U-creator
U dream, we create.

SSCOS V1.0
on S3CC9LC
Security Target
Public Version

Samsung SDS

SAMSUNG

SAMSUNG SDS

REVISION STATUS

Revision	Date	Author	Description of Change
1.13	2012.03.06	HS Chang JH Lee JH Kim JI Gu HH Han	ST final release

Table of Contents

List of Figures

List of Tables

1 Security Target Introduction

This document is the Security Target (ST) of SSCOS V1.0 on S3CC9LC, which is the TOE of MRTD IC chip product developed by Samsung SDS.

This section identifies the ST and the TOE and provides summary of the ST and the evaluation criteria to which the TOE conforms.

1.1 Security Target Identification

- Title: SSCOS V1.0 on S3CC9LC Security Target
- Document Number: SSCOS10-ASE-001_Security Target
- Version: V1.13
- Release Date: March 6, 2012
- Author: Samsung SDS
- Evaluation Criteria: Common Criteria for Information Technology Security Evaluation V3.1r3 [2][3]
- Evaluation Assurance Level: EAL4 Augmented (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)
- PP Compliance: ePassport Protection Profile V2.10 [1]
- PP certification number: KECS-PP-0163a-2009

1.2 TOE Identification

- Developer: Samsung SDS Delivery Innovation Division
- TOE Name: SSCOS V1.0 on S3CC9LC
- TOE Elements
  - Hardware: S3CC9LC IC Chip and RSA, ECC, and DRNG Library which is provided with hardware
  - Software: IC Chip operating system and MRTD Application which includes MRT D application data
  - Documents: Operational User Guidance, Preparative Procedures, and Personalization Guide
- TOE Version: 1.0

  - Hardware
    - IC Chip: S3CC9LC 16-bit Secure RISC Microcontroller for Smart Card, revision 11 with optional Secure RSA and ECC Library including specific IC Dedicated Software
    - RSA Library: Secure RSA library V3.8S
    - ECC Library: ECC Library V2.4S
    - DRNG Library: DRNG Software Library V2.1
  - IC Chip operating system and MRTD Application which includes MRTD application data
    - ROM Image Identification: C9LC_SSCOS10_R01.rom
    - EEPROM Image Identification: C9LC_SSCOS10_R01.eep
  - Documents

- Operational User Guidance: SSCOS10-AGD-001_Operational User Guidance V1.00
- Preparative Procedures: SSCOS10-AGD-002_Preparative User Guidance V1.00
- Personalization Guide: SSCOS10-AGD-003_Personalization Manual V1.00

1.3 TOE Overview

SSCOS10 on S3CC9LC (hereafter 'SSCOS10') which is a MRTD chip product of Samsung SDS is integrated with the booklet and antenna for contactless transmission and used for proving travelers identity.

The TOE (SSCOS V1.0 on S3CC9LC, hereafter 'SSCOS') includes IC Chip hardware elements and comprises of the native IC Chip Operating System (COS), MRTD Application, and MRTD Application data and uses IC Chip "S3CC9LC" manufactured by Samsung Electronics. Samsung Electronics has achieved Common Criteria certification for S3CC9LC from BSI as below. Because IC Chip operating system and MRTD application which are developed by Samsung SDS is loaded on the chip, the TOE is subject to composite evaluation according to CCDB-2007-09-001.

- PP Compliance: BSI-PP-0002-2001
- Certified IC Chip name: S3CC9LC 16-bit Secure RISC Microcontroller for Smart Card, revision 11 with optional Secure RSA and ECC Library including specific IC Dedicated Software
- Certification number: BSI-DSZ-CC-0624-2010
- Version of certified crypto library: Secure RSA library V3.8S and DRNG Software Library V2.1 and PKA-2 EC Library V2.4S
- Evaluation Assurance Level: EAL5 Augmented (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

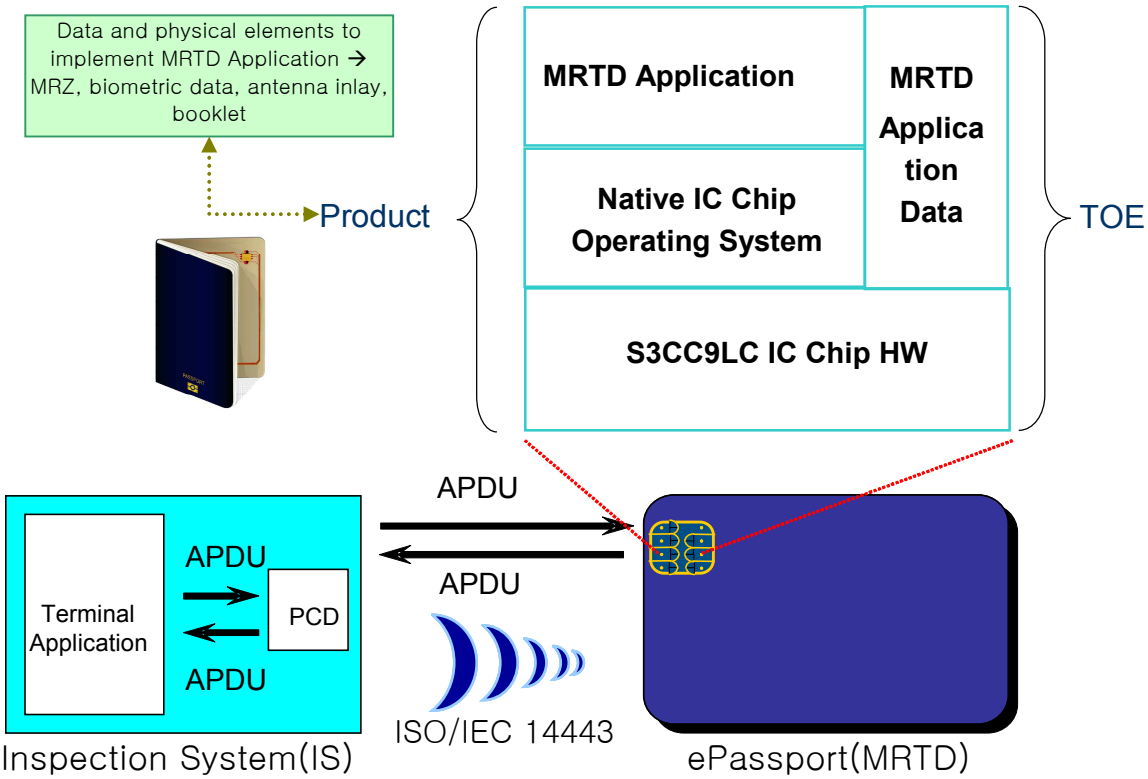


Figure 1. TOE Overview

The TOE stores MRTD Application data in Logical Data Structure (LDS) which is defined by International Civil Aviation Organization (ICAO) and runs MRTD Application as specified by ICAO and BSI to protect them.

The MRTD application of the TOE satisfies the ICAO's Machine Readable Travel Documents, DOC 9303 Part 1 Volume 2 [6] (hereafter "ICAO document") and the BSI's Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control V1.11 2008.02 [9] (hereafter "EAC specification").

The ePassport 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). 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.

Therefore TOE implements ePassport security mechanism, such as AA (Active Authentication), BAC (Basic Access Control), and EAC (Extended Access Control) etc. Additionally, to support secure personalization and management by Personalization Agent in Personalization Phase TOE authenticates Personalization Agent with Personalization agent key and issuing authorization is granted to Personalization Agent by TOE authenticating Personalization Agent with Personalization agent key.

TOE does cryptographic calculation to implement ePassport security mechanism and personalization agent authentication by using crypto library provided by IC chip elements. IC chip provides cryptographic functions, such as TDES, MAC, RSA, and SHA.

TOE interfaces with IC Chip hardware and performs communication, memory management, and cryptographic calculations, and implements ePassport security mechanism according to ICAO document and EAC specification through exchanging command and respond APDU (Application Protocol Data Unit).

1.4 TOE Descriptions

This section describes TOE operational environment, TOE physical scope, TOE logical scope, and TOE assets to be protected. Also, TOE lifecycle and operational mode are identified.

1.4.1 Product Configuration

TOE comprises of IC Chip hardware and the software which implements the native IC Chip operating system and MRTD Application. ePassport security mechanism is implemented in MRTD Application.

Underlying IC chip is EAC5+ certified S3CC9LC developed by Samsung Electronics and it is manufactured to SSCOS10 product which is a COB. In other word, the TOE is packaged to compose a COB in which IC Chip is embedded and it is named SSCOS10.

Figure 2. Image of ePassport

ePassport booklet presents identification data such as printed portrait of the MRTD holder and printed MRZ which are same as stored in the chip to the Inspection System so that the Inspection System can recognize. Fingerprints or iris biometric information can be stored in the chip as well depending on personalization agent's policy.

As shown in Figure 2, SSCOS10 and associated antenna for RF transmission are embedded on the plastic film and that will be placed within a data page or the cover of the booklet to form ePassport.

1.4.2 TOE Operational Environment

- ePassport System

Overall configuration of the ePassport system is shown in Figure 3.

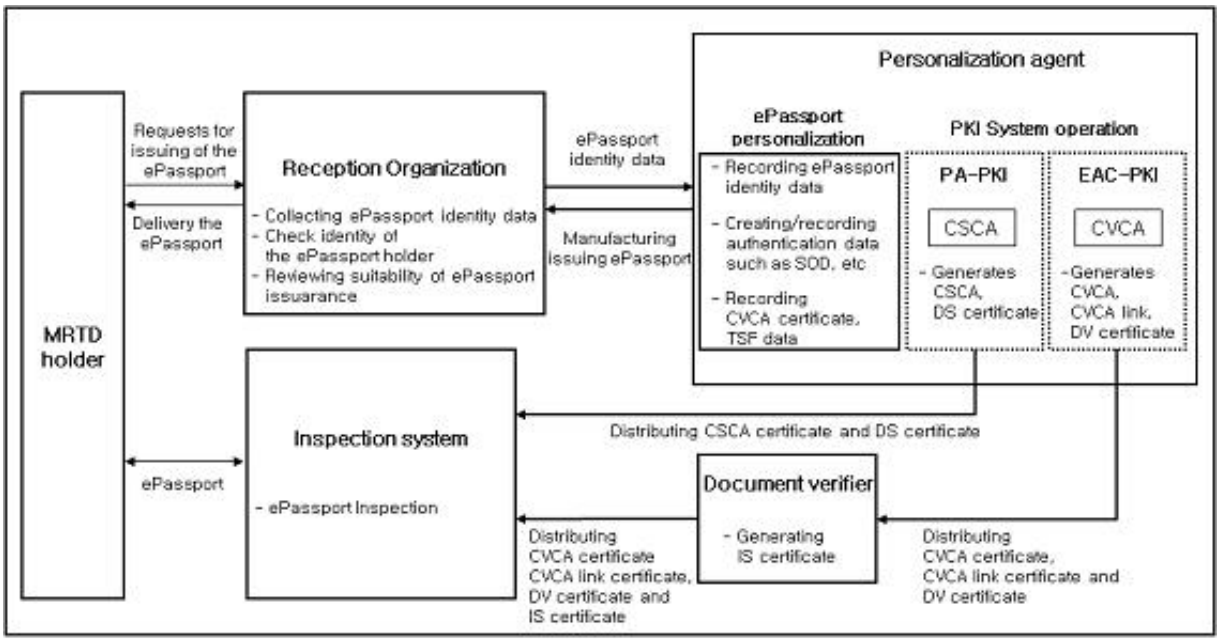


Figure 3. Overall Configuration of the ePassport System

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 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 1.4.6 TOE Assets.

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.

Figure 4 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.

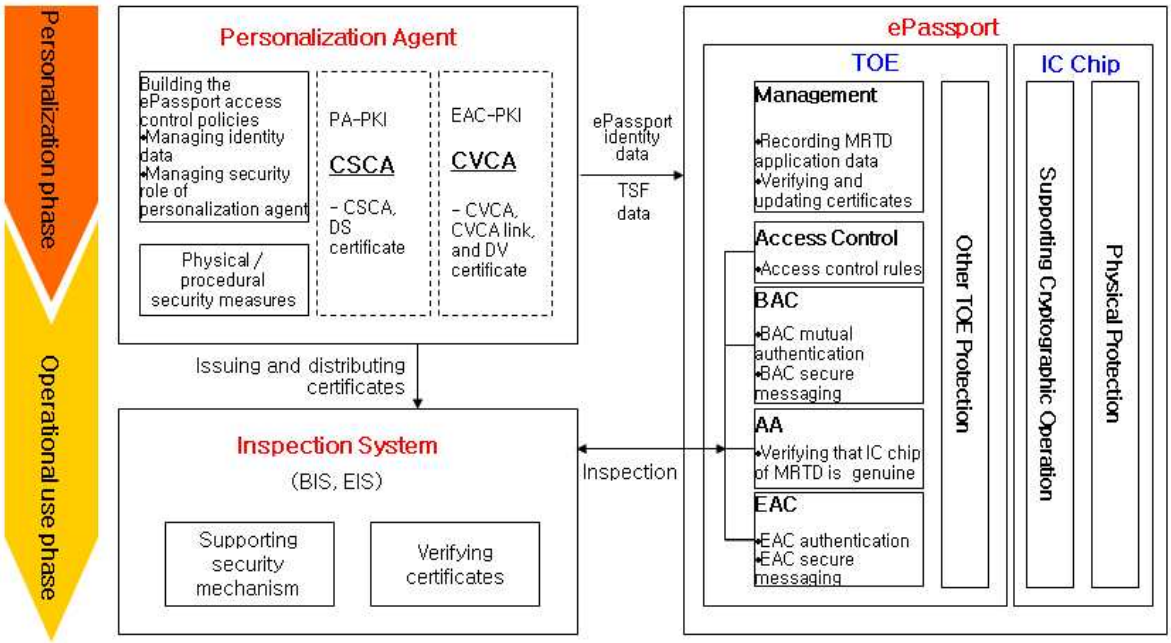


Figure 4. TOE Operational Environment – ePassport

The Inspection System performs BAC mutual authentication and EAC according to the security mechanism procedure enforced by TOE.

1.4.3 Security Functions of IC Chip

Following security functions are provided by the IC chip S3CC9LC and the crypto library provided with the hardware.

- Symmetric key cryptographic operation

  The IC chip provides DES and TDES accelerator and relevant control register in order that the TOE can perform operations such as (1) 112 bit TDES message encryption and decryption for BAC, (2) Retail MAC calculation based on 56 bit DES for BAC and EAC, and (3) Cryptogram generation based on 112bit TDES for Personalization Agent authentication.

- Asymmetric key cryptographic operation

The IC chip provides crypto-processor (Tornado^{TM}) and relevant cryptographic library capable of 2048-bit modulus RSA operations in order that the TOE can perform operations such as (1) key exchange and agreement based on DH for EAC-CA, (2) digital signature verification based on RSA for EAC-TA, and (3) digital signature generation based on RSA for AA.

- Hash functions

  The IC chip's cryptographic library provides on-way hash functions of SHA-1, SHA-224, and SHA-256 in order that the TOE can perform operations such as (1) KDF calculation which derives symmetric key used to perform Secure Messaging of BAC/EAC and (2) digital signature generation and verification based on RSA.

- Random number generation

  DRNG (DRNG Library v2.1) evaluated under AIS20 standard class K3 enables TOE to create unpredictable and irreproducible random number to be used in preventing replay attacks.

- Countermeasure against side channel attack

  The IC chip provides hardware-based countermeasures such as Random Current Generator, Random Wait-state Generator, Virtual DES/TDES against disclosing information from the changes of current, voltage, electro-magnetic or such kind of physical phenomenon during symmetric or asymmetric key cryptographic operations and also provides cryptographic library where countermeasures against DPA or SPA are implemented. Meanwhile, the IC chip provides Abnormal Condition Detector that shall reset the IC chip itself when detecting abnormal frequency, voltage, temperature, and light, removal of insulating shield, and power glitch, as well as Data Bus Scrambling function that enables EEPROM and RAM data bus to be scrambled. The relevant control register for each function is provided in order for TOE to use with ease.

1.4.4 Physical Scope of the TOE

The ePassport refers to the booklet and the MRTD chip and the antenna embedded in the cover of the booklet. The MRTD chip includes the IC chip operating system, the MRTD application, the MRTD application data and the IC chip elements. The IC chip elements consist of CPU, cryptographic co-processor, I/O port, memory (RAM, ROM, and EEPROM), random number generator, timer and contactless interface, etc.

The physical scope of the TOE is defined as the IC chip operating system (COS) which is masked on ROM, MRTD application, and MRTD application data which is loaded onto EEPROM and the underlying IC Chip element and the crypto library is included in the physical scope of the TOE

The TOE includes the IC Chip (S3CC9LC) of Samsung Electronics which Samsung Electronics has achieved CC EAL 5 for. The IC Chip provides CPU which executes instructions that includes executable code. The TOE also includes hardware such as DES and TDES accelerator and Tornado Coprocessor etc. Especially, RSA function is provided with Crypto Library which is included in the scope of the CC evaluation the IC Chip.

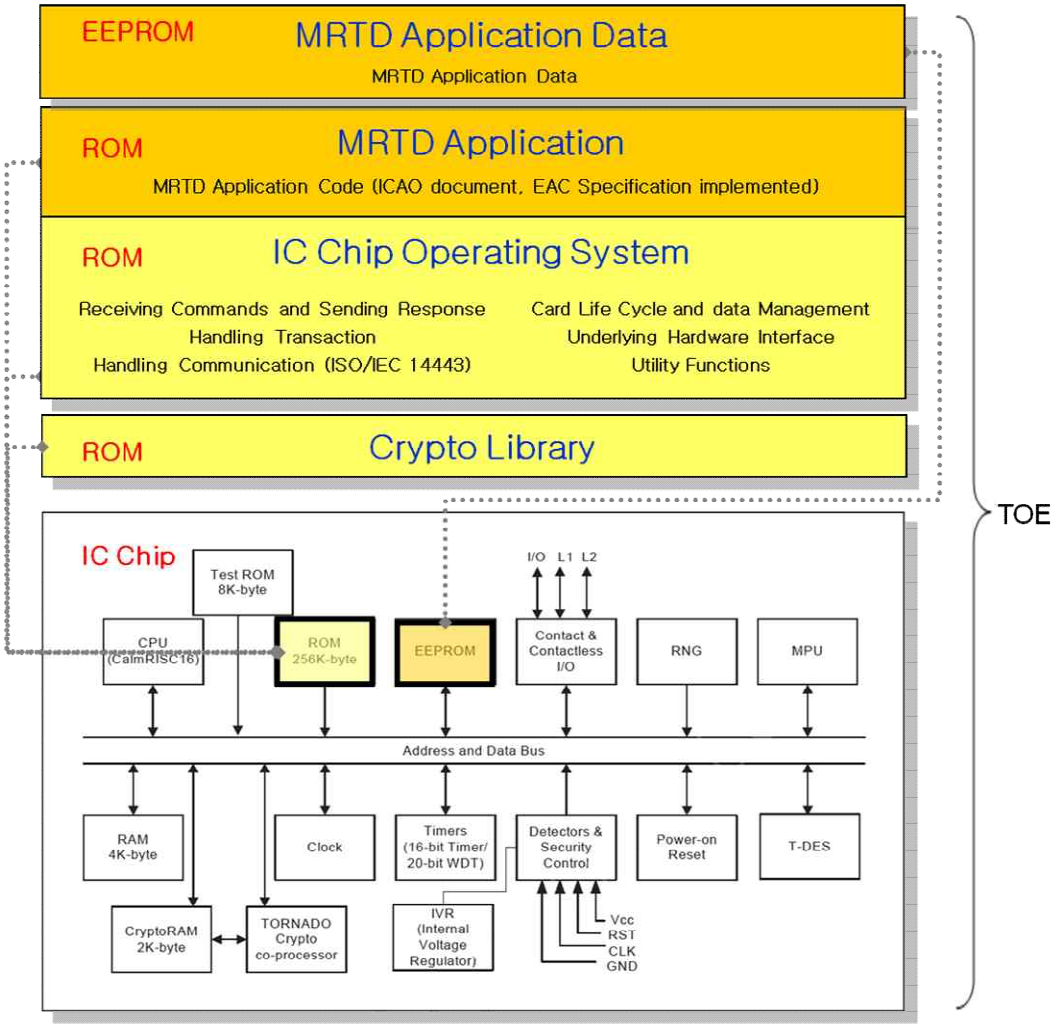


Figure 5. Physical Scope of the TOE

The COS provides functions for execution of MRTD application and management of the MRTD application data, such as commands processing and files management, etc. defined in ISO/ IEC 7816-4, 8 and 9. The IC Chip operating system implements EEPROM writing function based on the method provided by chip manufacturer, Samsung Electronics. The implemented library provides low-level process to write data on EEPROM for MRTD application personalization. SSCOS implements cryptographic functions using the run-time firmware library which supports RSA, random number generation, and hash function that is provided by the underlying IC chip.

MRTD application provides 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 such as BAC, AA, and Secure Messaging to securely protect the data. Biometric data may include according to the personalization agent's policy, so EAC defined in EAC specification is also implemented. MRTD application is programmed to provide security mechanisms such as BAC, AA, EAC-CA, and EAC-TA and is masked on ROM with the IC Chip operating system.

Meanwhile, MRTD application data which consists of ePassport user data and ePassport TSF data which is for performing security mechanisms and COS application data is also stored in EEPROM through secure writing method provided by IC chip operating system.

TOE and TOE component is identified in Table 1.

Table 1. TOE and TOE Component Identification

Category (Form)	Name	Configuration Identification (Including version/build no.)	Descriptions
TOE	SSCOS V1.0 on S3CC9LC	SSCOS V1.0 on S3CC9LC	A combination of IC Chip, IC chip operating system and MRTD application
TOE Component (HW)	S3CC9LC	S3CC9LC 16-bit Secure RISC Micro-controller for Smart Card, revision 11	IC Chip Hardware
		Secure RSA library V3.8S	Crypto library provided with IC Chip
		ECC Library V2.4S	
		DRNG Software Library V2.1	
TOE Component (SW)	MRTD application includes the IC chip operating system and MRTD application data	C9LC_SSCOS10_R01.rom	ROM Image Configuration Identification (SSCOS10 ROM Code Revision 1 based S3CC9LC)
		C9LC_SSCOS10_R01.eep	EEPROM Image Configuration Identification (SSCOS10 EEPROM Code Revision 1 based S3CC9LC)
TOE Component (Documents)	Operational User Guidance	SSCOS10-AGD-001_Operational User Guidance V1.00	Operational User Guidance
	Preparative Procedure	SSCOS10-AGD-002_Preparative User Guidance V1.00	Preparative Procedure
	Personalization Guide	SSCOS10-AGD-003_Personalization Manual V1.00	Personalization Guide

1.4.5 Logical Scope of the TOE (SW)

Below table shows logical components of TOE (SW) and subsystems according to each component and the security characteristics provided.

Logical Component	Logical Layered Architecture	Subsystem	Security Characteristics
MRTD Application	ePassport Layer	Security Service(SS)	- Interprets ePassport commands received from the Inspection System and the Personalization Agent - BAC, AA, EAC, Secure Messaging - Residual Information Protection - ePassport Security Mechanism for example ePassport access control - ePassport Security Mechanism management - Personalization Agent authentication mechanism - Integrity verification of code and data
		Identification & Authentication(IA)	
		Secure Messaging(SM)	

IC Chip Operating System (COS)	Hardware Independent Layer	Memory Manager(MM)	- Provides security functions to ePassport Layer by using cryptographic calculation functions of the IC Chip - Verifies randomness of the random number generated in start-up process
		Crypto Functions(CF)	
		Utility Service(US)	
		Command Handler(CH)	
	Hardware Dependent Layer	Device Service(DS)	- Secure operation of the TOE with support of the IC Chip - APDU transmission from an outside entity by implementing contact or contactless transmission protocol

TOE functionality is summarized as below.

ePassport layer provides ePassport functions and is responsible for interpreting ePassport commands received from the Inspection System or the Personalization Agent. ePassport security characteristics such as BAC, AA, EAC, Secure Messaging, residual information protection, and ePassport access control are provided and the management of those security characteristics and the Personalization Agent authentication mechanism is implemented. Integrity verification of code and data is provided as common security characteristics.

Hardware Independent Layer provides security functions based on cryptographic functions of the IC Chip and verifies randomness of random number when starting-up.

Hardware dependent layer assures secure operation of the TOE with the IC Chip's support. Also, contact and contactless transmission protocols are implemented. APDU is received from an outside entity and it is transferred to Hardware Independent Layer.

Table 2 below shows the ePassport security mechanisms of the TOE. PA is not the security function of the TOE.

Table 2. ePassport Security Mechanisms

The ePassport Security Mechanisms				**IT Security Characteristics of the TOE**
Security Mechanism	**Security Characteristic**	**Cryptography**	**Cryptographic Key/Certificate Type**	
PA	User Data Authentication	N/A	N/A	Access Control to the SOD - Read-rights: BIS, EIS - Write-rights: Personalization Agent
AA	Verification of the genuineness of the IC Chip	Asymmetric Key Digital Signature AA Security Mechanism SHA-1	AA Private Key (TOE private key for digital signature) AA Public Key (used by BIS, EIS	The TOE signs random numbers which are generated by the TOE and the Inspection System and the Inspection System verifies the digital signature to conform that the IC chip has not been substituted.

BAC	BAC Mutual Authentication	ISO/IEC 11770-2 Key Establishment Mechanism 6 TDES Retail MAC SHA-1	BAC Authentication Key (encryption key, MAC key)	The TOE verifies if the Inspection System has access-rights, by decryption and MAC operation for the transmitted value of the Inspection System. The TOE transmits the value to the Inspection System after encryption and MAC operation for authentication.
	BAC Key Distribution	ISO/IEC 11770-2 Key Establishment Mechanism 6 TDES Retail MAC SHA-1	BAC Session Key (encryption key, MAC key)	Generating BAC session key by using KDF from the exchanged key-sharing random number on the basis of the TDES-based key distribution protocol.
	BAC Secure Messaging	Secure Messaging	BAC Session Key (encryption key, MAC key)	Transmitting messages by creating the MAC after encryption with the BAC session key. Receiving messages by decryption it after verifying the MAC with the BAC session key.
EAC	EAC-CA	Diffie-Hellman key-agreement protocol	EAC Chip Authentication Public Key EAC Chip Authentication Private Key	The TOE executes the ephemeral- static DH key distribution protocol.
	EAC Secure Messaging	Secure Messaging	EAC Session Key (cryptographic key, MAC key)	Secure messaging by using the EAC session key shared in the EAC-CA.
	EAC-TA	RSASSA-PKCS1-v1.5-SHA-256 RSASSA-PKCS1-v1.5-SHA-1	CVCA certificate CVCA link certificate DV certificate IS certificate	Verifying the IS certificate by using the certificate chain and the link certificate. Verifying the digital signature for transmitted messages of the EIS for the EIS authentication.

1.4.6 TOE Assets

The TOE provides information security functions such as confidentiality, integrity, authentication and access controls in order to protect TOE assets as follows:

1. ePassport User Data

   The following user data are stored in the EF of the IC chip where the TOE is implemented.

- Personal data of the ePassport holder data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13, and EF.DG16
- Biometric data of the ePassport holder : data stored in EF.DG3 and EF.DG4
- ePassport authentication information : SOD, EAC-CA public key, and AA public key[1]
- EF.CVCA : the identifier list of the CVCA digital signature verification key used to verify CVCA certificate for the TOE to authenticate the Inspection System during the EAC-TA
- EF.COM: version information of the LDS, tag list of DGs in use, etc.

2. ePassport TSF Data

   The following TSF data are stored in the secure memory of the IC chip where the TOE is implemented.

   - BAC authentication key: BAC authentication encryption key, BAC authentication MAC key
   - EAC-CA private key : the chip private key used for EAC-CA to prove that the IC chip of the ePassport is not forged
   - AA private key: the chip key used for AA when the TOE generates a digital signature
   - CVCA certificate: the root CA certificate that EAC-PKI created during ePassport issuance
   - CVCA digital signature verification key : the public key of CVCA certificate newly generated by certificate update after the ePassport issuance
   - Current date: the current date is written as the issuance date of the ePassport at first but shall be internally updated in the latest issuance date among CVCA link certificate, DV certificate and IS certificate by the TOE at the Operational Use phase
   - MRTD Access Control Reference: attribute assigned by personalization agent to enable only BAC or both BAC and EAC after ePassport personalization phase

   The following TSF data are stored in the volatile memory of the IC chip where the TOE is implemented.

   - BAC session key : BAC session encryption key, BAC session MAC key
   - EAC session key : EAC session encryption key, EAC session MAC key

3. ePassport Personalization TSF data

   Personalization agent key which is used for personalization agent authentication is also TSF data. The initial personalization agent key which will be injected in Manufacturing Phase shall not be reveled to increase the security level. The personalization agent transfers the key to the developer of SSCOS securely and the developer injects the key into EEPROM image and transfers it to the IC Chip manufacturer.

   The following TSF data are stored in the volatile memory of the IC chip where the TOE is implemented.

   - Personalization agent key: Personalization agent authentication encryption key, Personalization agent authentication MAC key

[1] This is added to provide AA.

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, EF.DG4	
	ePassport Authentication Data		SOD, EAC chip authentication public key, AA public key for digital signature verification etc.	
	EF.CVCA		CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System in EAC-TA	
	EF.COM		LDS version information, tag list of DG used, etc.	
ePassport TSF Data	EAC chip authentication private key		Chip Private key used by the TOE in EAC-CA to demonstrate that MRTD chip is not forged	Secure Memory
	AA private key		Private key of the TOE for generating digital signature in AA	
	CVCA Certificate		Root CA Certificate issued in EAC-PKI in In personalization phase	
	CVCA Digital Signature Verification Key		CVCA certificate Public key newly created by certificate update after personalization phase	
	Current Date		Date of issuing the ePassport is recorded in personalization phase. 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	
	MRTD Access Control Reference		An attribute assigned by personalization agent to enable only BAC or both BAC and EAC after ePassport personalization phase	
	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	ePassport Operational Mode		ePassport DF Life Cycle	Secure Memory
	Personalization Agent Access Rule Reference		Reference file which defines keys and authorization for access control	Secure Memory
OS TSF Data	Personalization Agent Key		Personalization agent authentication encryption key, Personalization agent authentication MAC key	Secure Memory

Application Notes: The biometric data obtained from an ePassport holder include the face, the fingerprint and the iris. The face information is contained mandatory according to the ICAO document. The Fingerprint and iris information is contained optionally according to the Issuing policy of the ePassport. This security target includes security functional requirements for the EAC specifications by considering fingerprint information to be contained.

Application Notes: In personalization phase, TOE generates BAC authentication key on request of the personalization agent and stores BAC authentication key in the secure memory of the IC chip.

Application Notes: In order to support EAC, the Personalization agent generates the EAC chip authentication public and private key and records them in the TOE. The CVCA digital signature verification key is updated through the CVCA link certificate according to the EAC specifications. However, the first CVCA digital signature verification key for verifying the CVCA link certificate shall be recorded in secure memory of the MRTD chip in the personalization phase.

Application Notes: Personalization agent can update the personalization agent key after authentication with the key.

Application Notes: Personalization agent makes SOD by generating digital signature of ePassport user data.

Because the TOE is a product that a holder possesses and uses, it may be a target for attackers to steal. Thus, IC chip itself is an asset to be protected from physical threats.

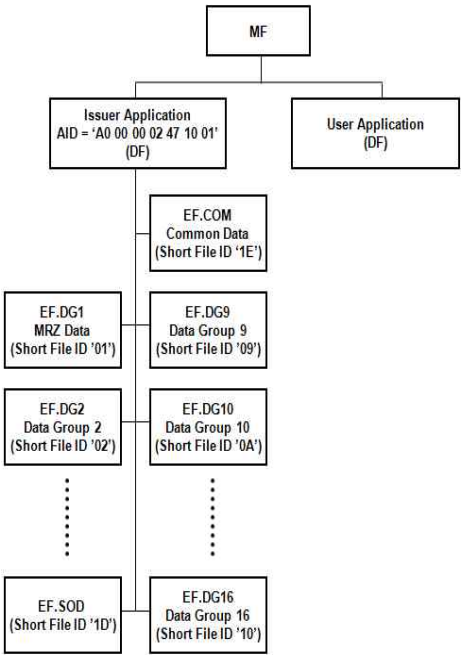
Some information is not such asset that the TOE protects directly, but are produced or used during the process of TOE manufacturing thus have considerable relations toward the integrity and confidentiality of the TOE. This information is called additional assets and the security of additional assets shall be met by the assurance requirements of EAL4+.

1.4.6.1 Contents of the ePassport User Data

The LDS in which the ePassport user data are stored defines MF, DF and EF file structure. The contents of DG are shown in Table 4.

Table 4. Contents of the LDS in which TOE ePassport User Data are Stored

Category	DG	Content	LDS Structure
Detail(s) Recorded in MRZ	DG1	Document Type	
		Issuing State	
		Name (of Holder)	
		Document Number	
		Check Digit – Doc Number	
		Nationality	
		Date of Birth	
		Check Digit - DOB	
		Sex	
		Data of Expiry or Valid Until Date	
		Check Digit DOE/VUD	
		Composite Check Digit	

Encoded Identification Features	DG2	Encoded face	
	DG3	Encoded finger(s)	
	DG4	Encoded Eye(s)	
Others	DG5	Displayed 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 Digital Signature Verification Key (optional)	
	DG16	Person(s) to Notify	

1.4.6.2 Types of Certificates in ePassport System

Types of certificates used in the ePassport system are as shown in Table 5.

Table 5. Type of ePassport Certificate

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

1.4.7 TOE Life Cycle

SSCOS ePassport lifecycle and related subjects are shown in Figure 6.

Chip initialization which includes changing life cycle and initial personalization agent key will be conducted in manufacturing phase; chip initialization can be conducted right after manufacturing inlay or manufacturing cover sheet according to the policy of personalization agent

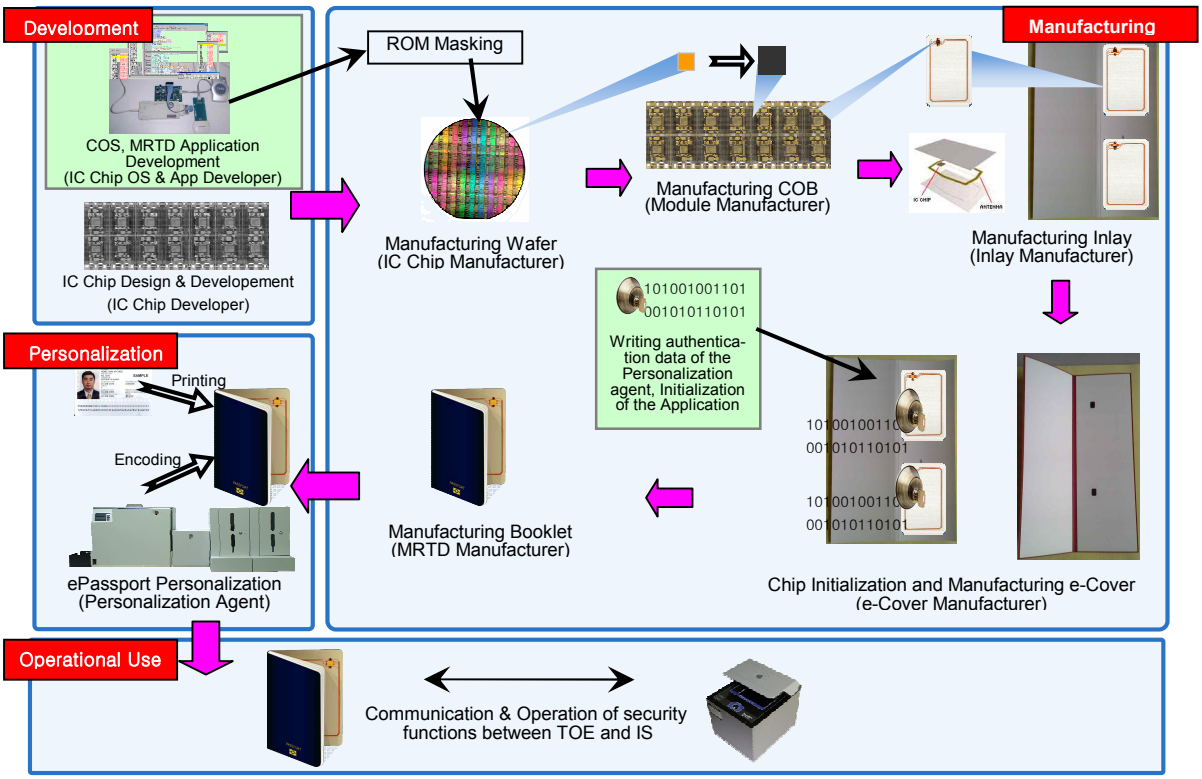


Figure 6. ePassport Life Cycle

Lifecycle of TOE(HW) and TOE(SW) are described in Table 6.

Table 6. TOE Life Cycle

Phase	Life Cycle of the TOE(HW)	Life Cycle of the TOE(SW)	TOE(SW) detailed steps
Phase 1 (Development)	① The IC chip manufacturer to design the IC chip and to develop the IC chip Dedicated S/W		
		② The S/W developer to develop the TOE (SW) by using the IC chip and the Dedicated S/W	TOE(SW) Development Process
Phase 2 (Manufacturing)		③-1 The S/W developer to inject initial personalization agent key into EEPROM and deliver the TOE to the IC Chip manufacturer	TOE(SW) Delivery Process
	③-2 The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier and to		

	produce the IC chip, and to manufacture the IC Chip wafer and COB module		
		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 ⑤ The ePassport manufacturer to record identification and authentication information of the ePassport Personalization agent in the EEPROM ⑥ The ePassport manufacturer to embed the IC chip in the passport book	TOE(SW) Installation, generation, and start-up process
Phase 3 (Personalization)		⑦ The Personalization agent to create SOD by a digital signature on the ePassport identity data ⑧ 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)		⑨ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE	

1.4.8 TOE (SW) Operational Mode

Operational Mode is defined for Files (DF and EF) and MF of TOE (SW). Operational Mode of Files is as shown in Table 7. Personalized (0x0A) is defined only for ePassport DF and ePassport DF can be entered into Personalized only from Operational (Active). ePassport access condition is forced to the subjects in the Personalized state.

Table 7. Operational Mode of Files

Operational Mode Code	Operational Mode	Relevant TOE Life Cycle
0x03	Initialize	Personalization
0x05	Operational(Active)	Operational Use (except ePassport)
0x06	Operational(Deactivated)	Operational Disuse
0x0C	Termination	Disuse

Operational Mode of Files can be changed as shown in Figure 7.

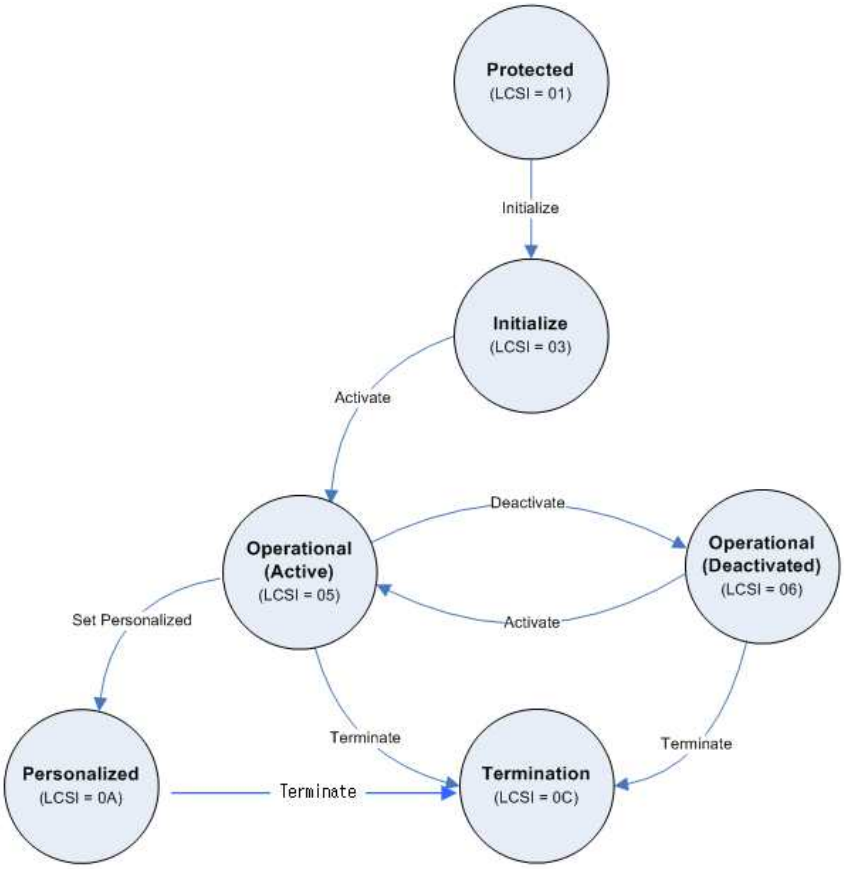


Figure 7. Relation Diagram for Operational Mode of File

Operational Mode of MF is shown in Table 8.

Table 8. Operational Mode of MF

Operational Mode Code	Operational Mode	Relevant TOE Life Cycle
0x01	Protected	Development, Manufacturing, and Personalization
0x03	Initialize	Personalization
0x05	Operational(Active)	Operational Use (except ePassport
0x06	Operational(Deactivated)	Operational Disuse
0x0C	Termination	Disuse

Operational Mode of MF can be changed as shown in Figure 8.

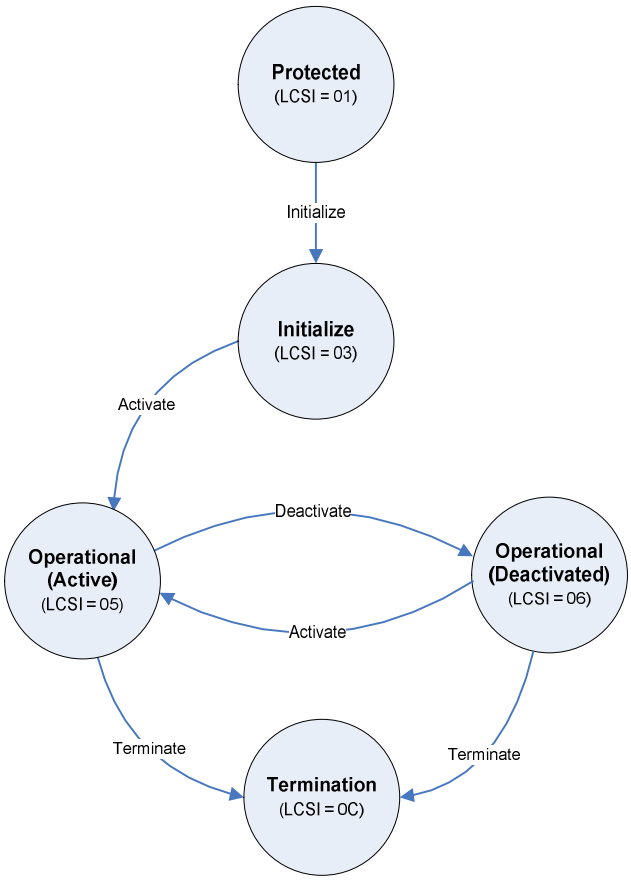


Figure 8. Relation Diagram for Operational Mode of MF

1.5 Security Target Organization

Section 1 provides introductory material required for the Protection Profile and PP references and the summary of TOE.

Section 2 provides the conformance claim that declares conformance for common criteria, protection profile, and packages.

Section 3 describes the TOE security problem definition and includes security problems of the TOE and its IT environment from such as threats, organizational security policies and assumptions.

Section 4 defines the security objectives for the TOE, its IT environment and rationale of security objectives to counter to identified threats, perform organizational security policies, and support the assumptions.

Section 5 defines extended components.

Section 6 contains the IT security requirements including the functional and assurance requirements and is drawn from Common Criteria Part2 and Part 3.

Section 7 describes TOE summary specification explaining TOE security functionality and assurance measures.

Section 8 defines the terms used in this Security Target.

Section 9 contains the materials referenced in this Security Target.

Terms and Abbreviations provides terms and abbreviations frequently used.

2 Conformance Claim

Conformance claim describes how the ST conforms to common criteria, protection profile and package.

2.1 Common Criteria Conformance Claim

This ST conforms to

- Common Criteria for Information Technology Security Evaluation, part 1: Introduction and general model, Version 3.1r3, July. 2009, CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation, part 2: Security functional requirements, Version 3.1r3, July. 2009, CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation, part 3: Security assurance requirements, Version 3.1r3, July. 2009, CCMB-2009-07-003

The conformance to common criteria is like the following:

- Part 2 Conformant
- Part 3 Conformant

2.2 Protection Profile Conformance

This ST is conforming to the protection profile as follows:

- Protection profile : ePassport Protection Profile V2.0
- Protection Profile Certification Number : KECS-PP-0163-2009
- Assurance package : EAL4 augmented(ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)
- Type of conformance : demonstrable conformance

2.3 Package Claim

This ST is conforming to assurance package as follows:

- Assurance Package : EAL4 augmented with(ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)

2.4 Conformance Claim Rationale

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type, the security problem definition and the statement of security objectives and the statement of security requirement in the ePassport Protection Profile V2.1 (hereafter referred to as ‘PP').

2.4.1 The Consistency of the TOE Type

The type of TOE in the PP is the software including IC chip operating system (COS) and the application of machine readable travel documents (ePassport application) which is embedded on the IC chip. The ePassport application includes the ePassport security mechanisms such as BAC, EAC and the ePassport access controls.

The type of TOE in this ST is the software including IC chip operating system (COS) and the application of machine readable travel documents (ePassport application) which is embedded on the IC chip.

The ePassport application includes the ePassport security mechanisms such as BAC, EAC and ePassport access controls as well as AA and the personalization agent authentication.

Therefore the type of TOE in this ST includes that in the PP and thus has consistency.

2.4.2 The Consistency of the Security Problem Definition

2.4.2.1 The Re-establishment of the Security Problem Definition

The following table shows that the security problem definition of this ST is equivalent to that of the PP and maintains the consistency.

Table 9. List of the Re-establishment of the Security Problem Definition

PP	ST	Description of reestablishment	Rationale
T.BAC_Authentication_Key_Disclose	T.BAC_Authentication_Key_Disclose	The BAC authentication key is generated and is stored in the secure memory in the Personalization phase.	Generating BAC authentication key by personalization agent in the Personalization phase is selected from 2 methods suggested in PP, and application note is modified in accordance. Therefore, ST conforms to PP more restrictively.
T.Residual_Info	T.Residual_Info	”BAC_Authentication_Key” Removed	Removed “BAC_Authentication_Key” since BAC authentication key is stored in secure memory and is stated in ‘T.BAC_Authentication_Key_Disclose”, not in temporary memory area which is stated in ‘T.Residual_Info’. Therefore, ST conforms to PP more restrictively.
A.Inspection_System	A.Inspection_System	Added “AA support“	Since TOE supplies AA security mechanism, added AA security mechanism considering the possibility of the ability that inspection system can use this. AA security mechanism is additionally supplied, thus conforms PP more restrictively.
A.IC_Chip	P.IC_Chip	Raise the level of the IC chip from EAL4+ to EAL5+ Changed IC Chip as TOE composition from TOE underlying platform.	Since TOE is composed of EAL5+ certificated IC chip, thus conforms to PP more restrictively. Because TOE is composed product which its scope includes IC chip, change assumptions to policy, and describes IC chip to the TOE composition.

2.4.2.2 The Augmentation to the Security Problem Definition

The following table proves that the security problem definition in this ST is more restrictive than that of the PP which is claimed to be conformed and thus it is consistent.

Table 10. List of Augmentation to the Security Problem Definition

Augmentation	Rationale
T. IC_Chip_Forgery	Adding a threat of IC chip forgery attack augments security object thus enhances the security attributes and restricts the security problem definition in the PP.

2.4.2.3 The Acceptance of the Security Problem Definition

The following table proves that the security problem definition in this ST is equivalent to that of the PP which is claimed to be conformed and thus it is consistent.

Table 11. List of the Acceptance of the Security Problem Definition

Acceptance	Rationale
T.TSF_Data_Modification	Equivalent to the security problem definition in the PP
T.Eavesdropping	Equivalent to the security problem definition in the PP
T.Forgery_Corruption_Personal_Data	Equivalent to the security problem definition in the PP
T.BAC_Replay_Attack	Equivalent to the security problem definition in the PP
T.Damage_to_Biometric_Data	Equivalent to the security problem definition in the PP
T.EAC-CA_Bypass	Equivalent to the security problem definition in the PP
T.IS_Certificate_Forgery	Equivalent to the security problem definition in the PP
T.SessionData_Reuse	Equivalent to the security problem definition in the PP
T.Skimming	Equivalent to the security problem definition in the PP
T.Malfunction	Equivalent to the security problem definition in the PP
T.Leakage_CryptographicKey_Info	Equivalent to the security problem definition in the PP
T.ePassport_Reproduction	Equivalent to the security problem definition in the PP
P.International_Compatibility	Equivalent to the security problem definition in the PP
P.Security_Mechanism_Application_Procedures	Equivalent to the security problem definition in the PP
P.Personalization_Agent	Equivalent to the security problem definition in the PP
P.ePassport_Access_Control	Equivalent to the security problem definition in the PP
P.PKI	Equivalent to the security problem definition in the PP
P.Range_RF_Communication	Equivalent to the security problem definition in the PP
A.Certificate_Verification	Equivalent to the security problem definition in the PP
A.MRZ_Entropy	Equivalent to the security problem definition in the PP

2.4.2.4 The Exclusion of the Security Problem Definition

The following table proves that the security problem definition excluded in this ST doesn't need to be considered as in the PP which is claimed to be conformed and thus it is consistent.

Table 12. List of the Exclusion of the Security Problem Definition

Exception	Rationale
P.Application_Install	TOE is native COS that disables personalization agent installing application on ePassport IC chip. The step that personalization agent verifies the safety of application is unnecessary, thus is consistent with security problem definition in the PP.

2.4.3 Security Objectives Rationale

2.4.3.1 The re-establishment of the Security Objectives

The following table shows the security objectives in this ST is equivalent to those in the PP thus is consistent.

Table 13. List of Re-establishment of the Security Objectives

PP security objectives	ST security objectives	Reestablishment	Rationale
O.Security_Mechanism_Application_Procedure	O.Security_Mechanism_Application_Procedure	Added AA to the security mechanisms that TOE supports	Added AA to the TOE security mechanisms defined in PP. Thus ST conforms to PP more strictly.
O.Session_Termination	O.Session_Management	Maintain EAC communication channel instead of session termination even if the EAC-TA fails Change the name. Added session termination when personalization agent authentication fails	EAC specification mandates maintaining the EAC secure messaging channel generated by successful EAC-CA to protect the transmission data even if the EAC-TA fails. Thus ST conforms to PP more strictly.
O.Secure_Messaging	O.Secure_Messaging	Added secure messaging in the personalization phase	Not only to guarantee data security and integrity at operational usage phase as defined in PP, but also to obtain data integrity, added security objectives. Thus ST conforms to PP more strictly.
O.Replay_Prevention	O.Replay_Prevention	Modified the application note, additional authentication data which requires a random number.	The coverage of authentication data which requires replay prevention is widened for AA and personalization authentication are added. Thus ST conforms to PP more strictly.

PP security objectives	ST security objectives	Reestablishment	Rationale
OE.IC_Chip	O.IC_Chip	Changed security characteristic of IC chip from the 'Security Objectives for Environment' to the 'TOE Security Objectives'	TOE is the composed product that includes IC chip to its TOE scope. So the security characteristic of IC chip is changed from the 'Security Objectives for Environment' to the 'TOE Security Objectives'.

2.4.3.2 The augmentation to the Security Objectives

The following table proves that the security objectives in this ST are more restrictive than that of the PP which is claimed to be conformed and thus it is consistent.

Table 14. List of Augmentation to the Security Objectives

Augmentation	Rationale
O.Personalization_agent_authentication	Conforms the security objectives of the PP more restrictively by additional security objective corresponding to the providing a method for authenticating ePassport personalization agent.
O.AA	Augmenting the security attribute of the TOE for verification of genuineness enhances the security properties of the PP and thus conforms more strictly.

2.4.3.3 The acceptance of the Security Objectives

The following table shows that the security objectives in this ST is equivalent to that of the PP and thus maintains its consistency.

Table 15. List of Acceptance of the Security Objectives

Acceptance	Rationale
O.Management	Equivalent to the security objective in the PP
O.Certificate_Verification	Equivalent to the security objective in the PP
O.Secure_State	Equivalent to the security objective in the PP
O.Deleting_Residual_Info	Equivalent to the security objective in the PP
O.Access_Control	Equivalent to the security objective in the PP
O.Handling_Info_Leakage	Equivalent to the security objective in the PP
O.BAC	Equivalent to the security objective in the PP
O.EAC	Equivalent to the security objective in the PP
OE.ePassport_Manufacturing_Security	Equivalent to the security objective in the PP
OE.Procedures_of_ePassport_Holder_Check	Equivalent to the security objective in the PP

Acceptance	Rationale
OE.Certificate_Verification	Equivalent to the security objective in the PP
OE.Personalization_Agent	Equivalent to the security objective in the PP
OE.Inspection_System	Equivalent to the security objective in the PP
OE.MRZ_Entropy	Equivalent to the security objective in the PP
OE.PKI	Equivalent to the security objective in the PP
OE.Range_RF_Communication	Equivalent to the security objective in the PP

2.4.3.4 The Exclusion of the Security Objectives

The following table proves that the security objectives excluded in this ST doesn't need to be considered as in the PP which is claimed to be conformed and thus it is consistent.

Table 16. List of the Exclusion of the Security Objectives

Exclusion	Rationale
OE.Application_Install	P.Application_Install TOE is native COS that disables personalization agent installing application on ePassport IC chip. The step that personalization agent verifies the safety of application is unnecessary, thus is consistent with security objectives in the PP.

2.4.4 The Rationale for the Consistency of Security Function Requirements

2.4.4.1 The Re-establishment of the Security Functional Requirements

The following table shows that the SFR in this ST is equivalent to the SFR in the PP and thus maintains its consistency.

Table 17. List of the Re-establishment of the SFR

SFR		Operation performed in this ST	Description on re-establishment
FCS_CKM.1	FCS_CKM.1.1	-	TOE generates BAC authentication key when changing to operational usage phase, thus conforms the PP more restrictively.
FCS_CKM.2(1)	FCS_CKM.2.1	Selection, Selection	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FCS_CKM.2(2)	FCS_CKM.2.1	Selection, Selection, Refinement	
FCS_CKM.4	FCS_CKM.4.1	Assignment, Assignment	
FCS_COP.1(1)	FCS_COP.1.1	Assignment, Selection, Selection, Selection	
FCS_COP.1(2)	FCS_COP.1.1	Selection, Selection, Selection	
FCS_COP.1(3)	FCS_COP.1.1	Assignment, Selection, Assignment, Selection	

SFR		Operation performed in this ST	Description on re-establishment
FCS_COP.1(4)	FCS_COP.1.1	Selection, Assignment, Selection, Assignment, Assignment	
FDP_ACC.1(1)		Iteration	Changed the name to FDP_ACC.1(1)
	FDP_ACC.1.1	Assignment, Assignment, Assignment	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FDP_ACC.1(2)	FDP_ACC.1.1	Assignment, Assignment, Assignment	Applied iteration to add security function, thus conforms the PP more restrictively
FDP_ACF.1(1)		Iteration	Changed the name to FDP_ACF.1(1)
	FDP_ACF.1.1	Assignment	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
	FDP_ACF.1.2	Assignment	
	FDP_ACF.1.3	Assignment	
	FDP_ACF.1.4	Assignment	
FDP_ACF.1(2)	FDP_ACF.1.1	Assignment	Applied iteration to add security function, thus conforms the PP more restrictively
	FDP_ACF.1.2	Assignment	
	FDP_ACF.1.3	Assignment	
	FDP_ACF.1.4	Assignment	
FDP_RIP.1	FDP_RIP.1.1	Assignment, Selection	Deleted the BAC authentication key from the list of objects, but added random value, thus conforms the PP more restrictively
FDP_UCT.1	FDP_UCT.1.1	-	No changes against the PP, thus equivalent to the PP
FDP_UIT.1	FDP_UIT.1.1	Selection	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
	FDP_UIT.1.2	Selection	
FIA_AFL.1(1)		Iteration	Changed the name to FIA_AFL.1(1)
	FIA_AFL.1.1	Assignment, Selection	Applied operations to meet the security objectives, and refined the method of handling the failure of authentication, thus conforms the PP more restrictively.
	FIA_AFL.1.2	Selection, Refinement	
FIA_UAU.1(1)	FIA_UAU.1.1	Assignment	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FIA_UAU.1(2)	FIA_UAU.1.1	Assignment	
FIA_UAU.4	FIA_UAU.4.1	Assignment	
FIA_UAU.5	FIA_UAU.5.1	Assignment	
	FIA_UAU.5.2	Assignment	
FIA_UID.1	FIA_UID.1.1	-	No changes against the PP, thus equivalent to the PP
	FIA_UID.1.2	-	
FMT_MOF.1(1)	-	Iteration	Changed to FMT_MOF.1(1) No changes against the PP, thus equivalent to the PP
FMT_MSA.1	FMT_MSA.1.1	-	No changes against the PP, thus equivalent to the PP
FMT_MSA.3	FMT_MSA.3.1	-	No changes against the PP, thus equivalent to the PP
	FMT_MSA.3.2	-	
FMT_MTD.1(1)	FMT_MTD.1.1	Assignment, Refinement	Changed the identification information of the iteration component to 'the certificate verification information and the authentication key' Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FMT_MTD.1(2)	FMT_MTD.1.1	-	No changes against the PP, thus equivalent to the PP

SFR		Operation performed in this ST	Description on re-establishment
FMT_MTD.3	FMT_MTD.3.1	Assignment	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FMT_SMF.1	FMT_SMF.1.1	Refinement, Assignment	
FMT_SMR.1	FMT_SMR.1.1	Assignment	
FPR_UNO.1	FPR_UNO.1.1	Assignment	
FPT_FLS.1	FPT_FLS.1.1	Assignment	No changes against the PP, thus equivalent to the PP
FPT_ITI.1	FPT_ITI.1.2	Assignment, Refinement	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FPT_TST.1	FPT_TST.1.1	Selection	Applied operations to meet the security objectives, thus conforms the PP more restrictively.
	FPT_TST.1.2	Selection	
	FPT_TST.1.3	Selection	

Application note on FCS_CKM.1(1) is modified since the TOE does not store the BAC authentication key during the BAC mutual authentication procedure but the key is generated by TSF in place of the ePassport personalization agent after storing DG1 file in personalization phase and is stored in the secure memory placed in the EEPROM.

FIA_AFL.1 (1) is refined because the EAC specification mandates maintaining the secure messaging channel instead of terminating the session to protect the transmitted data when the EAC-TA fails. At this point, the equivalent level of security to that of terminating the session is assured since the security of transmitted data is maintained and the access to DG3/DG4 is denied.

The application notes on FCS_CKM.2(2), FMT_MOF.1(1), FMT_MSA.3, FPT_ITI.1, and etc. are refined to reflect the implementation characteristics of the TOE.

2.4.4.2 The Augmentation to the Security Functional Requirement

The following table shows that the SFR in this ST is more restrictive and is consistent with the SFR in the PP by accepting them with additional SFR.

Table 18. List of the Augmentation to the SFR

Augmentation	Rationale
FDP_DAU.1	This SFR is added since the AA security mechanism is added to the security objective. The ePassport personalization agent provides the function to detect the forged IC chip thus the SFR in this ST accepts the PP restrictively
FIA_AFL.1(2)	This SFR is for providing an action which shall be performed when the additional ePassport personalization agent authentication failure. This change makes this ST to accept the PP restrictively because the action for the failure of ePassport personalization authentication is enhanced.
FIA_UAU.1(3)	This SFR is added for the requirement of the measure to authenticate a user as the ePassport personalization agent to connect and maintain the security role of the ePassport personalization agent to user and grant the subject right to the user.

Augmentation	Rationale
	This adds an ePassport personalization agent authentication function and accepts the PP restrictively.
FMT_MOF.1(2)	Explained BAC & EAC disable function that TOE offers to satisfy various personalization policy of the personalization agent, and added application note to maintain ePassport access control policy of PP, thus the security level is equivalent The PP does not require the secure messaging in personalization phase, but this ST added this SFR in order to provide the secure messaging and disable it if the personalization environment is secure and does not require the secure messaging. Applied operations to meet the security objectives, thus conforms the PP more restrictively.
FMT_MTD.1(3)	This SFR is added since the TOE is selected as a subject generates the BAC authentication key among the two options in the PP and the TSF generates and stores the BAC authentication key automatically after the DG1 is written successfully. Applied operations to meet the security objectives, thus conforms the PP more restrictively.

2.4.5 The Consistency of the Security Assurance Requirements

This ST maintains “demonstrable conformance” of the security assurance requirements of the PP since it includes the assurance package of the PP – EAL4 augmented with (ADV _IMP.2, ATE_DPT.2, AVA_VAN.4).

The assurance components augmented to EAL4 in PP are as below:

- ADV_IMP.2 “Complete mapping of the implementation representation of the TSF”
- ATE_DPT.2 “Security enforcing modules”
- AVA_VAN.4 “Systematic vulnerability analysis”

Table 19. List of Accepted Security Assuarance Requirements

Accepted Security Assurance Requirements		Rationale
Assurance Class	**Assurance Component**	
Security target evaluation	ASE_INT.1	Equivalent to the PP
	ASE_CCL.1	Equivalent to the PP
	ASE_SPD.1	Equivalent to the PP
	ASE_OBJ.2	Equivalent to the PP
	ASE_ECD.1	Equivalent to the PP
	ASE_REQ.2	Equivalent to the PP
	ASE_TSS.1	Equivalent to the PP
Development	ADV_ARC.1	Equivalent to the PP
	ADV_FSP.4	Equivalent to the PP
	ADV_IMP.2	Equivalent to the PP
	ADV_TDS.3	Equivalent to the PP
Guidance documents	AGD_OPE.1	Equivalent to the PP
	AGD_PRE.1	Equivalent to the PP
Life cycle support	ALC_CMC.4	Equivalent to the PP
	ALC_CMS.4	Equivalent to the PP
	ALC_DEL.1	Equivalent to the PP
	ALC_DVS.1	Equivalent to the PP
	ALC_LCD.1	Equivalent to the PP
	ALC_TAT.1	Equivalent to the PP
Tests	ATE_COV.2	Equivalent to the PP
	ATE_DPT.2	Equivalent to the PP
	ATE_FUN.1	Equivalent to the PP
	ATE_IND.2	Equivalent to the PP
Vulnerability analysis	AVA_VAN.4	Equivalent to the PP

2.5 Conventions

The notation, formatting and conventions used in this ST 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 ST.

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.).

Selection

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

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**.

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].

"Application Notes" are provided to help to clarify the intent of a requirement, identify implementation choices or to define "Pass/Fail" criteria for a requirement. Application Notes will follow relevant requirements where appropriate.

3 Security Problem Definition

Security Problem Definition defines threats, organizational policy and assumptions that intended to be processed by TOE and TOE environment.

3.1 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. TSF_Data_Modification

The threat agent may attempt access to the stored TSF data by using the external interface through the Inspection System.

< BAC-related Threats in the TOE Use phase >

T. Eavesdropping

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

T. Forgery_Corruption_ 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.

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 the related information.

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. The TOE uses the former method. Therefore the TOE considers the threat of disclose of the BAC authentication key stored in secure memory of the MRTD chip. The BAC authentication key is removed from the T.Residual_Info because it shall never be stored in the temporary memory.

T.BAC_ReplayAttack

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.

<EAC - related Threats in the TOE 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 biometric data of the ePassport holder with the read - rights. 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 of the ePassport holder to the biometric data, 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 TOE Operational Use phase >

T. SessionData_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 TSF and TSF data stored in the TOE, threat agent may cause malfunction of the TOE in the environmental stress outside the normal operating conditions.

< Other Threats in the Operational Use phase >

T. Leakage_CryptographicKey_Info

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. 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. Residual_Info

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, EAC session key, DV certificate and IS certificate, etc., are recorded and used in temporary memory.

T. IC chip duplication [2]

The threat agent may acquire the ePassport user data including SOD and store the acquired data to a new IC chip so that a duplicated ePassport is made.

3.2 Organizational Security Policies

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

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.

[2] Added as a security environment related to AA

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.

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.

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 20. ePassport Access Control Policy

List of Subjects		List of Objects	Objects									
			Personal data of the ePassport holder		Biometric data of the ePassport holder		ePassport Authentication data		EF.CVCA		EF.COM	
			Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	BIS	BAC Authorization	*Allow*	*Deny*	*Deny*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*
	EIS	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	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*

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_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.IC_Chip

The IC chip used in 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 : The chip used in TOE is the certified product of CCRA EAL5+(SOF-high)

3.3 Assumptions

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

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.

A. Inspection_System

The Inspection System shall implement security mechanisms of the PA, the BAC and the EAC 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. If the BIS supports the AA security mechanism as an option, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder explicitly by performing the AA and verifying the digital signature which is generated by the TOE.

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. If the EIS supports the AA security mechanism as an option, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder explicitly by performing the AA and verifying the digital signature which is generated by the TOE after performing the EAC-CA and the PA.

A. MRZ_Entropy

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

Application Notes: In order to be resistant to the middle-level threat agent, the entropy for the passport number, date of birth, date 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.

4 Security Objectives

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 by technical/process-relevant means supported from IT environment in order to provide TOE security functionality accurately.

4.1 Security Objectives for the TOE

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

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 Personallization phase, the Personalization Agent deactivates the writing function after recording the MRTD application data.

O.Personalization_Agent_Authentication

The TOE shall provide the authentication means, which have the equivalent level to BAC, to connect only the authorized Personalization Agent to issuing management role and subject security attributes.

O.Security_Mechanism_Application_Procedures

The TOE shall ensure instruction flow according to ePassport inspection precedures of the EAC specification.

Application Notes : The TOE shall ensure that the application order of PA, AA, BAC, and EAC security mechanisms conforms to 2.1.1 Standard ePassport Inspection Precedure and 2.1.2 Advanced ePassport Precedure of the EAC specifications and shall not allow requests from the Inspection System that do not correspond to the security mechanism application order.

O.Session_Management

The TOE shall terminate the session in case of failure of the BAC mutual authentication or detecting modification in the transmitted TSF data. Also, the TOE shall preserve EAC secure channel in case of failure of the EAC-TA.

O.Secure_Messaging

The TOE shall ensure confidentiality and integrity to protect the transmitted user and TSF data. Also, the TOE shall be able to handle that The Personalization Agent requests the secure messaging in Personalization phase.

O.Certificate_Verification

The TOE shall automatically update the certificate and current date by checking valid date on the basic of the CVCA link certificate provided by the Inspection System.

O.Secure_State

The TOE shall preserve secure state from attempt of modification of TSF operation code and data at start-up.

O.Deleting_Residual_Info

When allocating resouces, the TOE shall provide means to ensure that previous security-relevant information (Ex. BAC session key, EAC session key, etc.) is not included.

O.Replay_Prevention

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

Application Notes : The TOE shall generate the transmitted data to the Inspection System in the 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 to derive session key by generating the BAC session key with the same random number used in the BAC mutual authentication. The random number generated in the active authentication and the random number used in Persionalization agent authentication shall be differenctly generated per session.

O.Access_Control

The TOE shall provide the access control functionality so that access to the MRTD application data is allowed only to external entities granted with access-rights according to the ePassport access control policies of the Personalization Agent.

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

O.Handling_Info_Leakage

The crypto co-processor of the IC chip or cryptographic library loaded in the IC chip used by the TOE provides the means to prevent analyzing the leakage information (elecric power or wave, etc.) during cryptographic operation, and obtaining key information.

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.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.AA

The TOE shall be able to verify its own genuineness for the Inspection System to detect the forgery of MRTD chip.

O.IC_Chip

The IC chip, the component of 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.

4.2 Security Objectives for the Environment

The following are security objectives handled by technical/procedure-relevant means supported from IT environment in order to provide TOE security functionality accurately.

OE.ePassport_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. 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.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

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 de-activate the writing function before the TOE delivery to the Operational Use phase.

OE.Inspection_System

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

OE.MRZ_Entropy

The personalization agent shall ensure the MRZ entropy to ensure the secure BAC authentication key.

OE.PKI

The Issuing State of the ePassport shall execute certification practice to securely generate and manage a digital signature key and to generate issue, operate, or 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.Range_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 MRTD chip is not opened.

4.3 Security Objectives Rationale

Security Objectives Rationale demonstrates that the specified security objectives are appropriate, sufficient to trace security problems and are essential, rather than excessive.

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 21 shows the mapping between Security Problem Definition and Security Objectives.

Table 21. Mapping between Security Problem Definition and Security Objectives

Security Problem Definition \ Security Objectives	TOE Security Objectives														Security Objectives for the Environment							
	O.Management	O.Personalization_Agent_Authentication	O.Security_Mechanism_Application_Procedu	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.BAC	O.EAC	O.AA	O.IC_Chip	OE.ePassport_Manufacturing_Security	OE.Procedures_of_ePassport_Holder_Check	OE.Certificate_Verification	OE.Personalization_Agent	OE.Inspection_System	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Communication
T.TSF_Data_Modification	X	X		X	X					X									X				
T.Eavesdropping					X															X			
T.Forgery_Corruption _Personal Data				X						X		X								X			
T.BAC_Authentication_Key _Disclose	X			X						X							X						
T.BAC_ReplayAttack									X														
T.Damage_to_Biometric _Data				X	X	X				X			X					X		X		X	
T.EAC-CA_Bypass			X														X	X		X			
T.IS_Certificate_Forgery	X	X				X												X					
T.SessionData_Reuse									X											X			
T.Skimming										X		X	X							X			X
T.Malfunction							X								X								
T.Leakage _CryptographicKey_Info											X				X								
T.ePassport_Reproduction																X	X						
T.Residual_Info								X															
T.IC_Chip_Forgery														X									
P.International_Compatibility																			X				
P.Security_Mechanism _Application_Procedures			X																	X			
P.Personalization_Agent	X	X																	X				
P.ePassport _Personalization_Policy	X				X																		
P.ePassport_Access _Control	X									X		X	X						X	X			
P.PKI						X																X	
P.Range_RF _Communication																							X
P.IC_Chip															X								
A.Certificate_Verification																		X	X			X	
A.Inspection_System																				X			
A.MRZ_Entropy																					X		

4.3.1 Security Objective Rationale for the TOE

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 LDS 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.

This security objective provides the means to manage EAC disablement when personalizing ePassport excluding ePassport biometric information according to the issuing policy, therefore contributes to enforce the organizational security policy of P.ePassport_Personalization_Policy.

O.Personalization_Agent_Authentication

This security objective ensure that the TOE provides the means to authorize user as personalization agent for granting write-rights of TSF data in the Personalization phase, therefore is required to counter the threat of T.TSF_Data_Modification.

Since personalization agent authentication is conducted before performing the security role to write information relevant to CVCA certificate, a user without the security role shall not be able to write forged CVCA certificate. Therefore, forged IS certificate transmitted from outside shall be detected and this is required to counter the threat of T.I_Certificate_Forgery.

This security objective ensures that the TOE provides the means to authorize personalization agent to confirm that personalization subject is not changed, therefore contributes to enforce the organizational security policy of P.Personalization_Agent.

O.Security_Mechanism_Application_Procedures

This security objective is required to enforce the organizational security policy 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.Session_Management

This security objective ensures that the TOE prevents authentication attempts of authentication in order for access to forge and corrupt the personal 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 threat of T.Forgery_Corruption_Personal_Data, T.TSF_Data_Modification, and T.BAC_Authentication_Key_Disclose.

Also, this security objective ensures that the TOE detects the EAC-TA failure of whom attempts access to read, maintains the EAC secure channel, and reduces attack chances, therefore is required to counter the threat of T.Damage_to_Biometric_Data.

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 ensures that the TOE establishes the secure messaging when the authorized Personalization Agent wirtes TSF data, and provides integrity of TSF data. Therefore, this security objective is required to counter the threat of T.TSF_Data_Modification.

Also, this security objective ensures that if The Personalization Agent requests the secure messaging the TOE handles it, and that if The Personalization Agent does not request it, the TOE deactives the secure messaging. Therefore, this security objective contributes to enforce the organizational security policy of P.ePassport_Personalization_Policy.

O.Certificate_Verification

This security objective is required to enforce the organizational security policy 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.Secure_State

This security objective is required to counter the threat of T.Malfunction as the TOE detects modification of the TSF operation code and data through self-testing, provides means to prevent bypass TOE secure functions, and protects the TOE itself by preserving a secure state so that malfunction of TSF do not occur.

O.Deleting_Residual_Info

This security objective is required to counter the threat of T.Residual_Info 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 collects memory resources, therefore ensuring that information is not available.

O.Replay_Prevention

This security objective is required to counter the threat of T.BAC_ReplayAttack by ensuring that the TOE generates different values per session that are transmitted to the Inspection System in the BAC mutual authentication. Also, this security objective is required to counter the threat of T.SessionData_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.Access_Control

This security objective is required to counter the threats of T. Forgery_Corruption_Personal_Data, T.Damage_to_Biometric_Data and T.Skimming and enforce the organizational security policy 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 personalization agent in the Operational Use phase.

O.Handling_Info_Leakage

This security objective is required to counter the threat of T.Leakage_CryptographicKey_Info as the TOE provides the means to prevent analyzing the leakage information (electric power and wave, etc.) during cryptographic operation, and obtaining of key information.

O.BAC

This security objective is required to enforce the organizational security policy 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 grants 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_Corruption_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.EAC

This security objective is required to enforce the organizational security policy 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 grants 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.

O.AA

This security objective is required to counter the threat of T.IC_Chip_Forgery as the personalization agent provides the Inspection System with the verification data for genuineness to detect the forged MRTD chip.

O.IC_Chip

This security objective is required to enforce the organizational security policy of P.IC_Chip as it uses EAL5+ (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 is required to counter the threat of T.Malfunction as the IC chip detects malfunction outside the normal operating conditions, and it is required to counter the threat of T.Leakage_CryptographicKey_Info as it uses EAL5+ IC Chip that is assured.

4.3.2 Security Objective Rationale for Operating Environment

OE.ePassport_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.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.Certificate_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 maintain 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.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 policy 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.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_Corruption_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.SessionData_Reuse as the Inspection System generates different temporary public key per session 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.PKI

This security objective for environment is required to enforce the organizational security policy 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, and 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.Range_RF_Communication

This security objective for environment is required to counter the threat of T.Skimming and enforce the organizational security policy of P.Range_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.

5 Definition of Extended Component

This ST does not define extended component.

6 Security Requirements

Security requirements specify security functional requirements that must be satisfied by the TOE which is identified in this Security Target and security functional requirements that must be satisfied under the operational environment, and assurance requirements.

Subjects, objects, operations, and security attributes employed in security requirements are as shown in the below table. Terms mentioned in Table 22 is described in section 10.1.

Table 22. Major Terms in Security Target

Category		Items	Descriptions
Subject		Personalization Agent	-
		BIS	BAC Inspection System
		EIS	EAC Inspection System
Object	ePassport User Data	Personal Data of the ePassport holder	EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16
		Biometric Data of the ePassport holder	EF.DG3, EF.DG4
		ePassport Authentication Data	EF.DG14, EF.DG15, EF.SOD
		EF.CVCA	-
		EF.COM	-
	OS User Data	ePassport Operational Mode	-
		Personalization Agent access rule reference	-
External Entities		-	-
Operation		Read	-
		Write	-
Security Attributes	Access-rights of subject	BAC Authorization	Authorization obtained from BAC authentication
		EAC Authorization	Authorization obtained from EAC authentication
		Personalization Agent Issuing Authorization	Authorization obtained from Personalization Agent authorization
	Access-rights of object	BAC Authorization	-
		EAC Authorization	-
		Personalization Agent Issuing Authorization	-
	Operation of object	Read-rights	-
		Write-rights	-

6.1 TOE Security Functional Requirements

The security functional requirements specified in this Security Target consist of the following components from Part2 of the CC in order to satisfy security requirements identified in section 4.

Table 23. TOE Security Functional Requirements

Security Functional Class	Security Functional Component	
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.2(1)	Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)
	FCS_CKM.2(2)	Cryptographic key distribution (KDF Seed Distribution for EAC session key generation)
	FCK_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Symmetric Key Cryptographic Operation)
	FCS_COP.1(2)	Cryptographic operation (MAC)
	FCS_COP.1(3)	Cryptographic operation (Hash Function)
	FCS_COP.1(4)	Cryptographic operation (Digital signature Verification for Certificates Verification)
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (ePassport access control)
	FDP_ACC.1(2)	Subset access control (OS access control)
	FDP_ACF.1(1)	Security attribute based access control (ePassport access control)
	FDP_ACF.1(2)	Security attribute based access control (OS access control)
	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 (Inspection System authentication failure)
	FIA_AFL.1(2)	Authentication failure handling (Personalization Agent authentication failure)
	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 (Personalization Agent 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 behavior
	FMT_MOF.1(2)	Management of security functions behavior (Suspension of BAC, EAC, and Secure Messaging)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (Certification Verification Information and Authentication Key)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialization)
	FMT_MTD.1(3)	Management of TSF data (Generating and Writing BAC Authentication Key)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy (FPR)	FPR_UNO.1	Unobservability
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_TST.1	TSF testing

6.1.1 Cryptographic Support

FCS_CKM.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

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 BAC authentication key and writes BAC authentication key in itself when the Personalization agent changes the life cycle from Personalization phase to Operational Use phase. TOE generates BAC session key and EAC session key by using key derivation mechanism in Operational Use phase.

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

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*.

Application Notes : The TOE uses TDES accelerator and SHA-1 cryptographic library supported by the IC chip for KDF Seed Distribution for BAC session key generation.

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

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 *Diffie-Hellman key-agreement protocol* that meets the following: *PKCS#3*.

Application Notes : The TOE uses DH and SHA (SHA-1, SHA-256) cryptographic library supported by the IC chip for KDF Seed Distribution for the EAC session key and supports 1024 ~ 2048 bit key.

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 (Key Derivation Mechanism)]

FCS_CKM.4.1 The TSF shall destroy **encryption keys and MAC keys** in accordance with a specified cryptographic key destruction method [filling memory data with '0' or deleting physically by overwriting a new key] 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

FCS_COP.1.1 The TSF shall perform [message encryption, decryption operation] in accordance with a specified cryptographic algorithm *TDES* and cryptographic key sizes *112 bit* that meet the following: *[ICAO9303-1v2; Appendix 5]*.

FCS_COP.1(2) Cryptographic operation (MAC)

Hierarchical to : No other components.

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

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

FCS_COP.1(3) Cryptographic operation (Hash Function)

Hierarchical to : No other components.

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

FCS_COP.1.1 The TSF shall perform [hash operation] in accordance with a specified cryptographic algorithm *SHA-1, [SHA-256]* and cryptographic key sizes [none] that meet the following: *[FIPS 180-2]*.

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

FCS_COP.1.1 The TSF shall perform [Digital signature verification] in accordance with a specified cryptographic algorithm *RSASSA-PKCS1-v1.5-SHA-256, [RSASSA-PKCS1-v1.5-SHA-1]* and cryptographic key sizes [1024, 1280, 1536, and 2048 bit] that meet the following: *PKCS#1*.

6.1.2 User Data Protection

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

Hierarchical to : No other components.

Dependencies : FDP_ACF.1 Security attribute based access control

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

a) Subjects
(1) Personalization agent
(2) BIS
(3) EIS
(4) [None]

b) Objects
(1) Personal data of the ePassport holder
: EF.DG1, EF.DG2, EF.DG5 ~ EF.DG13, EF.DG16
(2) 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 (OS access control)

Hierarchical to : No other components.

Dependencies : FDP_ACF.1 Security attribute based access control

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

a) Subject

(1) Personalization agent

b) Objects

(1) ePassport Operational Mode

(2) Personalization agent access rule reference

c) Operations

(1) Read

(2) Write

(3) [None]

].

Table 24. OS access control policy

List of Object / List of Subject			Objects			
			ePassport Operational Mode		Personalization agent access rule reference	
			Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subject	Personalization Agent	Issuing Authorization	*Allow*	*Allow*	*Allow*	*Allow*

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

Hierarchical to : No other components.

Dependencies : FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [ePassport access control policy] to objects based on the following: [[Table 25], [Table 26], [none]].

Table 25. Subject-relevant Security Attributes

Subjects	Security Attributes
BIS	BAC authorization
EIS	BAC authorization, EAC authorization
Personalization Agent	Personalization agent issuing authorization

Table 26. 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 authentication data	Read-Rights	BAC authorization, EAC authorization
	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 to be successfully authenticated in the Personalization phase.

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 correspond 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: [In the Personalization phase, deletion of the object is allowed for the personalization agent which has issuing authorization.].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional 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 EIS that has the EAC authorization

c) Explicitly deny access (read, write, etc.) of the unauthorized Inspection System to all objects

d) [Explicitly deny access of the subjects to objects if the command is not allowed for the Operational Mode which the object is in]

FDP_ACF.1(2) Security attribute based access control (OS access control)

Hierarchical to : No other components.

Dependencies : FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [OS access control policy] to objects based on the following: [[Table 27], [Table 28], [none]].

Table 27. Subject-relevant Security Attributes

Subject	Security Attributes
Personalization Agent	Personalization agent issuing authorization

Table 28. Object-relevant Security Attributes

Objects	Security Attributes	
	Security attributes of object's operation	Security attributes of object's access rights
ePassport Operational Mode	Read-Rights	Personalization agent issuing authorization
	Write-Rights	Personalization agent issuing authorization
Personalization agent access rule reference	Read-Rights	Personalization agent issuing authorization
	Write-Rights	Personalization agent issuing authorization

Application Notes :

The Personalization agent issuing authorization is the right given to the Personalization agent when the Personalization agent authentication succeeds in Personalization phase.

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 correspond 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 additional rules:

a) [Explicitly deny access (read, write, etc.) of the unauthorized Inspection System to objects]

b) [Explicitly deny access of the subjects to objects if the command is not allowed for the Operational Mode which the object is in]

FDP_DAU.1 Basic data authentication

Hierarchical to : No other components.

Dependencies : No dependencies.

FDP_DAU.1.1 The TSF shall provide the capability to generate evidence that can be used as a guarantee of the validity of [Active Authentication private key].

FDP_DAU.1.2 The TSF shall provide [BIS, EIS] with the ability to verify evidence of the validity of the indicated information.

Application Notes : The TSF provides AA security mechanism up to 2048 bits.

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 *deallocation of the resource from* the following objects: [

a) BAC session key

b) EAC session key

c) [Random Number]

].

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. BAC authentication key is stored in the secure memory and protected safely, so it is not required to deallocate the resource from the key.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to : No other components.

Dependencies : [FTP_ITC.1 TSF 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 *transmit, receive* **object** 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 TSF Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

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

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

6.1.3 Identification and Authentication

FIA_AFL.1(1) Authentication failure handling (Inspection System authentication failure)

Hierarchical to : No other components.

Dependencies : FIA_UAU.1(1) Timing of authentication (BAC Mutual Authentication), FIA_UAU.1(2) Timing of Authentication (EAC-TA)

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

a) BAC mutual authentication

b) EAC-TA

c) [None]

].

- 1 unsuccessful authentication attempts related to BAC mutual authentication or EAC-TA within a single power-on session

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall perform [**as shown in Table 29**].

Table 29. Authentication Failure Handling relevant to Authentication Mechanism

Authentication Mechanism	Authentication Failure Handling
BAC Mutual Authentication	User Session Termination
EAC-TA	Maintaining EAC Secure Messaging

FIA_AFL.1(2) Authentication failure handling (Personalization Agent authentication failure)

Hierarchical to : No other components.

Dependencies : FIA_UAU.1(3) Timing of Authentication (Personalization Agent authentication)

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

a) Personalization agent authentication

].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall perform [user session termination]. **When 10 cumulative unsuccessful authentication attempts occur regardless of session, personalization agent authentication is not allowed permanently.**

Table 30. Authentication Failure Handling relevant to the number of unsuccessful authentication attempts

Unsuccessful Authentication Attempts	Authentication Failure Handling
1 time	Detection of the unsuccessful authentication attempt and user session termination
10 times	Personalization agent authentication is not allowed permanently

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) to indicate support of 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 the 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) [to perform AA]

] 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 the actions specified in FIA_UAU.1.1.

FIA_UAU.1(3) Timing of authentication (Personalization Agent authentication)

Hierarchical to : No other components.

Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow TSF [to select MF] which to be performed by the Personalization agent before the Personalization agent is authenticated.

FIA_UAU.1.2 The TSF shall require the Personalization agent to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions specified in FIA_UAU.1.1.

FIA_UAU.4 Single-use authentication mechanism

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) [Personalization agent 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) [Personalization agent 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 the CVCA certificate, DV certificate, and IS certificate. For this, the TSF shall provide the EAC-CA.

c) [The Personalization agent shall succeed the Personalization agent authentication in order to have the issuing authorization.]

].

FIA_UID.1 Timing of identification

Hierarchical to : No other components.

Dependencies : No dependencies.

FIA_UID.1.1 The TSF shall allow TSF [

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 the actions that is specified in FIA_UID.1.1.

Application Notes : When external entities communicated with the TOE request the use of the MRTD application, the TOE identifies it with **the Personalization agent or** the Inspection System.

6.1.4 Security Management

FMT_MOF.1(1) Management of security functions behavior

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 of **MRTD application data except EF.CVCA and current date** after recording the MRTD application data in the Personalization phase.

FMT_MOF.1(2) Management of security functions behavior (Suspension of BAC, EAC, and Secure Messaging)

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 [

a) BAC

b) EAC,

c) Secure Messaging in the Personalization phase

] to [Personalization agent in the Personalization phase].

Application Notes : To support the various Issuing Policy of the Personalization agent, TOE provides the ability to disable BAC. But to apply FDP_ACF.1, BAC shall not be disabled. If BAC is disabled, then the ePassport is not the certified TOE. The Personalization agent may disable EAC in the Personalization phase. In this case, the Personalization agent shall not issue biometric data of an ePassport holder. When the personalization agent implements and operates physical, human and procedural security measures equivalent level to Secure Messaging in the Personalization phase, Secure Messaging may not be applied.

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] to restrict the ability to *[initialisation]* the security attributes [security attributes of subjects defined in FDP_ACF.1] 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.

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] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Personalization agent] to specify alternative initial values to override the default values when an object or information is created.

Application Notes : When generating ePassport user data (EF.DG1~16, EF.SOD, EF.COM, EF.CVCA), the Personalization agent shall define security attributes to obtain object's read-rights and write-rights of the Personalization phase. When generating ePassport DF in the Personalization phase, the Personalization agent shall decide the MRTD Access Control Reference to define security attributes of object's operation and object's access-rights in FDP_ACF.1.1(1). When issuing biometric data of the ePassport holder, the Personalization agent shall define the MRTD Access Control Reference as to enable EAC.

FMT_MTD.1(1) Management of TSF data (Certification Verification Information and Authentication Key)

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 certificate

e) [AA chip authentication private key[3]

f) Personalization Agent 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].

[3] It is added to provide AA mechanism.

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 (Generating and Writing BAC Authentication Key)

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 *generate and write* the [BAC authentication key] to [TSF].

Application Notes : The TSF generates and stores BAC authentication key after writing DG1.

FMT_MTD.3 Secure TSF data

Hierarchical to : No other components.

Dependencies : FMT_MTD.1(1) Management of TSF data (Certificate Verification Information and Authentication Key)

FMT_ MTD.3.1 The TSF shall ensure that only secure values are accepted for [ePassport TSF data].

Application Notes : The TSF shall use only secure value safe as random numbers so that to respond to f moderate attack potential. 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. Additionally, AA security mechanism uses secure value as random numbers.

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, current data, **and SSC initialization** in the Operational Use phase

c) [Function to decide whether to enable BAC/EAC in the Personalization phase, to manage security attributes of ePassport objects and subjects, to change Operational Mode, and to disable writing function

d) Function to Generate and store BAC authentication key

e) Function to identify the TOE]

].

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 security management functions a), c), e) of FMT_SMF.1. The TSF executes security management functions of FMT_MTD.1(2) and b), d) of FMT_SMF.1. However, the TSF is not defined as the role since it is not a user.

6.1.5 Privacy

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) [None]

] on [

a) BAC authentication key

b) BAC session key

c) EAC session key

d) EAC chip authentication private key

e) [None]

] by [TSF].

6.1.6 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to : No other components.

Dependencies : No dependencies.

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

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) [None]

].

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 the session of the Personalization agent,

e) Deletion of the Personalization agent session key]

] if modifications are detected.

Application Notes : The strength of Retail MAC is equivalent to the secure Retail MAC specified in the ICAO document.

FPT_TST.1 TSF testing

Hierarchical to : No other components.

Dependencies : No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *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 *TSF*.

6.2 TOE Security Assurance Requirements

The security assurance requirements for this Security Target consist of the following components from Part 3 of the CC according to the Protection Profile and evaluation assurance level is EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4) as specified in the Protection Profile. The assurance components are augmented as follows.

- ADV_IMP.2 Complete mapping of the implementation representation of the TSF
- ATE_DPT.2 Testing : Security enforcing modules
- AVA_VAN.4 Systematic vulnerability analysis

The assurance components are summarized in Table 31.

Table 31. Security Assurance Requirements

Assurance Class	Assurance Components	
Security Target Evaluation	ASE_INT.1	ST Introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedure
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: Security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability analysis	AVA_VAN.4	Methodical vulnerability analysis

6.2.1 Security Target

ASE_INT.1 ST Introduction

Dependencies : No dependencies

Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview, and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

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

ASE_INT.1.2E The evaluator *shall confirm* that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies :

ASE_INT.1 ST Introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements

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

ASE_SPD.1 Security problem definition

Dependencies : No dependencies

Developer action elements

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements

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

ASE_OBJ.2 Security objectives

Dependencies :

ASE_SPD.1 Security problem definition

Developer action elements

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements

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

ASE_ECD.1 Extended components definition

Dependencies : No dependencies

Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements

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

ASE_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies :

ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements

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

ASE_TSS.1 TOE summary specification

Dependencies :

ASE_INT.1 ST Introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

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

ASE_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies :

ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements

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

ADV_FSP.4 Complete functional specification

Dependencies :

ADV_TDS.1 Basic design

Developer action elements

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

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

ADV_FSP.4.2E The evaluator *shall determine* that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_IMP.2 Complete mapping of the implementation representation of the TSF

Dependencies :

ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

ALC_CMC.5 Advanced support

Developer action elements

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

ADV_IMP.2.2D The developer shall provide a mapping between the TOE design description and the entire implementation representation.

Content and presentation elements

ADV_IMP.2.1C The implementation representation shall 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 in the form used by the development personnel.

ADV_IMP.2.3C The mapping between the TOE design description and the entire implementation representation shall demonstrate their correspondence.

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_TDS.3 Basic modular design

Dependencies :

ADV_FSP.4 Complete functional specification

Developer action elements

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements

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

ADV_TDS.3.2E The evaluator *shall determine* that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies :

ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance 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.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements

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

AGD_PRE.1 Preparative procedures

Dependencies : No dependencies

Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

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

AGD_PRE.1.2E The evaluator *shall apply* the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.4 Life-cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies :

ALC_CMS.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

ALC_LCD.1 Developer defined life-cycle model

Developer action elements

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

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements

ALC_CMC.4.1C The TOE shall be labeled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements

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

ALC_CMS.4 Problem tracking CM coverage

Dependencies : No dependencies

Developer action elements

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements

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

ALC_DEL.1 Delivery procedures

Dependencies : No dependencies

Developer action elements

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements

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

ALC_DVS.1 Identification of security measures

Dependencies : No dependencies

Developer action elements

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

Content and presentation 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.

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 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 Implementation representation of the TSF

Developer action elements

ALC_TAT.1.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

Content and presentation elements

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool 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.

6.2.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies :

ADV_FSP.2 Security-enforcing 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 elements

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

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

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: Security enforcing modules

Dependencies : ADV_ARC.1 Security architecture description

ADV_TDS.3 Basic modular 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 elements

ATE_DPT.2.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.2.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.2.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

Evaluator action 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 :

ATE_COV.1 Evidence of coverage

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 elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements

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

Content and presentation 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 execute* a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability analysis

AVA_VAN.4 Methodical vulnerability analysis

Dependencies : ADV_ARC.1 Security architecture description

ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_DPT.1 Testing: basic design

Developer action elements

AVA_VAN.4.1D The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.4.1C The TOE shall be suitable for testing.

Evaluator action elements

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

AVA_VAN.4.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.4.3E The evaluator *shall perform* an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.4.4E The evaluator *shall conduct* penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing Moderate attack potential.

6.3 Security Requirements Rationale

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.

6.3.1 Security Functional Requirements Rationale

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 32 presents the mapping between the security objectives and the security functional requirements.

Table 32. Summary of Mappings between Security Objectives and Security Functional Requirements

Security Functional Requirements \ Security Objectives	TOE Security Objectives														
	O.Management	O.Personalization_Agent_Authentication	O.Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.BAC	O.EAC	O.AA	O.IC_Chip
FCS_CKM.1												X	X		X
FCS_CKM.2(1)									X			X			X
FCS_CKM.2(2)													X		X
FCS_CKM.4								X							
FCS_COP.1(1)					X							X			X
FCS_COP.1(2)					X							X			X
FCS_COP.1(3)												X	X		X
FCS_COP.1(4)						X							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						X
FDP_UIT.1					X				X						X
FIA_AFL.1(1)			X	X						X		X	X		
FIA_AFL.1(2)		X		X											
FIA_UAU.1(1)				X						X		X			X
FIA_UAU.1(2)			X	X						X			X		X
FIA_UAU.1(3)	X	X		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					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	X													
FPR_UNO.1											X				X
FPT_FLS.1							X								X
FPT_ITI.1				X	X										X
FPT_TST.1							X								

FCS_CKM.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.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

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.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic and random number generation functions provided by the IC chip.

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 (DH key distribution protocol of PKCS#3).

The distribution method defined in this component satisfies the security objective of O.EAC and O.IC_Chip as it is enables to generate EAC session key of FCS_CKM.1 by generating KDF seed.

FCS_CKM.4 Cryptographic key destruction

This component satisfies the security objective of O.Deleting_Residual_Info as it provides the method of destroying the key generated by the TSF in accordance with the key derivation mechanism of FCS_CKM.1 and remained in temporary memory with the method.

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

This component defines TDES cryptographic operation 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 of O.Secure_Messaging as it ensures confidentiality of user data transmitted between the TOE and the Inspection System by using cryptographic algorithm.

The cryptographic operation defined in this component satisfies the security objective of O.BAC as it is necessary in implementing the BAC mutual authentication.

This component is implemented with the secure cryptographic operations provided by the IC Chip. Therefore, this component satisfies the security objective of O.IC_Chip.

FCS_COP.1(2) Cryptographic operation (MAC)

This component defines Retail MAC used to authenticate the Inspection System that supports the BAC or to detect modification of the transmitted user data.

The MAC operation defined in this component satisfies the security objective of O.Secure_Messaging as it ensures integrity by providing the method to detect modification of user data transmitted between the TOE and the Inspection System.

The MAC operation defined in this component satisfies the security objective of O.BAC as it is necessary in implementing the BAC mutual authentication.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

FCS_COP.1(3) Cryptographic operation (Hash Function)

This component defines SHA-1 hash function necessary in KDF implementation according to FCS_CKM.1.

The hash function defined in this component satisfies the security objective of O.BAC and O.EAC as it enables the KDF to generate the BAC and EAC session key.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

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

This component defines the method of digital signature verification necessary in the EAC-TA.

The digital signature verification method defined in this component satisfies the security objective of O.Certificate_Verification as it verifies the CVCS link certificate, DV certificate and IS certificate pro-

vided by the Inspection System to the TOE. Also, this component satisfies the security objective of O.EAC as it provides the digital signature verification method necessary in the EAC-TA in order to check the access-rights for the biometric data of the ePassport holder.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

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

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, BIS and EIS 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 (OS access control)

This component defines list of subjects, objects and operations in order to decide a scope of control for the OS 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 as subjects, the ePassport Operational Mode and Personalziation agent access rule reference as objects and their relationship as operations.

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

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 specifies the ePassport access control rules.

In this component, the write-rights for the ePassport user data is allowed only to the subjects holding the issuing authorization and the delete-rights for the objects is allowed only to the subjects holding the issuing authorization in Personalization phase. This component satisfies the security objectives of O.Personalization_Agent, O.Management, and O.Access_Control because the authorized Personalization agent is only allowed to manage ePassport user data as described above. Also, this component implements access control which denies access to all the objects when the command invoked by the subject is not allowed for the Operational Mode which the object is in. Therefore this component satisfies the security objective of O.Access_Control.

This component satisfies the security objectives of O.BAC, O.EAC and O.Access_Control because 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 (OS access control)

In order to enforce the ePassport access control policies, this component defines security attributes of subjects and objects defined in FDP_ACC.1(2) and specifies the OS access control rules.

This component satisfies the security objectives of O.Personalization_Agent_Authentication, O.Management, and O.Access_Control as only the authorized Personalization agent with the issuing authorization can perform management of ePassport user data. It is achieved by allowing write-rights for the OS user data only to the subjects who hold the issuing authorization. Also, this component implements access control which denies access to all the objects when the command invoked by the subject is not allowed for the Operational Mode which the object is in. Therefore this component satisfies the security objective of O.Access_Control.

FDP_DAU.1 Basic data authentication

This component provides BIS/EIS with a digital signature which is generated by signing the random number transmitted between the TOE and the Inspection System with uniquely assigned Active Authentication private key to ensure the genuineness of MRTD chips, thus proves that the MRTD chip is genuine. Therefore this component satisfies the security objective of O.AA.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

FDP_RIP.1 Subset residual information protection

This component ensures that previous information is not included when the TSF deallocates memory resources for the BAC authentication key, BAC session key, EAC session key and random numbers.

This component satisfies the security objective of O.Deleting_Residual_Info as it ensures that previous information of the 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 BAC mutual authentication, EAC-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. Also, if the Personalization agent decides to apply secure messaging, this component establishes the secure messaging by performing cryptographic operations for user data transmitted between the TOE and the Personalization agent with the Personalization agent session 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.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

FDP_UIT.1 Data exchange integrity

This component defines the method to protect from modification, deletion, insertion, and 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 calculating MAC 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. Also, if the Personalization agent decides to apply secure messaging, this component establishes the secure messaging by calculating MAC for user data transmitted between the TOE and the Personalization agent with the Personalization agent 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.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

FIA_AFL.1(1) Authentication failure handling (Inspection System Authentication Failure)

This component requires detection if the authentication attempt failure number is surpassed, this component detects it and requires handling the authentication failure.

This component satisfies the security objective of O.Session_Management as it terminates session if 1 unsuccessful BAC mutual authentication is attempted. If EAC-TA fails, EAC secure messaging from successful EAC-CA is maintained but the access to the biometric data of the ePassport holder is denied. Therefore this component satisfies O.Session_Management.

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 if the BAC mutual authentication fails.

In addition, this component satisfies the security objectives of O.BAC, O.EAC and O.Access_Control because access to user data is denied as BAC mutual authentication failure is considered that there is no the access-rights for user data.

FIA_AFL.1(2) Authentication failure handling (Personalization Agent Authentication Failure)

This component requires detection if the authentication attempt failure number is surpassed, this component detects it and requires handling the authentication failure.

If 1 unsuccessful Personalization agent authentication is attempt, this component detects the failure and terminates the session, thus satisfies the security objective of O.Session_Management.

If the number of unsuccessful Personalization agent authentication attempts reaches 10, this component detects it and disables Personalization agent authentication function permanently. Therefore, this component satisfies the security objective of O.Personalization_Agent_Authentication.

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_Management, 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.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

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 read user data except 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_Management, 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.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic and random number generation functions provided by the IC chip.

FIA_UAU.1(3) Timing of authentication (Personalization Agent Authentication)

This component defines the functions the user to be performed before the Personalization agent authentication and executes the Personalization agent authentication for the user.

Authentication method based on TDES is defined in this component satisfies the security objective of O.Personalization_Agent_Authentication as it authenticates a user as the Personalization agent and allows the Personalization agent issuing authorization. This component satisfies the security objectives of O.Session_Management, O.Access_Control and O.Management as it enables detection by FIA_AFL.1(1), if authentication fails and grants the issuing authorization and allows the write-rights if authentication succeeds.

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic and random number generation functions provided by the IC chip.

FIA_UAU.4 Single-use authentication mechanisms

This component requires that authentication-related information sent by the TSF to the Inspection System in the BAC mutual authentication and the EAC-TA and to the Personalization agent in the Personalization agent authentication is not replay.

This component satisfies the security objectives of O.Replay_Prevention, O.BAC, O.EAC and O.Personalization_Agent_Authentication as the TSF executes the BAC mutual authentication, EAC-TA and the Personalization authentication by generating different random numbers used in the BAC mutual authentication, EAC-TA and the Personalization agent authentication per session and transmitting them to the Inspection System or to the Personalization agent.

FIA_UAU.5 Multiple authentication mechanism

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.

The personalization agent issuing authorization is only allowed if the Personalization agent authentication succeeds. Therefore this component satisfies the security objectives of O.Personalization_Agent_Authentication and O.Access_Control.

This component satisfies the security objectives of O.Security_Mechanism_Application_Procedures, O.Access_Control, O.BAC and O.EAC as 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 establishing 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.Personalization_Agent_Authentication, O.BAC and O.EAC as the external entity is identified with the Inspection System or the 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 behavior

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 MRTD application data.

FMT_MOF.1(2) Management of security functions behavior (Suspension of BAC, EAC and Secure Messaging)

This component defines that the ability to disable BAC, EAC functions, and secure messaging in Personalization phase is given only to the Personalization agent in the Personalization phase.

This component satisfies O.Management and O.Access_Control as it provides management functions to support the Personalization agent's issuing policy and guidance for the secure use of TOE

In this component, functions defined in FDP_UIT.1, FDP_UCT.1, FPT_ITI.1 is performed if the personalization agent requests secure messaging in Personalization phase and those functions are disabled only if the personalization agent explicitly requests not to apply secure messaging. Therefore, this component satisfies the security objective of O.Secure_Messaging.

FMT_MSA.1 Management of security attributes

This component requires restricting 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 the Personalization agent to specify initial values in order 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 only the authorized Personalization agent generates user data in order to enforce the ePassport access control policies in the Personalization phase and specifies initial values to restrict security attributes of the data.

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, AA chip authentication private key, and personalization agent key 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, initial current data, initial CVCA certificate, initial CVCA digital signature verification key, AA chip authentication private key, and personalization agent key in secure memory in the Personalization phase

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

This component requires terminating 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 (Generating and Writing BAC authentication key)

This component restricts that TSF on behalf of the authorized Personalization agent generates and stores BAC authentication key. When changing life-cycle from Personalization to Operational Use, TSF generates BAC authentication key, provides methods to manage TSF data, and manages TSF data which are necessary for BAC mutual authentication which is to allow BIS for BAC authorization. Therefore this component satisfies the security objectives of O.Management and O.Access_Control.

FMT_MTD.3 Secure TSF data

This component requires allowing only secure values as the TSF data in order to ensure the security of 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 or the TSF performs AA security mechanism.

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 and the method to disable BAC or EAC function in the Personalization phase.

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 MRTP application and 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.

This component defines the roles of the Personalization agent and relates the roles to the user authenticated by FIA_UAU.1(3). Therefore, this component satisfies the security objective of O.Personalization_Agent_Authentication.

FPR_UNO.1 Unobersvability

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 and EAC chip authentication private key, etc. when the TSF performs a cryptographic operation.

This component satisfies the security objective of O.Handling_Info_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 when the TSF performs cryptographic operation of TDES, MAC and digital signature verification, etc.

This component satisfies the security objective of O.IC_Chip as it uses the secure physical protection provided by the IC chip.

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, abnormal operating conditions detected by the IC chip, and the failure detected from the randomness test which is tested on the random number generator provided 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.

This component satisfies the security objective of O.IC_Chip as it uses the secure physical protection provided by the IC chip.

FPT_ITI.1 Inter-TSF detection of modification

This component requires detecting 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 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

This component satisfies the security objective of O.IC_Chip as it uses the secure cryptographic operations provided by the IC chip.

FPT_TST.1 TSF testing

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

In this component, secure state of the TOE is preserved by the self-testing which verifies the randomness of the random number generated by the IC chip to ensure the security of the random number used for authentication mechanism in start-up process.

Also this component satisfies the security objective of O.Self_protection as it detects loss of the TSF and TSF data by verifying the integrity of them.

6.3.2 Security Assurance Requirements Rationale

The EAL (Evaluation Assurance Level) of this Security Target was selected as EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4) by considering the value of assets protected by the TOE and level of threats, etc. This section describes the reason why EAL4+ is selected and the rationale of the augmented with assurance components of the EAL4 assurance level.

Rationale of the EAL4 Assurance level

The security assurance requirements of EAL4 are the assurance package which requests methodical design, test and review. EAL4 is the highest level of assurance which commercial development phase requires and it provides good commercial development practices. Most of IC chips are developed and sold commercially. Considering the operational environment and the value of asset protected by the IC chip, higher level of assurance is required. Since, requirements of automated configuration management, though it is partial, and secure distribution is included, assurance higher than EAL3 is provided.

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 Security Target partially selected assurance components that are higher than EAL4. The rationale of the augmented assurance components are as follows.

- **ADV_IMP.2 Complete mapping of the implementation representation of the TSF**
- **ATE_DPT.2 Testing:security enforcing modules**
- **AVA_VAN.4 Methodical vulnerability analysis**

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 Protection Profile, 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_VAN.3 that resistant the enhanced-basic attack potential. Therefore, AVA_ VAN.4 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 and the TOE by threat agent possessing high attack potential and evaluation and verification for the IC chip may be assigned to the IC chip manufacturer.

It is difficult to correct 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 analyze completely in order to check if the TSF is accurately implemented and defect code does not exist, and ATE_DPT.2 is augmented to test for security enforcing module.

6.3.3 Rationale of Dependency

6.3.3.1 Dependency of TOE Security Functional Requirements

Table 33 shows dependency of TOE functional components.

Table 33. Dependency of TOE Functional Components

No.	Security Functional Component	Dependency	Ref. No.
1	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	2, 3 4
2	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
3	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
4	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	1
5	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4

6	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
7	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
8	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
9	FDP_ACC.1(1)	FDP_ACF.1	11, 12
10	FDP_ACC.1(2)	FDP_ACF.1	11, 12
11	FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	9, 10 28
12	FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	10 28
13	FDP_DAU.1	-	-
14	FDP_RIP.1	-	-
15	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	None 9, 10
16	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	9, 10 None
17	FIA_AFL.1(1)	FIA_UAU.1(1), FIA_UAU.1(2)	19, 20
18	FIA_AFL.1(2)	FIA_UAU.1(3)	21
19	FIA_UAU.1(1)	FIA_UID.1	24
20	FIA_UAU.1(2)	FIA_UAU.1(1)	19
21	FIA_UAU.1(3)	FIA_UID.1	24
22	FIA_UAU.4	-	-
23	FIA_UAU.5	-	-
24	FIA_UID.1	-	-
25	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	33 34
26	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	33 34
27	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	9, 10 33 34
28	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	27 34
29	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	33 34
30	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	33 34
31	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	33 34
32	FMT_MTD.3	FMT_MTD.1(1)	29
33	FMT_SMF.1	-	-
34	FMT_SMR.1	FIA_UID.1	24
35	FPT_FLS.1	-	-
36	FPT_ITI.1	-	-
37	FPT_TST.1	-	-

The security functional components such as FDP_UCT.1, FDP_UIT, and FIA_UAU.1(2) which do not satisfy the dependency claim the rationale of dependency in PP. That is, FDP_UCT.1 and FDP_UIT.1 have dependency with FTP_ITC.1 or FTP_TRP.1, but those are not included. 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.

FIA_UAU.1(2) shall have dependency with FIA_UID.1, but the dependency is changed to FIA_UAU.1(1) by refinement operation. 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.

6.3.3.2 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 is as shown in Table 34.

ADV_IMP.2 shall have dependency with ALC_CMC.5 but, 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. ADV_CMC.5 is not augmented in the Protection Profile, because Configuration Management at ALC_CMC.5 level which provides automated measure to identify if the changes in configuration items affect other configuration items is determined to be not necessarily required. This Security Target claims the Protection Profile as described above.

AVA_VLA.4 has dependency with ADV_IMP.1 and ATE_DPT.1. This is satisfied by ADV_IMP.2 and ATE_DPT.2 in hierarchical relationship with ADV_IMP.1 and ATE_DPT.1.

Table 34. Dependency of Augmented Assurance Component

No.	Assurance Component	Dependency	Ref. No.
1	ADV_IMP.2	ADV_TDS.3 ALC_TAT.1 ALC_CMC.5	EAL4 EAL4 None
2	ATE_DPT.2	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1	EAL4 EAL4 EAL4
3	AVA_VAN.4	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	EAL4 EAL4 EAL4 1 EAL4 EAL4 2

6.3.4 Rationale of Mutual Support and Internal Consistency

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

In ‘6.3.3.1 Dependency of TOE security functional requirements’ and ‘6.3.3.2 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 TSF generates and stores BAC authentication key (FMT_MTD.1(3)). The Personalization agent 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 Personalization agent can define security attributes of objects according to the Personalization agent's issuing policy and may not apply secure messaging in the Personalization phase when the Personalization agent implements and operates physical, human and procedural security measures equivalent level to secure messaging (FMT_MOF.1(2)). The role of the Personalization agent as described above 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)) and the OS access control policies (FDP_ACC.1(2), FDP_ACF.1(2)).

The TSF, after identifying the external entity (FIA_UID.1), executes the Personalization agent authentication or the BAC mutual authentication (FIA_UAU.1(1)) and the EAC-TA (FIA_UAU.1(2)) according to authentication mechanism application rules (FIA_UAU.5). If the Inspection System fails in authentication, the session is terminated or the access to the ePassport user data is denied (FIA_AFL.1(1), FDP_ACC.1(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 that the secure random numbers are used and the secure certificates are 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 IC chip must ensure that physical phenomena of current, voltage and electromagnetic waves, etc. occurred when performing cryptographic operations (FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4)) are not exploited by the threat agents (FPR_UNO.1). 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 (FPT_TST.1) under the conditions decided by the ST author. 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.

7 TOE Summary Specification

In this chapter the SSCOS security functionalities that satisfy the security function requirements are specified at the level of TOE subsystem overview, and the SSCOS assurance measures that satisfy the assurance requirements are defined.

7.1 TOE Security Functionality

In this section the security functionalities that is provided to satisfy the security function requirements defined in '6.1 TOE Security function requirements' are explained at the level of TOE subsystem behaviour overview.

TOE is composed of the following 3 layers.

- Hardware Dependent Layer
- Hardware Independent Layer
- ePassport Layer

Hardware Dependent Layer

Directly covers underlying IC chip function, supplying the kernel needed for IC chip OS and ePassport application program.

Hardware Independent Layer

Perform functions of general IC chip operating system, covering almost every logical function of TOE.

ePassport Layer

Composed of subsystems that supply ePassport Service

The following shows subsystem's role to supply ePassport related security characteristics.

- ePassport personalization agent certification

  Able to form secure channel based on ISO/IEC 14443-4 and receive Select command for MF. After receving MF Select command, select MF and perform ePassport personalization agent authentication mechanism. When authentication succeed, set as personalization agent right obtained. Send response code after setting available failure count number to the maximum if the possible personalization agent authentication trial count is not the maximum value.

- LDS application program Identification (AID: A0000002471001)

  When generating ePassport DF, setting File Descriptor to the value that indicates ePassport DF and DF name to the ePassport Application ID (A0000002471001) will generate ePassport DF in EEPROM.

  Application with ePassport ApplicationID as above is activated by the Select File command.

- ePassport Application Program operational mode management

  The change of the ePassport application program operational mode are only available when personalization right is acquired through personalization agent key(TK) authentication. The changes of the operational mode are as : Protected → Initialized → Operational(Active) → Personalized → Terminated

- Personalization of ePassport & OS user data and TSF data

  Personalization agent sends External authentication command by using personalization agent key(TK), and personalization agent right is set when authentication succeed

  Personalization agent changes TOE operational mode by using personalization agent right, and performs personalization of ePassport user data, ePassport TSF data, OS user data, OS TSF data by applying access control rules.

- BAC authentication & ePassport inspection

  Inspection system tries BAC authetnication if it fails inspecting becuase of not fullfilling secure condition during its inspecting EF.COM without Secure Messaging. Inspection system authenicates BIS by implementing BAC authentication mechanism described in ePassport specification, and set authorithy right to BAC right if authentication succeeds. Also generates BAC session key needed for generating BAC secure channel[6].

- Assymetric key based authentication to prevent replicated chip(Active Authentication: AA)

  If BAC authentication is performed successfully and AA security condition is set by ePassport personalization, randomly generate 1024/1280/2048 bit RSA assymetric key pair for AA and stores public key in LDS DG15 of TOE while storing AA private key securely in protected area, which can be used for the authentication that verifies the chip

- Key exchange & distribution by DH key exchange during EAC-CA

  If secure condition to perform access control for the sensitive data after BAC is set to EAC according to the ePassport TSP, private key information is stored in protected area of TOE during personalization, and public key information is encoded and stored to DG14 together with domain prameter information.

  Inspection System(EIS) gets Domain Parameter and DH public key of TOE for DH key exchange when reading DG14 of ePassport LDG DG group successfuly.

  Inspection system(EIS) randomly generates ephermeral DH key pair by using Domain Prameter, and sends the generated public key to TOE by using MSE Set KAT command.

  TOE generates EAC session key for EAC secure channel, and initializes SSC.

  Transmitting data is protected by the usage of session key and SSC when EAC-CA is successfully performed.

- EAC-TA (Terminal Authentication): Do External Auth & Verification of EAC certificate chain

  In order to obtain access right before reading sensitive data like fingerprint(DG3) or iris(DG4), Inspection System(EIS) get read-right authentication for the fingerprint data through EAC-TA. Also TOE procures spaces for the information of CVCA certificates, which is stored during personalization, and information about it that will be used for the verification of it.

- Protection of transmitting data after BAC or EAC-CA authentication

  After ePassport BAC mutual authentication & EAC-CA authentication, TOE performs Secure messaging by using BAC session key (or EAC session key) & SSC (counter) in order to protect the channel that transmits Command/Response APDU and its data.

The following shows subsystem's role to supply general security characteristics.

- Safe startup & usage of IC chip security characteristics

  When initializing the module neccesary to forming secure channel, set register values which is needed to use IC chip security characteristics such as UART in accordance with communication type like ISO 14443, and perform functions such as initializing transmittion rate, sending initial response, and etc.

  Verify whether randomness is procured in the processed value of the random number from IC chip per each startup, in order to maintain saftey for the random value used for the ePassport security mechanism.

- Guarantee of TSF safe operation

  Offers the way to verify the integrity of generated TSF & TSF data through "Check Data" command.

  In personalization phase, offeres the way to verify the integrity of TSF Data through the secure messaging that has the same security level of secure messaging in ePassport BAC or after EAC-TA.

  Maintains secure state by halting the execution of TSF if falure is detected during the random value verification which is performed at every startup.

  Maintains secure state by halting the execution of TSF if failure is detected during the TSF data integrity verficiation through Secure Messagging.

  Maintains secure state by halting the execution of TSF if IC chip detects abnormal operational environment.

  Prevents abusement of the cryptographic information which can be obtained from the physical pheonomenon that is generated when cryptographic calculation is performed.

Table 35. TOE SFR Satisfied by Security Characteristics

Type	Security Characteristic	SFR
ePassport related	ePassport personalization agent certification	FIA_AFL.1(2), FIA_UAU.1(3), FIA_UAU.4, FIA_UAU.5, FIA_UID.1,FMT_SMR.1
	LDS application program Identification	FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2), FDP_DAU.1
	ePassport Application Program operational mode management	FDP_ACC.1(2), FMT_MOF.1(1) , FMT_SMF.1
	Personalization of ePassport & OS user data and TSF data	FCS_CKM.1, FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1(1), FDP_ACF.1(2), FMT_MOF.1(2), FMT_MSA.3, FMT_MTD.1(1), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1
	BAC authentication & ePassport inspection	FCS_CKM.2(1), FCS_COP.1(1), FCS_COP.1(3), FDP_ACC.1(1), FDP_ACF.1(1), FIA_AFL.1(1), FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.4, FIA_UAU.5, FIA_UID.1
	Asymmetric key based authentication to prevent replicated chip	FDP_DAU.1
	Key exchange & distribution by DH key exchange during EAC-CA	FCS_CKM.2(2), FCS_COP.1(3), FIA_UAU.1(2), FMT_MTD.1(2), FMT_SMF.1
	EAC-TA	FCS_COP.1(4), FDP_ACC.1(1), FDP_ACF.1(1), FIA_AFL.1(1), FIA_UAU.1(2), FIA_UAU.4, FIA_UAU.5, FIA_UID.1, FMT_MTD.3, FMT_SMF.1, FMT_SMR.1
	Protection of transmitting data after BAC or EAC-CA authentication	FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FDP_RIP.1, FDP_UCT.1, FDP_UIT.1, FMT_SMF.1, FPT_ITI.1
General	Safe startup & usage of IC chip security characteristics	FMT_MTD.3, FPT_FLS.1, FPT_TST.1
	Guarantee of TSF safe operation	FMT_MTD.3, FPT_FLS.1, FPT.ITI.1, FPT_TST.1, FPR_UNO.1

7.2 Assurance Measures

This section defines assurance measures which is required in accordance with EAL 4+ TOE security assurance requirement. The augmented assurance requirements are ADV_IMP.2, ATE_DPT.2, AVA_VAN.4.

The assurance measures will be provided as specified in the following table.

Table 36. TOE Assurance Measures (Document Name)

Assurance Class	Assurance Component	Document Name (Assurance Measure)
Security Objectives Specifications Evaluation	ASE_INT.1	SSCOS10-ASE-001_Security Target
	ASE_CCL.1	SSCOS10-ASE-001_Security Target
	ASE_SPD.1	SSCOS10-ASE-001_Security Target
	ASE_OBJ.2	SSCOS10-ASE-001_Security Target
	ASE_ECD.1	SSCOS10-ASE-001_Security Target
	ASE_REQ.2	SSCOS10-ASE-001_Security Target
	ASE_TSS.1	SSCOS10-ASE-001_Security Target
Development	ADV_ARC.1	SSCOS10-ADV-001_Security Architecture
	ADV_FSP.4	SSCOS10-ADV-011_Functional Specification
	ADV_IMP.2	SSCOS10-ADV-021_Implementation Representation
	ADV_TDS.3	SSCOS10-ADV-031_TOE Design
Guidance Documents	AGD_OPE.1	SSCOS10-AGD-001_Operational User Guidance
	AGD_PRE.1	SSCOS10-AGD-002_Preparative User Guidance
Lifecycle Support	ALC_CMC.4	SSCOS10-ALC-001_Configuration Management
	ALC_CMS.4	SSCOS10-ALC-001_Configuration Management
	ALC_DEL.1	SSCOS10-ALC-011_Delivery
	ALC_DVS.1	SSCOS10-ALC-021_Development Security
	ALC_LCD.1	SSCOS10-ALC-031_Life-cycle Definition
	ALC_TAT.1	SSCOS10-ALC-041_Tools and Techniques
Tests	ATE_COV.2	SSCOS10-ATE-001_Test Plan
	ATE_DPT.2	SSCOS10-ATE-001_Test Plan
	ATE_FUN.1	SSCOS10-ATE-001_Test Plan
	ATE_IND.2	ePassport sample, Emulation board, Test Tool
Vulnerability Assessment	AVA_VAN.4	-

8 Compatibility between the Composite ST and the Platform ST

In this section, the platform TSF is separated in two groups: one is TSF being used by the composite ST and the other is TSF not being used by the composite ST. Then, the compatibility between the Composite ST and the Platform ST is examined. In other words, it will be shown that there is no conflict between the security environment, the security objectives, and the security requirements of the Composite Security Target and the Platform Security Target.

8.1 Security Assurance Requirement

The Platform certification was according to another CC version than the current composite certification is. Therefore, the security assurance requirements of the TOE should be compared with the security assurance requirements of the Platform.

TOE SAR		Platform SAR	
CC V3.1 R3 - EAL 4+ (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)	ASE	CC V2.3 - EAL 5+ (ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)	ASE
	ADV_ARC.1		ADV_INT.1
	ADV_FSP.4		ADV_FSP.3
	ADV_IMP.2		ADV_IMP.2
	ADV_TDS.3		ADV_LLD.1
			ADV_HLD.3
	-		ADV_RCR.2
	-		ADV_SPM.3
	AGD		AGD
	ALC_CMC.4		ACM_CAP.4
	ALC_CMS.4		ACM_SCP.3
	ALC_DEL.1		ACM_AUT.1
	ALC_DVS.1		ALC_DVS.2
	ALC_LCD.1		ALC_LCD.2
	ALC_TAT.1		ALC_TAT.2
	ATE_COV.2		ATE_COV.2
	ATE_DPT.2		ATE_DPT.2
	ATE_FUN.1		ATE_FUN.1
	ATE_IND.2		ATE_IND.2
	AVA_VAN.4		AVA_CCA.1
			AVA_MSU.3
			AVA_SOF.1
			AVA_VLA.4

The security assurance level of the TOE is EAL 4+ and it is the subset of EAL 5+ which is the security assurance level for the platform. The determination of equivalence of the security assurance components belonging to CC V3.1 and CC V2.3 is shown in below table. It is shown that the security assur-

ance components of the Platform which is certified according to CC V2.3 are equivalent to or include the security assurance components of SSCOS being certified according to CC V3.1.

TOE		Equivalence	Platform	
CC V3.1	ALC_DVS.1 Identification of security measures	= Leveled	ALC_DVS.2 Sufficiency of security measures	CC V2.3
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF (It is possible to provide whole source-code)	≒ Equivalent	ADV_IMP.2 Implementation of the TSF (Whole source-code provided)	
	ATE_DPT.2 Testing: security enforcing modules (SFR-Enforcing modules)	⊆ Inclusion	ATE_DPT.2 Testing: low-level design (Tests every module)	
	AGD_OPE.1 Operational user guidance	≒ Equivalent	AVA_MSU.3 Analysis and testing for insecure state	
	AVA_VAN.4 Methodical vulnerability analysis (Resistance to attacks performed by an attacker possessing moderate attack potential)	⊂ Inclusion	AVA_VLA.4 Highly resistant (Resistance to attacks performed by an attacker possessing high attack potential)	

8.2 Separation of the Platform-TSF

Platform-TSF and their use for the TOE are shown in below table. If the TOE uses the TSF, then it is marked as “Relevant TSF”. If the TOE does not use the TSF, then it is marked as “Irrelevant TSF”.

Platform TSF		Used by TOE
Major Categories	**Sub-Categories**	
SF1: Environmental security violation recording and reaction	Detectors	Relevant TSF
	Filters	Relevant TSF
SF2: Access control	Security registers access control	Relevant TSF
	Invalid address access	Relevant TSF
	Access rights for the code executed in EEPROM	Relevant TSF
SF3: Non-reversibility of TEST and NORMAL modes	Non-reversibility of TEST mode and NORMAL mode	Irrelevant TSF
	TEST mode communication protocol and data commands	Irrelevant TSF
	Functional tests	Relevant TSF
	Identification	Relevant TSF
SF4: Hardware countermeasures for unobservability	Static address/data scrambling for bus and memory	Relevant TSF
	Memory encryption	Relevant TSF
	Synthesizable processor core	Irrelevant TSF
	De-synchronization and signal-to-noise reduction mechanism	Relevant TSF
SF5: Cryptography	Triple Data Encryption Standard Engine	Relevant TSF
	Random Number Generator	Relevant TSF
	TORNADO RSA cryptographic library (optional)	Relevant TSF
	TORNADO ECC cryptographic library (optional)	Relevant TSF

SF1, SF2, SF3, and SF4 of the Platform-TSF are used by the TOE to ensure the secure operation of its TSF. SF5 of the Platform-TSF is used by the TOE to implement the Personalization agent authentication, management of ePassport Operational Mode, issuance of ePassport and OS user and TSF data, BAC authentication, inspection of the ePassport, authentication based on asymmetric key to protect chip reproduction, key exchange and distribution according to DH Key exchange for EAC-CA, verification of EAC certificate chain and External authentication for EAC-TA, and protection of transmitted data after BAC and EAC.

8.3 Platform SFR

Platform-SFR	Composite SFR	Compatibility
FRU_FLT.2		The Platform SFR is not used by the TOE.
FPT_FLS.1	FPT_FLS.1	The Platform provides methods to detect abnormal operations
FPT_SEP.1		
FMT_LIM.1		The Platform SFR is not used by the TOE.
FMT_LIM.2		
FAU_SAS.1		
FPT_PHP.3		
FDP_ITT.1	FPR_UNO.1	The Platform provides the basic transmission protection inside the IC chip and it makes external entities difficult to discover cryptographic related information.
FPT_ITT.1		
FDP_IFC.1	FPR_UNO.1	The Platform provides the memory encryption thus protect cryptographic related information stored in the memory.
FCS_RND.1	FCS.CKM.1 FCS_CKM.2(1) FIA_UAU.1(1) FIA_UAU.1(3) FIA_UAU.4 FMT_MTD.3	The Platform provides random numbers to perform crypto-graphic operation.
FDP_ACC.1		Platform SFR is not used by the TOE.
FDP_ACF.1		
FMT_MSA.3		
FMT_MSA.1		
FMT_SMF.1	FCS_COP.1(1) FCS_COP.1(2) FDP_UCT.1 FDP_UIT.1 FIA_UAU.1(1) FIA_UAU.1(3) FMT_MOF.1(2) FPT_FLS.1 FPT_ITI.1	The TOE implements cryptographic operation and counter-measure against side channel attack by accessing the Special Function Register of the Platform.
FCS_COP.1/3DES	FCS_COP.1(1) FCS_COP.1(2)	The Platform provides the necessary algorithms.
FCS_COP.1/RSA	FCS_COP.1(4)	The Platform provides the necessary algorithms.
FCS_COP.1/ECDSA		The Platform SFRs are not used by to the TOE.
FCS_CKM.1/ECDSA		
FCS_COP.1/ECDH		
FCS_COP.1/SHA	FCS_COP.1(3)	The Platform provides the necessary algorithms.

8.4 Security Objectives of the Platform

It is verified whether the Platform-SFR which traces back to the security objectives of the Platform is relevant to the composite SFR. If there is no relevant composite SFR, then the security objective of the Platform is excluded from the scope of analysis. The compatibility between the security objectives of the Platform traced by the Platform-SFR which is used by the composite SFR and the composed security objectives is analyzed below.

Security Objectives of the Platform	Composite Security Objectives	Compatibility
O.Leak-Inherent	O.Handling_Info_Leakage	The security objective of the Platform is equivalent to the security objective of the TOE and thus compatible.
O.Phys-Probing		This security objective is traced by the Platform SFR, FPT_PHP.3, and there is no composite SFR relevant to FPT_PHP.3. Therefore, O.Phys-Probing is excluded from the scope of analysis.
O.Malfunction	O.Secure_State	This security objective is used to achieve the security objective of the TOE.
O.Phys-Manipulation		This security objective is traced by the Platform SFR, FPT_PHP.3, and there is no composite SFR relevant to FPT_PHP.3. Therefore, O. Phys-Manipulation is excluded from the scope of analysis.
O.Leak-Forced	O.Secure_State	This security objective is used to achieve the security objective of the TOE.
O.Abuse-Func		The security objective of the Platform is not relevant to any of the security objective of the TOE.
O.Identification		This security objective is traced by the Platform SFR, FMT_LIM.1 and FMT_LIM.2 and there is no composite SFR relevant to FMT_LIM.1 and FMT_LIM.2. Therefore, O. Identification is excluded from the scope of analysis.
O.RND	O.Personalization_Agent_Authentication O.Secure_Messaging O.Replay_Prevention O.BAC O.EAC	This security objective is used to achieve the security objective of the TOE.
O.Add-Functions	O.Management O.Personalization_Agent_Authentication O.Secure_Messaging O.Certificate_Verification O.Access_Control O.Handling_Info_Leakage O.BAC O.EAC O.AA	This security objective is used to achieve the security objective of the TOE.
O.Mem-Access		The security objective of the Platform is not relevant to any of the security objective of the TOE.

8.5 Assumptions of the Platform

Assumptions of the Platform	Composite Security Objectives	Compatibility
A.Process-Card	O.Management O.Personalization_Agent_Authentication O.Access_Control OE.Personalization_Agent	It is assumed in the Platform-ST that confidentiality and integrity of the TOE and its manufacturing and testing data is maintained after manufacturing the Platform up to delivery to the end-user. It is covered by the composite security objectives: O.Management, O.Personalization_Agent_Authentication, O.Access_Control, and OE.Personalization_Agent.
A.Plat-Appl	P.IC_Chip	It is assumed in the Platform-ST that the requirements specified in documents of the Platform are met. It is covered by the composite security evaluation.
A.Resp-Appl	O.Security_Mechanism_Application_Protocol O.Secure_State O.Access_Control O.BAC O.EAC	It is assumed in the Platform-ST that all user data are owned by the Smartcard Embedded Software. It is covered by the composite security objectives: O.Security_Mechanism_Application_Protocol, O.Secure_State, O.Access_Control, O.BAC, and O.EAC.
A.Key-Function	O.Handling_Info_Leakage	It is assumed in the Platform-ST that functions which use key does not reveal related information. It is covered by O.Handling_Info_Leakage of the composite security objective.

8.6 Organizational Security Policies for the Platform

Organizational Security Policies of the Platform	Composite Organizational Security Policies and Threats	Compatibility
P.Process-TOE		The organizational security policy of the Platform is mapped to OE.Process-TOE and O.Identification of the security objectives of the Platform and there are no security objectives of the TOE relevant to OE.Process-TOE and O.Identification. Therefore, P.Process-TOE is excluded from the scope of analysis.
P.Add-Functions	P.Personalization_Agent P.ePassport_Personalization_Policy P.ePassport_Access_Control T.TSF_Data_Modification T.IS_Certificate_Forgery T.Damage_to_Biometric_Data T.Eavesdropping, T.Forgery_Corruption_Personal_Data, T.Skimming, T. Leakage_CryptographicKey_Info	The organizational security policy of the Platform is to provide smartcard embedded software with 3DES, RSA, ECC, and SHA. It is relevant and not contradictory to P.Personalization_Agent, P.ePassport_Personalization_Policy, and P.ePassport_Access_Control. It is relevant and not contradictory to threats of the TOE, T.TSF_Data_Modification, T.IS_Certificate_Forgery, T.Damage_to_Biometric_Data, T.Eavesdropping, T.Forgery_Corruption_Personal_Data, T.Skimming, and T. Leakage_CryptographicKey_Info.

8.7 Threats of the Platform

Threats of the Platform	Composite Threats	Compatibility
T.Leak-Inherent	T.Leakage_CryptographicKey_Info	The threat of the Platform is compatible with the threat of the TOE.
T.Phys-Probing	T.BAC_Authentication_Key_Disclose T.ePassport_Reproduction T.Residual_Info T.IC_Chip_Forgery	The threat of the Platform is compatible with the threats of the TOE.
T.Malfunction	T.Malfunction	The threat of the Platform is compatible with the threat of the TOE.
T.Phys-Manipulation	T.TSF_Data_Modification T. Forgery_Corruption_Personal_Data T. Damage_to_Biometric_Data T.Malfunction	The threat of the Platform is compatible with the threats of the TOE.
T.Leak-Forced	T. Leakage_CryptographicKey_Info T. Malfunction	The threat of the Platform is compatible with the threats of the TOE.
T.Abuse-Func	T.TSF_Data_Modification T. BAC_Authentication_Key_Disclose	The threat of the Platform is compatible with the threats of the TOE.
T.RND	T.BAC_ReplayAttack T.SessionData_Reuse	The threat of the Platform is compatible with the threats of the TOE.
T.Mem-Access		The threat of the Platform T.Mem-Access is mapped to the O.Mem-Access of the Platform and there is no security objective of the TOE relevant to O.Mem-Access of the Platform. Therefore, T.Mem-Access is excluded from the scope of analysis.

9 Reference Documentations

[1] ePassport Protection Profile V2.1, National Intelligence Service, KECS-PP-0163a-2009, 2010-06-10

[2] Common Criteria for Information Technology Security Evaluation, Notification No. 2009-52 of MOPAS

[3] Common Criteria for Information Technology Security Evaluation – Evaluation Methodology, Notification No. 2009-51 of MOPAS

[4] ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts

[5] ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards

[6] ICAO Doc 9303 *Machine Readable Travel Documents* Part 1 *Machine Readable Passports*, 6th edition, 2006

[7] MRTD Technical Report, PKI for MRTD Offering ICC Read-Only Access, Ver. 1.1, 2004-10-1

[8] ISO/IEC JTC1/SC17 Supplement to Doc 9303, Release 7, ICAO, 2008-11-19

[9] BSI Technical Guideline TR-03110, Advanced Security Mechanisms for MRTD – Extended Access Control, Ver. 1.11, 2008. 02. 21

[10] S3CC9LC/LA/L5 16-bit Microcontroller for SmartCard User's Manual, 2008.12

[11] Application Note RSA Crypto Library with TORNADO V3.8S, 2011-08-03

[12] Composite product evaluation for Smart Cards and similar devices, Ver. 1.0 Revision 1, CCDB-2007-09-001, 2007.09

[13] SSCOS V1.0 on S3CC9LC Security Architecture, SSCOS10-ADV-001

[14] SSCOS V1.0 on S3CC9LC Functional Specification, SSCOS10-ADV-011

[15] SSCOS V1.0 on S3CC9LC Implementation Representation, SSCOS10-ADV-021

[16] SSCOS V1.0 on S3CC9LC TOE Design, SSCOS10-ADV-031

[17] SSCOS V1.0 on S3CC9LC Terms and Abbreviations, SSCOS10-PMS-002

10 Terms and Abbreviations

10.1 Terms

The terms that are used in this PP and defined in the CC as well are to have the same meaning as in the CC.

Active Authentication (AA)
The security mechanism with which the MRTD chip demonstrates its genuiness 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

Active Authentication Private Key
The private key based on the asymmetric key which the TOE uses to sign random number during AA Authentication

Active Authentication Public Key
The public key based on the asymmetric key which IS uses to verify the signed values of the TOE during AA authentication

APDU (Application Protocol Data Unit)
APDU is a message unit of a transmission protocol specified in ISO/IEC 7816-4 to transmit commands between application or OS loaded on the IC Chip and the external program

Assets
Information and resources that the owner of the TOE presumably places value upon and protected by the TOE security measures

Assignment
One of the operations of CC, the specification of an identified parameter in a component or requirement

Attack potential
Measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation

Augmentation
Addition of one or more security assurance components to an evaluation assurance level or assurance package

Authentication Data
Information used to verify the claimed identity of a user

BAC Authentication Key (Document Basic Access Keys)
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 encrypting the transmitted data with the BAC session encryption key and transmitting the data with message authentication value generated with the BAC session MAC key

BAC Session Keys
The BAC session encryption key and the BAC session MAC key generated by using the KDM from random numbers shared in the BAC mutual authentication for generating session keys.

Basic Access Control (BAC)
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

Biometric Data of the ePassport Holder (Sensitive Data)
Fingerprint and/ or iris data of ePassport holder stored in the MRTD chip in the LDS structure

BIS: BAC Inspection System
The IS implemented with the BAC and the PA security mechanisms and the AA as an option

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

Chip Authentication
The mechanism which the ePassport cetified implicitly to the Inspection System by DH key agreement mechanism and generates the secure messaging in EAC according to the BSI

Ciphertext Only Attack
Attack by the threat agent to attempt decryption based on the collected cipher text

Class
Set of CC families that share a common focus

Component
Smallest selectable set of elements on which requirements may be based

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 signing the digital signature verification key with digital signature generation key of the PA-PKI root CA

CVCA Certificate
The certificate that includes digital signature value of the digital signature verification key generated by the EAC-PKI root CA with digital signature generation key of the EAC-PKI root CA in order to demonstrate validity of the CVCA link certificate and the DV certificate

CVCA Link Certificate
The certificate that includes digital signature value which is signed with the digital signature generation key that corresponds to the previous CVCA certificate when generating a new CVCA certificate before expiring the valid date of the CVCA certificate by the EAC-PKI root CA

Dependency

Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be include in the PP, ST or package

DG (Data Group)

The data unit stored inside of ePassport accoding to the LDS of ePassport

DS (Document Signer) Certificate

The certificate of the personalization agent signed with the digital signature generation key of the PA-PKI root CA in order to verify the SOD by the IS according to the PA security mechanism

DV: Document Verifier

The CA (Certification Authority) that generates and issues the IS certificate

DV Certificate

The certificate that includes digital signature value signed 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 (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-CA (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 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 and recorded by the personalization agent in the Personalization phase

EAC-PKI: CVCA (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

EAC Session Keys

The session key used to establish secure messaging to protect transmission of the biometric data of the ePassport holder and that consists of the EAC session encryption key and the EAC session MAC key generated according to KDF by using keys shared with the EIS through the Ephemeral-Static DH key distribution protocol in the EAC-CA as a seed

EAC-TA (EAC-Terminal Authentication)

The security mechanism that the MRTD chip verifies the digital signature received from the EIS and signed with the EIS temporary public digital signature generation key used in the EAC-CA by using IS certificate. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS

e-Cover

The e-Cover refers to the sheet including IC chip and antenna inlay in the ePassport.

EEPROM (Electrically Erasable Programmable Read-Only Memory)

EEPROM is a non-volatile memory which can save data without power. This was modified from Erasable Programmable Read-Only Memory (EPROM) and written data can be electrically removed and re-writable. Therefore it is easily reprogrammable. Data is written and removed by changing the electrical charge of the element. EEPROM can be reprogrammed in circuit, because data can be read or written electrically.

EF.COM

Including the LDS version information and 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

EIS: EAC Inspection System

The IS implemented with the BAC, the PA and the EAC security mechanisms and the AA as an option

Element

Indivisible statement of a security need

Encryption Key

Key used in the symmetric cryptographic algorithm for data encryption(TDES) 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 Application Data

Including user data and TSF data of the MRTD

ePassport Authentication Data

The data stored in the MRTD chip with the LDS format to support ePassport security mechanisms that includes the SOD for PA, the EAC chip authentication public key and the active authentication public key, etc

ePassport Identity Data

Including personal data of the ePassport holder and biometric data of the ePassport holder

ePassport Operational Mode

Operational Mode of the ePassport DF, ePassrpot DF will be in one of Protected, Initialize, Operational(Active), Operational(Deactivated) and Termination

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 check the issuance 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

ePassport TSF Data
The data stored in the secure memory of the MRTD chip to support ePassport security mechanisms

ePassport User Data
Including the ePassport identity data and the ePassport authentication data

Evaluation Assurance Level (EAL)
Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

External IT Entity
Any IT product or a system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family
Set of components that share a similar goal but differ in emphasis or rigor

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

IC Chip (Integrated Circuit Chip)
The important semiconductor to process smart card functionality, and it is the processing unit which includes four functional units(mask ROM, EEPROM, RAM, and I/O port)

ICAO-PKD
The DS certificate storage operated and managed by the ICAO that distributes online in case the domestic/ overseas IS requests the DS certificate of the corresponding country

Identity
Representation uniquely identifying entities within the context of the TOE

Initial Personalization Key
Initially shared personalization key between the personalization agent and the manufacturer which performs the TOE intialization delegated by the personalization agent

Inspection
Procedure in which immigration office checks identity of the ePassport holder by inspecting the MRTD chip presented by the ePassport holder, thus verifies genuineness of the MRTD chip

IS: Inspection System
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

Iteration
Use of the same component to express two or more distinct requirements

KDM: Key Derivation Mechanism

The mechanism to generate the encryption key and the MAC key by using hash algorithm from the Seed

KDF: Key Derivation Function

The function 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 that describes how ePassport user data is to be written in the IC chip

MAC Key (Key for Message Authentic Code)

Key that is used in the symmetric key algorithm as specified by ISO 9797 to generate Message Authentic Code for preventing forgery and corruption of data

MRTD (Machine Readable Travel Document)

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 according to the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc.

MRTD Application Security Attributes

Attributes stored in MRTD Application: ePassport Operational Mode and MRTD access control reference

MRTD Chip

The contactless IC chip that includes the MRTD application and the IC chip operating system necessary in operation of the MRTD application and that supports communications protocol according to ISO/IEC 14443

MRZ (Machine Readable Zone)

A fixed standard area located on the data page of MRTD, it includs the formatted necessary data and optional data for machine-read with OCR

Object

Passive entity in the TOE, that contains or receives information, and upon which subjects perform operation

Operation

Modification or repetition of a component in order to counteract against the specific threat or satisfy the specific security policy (ex: assignment, iteration, refinement and selection)

Organizational Security Policies

Set of security rules, procedures, or guidelines for an organization

PA (Passive Authentication)

The security mechanism to demonstrate that identity data recorded in the ePassport has not been forged and corrupted 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.

PA-PKI: (CSCA: 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

Personal Data of the ePassport Holder

Visually identifiable data printed on identity information page of the 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 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.

Personalization Agent Access Rule Reference

A file that defines keys to be authenticated which is for access control to the file

Personalization Authentication Key

The symmetric key which the personalization agent uses to obtain issuing authorization by external authentication. It refers to the initial personalization agent key and the keys stored in the symmteric key file and used for the personalization

Personalization Key

The symmetric key which the personalization agent uses to obtain issuing authorization and to wirte TSF data securely. It refers to the personalization authentication key and the personalization secure messaging key

Personalization Secure Messaging Key

The symmteric key which the personalization agent uses to write TSF data securely with secure messaging

PP, Protection Profile

Implementation-independent statement of security needs for a TOE type

Probing

Attack to search data by inserting probing pin in the IC chip

RAM (Random Access Memory)

Ram is a memory to store OS and application data being used in order to enable the processor to access those data fast. RAM can read and write data faster than any other computer storage device, such as hard disk, floppy disk and CD-ROM. But, data in RAM are only maintained while a computer is operating and data will be removed when power is off. OS and other files stored in hard disk will be loaded in RAM when power is on again

Refinement

One of the operations of CC, addition of details to a component

Reverse Engineering

To identify and reproduce the basic design concept and applied technologies of the product through detailed analysis of the completed product

Role

Predefined set of rules establishing the allowed interactions between a user and the TOE (ex: Operator, Manager)

ROM (Read-Only Memory)

ROM is a class of storage. Comparing with RAM which can read and write data, data stored in ROM can be read but cannot be modified. Data is maintained without power, so it is usually used for embedding basic OS functions or interpreter

Selection
One of the operations of CC, specification of one or more items from a list in a component

SOD: 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

SOF (Strength-of-Function)
A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms

SOF high
A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential

ST, Security Target
Implementation-dependent statement of security needs for a specific identified TOE with security requirements and security functionality

Subject
Active entity in the TOE that performs operations on objects

Terminal Authentication
The mechanism which the ePassport authenticates the Inspection System expliciitly through digital signature verification based on a public-key cyrptosystem and thus generates the Secure Messaging for EAC according to the BSI

Threat Agent
Untrsuted user or external IT entity that can adversely act on assets

TOE (Target of Evaluation)
Set of software, hardware and/or hardware possibly accompanied by guidance

TOE Security Functionality (TSF)
Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data
Data for the operation of the TOE upon which the enforcement of the SFR relies

User
Human or IT entity possibly interacting with the TOE from outside of the TOE boundary

10.2 Abbreviations

AA	Active Authentication
ABEND	Abnormal End
ATR	Answer To Reset
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CLK	Clock (input to smartcard)
COS	Card Operating System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem (algorithm)
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
ECB	Electronic Code Book
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIS	Extended Inspection System
HW	Hardware
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IFD	Interface Device
IO	Input/Output
IS	Inspection System
ISO	International Organization for Standardization
IT	Information Technology
KDF	Key Derivation Function
KDM	Key Derivation Mechanism
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone

OTP	One-Time Programmable (memory)
PA	Passive Authentication
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
PIS	Passive Inspection System
PKI	Public Key Infrastructure
PP	Protection Profile
PPS	Protocol and Parameters Selection (ref ISO7816)
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman (algorithm)
RST	Reset (input to smartcard)
SFI	Short File ID
SFP	Security Function Policy
SFR	Security Function Requirement
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
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Subsystem, TSF Subsystem

U-creator
U dream, we create.

END OF DOCUMENT

TEL: +82-2-3429-2114
E-mail: sdspr@samsung.com
http://www.sds.samsung.co.kr

삼성SDS SAMSUNG