TOE security policy model

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

a) Failure detected in self-testing by FPT_TST.1

b) Conditions outside the normal operating of the TSF detected by the IC chip

c) [ Power supply blocked during the TSF action ]

].

**FPT_ITI.1 Inter-TSF detection of modification**
Hierarchical to : No other components.
Dependencies : No dependencies.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [ strength of Retail MAC ].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [

a) Termination of the BAC secure messaging or EAC secure messaging
b) Deletion of BAC session key or EAC session key
c) Management action specified in FMT_MSA.1
d) Termination of Personalization agent communication channel
e) [ Deletion of Personalization agent communication channel session key ]

] if modifications are detected.

Application Notes :
The Strength of Retail MAC is equivalent to the secure Retail MAC specified in FCS_COP.1(2). Personalization agent uses SCP02 secure channel, which detects changes by Retail Mac.

**FPT_RVM.1 Non-bypassability of the TSP**
Hierarchical to : No other components.
Dependencies : No dependencies.

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

**FPT_SEP.1 TSF domain separation**
Hierarchical to : No other components.
Dependencies : No dependencies.

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

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

Application Notes :
The TSF shall separate secure memory not to be affected by interference and tampering from other memory domains. Also, the TSF shall separate the MRTD application not to be affected by interference and tampering from other application programs.

**FPT_TST.1 TSF Testing**
Hierarchical to : No other components.
Dependencies : FPT_AMT.1 Abstract machine testing

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

## 5.2. Security Requirements for IT Environment

IC chip providing part of TOE Security Functional Requirements of ePassport Protection Profile V1.0 (KECS-PP-0084-2008) is modified to Security Requirements for this IT Environment.

**Table 12 Security Requirements for IT Environment**

| Security Function Class | Security Function Component | |
|---|---|---|
| Cryptographic Support (FCS) | FCS_CKM.2(2) | Cryptographic key distribution (KDF Seed Distribution for EAC session key generation) |
| | FCS_COP.1(2) | Cryptographic operation (Symmetric Key Cryptographic operation) |
| | FCS_COP.1(3) | Cryptographic operation (MAC) |
| | FCS_COP.1(4) | Cryptographic operation (Digital signature Verification for Certificates Verification) |
| | FCS_COP.1(5) | Cryptographic operation (Digital signature generation for AA) |
| Privacy (FPR) | FPR_UNO.1(2) | Unobservability (IC Chip) |

**FCS_CKM.2(2) Cryptographic key distribution (KDF Seed Distribution for EAC session key generation)**

Hierarchical to : No other components.

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

FCS_CKM.2.1 The TSF shall distribute **KDF Seed for the EAC session key generation** in accordance with a specified cryptographic key distribution method [ *Elliptic Curve Diffie-Hellman key-agreement protocol* ] that meets the following : [ *ISO/IEC 15946-3* ]

**FCS_COP.1(2) Cryptographic operation (Symmetric Key Cryptographic operation)**

Hierarchical to : No other components.

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

FCS_COP.1.1 The TSF shall perform [ message encryption and decryption operation ] in accordance with a specified cryptographic algorithm [ *TDES* ] and cryptographic key sizes [ *112 bit* ] that meet the following: [ *ISO/IEC 18033-3* ].

Application Notes :

The TOE uses the TDES algorithm for the integrity protection of the transmitted data of the BAC or EAC secure messaging and for the BAC mutual authentication. Operational mode of encryption algorithm uses CBC mode whose IV is zero which is defined in ISO/IEC 10116. TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip.

**FCS_COP.1(3) Cryptographic operation (MAC)**

Hierarchical to : No other components.

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

FCS_COP.1.1 The TSF shall perform [ MAC operation ] in accordance with a specified cryptographic algorithm [ *Retail MAC*, [ *Full Triple DES MAC* ] ] and cryptographic key sizes [ *112 bit* ] that meet the following: [ *ISO/IEC 9797-1* ].

Application Notes :

The TOE uses the Retail MAC algorithm for the integrity protection of the transmitted data of the BAC or EAC secure messaging and for the BAC mutual authentication. The Retail MAC uses the MAC algorithm 3, the block cipher DES, the sequence message counter and the padding mode 2 defined in ISO/IEC 9797-1. TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement can be changed as a requirement for the IT environment.

**FCS_COP.1(4) Cryptographic operation (Digital signature Verification for Certificates Verification)**

Hierarchical to : No other components.

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

FCS_COP.1.1 The TSF shall perform [ digital signature verification ] in accordance with a specified cryptographic algorithm [ *ECDSA-SHA-1, ECDSA-SHA-224* ] and cryptographic key sizes [ 192 bit, 224 bit] that meet the following: [ *ISO/IEC 15946-2* ].

Application Notes :

Appendix A.3 Terminal Authentication of the EAC specifications, the digital signature algorithm, hash algorithm and digital signature key sizes are defined as of the following.

**Table 13 Details of Digital Signature in the EAC Specification**

| Digital Signature Algorithm | Hash Algorithm | Digital Signature Key Sizes |
|---|---|---|
| ECDSA-SHA-1 | SHA-1 | 192 bit, 224 bit |
| ECDSA-SHA-224 | SHA-224 | 224 bit |

**FCS_COP.1(5) Cryptographic operation (Digital signature generation for AA)**

Hierarchical to : No other components.

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

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 The TSF shall perform [ digital signature generation ] in accordance with a specified cryptographic algorithm [ *ECDSA-SHA-1* ] and cryptographic key sizes [ 192 bit, 224 bit] that meet the following: [ *ISO/IEC 15946-2* ].

**FPR_UNO.1 Unobservability**
Hierarchical to : No other components.
Dependencies : No dependencies.

FPR_UNO.1.1 The TSF shall ensure that [ external entity ] are unable to observe the operation [

a) FCS_COP.1(1) Cryptographic operation (Symmetric Key Cryptographic Operation)
b) FCS_COP.1(2) Cryptographic operation (MAC)
c) FCS_COP.1(4) Cryptographic operation(Digital signature Verification for Certificates Verification)
d) [ FCS_COP.1(5) Cryptographic operation (Digital signature generation for AA) ] ] on [
a) BAC authentication key
b) BAC session key
c) EAC session key
d) EAC chip authentication private key
e) [ SCP02 session key, AA chip authentication private key ] by [ TSF ].

Application Notes :
The external entity may find out and exploit the cryptographic-related data from physical phenomena (change of current, voltage and electromagnetic, etc.) occurred when the TSF performs cryptographic operations. The TSF provides the means to handle attacks, such as DPA and SPA, etc. Because TOE performs symmetric key cryptographic operation, MAC, Digital signature verification, etc. by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, the requirement for the cryptographic operation is changed as a requirement for the IT environment. Measures to handle attacks, such as DPA and SPA, etc., shall be included in the evaluation scope of the certified IC chip.

## 5.3. TOE Assurance Requirements

The security assurance requirements for this Security target consist of the following components from Part 3 of the CC, summarized in the following [Table 14] and evaluation assurance level is EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.3).

The assurance components are augmented follows:

- ADV_IMP.2 Implementation of the TSF
- ATE_DPT.2 Testing: low-level design
- AVA_VLA.3 Moderately resistant

**Table 14 Assurance Requirements**

| Assurance Class | Assurance Component | |
|---|---|---|
| Configuration Management (ACM) | ACM_AUT.1 | Partial CM automation |
| | ACM_CAP.4 | Generation support and acceptance procedures |
| | ACM_SCP.2 | Problem tracking CM coverage |

| | | |
|---|---|---|
| Delivery and Operation (ADO) | ADO_DEL.2 | Detection of modification |
| | ADO_IGS.1 | Installation, generation, and start-up procedures |
| Development (ADV) | ADV_FSP.2 | Fully defined external interfaces |
| | ADV_HLD.2 | Security enforcing high-level design |
| | ADV_IMP.2 | Implementation of the TSF |
| | ADV_LLD.1 | Descriptive low-level design |
| | ADV_RCR.1 | Informal correspondence demonstration |
| | ADV_SPM.1 | Informal TOE security policy model |
| Guidance documents (AGD) | AGD_ADM.1 | Administrator guidance |
| | AGD_USR.1 | User guidance |
| Life cycle support (ALC) | ALC_DVS.1 | Identification of security measures |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_TAT.1 | Well-defined development tools |
| Testing (ATE) | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.2 | Testing: low-level design |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing – sample |
| Vulnerability (AVA) | AVA_MSU.2 | Validation of analysis |
| | AVA_SOF.1 | Strength of TOE security function evaluation |
| | AVA_VLA.3 | Moderately resistant |

### 5.3.1. Configuration Management

**ACM_AUT.1 Partial CM automation**

Dependencies :

ACM_CAP.3 Authorization controls

Developer action elements :

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements

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

**ACM_CAP.4 Generation support and acceptance procedures**

Dependencies :

ALC_DVS.1 Identification of security measures

Developer action elements

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D he developer shall provide CM documentation.

Content and presentation of evidence elements

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.8C The CM plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements

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

**ACM_SCP.2 Problem tracking CM coverage**

Dependencies :

ACM_CAP.3 Authorization controls

Developer action elements

ACM_SCP.2.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements

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

### 5.3.2. Delivery and Operation

**ADO_DEL.2 Detection of modification**

Dependencies :

ACM_CAP.3 Authorization controls

Developer action elements

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements

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

**ADO_IGS.1 Installation, generation, and start-up procedures**

Dependencies :

AGD_ADM.1 Administrator guidance

Developer action elements

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements

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

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

### 5.3.3. Development

**ADV_FSP.2 Fully defined external interfaces**

Dependencies :

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements
ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2C The functional specification shall be internally consistent.
ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4C The functional specification shall completely represent the TSF.
ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements
ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

**ADV_HLD.2 Security enforcing high-level design**
Dependencies :
ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

Developer action elements
ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements
ADV_HLD.2.1C The presentation of the high-level design shall be informal.
ADV_HLD.2.2C The high-level design shall be internally consistent.
ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements
ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate

and complete instantiation of the TOE security functional requirements.

**ADV_IMP.2 Implementation of the TSF**

Dependencies :

ADV_LLD.1 Descriptive low-level design
ADV_RCR.1 Informal correspondence demonstration
ALC_TAT.1 Well-defined development tools

Developer action elements

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

Content and presentation of evidence elements

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements

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

ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

**ADV_LLD.1 Descriptive low-level design**

Dependencies :

ADV_HLD.2 Security enforcing high-level design
ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C he low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into

TSP-enforcing and other modules.

Evaluator action elements

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all .

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

**ADV_RCR.1 Informal correspondence demonstration**

Dependencies : No dependencies.

Developer action elements

ADV_RCR1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements

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

**ADV_SPM.1 Informal TOE security policy model**

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements

ADV_SPM.1.1C TSP The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements

ADV_SPM.1.1E he evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### 5.3.4. Guidance Documents

**AGD_ADM.1 Administrator guidance**

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements

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

**AGD_USR.1 User guidance**

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE .

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements

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

### 5.3.5. Life cycle support

**ALC_DVS.1 Identification of security measures**

Dependencies : No dependencies.

Developer action elements

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements

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

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

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

Dependencies : No dependencies.

Developer action elements

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

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

Content and presentation of evidence elements

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

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

Evaluator action elements

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

**ALC_TAT.1 Well-defined development tools**

Dependencies:

ADV_IMP.1 TSF Subset of the implementation of the TSF

Developer action elements

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements

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

### 5.3.6. Tests

**ATE_COV.2 Analysis of coverage**

Dependencies :

ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements

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

Content and presentation of evidence elements

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements

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

**ATE_DPT.2 Testing: low-level design**

Dependencies :

ADV_HLD.2 Security enforcing high-level design
ADV_LLD.1 Descriptive low-level design
ATE_FUN.1 Functional testing

Developer action elements

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

Content and presentation of evidence elements

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

**ATE_FUN.1 Functional testing**
Dependencies : No dependencies.

Developer action elements
ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements
ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

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

**ATE_IND.2 Independent testing - sample**
Dependencies :
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
ATE_FUN.1 Functional testing

Developer action elements
ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements
ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements
ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

### 5.3.7. Vulnerability Assessment

**AVA_MSU.2 Validation of analysis**
Dependencies :
ADO_IGS.1 Installation, generation, and start-up procedures

ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D he developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements

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

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

**AVA_SOF.1 Strength of TOE security function evaluation**

Dependencies :

ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design

Developer action elements

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements

AVA_SOF.1.1C For each mechanism with strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the ST.

Evaluator action elements

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

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

**AVA_VLA.3 Moderately resistant**

Dependencies :

ADV_FSP.1 Informal functional specification
ADV_HLD.2 Security enforcing high-level design
ADV_IMP.1 TSF Subset of the implementation of the TSF
ADV_LLD.1 Descriptive low-level design
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements

AVA_VLA.3.1D The developer shall perform a vulnerability analysis.

AVA_VLA.3.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements

AVA_VLA.3.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.3.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.3.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

Evaluator action elements

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

AVA_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.3.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

# 6. TOE Summary

## 6.1. TOE Security Function

This chapter describe TOE의 Security Function(TSF) satisfied Security Requirement in previous chapters. Each Security Function is described as name of function and brief description. The Function Specification (FSP) describes the further more information.

This security function is ‘SOF-high’

**Table 15 TOE Security Function**

| Security Function | Description |
|---|---|
| SF.Identification and Authentication | User Identification and Authentication |
| SF.User Data Protection | User data protection |
| SF.Security Management | TOE Security Management |
| SF.TSF Protection | TSF Protection |
| SF.Cryptography | Cryptographic Support |

### 6.1.1. SF.Identification and Authentication (SF.IA)

This Security Function provides functions of SCP02 Mutual Authentication, BAC Mutual Authentication, EAC-CA, EAC-TA, PA and AA for identification and authentication of users who access TOE.

### 6.1.2. SF.User Data Protection (SF.DP)

This Security Function provides functions of access control and secure messaging for protecting ePassport user data and operating system user data from external IT entities.

### 6.1.3. SF.Security Management (SF.MT)

This Security Function provides security management functions of ePassport and Operating System such as management of application, lifecycle and ePassport data.

### 6.1.4. SF.TSF Protection (SF.PT)

This Security Function protects the TSF functionality ( firewall, atomic transaction, clearing sensitive information and reference monitor ), TSF data and user data.

### 6.1.5. SF.Cryptography (SF.CS)

This Security Function provides the cryptographic support such as Random number generation, Hash generation, Encryption and Decryption, Digital signature key ration, and Digital signature verification.

## 6.2. Security Assurance Requirements

This chapter describes the Assurance Measures fulfilling the requirements listed in chapter 5 Security Requirements.

The following table lists the Assurance measures and references the corresponding documents describing the measures. And additional Assurance Requirements are ADV_IMP.2, ATE_DPT.2 and ALC_VLA.3.

**Table 16 TOE Security Assurance Requirements**

| Assurance Requirement | Security Assurance Requirements (Document Name) |
|---|---|
| ACM_AUT.1 | XSmart ePassport V1.0 Configuration Management V1.3 [ Chapter 3. Configuration Management Automation ] |
| ACM_CAP.4 | XSmart ePassport V1.0 Configuration Management V1.3 [Chapter 2. Configuration Management Ability ] |
| ACM_SCP.2 | XSmart ePassport V1.0 Configuration Management V1.3 [Chapter 2. Configuration Management Ability ] |
| ADO_DEL.2 | XSmart ePassport V1.0 Distribution Guide V1.4 [ Chapter 1. Distribution ] |
| ADO_IGS.1 | XSmart ePassport V1.0 Distribution Guide V1.4 [ Chapter 2. Install/Creation/Stating ] |
| ADV_FSP.2 | XSmart ePassport V1.0 Function Specification V1.4 |
| ADV_HLD.2 | XSmart ePassport V1.0 High Level Design V1.4 |
| ADV_IMP.2 | XSmart ePassport V1.0 Implementation Verification V1.3 |
| ADV_LLD.1 | XSmart ePassport V1.0 Low Level Design V1.4 |
| ADV_RCR.1 | XSmart ePassport V1.0 Function Specification V1.4<br>XSmart ePassport V1.0 High Level Design V1.4<br>XSmart ePassport V1.0 Low Level Design V1.4<br>XSmart ePassport V1.0 Implementation Verification V1.3<br>XSmart ePassport V1.0 Security Plan Model V1.3 |
| ADV_SPM.1 | XSmart ePassport V1.0 Security Plan Model V1.3 |
| AGO_ADM.1 | XSmart ePassport V1.0 Administrator Manual V1.3 |
| AGO_USR.1 | XSmart ePassport V1.0 User Manual V1.3 |
| ALC_DVS.1 | XSmart ePassport V1.0 Life Cycle Management V1.2 [ Chapter 1. Development Security ] |
| ALC_LCD.1 | XSmart ePassport V1.0 Life Cycle Management V1.2 [ Chapter 2. Life Cycle Definition ] |
| ALC_TAT.1 | XSmart ePassport V1.0 Life Cycle Management V1.2 [ Chapter 3. Tool and Technique ] |
| ATE_COV.2 | XSmart ePassport V1.0 Test Analysis V1.2 [ Range Analysis (1~2) ] |
| ATE_DPT.2 | XSmart ePassport V1.0 Test Analysis V1.2 [ Depth Analysis (1~4) ] |
| ATE_FUN.1 | XSmart ePassport V1.0 Test V1.2 |
| ATE_IND.2 | XSmart ePassport V1.0 Test V1.2 |
| AVA_MSU.2 | XSmart ePassport V1.0 Misuse Anaysis V1.2 |
| AVA_SOF.1 | XSmart ePassport V1.0 Vulnerability Analysis V1.2 [ Chapter 2. Function Strength Analysis ] |
| AVA_VLA.3 | XSmart ePassport V1.0 Vulnerability Analysis V1.2 [ Chapter 1. Vulnerability Analysis ] |

# 7. Protection Profile Compliance

This chapter describes that SecurityTarget is in correspondence with Protection Profile.

## 7.1. Protection Profile Reference

TOE is compliant all the requirements in the followed Protection Profile.

- ePassport Protection Profile V1.0 (KECS-PP-0084-2008)
  EAL4+ Assurance Level (ADV_IMP.2, ATE_DPT.2, AVA_VLA.3)

## 7.2. Protection Profile Redefinition

Redefined objects of Security Target are as followed;

**TOE Security Environment**

- A.INSPECTION SYSTEM
- T.Residual Information
- P.Personalization Agent
- P.ePassport Access Control

**Security Objects**

- O.Session Termination
- O.Access Control
- OE.Handling Information Leakage

**Security Function Requirement**

- FCS_CKM.2(1), FCS_CKM.4, FCS_COP.1(1)
- FDP_ACC.1(1), FDP_ACF.1(1), FDP_RIP.1, FDP_UIT.1
- FIA_AFL.1(1), FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.4, FIA_UAU.5
- FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_SMF.1, FMT_SMR.1
- FPT_FLS.1, FPT_ITI.1, FPT_TST.1

**Security Requirement for IT environment**

- FCS_CKM.2(2), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4)
- FPR_UNO.1

## 7.3. Protection Profile Addition

Additional objects of Security Target are as followed;

**TOE Security Environment**

- T.Reuse Issuer Certification

**Security Objects**

- O.SCP02
- O.AA

**Security Function Requirement**

- FCS_CKM.1(2)
- FDP_ACC.1(2), FDP_ACF.1(2), FDP_DAU.1
- FIA_AFL.1(2), FIA_UAU.1(3)
- FMT_MOF.1(2), FMT_MTD.1(3)

**Security Requirement for IT Environment**

- FCS_COP.1(5)

# 8. Rationale

This chapter describes the rationale of security objectives rationale of security requirements, rational of dependency, rational of strength of function and rationale of PP compliance. The rationales are shown that TOE provides effective IT security measure in E TOE Security Environment.

## 8.1. Rationale of Security Objects

The rationale of security objectives demonstrates that the specified security objectives are appropriate, sufficient to trace security problems and are essential, rather than excessive.

### 8.1.1. Rationale of TOE Security Objects

The rationale of security objectives demonstrates the following:.

- Each assumption, threat or organizational security policy has at least one security objective tracing to it.
- Each security objective traces to at least one assumption, threat or organizational security policy.

Table 17 shows the mapping for security objectives.

Table 17 Summary of Mappings for Security Objectives

| Security Objects | TOE Security Objects | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TOE Security Environment | O.Management | O.Security Mechanism Application Procedures | O.Session Termination | O.SECURE MESSAGING | O.domain separation | O.CERTIFACATE VERIFICATION | O.SELF-PROTECTION | O.DELETING Residual Information | O.REPLAY PREVENTION | O.Access Control | O.AA | O.BAC | O.EAC | O.SCP02 |
| T.Application Program Interference | | | | | X | | | | | | | | | |
| T.Reuse Issuer Certification | | | | | | | | | X | | | | | |
| T.TSF Data Modification | X | | X | X | X | | | | | X | | | | |
| T.Eavesdropping | | | | X | | | | | | | | | | |
| T.Forgery and Corription of Personal Data | | | X | | | | | | | X | | X | | |
| T.BAC Authentication Key Disclose | X | | X | | | | | X | | X | | | | |
| T.BAC REPLAY ATTACK | | | | | | | | | X | | | | | |
| T.Damage to Biometric Data | | | X | X | | X | | | | X | | | X | |
| T.EAC-CA BYPASS | | X | | | | | | | | | | | | |
| T.IS CERTIFICATE FORGERY | X | | | | X | X | | | | | | | | |
| T.SESSION DATA REUSE | | | | | | | | | X | | | | | |
| T.Skimming | | | | | | | | | | X | | X | X | |
| T.MALFUNCTION | | | | | | | X | | | | | | | |
| T.Leakage to cryptographic key information | | | | | | | | | | | | | | |
| T.ePassport Reproduction | | | | | X | | | | | | X | | X | |
| T.Residual Information | | | | | | | | X | | | | | | |
| P.INTERNATIONAL COMPATIBILITY | | | | | | | | | | | | | | |
| P.Security Mechanism Application Procedures | | X | | | | | | | | | | | | |
| P.APPLICATION PROGRAM LOADING | | | | | | | X | | | | | | | |
| P.Personalization Agent | X | | | | | | | | | X | | | | x |
| P.ePassport Access Control | X | | | | | | | | | X | | X | X | x |
| P.PKI | | | | | | X | | | | | | | | |
| P.Range of RF Communitation | | | | | | | | | | | | | | |
| A.CERTIFICATE VERIFICATION | | | | | | | | | | | | | | |
| A.INSPECTION SYSTEM | | | | | | | | | | | | | | |
| A.IC Chip | | | | | | | | | | | | | | |
| A.MRZ ENTROPY | | | | | | | | | | | | | | |

**O.Access Control**
This security objective is required to counter the threats of T. Forgery and Corruption of Personal Data, T. Damage to Biometric Data and T. Skimming and enforce the organizational security policies of P. ePassport Access Control by implementing the rules of allowing or denying of Inspection System to read user data in accordance with the ePassport access control policies by the Personalization agent.
This security objective is required to counter the threats of T. TSF Data Modification and T. BAC Authentication Key Disclose as it allows the authorized personalization agent has the write-rights of the MRTD application data in the Personalization phase and denies the access by P.Personalization Agent in the Operational Use phase.

**O.AA**
This security objective is required to counter the threats of T.ePassport Reproduction by implementing the rules of allowing of Inspection System to verify a counterfeit with AA Security Mechanism.

**O.BAC**
This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the BAC security mechanism to control access to the personal data of the ePassport holder, therefore gives the read-rights for the personal data of the ePassport holder only to the authorized Inspection System of which the BAC mutual authentication is successfully completed.
This security objective is required to counter the threats of T. Forgery and Corruption of Personal Data and T. Skimming as the TOE allows the read-rights for the personal data of the ePassport holder only to the authorized Inspection System by generating the BAC session key during the BAC mutual authentication and denies access by the Inspection System that does not have the read-rights.

**O.CERTIFACATE VERIFICATION**
This security objective is required to enforce the organizational security policies of P. PKI as it ensures for the TOE to check the valid date on the basis of the CVCA link certificate provided by the Inspection System, therefore to automatically update the certificate and the current date. This security objective is required to counter the threats of T. Damage to Biometric Data and T. IS Certificate Forgery by determining the status of forgery as the TOE verifies validity of the CVCA link certificate, DV certificate and IS certificate in the EAC-TA.

**O.DELETING Residual Information**
This security objective is required to counter the threat of T. Residual Information by deleting all of the previous security-related information (BAC session key and EAC session key, etc.) so that it is not included when the TOE allocates or deallocates memory resources, therefore ensuring that information is not available. This security objective is required to counter the threat of T. BAC Authentication Key Disclose by providing the means to ensure that residual information remaining in temporary memory is not available.

**O.Domain separation**
This security objective is required to counter the threat of T. Application Program Interference as the TOE provides the means to prevent interference and tampering from external IT entities by separating execution domains between the TSF loaded in the MRTD chip and other application programs. This security objective is required to counter the threat of T. TSF Data Modification by preventing TSF data modification as

the COS blocks an access from external entities when the TOE records the TSF data in secure memory.
This security objective is required to counter the threat of T. IS Certificate Forgery by protecting the CVCA certificate recorded by the Personalization agent in secure memory in order to detect forgery of the CVCA link certificate from external interference and tampering. This security objective is required to counter the threat of T. ePassport Reproduction because reproduction of TSF data stored in secure memory is not possible even though an attacker reproduces user data in EF domain by manufacturing illegal chip.

**O.EAC**

This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the ePassport holder, therefore gives the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System of which the EAC-TA is successfully completed.
This security objective is required to counter the threats of T. Damage to Biometric Data and T. Skimming as the TOE allows the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System through the EAC-TA by generating the EAC session key during the EAC-CA and denies access by the Inspection System that does not have the read-rights. Moreover, this security objective is required to counter the threats of T.ePassport Reproduction as the TOE allows the method to judge the illegal counterfeit during EAC-CA.

**O.MANAGEMENT**

This security objective ensures that the TOE provides the means to write user data in EF domain and the means to write TSF data in secure memory only to the authorized Personalization agent in the Personalization phase and prevents unauthorized access using external interface by deactivating the MRTD application data writing function of the Personalization agent in the Operational Use phase. Therefore, this security objective is required to counter the threats of T. TSF Data Modification and T. BAC Authentication Key Disclose and to enforce the organizational security policies of P. ePassport Access Control and P. Personalization Agent
Also, this security objective provides the Personalization agent with the means to record CVCA certificate in secure memory in the Personalization phase, therefore is required to counter the threat of T. IS Certificate Forgery.

**O.REPLAY PREVENTION**

This security objective is required to counter the threat of T. BAC Replay Attack and T.Reuse Issuer Certification by ensuring that the TOE generates different values per session that are transmitted to the Inspection System in the BAC mutual authentication and SCP02 mutual authentication. Also, this security objective is required to counter the threat of T. Session Data Reuse by ensuring that different random numbers are generated and used per each session of security mechanism because the TOE ensures that the BAC authentication key is not used as the BAC session key in the BAC mutual authentication and the BAC session key is not generated with the same random number used in the BAC mutual authentication and checks the status of replay of random number transmitted by the EIS in the EAC.

**O.SECURE MESSAGING**

This security objective ensures that the TOE establishes the BAC or EAC secure messaging for secure transmission of the personal and biometric data of the ePassport holder to the Inspection System, and provides the confidentiality and integrity for the transmitted personal and biometric data of the ePassport holder. Therefore, this security objective is required to counter the threats of T. Damage to Biometric Data and T. Eavesdropping. Also, this security objective is required to counter the threat of T. TSF Data Modification by establishing SCP02 secure messaging when the authorized Personalization agent records TSF data in the Personalization phase, therefore providing integrity for TSF data.

**O.Security Mechanism Application Procedures**
This security objective is required to enforce the organizational security policies of P. Security Mechanism Application Procedures since the TOE ensures that the application order of the PA, BAC and EAC security mechanisms according to 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specifications and by not allowing requests from the Inspection System that do not correspond to the security mechanism application order. Also, this security objective is required to counter the threat of T. EAC-CA Bypass by eliminating the cases of demonstrating the genuine TOE to the unauthorized Inspection System as it ensures the application order of security mechanisms so that to enable the EAC-CA execution by only the Inspection System with access-rights for the EAC chip authentication public key through the BAC execution.

**O.SELF-PROTECTION**
This security objective is required to counter the threat of T. Malfunction as the TOE detects modification of the TOE executable code and data through self-testing, provides the means to prevent TOE security function bypassing attempts and protects the TOE itself by preserving a secure state so that malfunction of TSF do not occur. Also, this security objective prohibits from deleting ePassport applet by Organizational Security Policies P.APPLICATION PROGRAM LOADING.

**O.SESSION TERMINATION**
This security objective ensures that the TOE prevents continuous authentication attempts of authentication in order for access to forge and corrupt the personal or biometric data of the ePassport holder and terminates session in case modification for the transmitted TSF data is detected. Therefore, this security objective is required to counter the threats of T. Forgery and Corruption of Personal Data, T. Damage to Biometric Data, T. BAC Authentication Key Disclose and T. TSF Data Modification

**O.SCP02**
This security objective is required to enforce the organizational security policies of P.ePassport Access Control, P.Personalization Agent as the TOE implements SCP02 mutual authentication to ensure the ePassport Issuer center and issue ePassport in secure and TOE provides the way to manage the ePassport user data and TSF data in personalization phase.

### 8.1.2. Rationale of Security Objectives for the Environment

Table 18 shows the mapping for security environments.

**Table 18 TOE Summary of Mappings for Security Environment**

| Security Objects | Security Objectives for the Environment |
|---|---|

| | OE.PASSPORT BOOK MANUFACTURING SECURITY | OE.PROCEDURES OF ePassport HOLDER CHECK | OE.APPLICATION PROGRAM LOADING | OE.CERTIFACATE VERIFICATION | OE.PERSONALIZATION AGENT | OE.Handling Information Leakage | OE.INSPECTION SYSTEM | OE.IC Chip | OE.MRZ ENTROPY | OE.PKI | OE.RANGE OF RF COMMUNICATION |
|---|---|---|---|---|---|---|---|---|---|---|---|
| T.APPLICATION PROGRAM INTERFERENCE | | | X | | | | | | | | |
| T.Reuse Issuer Certification | | | | | | | | | | | |
| T.TSF Data Modification | | | | | X | | | | | | |
| T.Eavesdropping | | | | | | | X | | | | |
| T.FORGERY AND CORRIPTION OF PERSONAL DATA | | | | | | | X | | | | |
| T.BAC Authentication Key Disclose | | X | | | | | | | | | |
| T.BAC REPLAY ATTACK | | | | | | | | | | | |
| T.Damage to Biometric Data | | | | X | | | X | | | X | |
| T.EAC-CA BYPASS | | X | | X | | | X | | | | |
| T.IS CERTIFICATE FORGERY | | | | X | | | | | | | |
| T.SESSION DATA REUSE | | | | | | | X | | | | |
| T.Skimming | | | | | | | X | | | | X |
| T.MALFUNCTION | | | | | | | | X | | | |
| T.Leakage to cryptographic key information | | | | | | X | | X | | | |
| T.ePassport Reproduction | X | X | | | | | X | | | | |
| T.Residual Information | | | | | | | | | | | |
| P.INTERNATIONAL COMPATIBILITY | | | | | X | | | | | | |
| P.Security Mechanism Application Procedures | | | | | | | X | | | | |
| P.APPLICATION PROGRAM LOADING | | | X | | | | | | | | |
| P.Personalization Agent | | | | | X | | | | | | |
| P.ePassport Access Control | | | | | X | | X | | | | |
| P.PKI | | | | | | | | | | X | |
| P.Range of RF Communication | | | | | | | | | | | X |
| A.CERTIFICATE VERIFICATION | | | | X | X | | | | | X | |
| A.INSPECTION SYSTEM | | | | | | | X | | | | |
| A.IC Chip | | | | | | | | X | | | |
| A.MRZ ENTROPY | | | | | | | | | X | | |

### OE. Application Program Loading

This security objective for environment is required to enforce the organizational security policies of P.APPLICATION PROGRAM LOADING by approving application program loading after checking that application programs loaded in the MRTD chip does not affect the secure TOE. This Security Objectives for the Environment is required to counter the threats of T.APPLICATION PROGRAM INTERFERENCE as only certified personalization agent should load application program due to protecting from interference and infringement of TSF

### OE.CERTIFACATE VERIFICATION

This security objective for environment verifies the SOD after verifying regularly the DS certificate and CRL in order for the Inspection System, such as the BIS and EIS, to verify for forgery and corruption of the ePassport identity data recorded in the TOE. Also, this security objective for environment ensures for the EIS to securely maintains digital signature generation key that corresponds to the IS certificate and to provide the TOE with the CVCA link certificate, DV certificate and IS certificate in the EAC-TA. Therefore, this security objective for environment is required to counter the threats of T. Damage to Biometric Data, T. EAC-CA Bypass and T. IS Certificate Forgery and support the assumption of A. Certificate Verification.

### OE.Handling Information Leakage

This security objective for environment is required to counter the threats of T.Leakage To Cryptographic Key Information by protecting from achieving key information using analyzing power or RF wave during calculating crypto algorithm.

### OE.IC Chip

This security objective for environment is required to support the assumption of A. IC Chip as it uses EAL4+(SOF-high) IC chip that generates random number and provides cryptographic operation in order to support security functions of the TOE and provides the malfunction detection and physical protection, etc.

Also, this security objective for environment is required to counter the threat of T.Malfunction and T.Leakage To Cryptographic Key Information as the IC chip detects malfunction outside the normal operating conditions.

### OE.INSPECTION SYSTEM

This security objective for environment is required to support the assumption of A.Inspection System and enforce the organizational security policies of P. Security Mechanism Application Procedures and P. ePassport Access Control as the Inspection System implements and ensures application order of security mechanisms in accordance with the type of the Inspection System so that not to violate the ePassport access control policies of the Personalization agent and by ensuring that information used in communication with the TOE is securely destroyed after session termination.

This security objective for environment is required to counter the threat of T.Eavesdropping as the confidentiality and integrity of the transmitted data are ensured by establishing the BAC secure messaging after generating the BAC session key through the BAC key distribution when the Inspection System communicates with the TOE.

This security objective for environment is required to counter the threats of T. Forgery and Corruption of Personal Data, T. Damage to Biometric Data, T. Skimming and T.EAC-CA Bypass as the Inspection System supports the BAC mutual authentication, EAC and PA.

This security objective for environment is required to counter the threat of T. Session Data Reuse as the Inspection System generates different temporary public key precession to be transmitted to the TOE in the EAC-CA.

**OE.MRZ ENTROPY**
This security objective for environment is required to support the assumption of A. MRZ Entropy by providing MRZ entropy necessary for the Personalization agent to ensure the secure BAC authentication key.

**OE.PASSPORT BOOK MANUFACTURING SECURITY**
This security objective for environment is required to counter the threat of T. ePassport Reproduction by ensuring that Physical security measures(security printing, etc.) for the ePassport are prepared to detect reproduction of the MRTD chip and attack attempt of the Grandmaster chess, replacement of the portrait and modification of the MRZ data, etc.

**OE.PERSONALIZATION AGENT**
This security objective for environment is required to enforce the organizational security policies of P. International Compatibility and P. Personalization Agent by ensuring that the TOE is delivered to the Operational Use phase after securely issuing the ePassport so that the Personalization agent can check that the issuing subject has not been changed, verifying normal operation and compatibility of the ePassport in the Personalization phase and deactivating writing function. This security objective for environment also is required to enforce the organizational security policies of P.ePassport Access Control as it defines the role of the Personalization agent. Also, this security objective for environment is required to support the assumption of A. Certificate Verification because the Personalization agent makes certificates necessary in the PA and EAC support available to the Inspection System. This security objective for environment is required to counter the threat of T. TSF Data Modification because the Personalization agent deactivates writing function in the Operational Use phase, therefore disables the writing function for modification of the TSF data.

**OE.PKI**
This security objective for environment is required to enforce the organizational security policies of P.PKI and supports the assumption of A.Certificate Verification by implementing and operating the ePassport PKI System that executes certification practice according to CPS, such as to generate digital signature key and to generate· issue· distribute of certificates necessary in supporting PA and EAC security mechanisms. Also, this security objective for environment is required to counter the threat of T.Damage to Biometric Data by generating, issuing and distributing certificates necessary in the EAC through implementation of the EAC-PKI.

**OE.PROCEDURES OF ePassport HOLDER CHECK**
This security objective for environment is required to counter the threats of T.ePassport Reproduction, T.BAC Authentication Key Disclose and T.EAC-CA Bypass by implementing procedural security measures in immigration process, such as procedures to check the printed identify information page of the ePassport and to determine the forgery status of the ePassport book, etc.

**OE.RANGE OF RF COMMUNICATION**
This security objective for environment is required to counter the threat of T.Skimming and enforce the organizational security policies of P.Range of RF communication by ensuring that RF communication distance between the MRTD chip and the Inspection System is less than 5cm and that RF communication channel is not established if the page of the ePassport attached with the IC chip is not opened.

## 8.2. Rationale for Security Requirements

The rationale for security requirements demonstrates that the described IT security requirements are suitable to satisfy security objectives and, as a result, appropriate to address security problems.

### 8.2.1. Rationale of TOE Security Function Requirement

The rationale of TOE security functional requirements demonstrates the followings :

- Each TOE security objective has at least one TOE security function requirement tracing to it.
- Each TOE security functional requirement traces back to at least one TOE security objectives.
-

Table 19 presents the mapping between the security objectives and the security functional requirements.

### Table 19 Summary of Mappings between Security Objectives and Security Functional Requirements

| Security Objects | TOE Security Objects | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Security Functional Requirements | O.Management | O.Security Mechanism Application Procedures | O.Session Termination | O.SECURE MESSAGING | O.domain separation | O.CERTIFACATE VERIFICATION | O.SELF-PROTECTION | O.DELETING Residual Information | O.REPLAY PREVENTION | O.Access Control | O.AA | O.BAC | O.EAC | O.SCP02 |
| FCS_CKM.1(1) | | | | | | | | | | | | X | X | |
| FCS_CKM.1(2) | | | | | | | | | | | | | | X |
| FCS_CKM.2(1) | | | | | | | | | X | | | X | | |
| FCS_CKM.4 | | | | | | | | X | | | | | | |
| FCS_COP.1(1) | | | | | | | | | | | | X | X | |
| FDP_ACC.1(1) | | | | | | | | | | X | | | | |
| FDP_ACC.1(2) | | | | | | | | | | X | | | | |
| FDP_ACF.1(1) | X | X | | | | | | | | X | | X | X | X |
| FDP_ACF.1(2) | X | | | | | | | | | X | | | | X |
| FDP_DAU.1 | | | | | | | | | | | X | | X | |
| FDP_RIP.1 | | | | | | | | X | X | | | | | |
| FDP_UCT.1 | | | | X | | | | | X | | | | | |
| FDP_UIT.1 | | | | X | | | | | X | | | | | |
| FIA_AFL.1(1) | | X | X | | | | | | | X | | X | | X |
| FIA_AFL.1(2) | | X | | | | | | | | X | | | X | |
| FIA_UAU.1(1) | | | X | | | | | | | X | | X | | |
| FIA_UAU.1(2) | | X | X | | | | | | | X | | | X | |
| FIA_UAU.1(3) | | | X | | | | | | | X | | | | X |
| FIA_UAU.4 | | | | | | | | | X | | | X | X | X |
| FIA_UAU.5 | | X | | | | | | | | X | | X | X | X |
| FIA_UID.1 | | | | | | | | | | | | X | X | X |
| FMT_MOF.1(1) | X | | | | | | | | | X | | | | |
| FMT_MOF.1(2) | X | | | | | | | | | X | | | | |
| FMT_MSA.1 | | | | X | | | | | | X | | | | |
| FMT_MSA.3 | X | | | | | | | | | X | | | | |
| FMT_MTD.1(1) | X | | | | | | | | | X | | | | |
| FMT_MTD.1(2) | | X | | | | | | | | | | | | |
| FMT_MTD.1(3) | X | | | | | | | | | X | | | | |
| FMT_MTD.3 | | | | | | X | | | X | | | | X | |
| FMT_SMF.1 | X | | | | | X | | | | | | | | |
| FMT_SMR.1 | X | | | | | | | | | | | | | |
| FPT_FLS.1 | | | | | | | X | | | | | | | |
| FPT_ITI.1 | | | X | X | | | | | | | | | | |
| FPT_RVM.1 | | | | | | | X | | | X | | | | |
| FPT_SEP.1 | | | | | X | | | | | X | | | | |
| FPT_TST.1 | | | | | | | X | | | | | | | |

**FCS_CKM.1(1) Cryptographic key generation (KEY DERIVATION MECHANISM)**

This component requires to generate the 112 bit BAC authentication key, BAC and EAC session keys according to the cryptographic key generation algorithm specified in the ICAO document. Through this, the BAC authentication key is generated for use in the BAC mutual authentication and BAC/EAC session key is generated for use in the BAC/EAC secure messaging. Therefore, this component satisfies the security objectives of O.BAC and O.EAC.

**FCS_CKM.1(2) Cryptographic key generation (SCP02 Session Key)**

This component requires to generate the 112 bit SCP02 session keys according to the cryptographic key generation algorithm specified in the [VGP]. Through this, SCP02 session key is generated for use in the SCP02 mutual authentication and SCP02 secure messaging.

**FCS_CKM.2(1) Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)**

This component defines the method to distribute seed of key derivation mechanism necessary in generating the BAC session key to the Inspection System (ISO/IEC 11770-2 Key Establishment Mechanism 6). The distribution method defined in this component satisfies the security objective of O.Replay Prevention as it uses random numbers and O.BAC as it enables to generate the BAC session key of FCS_CKM.1 by generating KDF seed.

**FCS_CKM.4 Cryptographic key destruction**

This component defines the method to securely destroy the key generated by key derivation mechanism of FCS_CKM.1(1) and SCP02 session key generation mechanism of FCS_CKM.1(2). This component satisfies the security objective of O.Deleting Residual Information as it provides the method of destroying the key generated by the TSF and remained in temporary memory with the resetting 'zero' method.

**FCS_COP.1(1) Cryptographic operation (Symmetric Key Cryptographic Operation)**

This component defines SHA-1(ISO/IEC 10118-3) hash operation used to KDF distribution of FCS_CKM.1(1). This hash operation defined in this component satisfies the security objective of O.BAC, O.EAC as it enable to generate the BAC session key and EAC session key by generating KDF seed.

**FDP_ACC.1(1) Subset access control (ePassport)**

This component defines list of subjects, objects and operations in order to decide a scope of control for the ePassport access control policies. The ePassport access control policies defined in this component satisfies the security objective of O.Access Control as it defines the Personalization agent, Inspection System as subjects, the personal data and biometric data of the ePassport holder and ePassport authentication data, etc. as objects and their relationship as operations.

**FDP_ACC.1(2) Subset access control (Operating System)**

This component defines list of subjects, objects and operations in order to decide a scope of control for the Operating System access control policies. The Operating System access control policies defined in this component satisfies the security objective of O.Access Control as it defines the Personalization agent as subjects, the data of the Personalization agent and Personalization agent authentication data as objects and their relationship as operations.

### FDP_ACF.1(1) Security attribute based access control (ePassport)

In order to enforce the ePassport access control policies, this component defines security attributes of subjects and objects defined in FDP_ACC.1(1) and specify the ePassport access control rules. Security attributes and the ePassport access control rules defined in this component satisfy the security objectives of O.Management and O.Access Control as only the authorized Personalization agent with the Personalization agent issuing authorization can perform management functions.
Also, this component satisfies the security objectives of O.BAC, O.EAC and O.SCP02 because the read-rights for the personal data of the ePassport holder and TSF data is allowed only to the subjects holding the personalization authorization, the read-rights for the personal data of the ePassport holder and ePassport authentication data, etc. is allowed only to the subjects holding the BAC authorization and the read-rights for the biometric data of the ePassport holder is allowed only to the subjects holding the EAC authorization.
The explicitly deny rules of FDP_ACF.1.4 defined in this component satisfy the security objective of O.Security Mechanism Application Procedures because the application order of security mechanisms is ensured as access by the Inspection System is denied when the order of transmitted instructions specified in 2.1 Inspection Procedures of the EAC specifications is violated.

### FDP_ACF.1(2) Security attribute based access control (Operating System)

In order to enforce the Operating System access control policies, this component defines security attributes of subjects and objects defined in FDP_ACC.1(2) and specifies the Operating System access control rules. Security attributes and the Operating System access control rules defined in this component satisfy the security objectives of O.Management and O.Access Control as only the authorized Personalization agent with the Personalization agent issuing authorization can perform Operating System management functions. Also, this component satisfies the security objectives of O.SCP02 because the read-rights for the Operating System management function is allowed only to the subjects holding the personalization authorization

### FDP_DAU.1 Basic Data Authentication

When receiving AA request from Inspection System to ensure the validity of ePassport user data, TOE generates digital signature on random number received in AA request process with AA chip authentication private key in secure memory and provides inspection system with it. This component satisfies the security objectives of O.AA because inspection system verifies whether TOE is illegally copied with AA chip authentication public key from EF.DG15.
Also, this component satisfies the security objectives of O.EAC because EIS performs ECDH operation by using temporary public key generated using EAC-CA chip authentication public key information and EAC-CA chip authentication private key in secure memory. So EIS verifies illegal copy of TOE depending on the success of EAC-CA in the case of EAC-CA request from EIS.

### FDP_RIP.1 Subset residual information protection

This component ensures that previous information is not included when the TSF allocates or deallocates memory resources for the SCP02 session key, BAC authentication key, BAC session key, EAC session key and random numbers.
This component satisfies the security objective of O.Deleting Residual Information as it ensures that previous information of the SCP02 session key, BAC authentication key, BAC session key and EAC session key is not available when destroying these keys

according to the method of destruction defined in FCS_CKM.4. Also, this component satisfies the security objective of O.Replay Prevention by ensuring that previous information of random numbers used for the SCP02 mutual authentication, BAC mutual authentication, TAC-TA and generation of session key is not available.

**FDP_UCT.1 Basic data exchange confidentiality**

This component defines the method to protect from disclosure when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies. This component establishes the BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session encryption key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session encryption key. Therefore, this component satisfies the security objective of O.Secure Messaging as the confidentiality of user data is ensured.

This component satisfies the security objective of O.Replay Prevention by ensuring that the BAC session encryption key is not used the same as the BAC authentication key when establishing the BAC secure messaging.

**FDP_UIT.1 Data exchange integrity**

This component defines the method to protect from modification, deletion, insertion, replay when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies.

This component establishes the BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session MAC key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session MAC key. Therefore, this component satisfies the security objective of O.Secure Messaging as the integrity of user data is ensured.

This component satisfies the security objective of O.Replay Prevention by ensuring that the BAC session MAC key is not used the same as the BAC authentication key when establishing the BAC secure messaging.

**FIA_AFL.1(1) Authentication failure handling (USER SESSION TERMINATION)**

If the SCP02 mutual authentication and BAC mutual authentication attempt failure number is more than 1, this component detects it and requires to terminate a user session.

This component satisfies the security objective of O.Session Termination as the session is terminated if the authentication attempt failure number of the BAC mutual authentication and SCP02 mutual authentication is surpassed. Also, this component satisfies the security objective of O.Security Mechanism Application Procedures by disabling the unauthorized external entity to move on to the next phase of inspection procedures by terminating session if the BAC mutual authentication fails.

In addition, this component satisfies the security objectives of O.SCP02, O.BAC and O.Access Control because access to user data is denied by terminating session as BAC mutual authentication or SCP02 mutual authentication failure is considered that there is no the access-rights for user data.

**FIA_AFL.1(2) Authentication failure handling (REPLAY PREVENTION)**

If the authentication EAC-TA attempt failure number is more than 1, this component detects it and requires that additional EAC-TA on the same EAC secure communication channel is not permitted.

This component satisfies the security objective of O.Security Mechanism Application, Procedures, O.EAC and O.Access Control because access to biometric data is denied as EAC-TA failure is considered that there is no the access-rights for biometric data.

**FIA_UAU.1(1) Timing of authentication (BAC mutual authentication)**
This component defines the functions the user to be performed before the BAC mutual authentication and executes the BAC mutual authentication for user.
In this component, the BAC mutual authentication is executed in order to enable the Inspection System identified in FIA_UID.1 to execute the indication function to support the BAC mechanism and to read the personal data of the ePassport holder. This component satisfies the security objectives of O.Session Termination, O.BAC and O.Access Control as it enables detection by FIA_AFL.1(1) if the authentication fails and allows the read-rights for the personal data of the ePassport holder if the authentication succeeds.

**FIA_UAU.1(2) Timing of authentication(EAC-TA)**
This component defines the functions the user to be performed before the EAC-TA and executes the EAC-TA for user.
In this component, only the Inspection System of which the BAC mutual authentication succeeded in FIA_UAU.1(1) can execute EAC-CA and reading of user data (exception of the biometric data of the ePassport holder). To read the biometric data of the ePassport holder, the EAC-TA shall be executed. This component satisfies the security objectives of O.Security Mechanism Application Procedures, O.Session Termination, O.EAC and O.Access Control as it enables detection by FIA_AFL.1(1) if authentication fails and allows the read-rights for the biometric data of the ePassport holder if authentication succeeds.

**FIA_UAU.1(3) Timing of authentication(SCP02 mutual authentication)**
This component defines the functions the user to be performed before the SCP02 mutual authentication and executes the SCP02 mutual authentication for user.
In this component, the Personalization Agent specified in FIA_UAU.1 should execute the SCP02 mutual authentication before allowing any other TSF-mediated actions.
This component satisfies the security objectives of O.Session Termination, O.SCP02 and O.Access Control as it enables detection by FIA_AFL.1(2) if authentication fails and allows the read-rights for the user data of the ePassport holder and TSF-mediated actions if authentication succeeds.

**FIA_UAU.4 Single-use authentication mechanisms**
This component requires that authentication-related information sent by the TSF to the Inspection System in the SCP02 mutual authentication, BAC mutual authentication and the EAC-TA, is not replay.
This component satisfies the security objectives of O. Replay Prevention, O. BAC and O.EAC as the TSF executes the SCP02 mutual authentication, BAC mutual authentication and EAC-TA by generating different random numbers used in the SCP02 mutual authentication, BAC mutual authentication and EAC-TA per session and transmitting them to the Inspection System.

**FIA_UAU.5 Multiple authentication mechanisms**
This component defines multiple authentication mechanisms and the rules of applying authentication mechanism according to type of user data to be accessed by the Inspection System.
This component satisfies the security objectives of O.Security Mechanism Application Procedures, O.Access Control, O.BAC, O.EAC, O.SCP02 as the Personalization Agent

holds the personalization authorization and management authority by succeeding in SCP02 mutual authentication and the Inspection System holds the BAC authorization by succeeding in BAC mutual authentication and the EAC authorization by succeeding in the EAC-CA, EAC-TA and certificate verification after the BAC mutual authentication according to authentication mechanism application rules.

**FIA_UID.1 Timing of identification**

This component requires to establish the communication channel based on contactless IC card transmission protocol (ISO/ IEC 14443-4) as the functions the user to be performed before the identification and to identify the user.

This component satisfies the security objectives of O.BAC, O.SCP02 and O.EAC as the external entity is identified with the Inspection System or Personalization Agent, if an external entity to establish the communication channel request to use the MRTD application.

**FMT_MOF.1(1) Management of security functions behaviour(WRITING ePassport)**

This component defines that the ability to disable writing function is given only to the Personalization agent in the Personalization phase.

This component satisfies the security objectives of O.Management and O.Access Control by deactivating the writing function of the Personalization agent in the Personalization phase so that the TOE in the Operational Use phase cannot record any data.

**FMT_MOF.1(2) Management of security functions behaviour (CHANGING LIFECYCLE OF Operating System)**

This component defines that the ability to decide action to change lifecycle of Operating System function is given only to the Personalization agent.

This component satisfies the security objectives of O.Management by determining the delegation of authority of changing lifecycle of Operating System to application when Personalization agent installs application.

**FMT_MSA.1 Management of security attributes**

This component requires to restrict the ability of initializing user security attributes only to the TSF as an action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1.

This component satisfies the security objectives of O.Secure Messaging and O.Access Control as the integrity is ensured and access to the MRTD application data is blocked by resetting the previously given security attributes of the Personalization agent or the Inspection System as an action to be taken if the TSF detects modification of the transmitted TSF data.

**FMT_MSA.3 Static attribute initialization**

This component requires to prohibit from describing the initial values for security attributes and to restrict default values for security attributes when an object is created

This component satisfies the security objectives of O.Management and O.Access Control as security attributes of user data and Operating System user data are in implementation logic of the TOE in order to enforce the ePassport access control policies Operating System access control policies and specifies initial values are not allowed.

**FMT_MTD.1(1) Management of TSF data (Certificate Verification Info.)**

This component restricts that only the Personalization agent in the Personalization phase writes certificate verification information necessary for the EAC-TA in secure memory.

This component satisfies the security objectives of O.Management and O.Access Control by enabling only the authorized Personalization agent to have the ability to write TSF data, such as the EAC chip authentication private key, current data, CVCA certificate and CVCA digital signature verification key, etc., in secure memory in the Personalization phase

**FMT_MTD.1(2) Management of TSF data (SSC Initialization)**

This component requires to terminate BAC secure messaging before the EAC secure messaging is established.

This component satisfies the security objective of O.Security Mechanism Application Procedures by initializing SSC (send sequence counter) to '0' in order to terminate the BAC secure messaging after generating the EAC session key and newly establishing the EAC secure messaging.

**FMT_MTD.1(3) Management of TSF data (Management Operating System)**

This component restricts that only the Personalization agent succeed in SCP02 authentication changes GP registry.

This component satisfies the security objective of O.Management by restricting the change-right of GP registry to Personalization Agent.

**FMT_MTD.3 Secure TSF Data**

This component requires to allow only secure values as the TSF data in order to ensure the secure random numbers and to ensure that valid date of certificates used in EAC-TA has not expired.

This component satisfies the security objective of O.Replay Prevention because only the secure random numbers are used in order to prevent a replay attack when the TSF generates session key.

Also, the TSF compares the CVCA link certificate provided by the Inspection System with the CVCA certificate stored in the TOE in order for verification of the IS certificate used in the EAC-TA. If the CVCA certificate update is necessary, the TSF internally updates the CVCA certificate, CVCA digital signature verification key, current dates and EF.CVCA, therefore maintains the TSF data as secure values. This component satisfies the security objectives of O.Certificate Verification and O.EAC because the EAC-TA can be successfully executed by verifying the DV certificate and IS certificate with the secure CVCA certificate.

**FMT_SMF.1 Specification of management functions**

This component provides the means to manage the MRTD application data in the Personalization phase.

This component satisfies the security objective of O.Management as it defines the writing function of user data and TSF data in the Personalization phase and it provides the various functions (Management Application, Writing and changing of Personalization Agent data, Personalization Agent authentication data and GP registry, delegation of changing lifecycle of Operating System to application ) as a way of managing data of Operating System.

Also, this component satisfies the security objective of O.Certificate Verification as it provides the function for the TSF to update the CVCA certificate, the CVCA digital signature verification key and current dates, etc. by itself in the Operational Use phase.

**FMT_SMR.1 Security roles**

This component defines the role of the Personalization agent to manage the MRTD

application data.
This component satisfies the security objective of O.Management as it defines the role of the Personalization agent that executes the writing function of user data and TSF data in the Personalization phase.

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

This component requires to preserve a secure state when the types of failures occur, such as the failure detected from the self-testing and abnormal operating conditions detected by the IC chip, etc.
This component satisfies the security objective of O.Self-protection as it preserves a secure state to prevent the malfunction of the TSF when the modification of integrity of the TSF data or executable code from the self-testing of FPT_TST.1 is detected or the IC chip detects abnormal operating conditions. When the IC chip detects abnormal operating conditions, TOE is able to stop the malfunction for the prevention of malfunction of TSF.

### FPT_ITI.1 Inter-TSF detection of modification

This component requires to detect modification in the transmitted TSF data and defines an action to be taken if modifications are detected.
This component satisfies the security objectives of O.Secure Messaging and O.Session Termination by detecting modification of the transmitted TSF data in the Personalization and Operational Use phases and by performing an action to be taken, such as terminating the related communication channels, deleting the related session key and management actions specified in FMT_MSA.1, etc., if modifications are detected

### FPT_RVM.1 Non-bypassability of the TSP

This component requires to always invoke the ePassport access control function as a reference monitor to protect the TSF from manipulating operation and bypassing access control policy, etc. by untrusted subjects.
This component satisfies the security objectives of O.Self-protection and O.Access Control together with FPT_SEP.1 as the ePassport access control function is always invoked, therefore serves the role as a reference monitor in order to protect all subjects, objects and operations included within a scope of control for the ePassport access control policies defined in FDP_ACC.1.(1)

### FPT_SEP.1 TSF domain separation

This component defines the security domains in order to protect subjects, objects, operations and the TSF data included within a scope of control of the ePassport access control policies from external interference and tampering by untrusted subjects.
This component satisfies the security objectives of O.Access Control and O.Domain Separation by separating domains used by untrusted subjects, such as other application programs, etc. from the domain in which the ePassport access control function is executed.
Also, this component satisfies the security objective of O.Domain Separation by separating secure memory domain from other memory domains, therefore protecting the TSF data from external IT entities.

### FPT_TST.1 TSF Testing

This component requires self-testing to detect loss of the TSF executable code and the TSF data by various failures (unexpected failure mode, lack of the IC chip design and intentionally damage to the TSF, etc.).

This component satisfies the security objective of O.Self-protection by running self-testing under the self-testing execution conditions during booting TOE , therefore demonstrating the correct operation of the TSF.
Also, this component satisfies the security objective of O.Self-protection by verifying the integrity of TSF data and the TSF executable code stored in the TOE, therefore detecting loss of the TSF data and the executable code.

### 8.2.2. Rationale for Security Requirement for the environment

| Security Objectives for the Environment / Security Functional Requirements | OE.IC Chip | OE.Handling Information Leakage |
|---|---|---|
| FCS_CKM.2(2) | X | |
| FCS_COP.1(2) | X | |
| FCS_COP.1(3) | X | |
| FCS_COP.1(4) | X | |
| FCS_COP.1(5) | X | |
| FPR_UNO.1 | | X |

**FCS_CKM.2(2) Cryptographic key distribution (KDF Seed Distribution for EAC session key generation)**
This component defines the method to distribute seed of key derivation mechanism necessary in generating the EAC session key to the Inspection System (ECDH key distribution protocol of ISO/IEC 15946-3).
The distribution method defined in this component satisfies the security objective for the environment of OE.IC Chip by providing ECC crypto algorithm imbedded in IC Chip.

**FCS_COP.1(2) Cryptographic operation (Symmetric Key Cryptographic operation)**
This component defines TDES cryptographic operation (ISO/IEC 18033-3) used to authenticate the Inspection System that supports the BAC or to protect the transmitted user data from disclosure.
The cryptographic operation defined in this component satisfies the security objective for the environment of OE.IC Chip by providing TDES calculation hardware on IC Chip.

**FCS_COP.1(3) Cryptographic operation (MAC)**
This component defines Full Triple DES MAC, Retail MAC (ISO/IEC 9797-1) used to authenticate the Inspection System that supports the BAC or to detect modification of the transmitted user data or to authenticate Personalization Agent.
The MAC operation defined in this component satisfies the security objective for the environment of OE.IC Chip by providing TDES calculation hardware on IC Chip.

**FCS_COP.1(4) Cryptographic operation (Digital signature Verification for**

**Certificates Verification)**
This component defines the method of digital signature verification (ISO/IEC 15946-2) necessary in the EAC-TA.
The digital signature verification method defined in this component satisfies the security objective for the environment of OE.IC Chip by providing ECC crypto algorithm imbedded in IC Chip.

**FCS_COP.1(5) Cryptographic operation (Digital signature generation for AA)**
This component defines the method of digital signature generation (ISO/IEC 9796-2 의 ECDSA-SHA-1) necessary in the AA.
The digital signature generation method defined in this component satisfies the security objective of O.AA by generating and transmit the digital signature required by Inspection System.

**FPR_UNO.1 Unobservability**
This component ensures that external entities are unable to observe the cryptographic-related data, such as the BAC authentication key, BAC session key, EAC session key, EAC chip authentication private key and AA chip authentication private key, etc. when the TSF performs a cryptographic operation.
This component satisfies the security objective for the environment of OE. Handling Information Leakage as it ensures that external entities cannot find out any cryptographic-related data by exploiting physical phenomena (change of current, voltage and electromagnetic, etc.) occurred due to TDES hardware and ECC crypto algorithm in IC Chip when the TSF performs cryptographic operation of TDES, MAC and digital signature verification, etc.

### 8.2.3. Dependency of TOE Security Assurance Requirements

The EAL(Evaluation Assurance Level) of this Security Target was selected as EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) by considering the value of assets protected by the TOE and level of threats, etc.
EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs. This SecurityTarget partially selected assurance components that are higher than EAL4. The rationale of the augmented with assurance components are as follows.

**ADV_IMP.2 Implementation of the TSF, ATE_DPT.2 Testing: low-level design, AVA_VLA.3 Moderately resistant**

The TOE is an operating system and application program operated in the MRTD chip. Therefore, it largely depends on the IC chip in terms of cryptographic operation function and physical security. To ensure the secure MRTD chip, the reliability and secure operation of not only the TOE, but also the IC chip must be verified.

The TOE is developed by using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to design and operation of the TOE. Also, TOE is easily accessed as it is used in open environment and it is difficult to trace an attack. However, since the IC chip is not included in the scope of the TOE, it does not require understanding on hardware structure and advanced specialized equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing moderate attack potential. EAL4 includes AVA_VLA.2 that resistant the low attack potential. Therefore, AVA_VLA.3 is augmented to require execution of systematic vulnerability analysis and resistant to attackers possessing moderate attack potential. However, there still exists direct attack potential to the IC chip by threat agent possessing high attack potential and evaluation and verification for this may be assigned to the IC chip manufacturer.

It is difficult to correct of defects even if defects are occurred after issuing the ePassport loaded with the IC chip and this may be exploited by attackers. Therefore, ADV_IMP.2 is augmented to enable analysis on the entire implementation representation in order to check if the TSF is accurately implemented and defect code does not exist. Also, ATE_DPT.2 is augmented to enable detection of defects not discovered while developing the TOE through testing for subsystems and modules closely related to internal structure of the TSF.

## 8.3. Rationale of Dependency

### 8.3.1. Dependency of TOE Security Function Requirement

Table 20 shows dependency of TOE functional components

**Table 20 Dependency of TOE Security Functional Component**

| No. | Security Functional Component | Dependency | Ref. No. |
|---|---|---|---|
| 1 | FCS_CKM.1(1) | [FCS_CKM.2 or FCS_COP.1] | 3 |
| | | FCS_CKM.4 | 4 |
| | | FMT_MSA.2 | none(NO.1) |
| 2 | FCS_CKM.1(2) | [FCS_CKM.2 or FCS_COP.1] | 3 |
| | | FCS_CKM.4 | 4 |
| | | FMT_MSA.2 | none(NO.1) |
| 3 | FCS_CKM.2(1) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | 1 |
| | | FCS_CKM.4 | 4 |
| | | FMT_MSA.2 | none(NO.1) |
| 4 | FCS_CKM.4 | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | 1 |
| | | FMT_MSA.2 | none(NO.1) |
| 5 | FCS_COP.1(1) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | 1 |
| | | FCS_CKM.4 | 4 |
| | | FMT_MSA.2 | none(NO.1) |
| 6 | FDP_ACC.1(1) | FDP_ACF.1 | 8 |

| No. | Security Functional Component | Dependency | Ref. No. |
|---|---|---|---|
| 7 | FDP_ACC.1(2) | FDP_ACF.1 | 9 |
| 8 | FDP_ACF.1(1) | FDP_ACC.1 | 6 |
| | | FMT_MSA.3 | 25 |
| 9 | FDP_ACF.1(2) | FDP_ACC.1 | 7 |
| | | FMT_MSA.3 | 25 |
| 10 | FDP_DAU.1 | – | – |
| 11 | FDP_RIP.1 | – | – |
| 12 | FDP_UCT.1 | [FTP_ICT.1 or FTP_TRP.1] | none(NO.2) |
| | | [FDP_ACC.1 or FDP_IFC.1] | 6 |
| 13 | FDP_UIT.1 | [FDP_ACC.1 or FDP_IFC.1] | 6 |
| | | [FTP_ITC.1 or FTP_TRP.1] | none(NO.2) |
| 14 | FIA_AFL.1(1) | FIA_UAU.1 | 16, 18 |
| 15 | FIA_AFL.1(2) | FIA_UAU.1 | 17 |
| 16 | FIA_UAU.1(1) | FIA_UID.1 | 21 |
| 17 | FIA_UAU.1(2) | FIA_UAU.1(1) | 16 (NO.3) |
| 18 | FIA_UAU.1(3) | FIA_UID.1 | 21 |
| 19 | FIA_UAU.4 | – | – |
| 20 | FIA_UAU.5 | – | – |
| 21 | FIA_UID.1 | – | – |
| 22 | FMT_MOF.1(1) | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 23 | FMT_MOF.1(2) | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 24 | FMT_MSA.1 | [FDP_ACC.1 or FDP_ICF.1] | 6 |
| | | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 25 | FMT_MSA.3 | FMT_MSA.1 | 24 |
| | | FMT_SMR.1 | 31 |
| 26 | FMT_MTD.1(1) | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 27 | FMT_MTD.1(2) | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |
| 28 | FMT_MTD.1(3) | FMT_SMF.1 | 30 |
| | | FMT_SMR.1 | 31 |

| No. | Security Functional Component | Dependency | Ref. No. |
|---|---|---|---|
| 29 | FMT_MTD.3 | ADV_SPM.1 | EAL4 |
| | | FMT_MTD.1 | 26 |
| 30 | FMT_SMF.1 | – | – |
| 31 | FMT_SMR.1 | FIA_UID.1 | 21 |
| 32 | FPT_FLS.1 | ADV_SPM.1 | EAL4 |
| 33 | FPT_ITI.1 | – | – |
| 34 | FPT_RVM.1 | – | – |
| 35 | FPT_SEP.1 | – | – |
| 36 | FPT_TST.1 | FPT_AMT.1 | none(NO.4) |

**NO.1**
FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2(1), FCS_CKM.4, FCS_COP.1(1) have dependency with FMT_MSA.2, but the dependency in this ST is not satisfied. The target of generating, operating and destroying cryptographic key of FCS is TSF data. Therefore, rather than secure security attributes (FMT_MSA.2), FMT_MTD.3 of secure TSF data is satisfied.

**NO.2**
FDP_UCT.1 and FDP_UIT.1 have dependency with FTP_ITC.1 or FTP_TRP.1, but the dependency in this ST is not satisfied. FDP_UCT.1 and FDP_UIT.1 require secure messaging between the Inspection System and the TOE. Since the secure messaging between Inspection System and TOE is the unique channel, it is not necessary to be logically separated from other communicational channels. Therefore, in this security target, requirements of FTP_ITC.1 are not defined.

**NO.3**
FIA_UAU.1(2) has dependency with FIA_UID.1, but the dependency in this ST is not satisfied. Since the EAC-TA is executed after the BAC mutual authentication, FIA_UAU.1(2) depends on FIA_UAU.1(1) and FIA_UAU.1(1) depends on FIA_UID.1. Therefore, indirectly, the dependency is satisfied.

**NO.4**
FPT_TST.1 has dependency with FPT_AMT.1, but the dependency in this ST is not satisfied. FPT_AMT.1 is executed by the IC chip, the TSF underlying abstract machine rather than by the TOE. Therefore, testing if the IC chip is operating normally to support security functions of the TOE is satisfied by security objective for environment of OE. IC Chip.

### 8.3.2. Dependency of TOE Security Assurance Requirements

The dependency of EAL4 provided in Common Criteria is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements are as shown in Table 21.

AVA_VLA.3 has dependency with ADV_FSP.1 and ADV_IMP.1. This is satisfied by

ADV_FSP.2 and ADV_IMP.2 in hierarchical relationship with ADV_FSP.1 and ADV_IMP.1

**Table 21 Dependency of the Added Assurance Components**

| No. | Assurance Component | Dependency | Ref. No. |
|---|---|---|---|
| 1 | ADV_IMP.2 | ADV_LLD.1 | EAL4 |
|  |  | ADV_RCR.1 | EAL4 |
|  |  | ALC_TAT.1 | EAL4 |
| 2 | ATE_DPT.2 | ADV_HLD.2 | EAL4 |
|  |  | ADV_LLD.1 | EAL4 |
|  |  | ADV_FUN.1 | EAL4 |
| 3 | AVA_VLA.3 | ADV_FSP.1 | EAL4 |
|  |  | ADV_HLD.2 | EAL4 |
|  |  | ADV_IMP.1 | 1 |
|  |  | ADV_LLD.1 | EAL4 |
|  |  | AGD_ADM.1 | EAL4 |
|  |  | AGD_USR.1 | EAL4 |

## 8.4. Rationale of Strength of Function

This SecurityTarget requires 'SOF-high' for security functional requirements of F FCS_CKM.1(1), FCS_CKM.1(2), FIA_UAU.4 and FMT_MTD.3.

The key sizes in FCS_CKM.1(1) and FCS_CKM.1(2) shall be selected so that the TOE is resistant to high attack potential. Since keys used in cryptographic operation may be exposed by Brute-Force Attack of attackers, the key length must be selected to handle this situation. Therefore, SOF-high is claimed.

FIA_UAU.4 and FMT_MTD.3 must have resistant to high attack potential. Therefore, it ensures the secure random numbers. The random numbers are used to handle replay attack. The random numbers used must not be predicted by attackers. Therefore, SOF-high is claimed.

The MRZ used as the seed for BAC the authentication key generation is determined according to Issuing policy of the Personalization agent. Therefore, the TOE does not ensure SOF of the BAC authentication key. The BAC authentication key does not include in the SOF scope of this SecurityTarget.

## 8.5. Rationale of Mutual Support and Internal Consistency

This rationale demonstrates that the TOE security requirements have a mutually supportive and internally consistency.

"8.3.1 Dependency of TOE Security Function Requirement" and "8.3.2 Dependency of TOE Security Assurance Requirements" the dependency is analyzed as a supportive relationship among security requirements of which it is necessary to depend on other security requirements in order to achieve a security objective because a

security requirement is insufficient. In case the dependency was not satisfied, additional rationale is provided.
Also, security functional requirements, although there is no dependency among security functional requirements, are mutually supportive and internally consistency in relation to the TSF operations as of the following.

In the Personalization phase, the Personalization agent records the MRTD application data (FMT_MTD.1(1), FMT_MSA.3) and deactivates writing function so that the TOE is not modified by external entities when delivering the TOE to the Operational Use phase (FMT_MOF.1(1), FMT_SMF.1). The role of the Personalization agent as such is defined as the security role (FMT_SMR.1) and is controlled by the ePassport access control policies (FDP_ACC.1(1), FDP_ACF.1(1)). It is separated the execution domain of subjects and objects within the scope of control of the ePassport access control policies from other domains (FPT_SEP.1) and ensured to invoke the access control function at all times as a reference monitor to protect these subjects and objects(FPT_RVM.1). Therefore, these security requirements are mutually supportive and internally consistent.

The TSF, after identifying the Inspection System (FIA_UID.1), executes the BAC mutual authentication (FIA_UAU.1(1)), the EAC-TA (FIA_UAU.1(2)) and SCP02 Mutual Authentication(FIA_UAU.1(3)) according to authentication mechanism application rules (FIA_UAU.5). If the Inspection System fails in authentication, the session is terminated (FIA_AFL.1). The random numbers must be used so that to prevent reuse of authentication-related data used in authentication (FIA_UAU.4). In order to ensure the secure random numbers used and the secure certificates used in the EAC-TA, the certificates must be verified and updated (FMT_MTD.3). Therefore, these security requirements are mutually supportive and internally consistent.

The TSF must initialize SSC to 0 (FMT_MTD.1(2)) in order to indicate the channel termination when terminating the BAC secure messaging (FDP_UCT.1 and FDP_UIT.1) established in order to protect the transmitted user data. Therefore, these security requirements are mutually supportive and internally consistent.

The cryptographic-related data created in temporary memory after cryptographic operations must be destroyed to prevent reuse (FCS_CKM.4, FDP_RIP.1). Therefore, these security requirements are mutually supportive and internally consistent.

In case the modification of the transmitted TSF data is detected, the TSF must terminate the session (FPT_ITI.1) and reset the access-rights of the Inspection System (FMT_MSA.1). Therefore, these security requirements are mutually supportive and internally consistent.

The TSF must execute self-testing under the conditions decided by the ST author (FPT_TST.1). In case the failure is detected, the TOE must preserve a secure state (FPT_FLS.1). Therefore, these security requirements are mutually supportive and internally consistent.

## 8.6. Rationale of Protection Profile compliance

This SecurityTarget complaints 'ePassport Protection Profile V1.0'

### 8.6.1. Rationale of TOE Security Environment compliance

This SecurityTarget redefines Threats T.Residual Information, Assumptions A.Inspection System and Organizational Security Policies P.Personalization Agent, P.ePassport Access Control and is compliant other all the TOE Security Environment in 'ePassport Protection Profile'. Also, additional defined TOE Security Environment is Threats T.Reuse Issuer Certification.

### 8.6.2. Rationale of Security Objects compliance

This SecurityTarget redefines Security Objects O.Management, O.Session Termination, O.Access Conrtol and is compliant other all the Security Objects in 'ePassport Protection Profile'. Also additional defined Security Objects O.AA and O.SCP02

### 8.6.3. Rationale of Security Function Requirement compliance

This SecurityTarget is compliant all the Security Function Requirement in 'ePassport Protection Profile' and redefines the operations of Security Function Requirement at Table 22 by allowed conventions, defines additional Security Function Requirement at Table 23.

**Redefined Security Function Requirement**

**Table 22 Rationale of Redefined Security Function Requirement**

| Protection Profile | SecurityTarget | Rationale |
|---|---|---|
| FCS_CKM.2(1) | FCS_CKM.2(1) | Selection |
| FCS_CKM.4 | FCS_CKM.4 | Assignment |
| FCS_COP.1(3) | FCS_COP.1(1) | Selection |
| FDP_ACC.1 | FDP_ACC.1(1) | Assignment, Refinement |
| FDP_ACF.1 | FDP_ACF.1(1) | Assignment, Refinement |
| FDP_RIP.1 | FDP_RIP.1 | Assignment, Selection |
| FDP_UIT.1 | FDP_UIT.1 | Selection |
| FIA_AFL.1 | FIA_AFL.1(1) | Assignment, Selection, Refinement |
| FIA_UAU.1(1) | FIA_UAU.1(1) | Assignment |
| FIA_UAU.1(2) | FIA_UAU.1(2) | Assignment |
| FIA_UAU.4 | FIA_UAU.4 | Assignment |
| FIA_UAU.5 | FIA_UAU.5 | Assignment |
| FMT_MSA.1 | FMT_MSA.1 | Refinement |
| FMT_MSA.3 | FMT_MSA.3 | Refinement |
| FMT_MTD.1(1) | FMT_MTD.1(1) | Assignment |
| FMT_SMF.1 | FMT_SMF.1 | Assignment |
| FMT_SMR.1 | FMT_SMR.1 | Assignment |
| FPT_FLS.1 | FPT_FLS.1 | Assignment |
| FPT_ITI.1 | FPT_ITI.1 | Assignment |
| FPT_TST.1 | FPT_TST.1 | Selection |

## Additional Security Function Requirement

**Table 23 Additional Security Function Requirement**

| Security Function Requirement | Rationale |
|---|---|
| FCS_CKM.1(2) | Define the Security Function Requirement of SCP02 session key generation for SCP02 Mutual Authentication. |
| FCS_ACC.1(2) | Define the Security Function Requirement of Operating System Access Control |
| FCS_ACF.1(2): | Define the Security Function Requirement of Operating System Access Control Policies |
| FIA_AFL.1(2): | Define the Security Function Requirement of failure of Personalization Agent Authentication |
| FIA_UAU.1(3): | Define the Security Function Requirement of SCP02 Mutual Authentication for Personalization Agent Authentication |
| FMT_MOF.1(2): | Add the Security Function Requirement which function is only Personalization Agent delegates to application to change lifecycle of Operating System. |
| FMT_MTD.1(3): | Define the Security Function Requirement of managing GP registry of Operating System |

## Security Requirement for IT environment

**Table 24 Security Requirement for IT environment**

| Protection Profile | SecurityTarget | Rationale |
|---|---|---|
| FCS_CKM.2(2) | FCS_CKM.2(2) | OE.IC Chip |
| FCS_COP.1(1) | FCS_COP.1(2) | OE.IC Chip |
| FCS_COP.1(2) | FCS_COP.1(3) | OE.IC Chip |
| FCS_COP.1(4) | FCS_COP.1(4) | OE.IC Chip |
| N/A | FCS_COP.1(5) | OE.IC Chip |
| FPR_UNO.1 | FPR_UNO.1 | OE.Handling Information Leakage |

### 8.6.4. Rationale of Assurance Requirement compliance

This SecurityTarget is compliant all the Assurance Requirement of EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) Assurance in 'ePassport Protection Profile' and no additional Assurance Requirement.

# References

| | |
|---|---|
| [CC] | Common Criteria for Information Technology Security Evaluation, Version 2.3, Aug. 2005, |
| [CEM] | Common Methodology for Information Technology Security Evaluation, Version 2.3, CCMB, 2005. 8. |
| [OSCPP] | ePassport Protection Profile V1.0, National Intelligence Service, 2008.8 |
| [JCSPP] | Java Card System Protection Profile Collection, Version 1.0b, Sun Microsystems, Inc. August 2003 |
| [ICPP] | Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002, Atmel Smart Card IC, Hitachi Europe Ltd., Infineon Technologies AG, and Philips Semiconductors, July 2001. |
| [MRTDPP] | Machine Readable Travel Document with ,,ICAO Application", Basic Access Control, Version 1.0, BSI-PP-0017, BSI, August 2005 |
| [MRTDEPP] | Machine Readable Travel Document with ,,ICAO Application", Extended Access Control, Version 1.1, BSI-PP-0026, BSI, September 2006 |
| [ICST] | SLE66CLX800PE/m1581-e13/a14, SLE66CLX800PEM/m1580-e13/a14, SLE66CLX800PES/m1582-e13/a14, SLE66CLX800PE/m1599-e13/a14, SLE66CLX360PE/m1587-e13/a14, SLE66CLX360PEM/m1588-e13/a14, SLE66CLX360PES/m1589-e13/a14, SLE66CLX180PE/m2080-a14, SLE66CLX800PEM/m2081-a14, SLE66CLX120PE/m2081-a14, SLE66CLX800PEM/m2082-a14 all optional with RSA 2048 V1.5 and ECC1.1 Security Target V1.3, Infineon Technologies AG, 2008-03-14, |
| [GPCS] | Global Platform Card Specification, Version 2.1.1, Global Platform Inc., March 2003. |
| [VGP] | VISA Global Platform 2.1.1 Card Implementation Requirements, Version 1.0, VISA, May 2003. |
| [VGPG] | VISA Global Platform 2.1.1 Card Production Guide, Version 1.0, VISA, February 2004. |
| [JCVM] | Java Card Platform 2.2.1, Virtual Machine Specification, Sun Microsystems, October 2003. |
| [JCRE] | Java Card Platform 2.2.1, Runtime Environment Specification, Sun Microsystems, October 2003. |
| [JCAPI] | Java Card Platform 2.2.1, Application Programming Interface, Sun Microsystems, October 2003. |
| [MRTD] | Machine Readable Travel Document, Part 1 Machine Readable Passport, Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability, Doc 9303, ICAO, Sixth Edition, 2006 |
| [EAC] | Advanced Security Mechanism for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, BSI, 2008 |

# Terms and Definition

| Terms | Definitions |
|---|---|
| AA<br>(Active Authentication) | The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values |
| Applet | Javacard Application Program implemented Javacard Platform |
| BAC<br>(Basic Access Control) | The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the secure messaging for the MRTD chip and the IS |
| BAC authentication key | The BAC authentication encryption key and the BAC authentication MAC key generated by using the KDM from the MRZ (passport No., passport No. check digit, date of birth, date of birth check digit, valid date, valid date check digit) for mutual authentication of the MRTD chip and the IS |
| BAC Mutual authentication | The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol |
| BAC Secure messaging | The communication channel to provide the confidentiality and the integrity of transmitted data by encryption the transmitted data with the BAC session encryption key and generating, therefore transmitting after generating message authentication value with the BAC session MAC key |
| BAC Session Key | The BAC session encryption key and the BAC session MAC key for generated by using the KDM from random numbers for generating session keys shared in the BAC mutual authentication |
| Biometric data of the ePassport holder | Fingerprint and/ or iris data of ePassport holder stored in the MRTD chip in the LDS structure |
| BIS<br>(BAC Inspection System) | The IS implemented with the BAC and the PA security mechanisms |
| Certificate | The electronic data by a digital signature on the digital signature verification key by the CA in order to check and demonstrate that the digital signature generation key belongs only to the person who holds the key |
| Ciphertext Only Attack | Attack by the threat agent to attempt decryption based on the collected ciphertext |
| CSCA<br>(Country Signing Certification Authority) | The root CA that generates and issues the CSCA certificate and the DV certificate by securely generating the digital signature key in the PA-PKI to support the PA security mechanisms |
| CSCA Certificate | The certificate to demonstrate validity of the digital signature verification key for the digital signature generation key of the PA-PKI root CA by signature on the digital signature verification key with digital signature generation key of the PA-PKI root CA |
| CVCA<br>(Country Verifying Certification Authority) | The root CA that generates and issues the CVCA certificate, the CVCA link certificate and the DV certificate by securely generating digital signature key in the EAC-PKI to support the EAC security mechanisms |

| | |
|---|---|
| CVCA Certificate | The certificate that includes digital signature value by the EAC-PKI root CA with digital signature generation key of the EAC-PKI root CA on the digital signature verification key in order to demonstrate validity of the CVCA link certificate and the DV certificate |
| CVCA Link Certificate | The certificate that includes digital signature value that the EAC-PKI root CA with the digital signature generation key that corresponds to the previous CVCA certificate after generating a new CVCA certificate before expiring the valid date of the CVCA certificate |
| DS (Document Signer) Certificate | The certificate of the Personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism |
| DV<br>(Document Verifier) | The CA(Certification Authority) that generates and issues the IS certificate |
| DV Certificate | The certificate that includes digital signature value on the digital signature verification key of the IS with the digital signature generation key of the DV in order to demonstrate validity of the digital signature verification key of the IS |
| EAC-CA<br>(EAC-chip Authentication) | The security mechanism to implement the Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) to enable the MRTD chip authentication by the EIS through key checking for the EAC chip authentication public key and private key of the MRTD chip and temporary public key and private key of the EIS |
| EAC-TA<br>(EAC-terminal Authentication) | The security mechanism that The EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS. |
| EAC<br>(Extended Access Control) | The security mechanisms consisted with the EAC-CA for chip authentication and the EAC-TA for the IS authentication in order to enable only the EAC supporting Inspection System (EIS) to read the biometric data of the ePassport holder for access control to the biometric data of the ePassport holder stored in the MRTD chip |
| EAC Chip Authentication Public Key and EAC Chip Authentication Private key | Set of the DH keys used by the MRTD chip to authenticate itself to the EAC supporting IS in the EAC-CA that contains data recorded by the Personalization agent in the Personalization phase. |
| EAC Inspection System (EIS: EAC Inspection System) | The IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option |
| EAC Session Key | The session key used to establishing secure messaging to protect transmission of the biometric data of the ePassport holder that consist of the EAC session encryption key and the EAC session MAC key generated by using the KDF of which keys shared with the EIS through the Ephemeral-Static DH key distribution protocol in the EAC-CA are used as Seed |
| EF.COM | Including the LDS version info. Data Groups tag information |
| EF.CVCA | The EF format file to specify the read-right and the list of the CVCA digital signature verification key identifier necessary in verification of the CVCA certificate validity in the EAC-TA |
| Encryption Key | Key used in the symmetric cryptographic algorithm for data encryption in order to prevent the data disclosure |

| | |
|---|---|
| ePassport | The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO). |
| ePassport authentication data | The data stored in the MRTD chip with the LDS format to support ePassport security mechanisms that includes the PA SOD, the EAC chip authentication public key and the AA chip authentication public key, etc. |
| ePassport identity data | Including personal data of the ePassport holder and biometric data of the ePassport holder |
| ePassport PKI | Unique data signed on the ePassport by the Personalization agent with digital signature generation key issued in the ePassport PKI System in order to issuance and check of the electronically processed passport |
| ePassport PKI System | System to provide certification practice, such as issuance of certificates necessary in passport's digital signature and management of certification-related records, etc. |
| Grandmaster Chess Attack | Attack by masquerading as the MRTD chip using the IC chip to hookup the communication channel between the MRTD chip and the IS |
| ICAO-PKD | The DS certificate storage operated and managed by the ICAO that online distributes in case the domestic/ overseas IS requests the DS certificate of the corresponding country |
| Inspection | Procedure in which immigration office checks identity of the ePassport holder by inspecting the MRTD chip presented by the ePassport holder, therefore verifying genuine of the MRTD chip |
| IS (Inspection System) | As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands. |
| IS Certificate | Certificate used by the MRTD chip to verify the digital signature transmitted by the IS in the EAC-TA. The DV performs a digital signature on the digital signature verification key of the EIS with the digital signature generation key. |
| KDF (Key Derivation Function) | The function to generate the encryption key and the MAC key by using hash algorithm from the Seed |
| KDM (Key Derivation Mechanism) | The mechanism to generate the encryption key and the MAC key by using hash algorithm from the Seed |
| LDS (Logical Data Structure) | Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip |
| MAC Key (Key for Message Authentic Code) | Key used by symmetric cryptographic algorithm according to ISO9797 to generate the message authentication code in order to prevent data forgery and corruption |
| MRTD | Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes |
| MRTD Application | Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc. |
| MRTD Application Data | Including user data and TSF data of the MRTD |

| | |
|---|---|
| MRTD Chip | the IC chip operating system necessary in operation of the MRTD application and that supports communications protocol by ISO/IEC 14443 |
| PA<br>(Passive Authentication) | The security mechanism to demonstrate that identity data recorded in the ePassport has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the ePassport access control policy. |
| Personal data of the ePassport holder | Visually identifiable data printed on identity information page of the of ePassport and other identity data stored in the MRTD chip in the LDS structure |
| Personalization agent | The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI. |
| Probing | Attack to search data by inserting probing pin in the IC chip |
| Reverse Engineering | To identify and reproduce the basic design concept and applied technologies of product through detailed analysis of the completed product |
| SOD<br>(Document Security Object) | The SOD refers to the ePassport identity data and the ePassport authentication data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and encoded with DER method. |
| TSF Data | The data stored in the secure memory of the MRTD chip to support ePassport security mechanisms |
| User Data | Including the ePassport identity data and the ePassport authentication data |

# Acronyms

| | |
|---|---|
| **AA** | active Authentication |
| **BAC** | Basic Access Control |
| **BIS** | BAC Inspection System |
| **CA** | Chip Authentication |
| **CC** | Common Criteria |
| **CCMB** | Common Criteria Maintenance Board |
| **CCRA** | Common Criteria Recognition Arrangement |
| **COS** | Card Operating System |
| **CSCA** | Country Signing Certification Authority |
| **CVCA** | Country Verifying Certification Authority |
| **DES** | Data Encryption Standard |
| **DF** | Dedicated File |
| **DG** | Data Group |
| **DH** | Diffie-Hellman |
| **DPA** | Differential Power Analysis |
| **DS** | Document Signer |
| **DV** | Document Verifier |
| **EAC** | Extended Access Control |
| **EAL** | Evaluation Assurance Level |
| **ECDH** | Elliptic Curve Diffie-Hellman |
| **EEPROM** | Electrically Erasable Programmable Read-Only Memory |
| **EF** | Elementary File |
| **EIS** | EAC Inspection System |
| **IC** | Integrated Circuit |
| **ICAO** | International Civil Aviation Organization |
| **IS** | Inspection System |
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **KDM** | Key Derivation Mechanism |
| **KDF** | Key Derivation Function |
| **LDS** | Logical Data Structure |
| **MAC** | Message Authentication Code |

| | |
|---|---|
| **MF** | Master File |
| **MRTD** | Machine Readable Travel Document |
| **MRZ** | Machine Readable Zone |
| **PA** | Passive Authentication |
| **PKI** | Public Key Infrastructure |
| **PP** | Protection Profile |
| **RAM** | Random Access Memory |
| **RF** | Radio Frequency |
| **ROM** | Read Only Memory |
| **SCP02** | Secure Channel Protocol02 |
| **SFP** | Security Function Policy |
| **SOD** | Security Object of Document |
| **SOF** | Strength of Function |
| **SPA** | Simple Power Analysis |
| **SSC** | Send Sequence Counter |
| **ST** | Security Target |
| **TA** | Terminal Authentication |
| **TDES** | Triple-DES |
| **TSC** | TSF Scope of Control |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |