KOMSCO

Security Target Lite

KCOS e-Passport Version 1.1

Version: 1.0

Date: 2010. 04. 06

Filename: EPS-02-AN-ST (Lite-EN)

KOMSCO

Technology Research Institute

IT Research Dept.

This page left blank on purpose for double-side printing

[Table of Contents]

[List of Tables]

[List of Figures]

1. Introduction

This document is the Security Target (ST) to describe KCOS e-Passport Version 1.1 S3CC9LC/GC/GW developed by the Korea Minting & Security Printing Corporation (KOMSCO).

This chapter identifies the ST and TOE and supports the ST overview, Common Criteria conformance and other areas.

1.1 Security Target Identification

- Title : EPS-01-AN-ST
- ST Version Number : V1.4
- Author : IT Research Department, Technology Research Institute, KOMSCO
- Applicant : Korea Minting & Security Printing Corporation
- Evaluation Criteria : Common Criteria for Information Security Evaluation (Ministry of Public Administration and Security Public Notice No. 2008-26)
- Common Criteria Version : V2.3
- Compliant to : ePassport Protection Profile V1.0 (KECS-PP-0084-2008)
- Assurance Level : EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.4)
- Keywords : ePassport, COS, MRTD, ICAO

1.2 TOE Identification

- TOE Name : KCOS e-Passport Version 1.1 S3CC9LC/GC/GW
- TOE Version : v1.1
- TOE Identification : S3CC9LC(K1.1.01.00.SS.150C), S3CC9GC(K1.1.01.00.SS.100C), S3CC9G W (K1.1.01.00.SS.1020)
- MRTD Chip : S3CC9LC/GC/GW, Samsung electronics

1.3 Security Target Overview

This security target defines the security objectives and requirements for "KOMSCO KCOS e-Passport Version 1.1 S3CC9LC/GC/GW".

TOE is the native chip operation system (COS), MRTD application and MRTD application data implemented on the S3CC9LC, which is a contactless IC Chip of Samsung Electronics and is certified according to CC EAL 5+(BSI-DSZ-CC-0501-2008), S3CC9GC which is a contactless IC chip of Samsung Electronics and is certified according to CC EAL 4+(BSI-DSZ-CC-0438-2007), S3CC9GW, which is a contactless IC chip of Samsung Electronics and is certified according to CC EAL 4+(BSI-DSZ-CC-0400-2007)

The MRTD application of the TOE follows ePassport Spec. (ICAO "Machine Readable Travel Documents, Doc 9303 Part1 Volume 2[1]) and EAC Spec. (BSI, Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.1 (2007.08)).

Therefore, the TOE carries out the security mechanisms of the ePassport such as AA (Active Authentication), BAC (Basic Access Control) and EAC (Extended Access Control). Additionally, the TOE also carries out the PAC (Personalization Access Control), which is a security mechanism for the secure personalization and management on the personalization phase at the personalization agent. Also, PAC is the security mechanism of KCOS; it authenticates the personalization agent and performs the function that grants the permission to personalize to the Personalization agent by supporting the multi-authentication mechanism according to departmentalizing the security roles of the personalization agent.

This ST includes the TOE description and the TOE Security Environment, Security Objectives and IT Security Requirement, which are described in ePassport Protection Profile V1.0. This ST also describes the security functions and assurance measures.

The TOE includes hash functions using random numbers. TDES, Retail MAC, RSA and ECC are supported by the MRTD chip. Therefore, the random number, TDES, Retail MAC, RSA and ECC are included in the TOE Security Environment.

This ST describes

• An overview of the TOE and the physical and logical scope of the TOE

• TOE Security Environment (assumptions, threats and organizational security policies)

• The security objective for the TOE and its IT environment

• IT security requirements (security requirements for TOE and IT environment) and assurance

requirements

• TOE summary specification (security functions, assurance measures)

• PP claims

• Rationales

1.4 CC Conformance

This ST claims conformance to:

• ePassport Protection Profile V1.0 (KECS-PP-0084-2008)

This ST claims conformance to:

• Common Criteria for Information Technology Security Evaluation, part 1: Introduction and general model, Version 2.3, Aug. 2005, CCMB-2005-08-001

• Common Criteria for Information Technology Security Evaluation, part 2: Security functional requirements, Version 2.3, Aug. 2005, CCMB-2005-08-002

• Common Criteria for Information Technology Security Evaluation, part 3: Security assurance requirements, Version 2.3, Aug. 2005, CCMB-2005-08-003

as follows:

• Part 2 Conformant

• Part 3 Conformant

• Package Conformant to EAL4 augmented with ADV_IMP2, ATE_DPT2 andAVA_VLA.4

1.5 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

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

Selection

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

Refinement

This is used to add detail to a requirement. It therefore restricts a requirement further. The result of a refinement is shown in **bold text**.

Assignment

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

Application Notes

"Application Notes" are provided to help to clarify the intent of the TOE description, TOE security environment, security objectives, IT security requirements and TOE summary specifications.

1.6 Security Target Organization

Chapter 1 provides the introductory material for the Security Target.

Chapter 2 defines the TOE and describes the TOE environment.

Chapter 3 describes the assumptions, threats and organizational security policies for the TOE and TOE environment.

Chapter 4 describes the security objectives of the TOE and environment by supporting the assumptions and organizational security policies to counter the threats.

Chapter 5 describes the security function requirements and assurance measures for the security objectives.

Chapter 6 provides the TOE security functions. The TOE security functions contain IT security

functions and describe how to meet the requirement of the TOE security function. The assurance measure describes the assurance declared for meeting the specified assurance requirements.

Chapter 7 describes the PP claims.

Chapter 8 describes rationale.

This page left blank on purpose for double-side printing

2. TOE Description

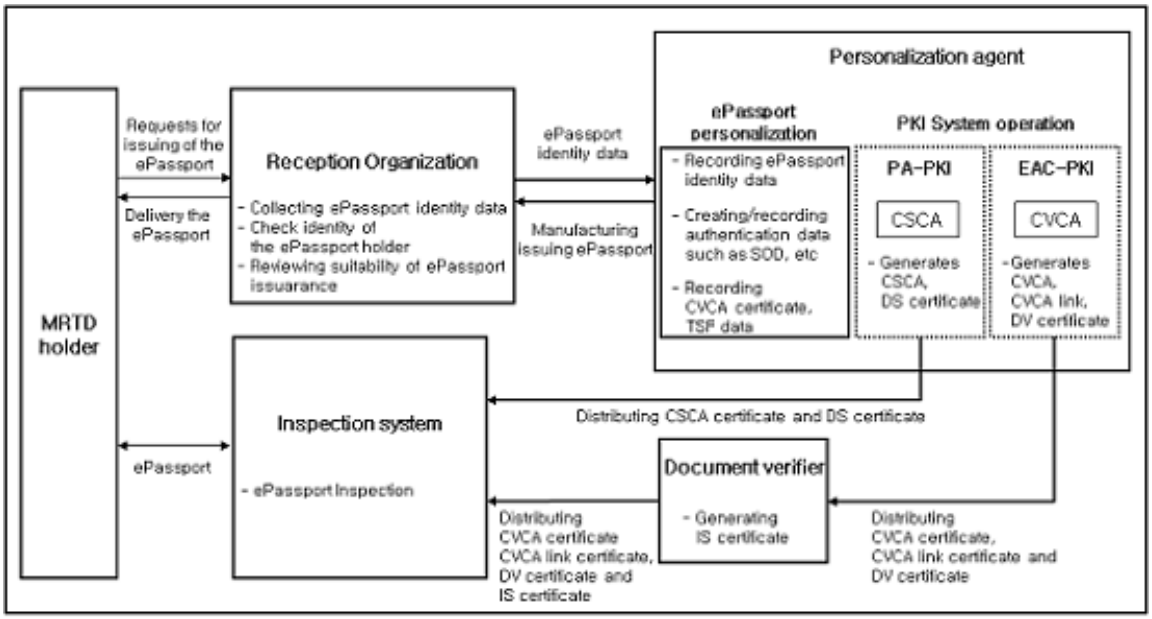
2.1 TOE Overview

ePassport

The ePassport is a passport embedding a contactless IC Chip in which the identity and other data of the ePassport holder are 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 a 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 the electronic storage, processing and handling of the ePassport identity data.

ePassport System

The [Figure 1] shows the overall configuration of the ePassport system.



[Figure 1] Overall Configuration of the ePassport System

The ePassport holder requests an issue 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 can be inspected at immigration control. For immigration control, the ePassport is verified by an immigration officer or by 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 the identity of the ePassport holder through cooperation with the related organizations, such as National Police Agency, and sends to the personalization agent for the issuing of the ePassport with these data collected.

The Personalization agent generates a Document Security Object (''SOD'' hereinafter) using a 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 MRTD chip to the passport. Details of data recorded in the ePassport are described in (Table 4) of 2.2.3 Logical Scope in the TOE.

The Personalization agent generates a digital signature key to check against 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 the CSCA Certificate and DS Certificate. According to the Issuing Policy of the ePassport, the Personalization agent generates a digital signature key to verify access-rights to the biometric data of the ePassport holder to support the EAC security mechanism. The Personalization agent then generates, issues, and manages the CVCA Certificate, CVCA Link Certificate and the DV Certificate. Details related to of the ePassport PKI System and certification procedure, including the certification server, key generation devices and the physical and procedural security measures depend on the Issuing Policy of the ePassport.

The Document verifier generates an IS Certificate using the CVCA and DV Certificates and then provides these certificates to the Inspection System.

The types of certificates used in the ePassport system are shown in (Table 1) below.

(Table 1) Type of Certificates

Usage	ePassport PKI System	Subject	Certificate
To verify forgery and corruption of the user data	PA-PKI	CSCA	CSCA Certificate
		Personalization agent	DS Certificate
To verify the access-right of the biometric data of the ePassport holder	EAC-PKI	CVCA	CVCA Certificate
To verify the access-right of the biometric data of the ePassport holder	EAC-PKI	CVCA	CVCA Link Certificate
To verify the access-right	EAC-PKI	Document verifier	DV Certificate

Usage	ePassport PKI System	Subject	Certificate
of the biometric data of the ePassport holder			
To verify the access-right of the biometric data of the ePassport holder	EAC-PKI	EAC supporting Inspection System	IS Certificate

Application Notes: The Personalization agent generates and issues certificates for the PA and EAC and distributes the certificates online and/or offline according to the Issuing policy of the ePassport. If the Issuing State of the ePassport has joined the ICAO-PKD, it is possible to register a DS Certificate and distribute it online. Moreover, the Document verifier generates the IS Certificate and distributes it to the Inspection System according to the Issuing policy of the ePassport.

2.2 TOE Product Type

The TOE is the native chip operation system (COS), MRTD application and MRTD application data implemented on S3CC9LC, which is a contactless IC chip product of Samsung Electronics and is certified according to CC EAL 5+(GC/GW CC EAL 4+).

The ePassport manufacturer makes an ePassport book by embedding a MRTD chip and RF antenna into a passport book. The Personalization agent personalizes the MRZ information and biometric data of the face and the finger print of the ePassport holder into the MRTD chip along with the TSF data for authentication and secure messaging between the MRTD chip and the inspection system. The inspection system verifies the ePassport presented by the ePassport holder.

2.3 TOE Life Cycle and Environment

This section defines the life cycle of the TOE, including the development, manufacturing, personalization and operational use of the ePassport. It also defines the TOE environment and physical/ logical scope of the TOE.

2.3.1 Life Cycle and Environment of TOE

The Life Cycle of the MRTD Chip and the TOE

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

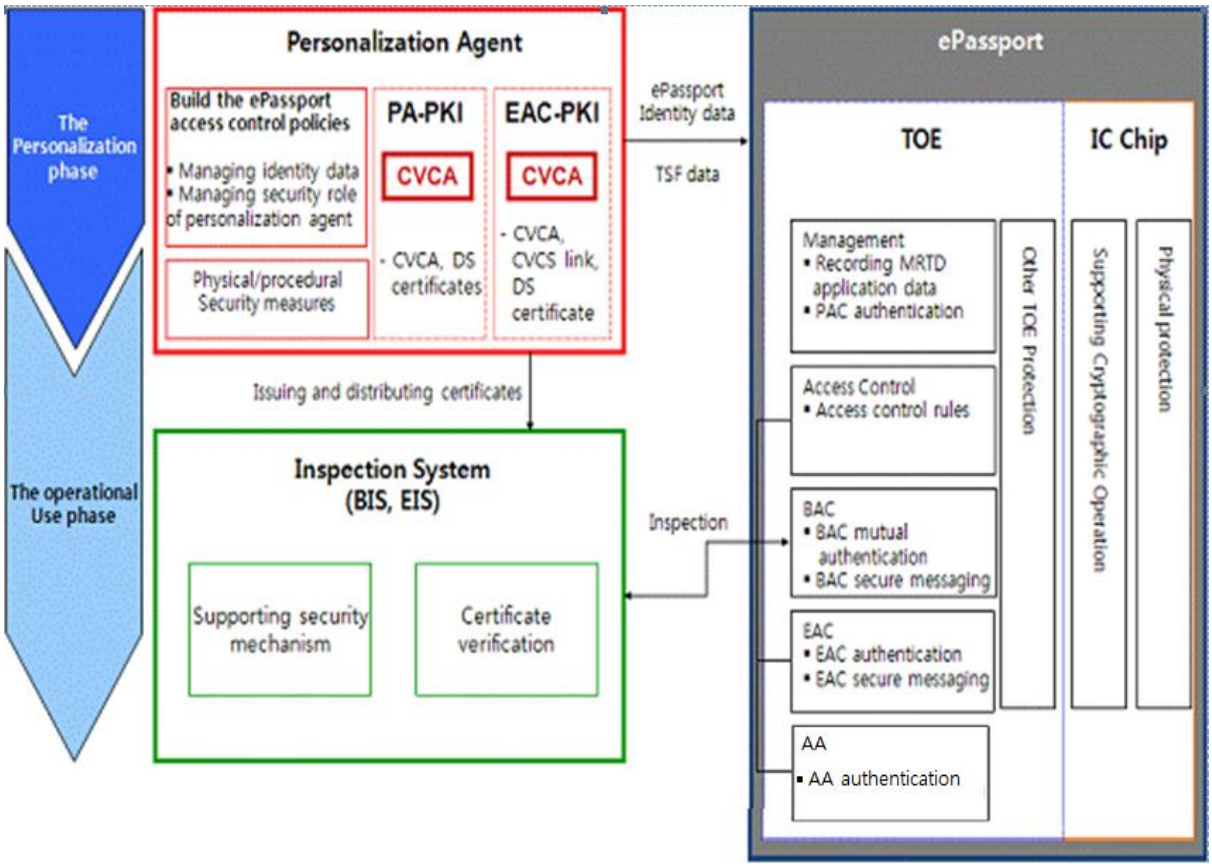
(Table 2) Life Cycle of the MRTD Chip and the TOE

Phase	Life Cycle of the MRTD Chip	Life Cycle of the TOE
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W.	
		② The S/W developer to develop the TOE (COS, MRTD application) by using the IC chip and the Dedicated S/W. ③ Delivery to IC chip manufacturer the ROM code including the initial PAC authentication key.
Phase 2 (Manufacturing)	④ The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier and to produce the IC chip.	
	⑤ The ePassport manufacturer to embed the IC chip in the passport book by requesting the Personalization agent.	
Phase 3 (Personalization)		⑥ The Personalization agent to operate the functions of the PAC authentication key update and patch. ⑦ The Personalization agent to create a user data storage space according to the LDS format or the ICAO document and to record it in EEPROM. ⑧ The Personalization agent to create a SOD using a digital signature on the ePassport identity data. ⑨ The Personalization agent to record the ePassport identity data, the authentication data (including SOD) and the TSF data (The TOE itself creates the BAC authentication key using the command of the personalization agent) in the TOE. ⑩ The Personalization agent to verify

Phase	Life Cycle of the MRTD Chip	Life Cycle of the TOE
		the normal operation. ⑪ Issue, discard or re-personalization according to the verifying result.
Phase 4 (Operational Use)		⑫ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE.

TOE Operational Environment

[Figure 2] 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 the TOE and external entities (the Personalization agent, the Inspection System) that interact with the TOE.



[Figure 2] The TOE Operation Environment

TOE Personalization Phase

The TOE manages eight statuses as operational modes for secure personalization and management. The personalization phase is divided into pre-personalization, personalization, verification and the operational mode transition.

2.4 TOE Scope

In this section, the physical and logical scope of the TOE is defined.

2.4.1 Physical Scope of the TOE

The MRTD IC chip includes the native IC chip operating system (COS), the MRTD application, the MRTD application data, cryptography operation and the IC chip constituent.

In the ST, the TOE is defined with the native IC chip operating system (COS), the MRTD application and the MRTD application data.

The native IC chip operating system (COS) provides functions for the execution of the MRTD application and management of the MRTD application data, including command processing and file management, as defined in ISO/ IEC 7816-4, 8 and 9.

The MRTD chip application is the IC chip application that implements the function to store and process the ePassport identity data according to the LDS (Logical Data Structure) format defined in the ICAO document in addition to the security mechanism to protect the function securely. In addition, the MRTD application is added to the EAC security mechanism by the EAC specifications, as the biometric data of the ePassport holder is included in the ePassport identity data. The MRTD chip application also includes the PAC security mechanism, which is the security mechanism of KCOS for ePassport personalization. The MRTD chip application is stored in the ROM of the MRTD IC chip.

The MRTD application data consists of the user data, including the ePassport identity data and the TSF data required in the security mechanism. The MRTD application data is stored the ROM of the MRTD IC chip.

2.4.2 Logical Scope of the TOE

The TOE communicates with the Inspection System and Personalization agent according to the

transmission protocol defined in ISO/IEC 14443-4. The TOE implements the PAC security mechanism and the security mechanism defined in the ICAO document and the EAC specifications. It also provides access control and security management functions. In addition, the TOE provides functions of TSF self-protection, such as TSF self-testing, preservation of a secure state and domain separation.

The logical scope of the TOE is divided into subsystems and assets. The subsystems operate security mechanisms, TOE access control, security management and the TOE protection functions. The assets consist of MRTD user data and MRTD TSF data.

Subsystems

The functions of the subsystems are outlined below.

(Table 3) Subsystems and Functions

Subsystems	Functions	Security Functions
Authentication	. BAC mutual authentication and BAC session key generation . PAC mutual authentication and PAC session key generation . EAC-CA and EAC session key generation . EAC-TA and CVCA Certificate verification/update . PAC authentication key update and BAC authentication key generation . Writing TSF data . TSF data integrity verification	SF.MUT_AUTH SF.CHIP_AUTH SF.TERMINAL_AUTH SF.ACTIVE_AUTH SF.ACC_CONTROL SF.RELIABILITY
Card Manager	. IC chip sensor test activation . APDU receiving/transmitting(Command access control according to the operational mode) . Checking the status of patch for the TSF executable code and changing the operational mode .The file table and security properties initialization, the TOE personalization initialization, the TOE re-personalization initialization, and the TOE Block operational mode release (Unblock) .Temporary function stop(when BAC mutual authentication fail) . extra information control . executable code integrity verification	SF.ACC_CONTROL SF.RELIABILITY SF.MUT_AUTH

Crypto	. IC chip function call and handling to compute the hash(SHA-1, SHA-224, SHA-256) . Hash operation (SHA-1, SHA-256) . IC chip function call and handling to compute the TDES, Retail MAC, random number generation and CRC . IC chip function call and handling to compute the RSA and ECC . IC chip function call and handling to compute the TDES, Retail Mac	SF.MUT_AUTH SF.CHIP_AUTH SF.TERMINAL_AUTH SF.ACTIVE_AUTH SF.ACC_CONTROL
Memory Manager	. Access control reading and writing the user data	SF.ACC_CONTROL, SF.RELIABILITY
Secure Messaging	. PAC trusted channel, BAC trusted channel, EAC trusted channel	SF.SEC_MESSAGE

Assets

In order to protect the TOE assets shown in (Table 4), the TOE provides security functions such as the confidentiality, the integrity, the authentication and the access control.

(Table 4) TOE Assets

Category			Description	Storage Space
User Data	ePassport Identity Data	Personal Data of the ePassport holder	EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16	EF file
		Biometric Data of the ePassport holder	EF.DG3, EF.DG4	
	ePassport Authentication Data		EF.SOD, EF.DG14 (EAC chip authentication public key), EF.DG15 (AA public key)	
	EF.CVCA		In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System	
	EF.COM		LDS version info., tag list of DG used, etc.	
TSF Data	EAC Chip Authentication Private Key		In EAC-CA, Chip Private key used by the TOE to demonstrate a non-forged MRTD chip	Secure memory

Category		Description	Storage Space
	CVCA Certificate	In personalization phase, Root CA Certificate issued in EAC-PKI	
	CVCA Digital Signature Verification Key	After the personalization phase, CVCA Certificate Public key is newly created by a certificate update	
	Current Date	In the personalization phase, the date of issue of the ePassport is recorded. However, in the operational use phase, the TOE internally updates it as the latest date among the issuing dates of the CVCA Link Certificate, the DV Certificate or the Issuing State IS Certificate.	
	BAC Authentication Key	BAC authentication encryption key BAC authentication MAC key	
	AA Private Key	Private key of the chip used by the TOE to prove that the chip is not substituted	
	PAC Authentication Key	Symmetric key for PAC mutual authentication and PAC personalization management authentication	
	TSF execute Code for patching	Additional Execute code for improving function	
	TSF integrity verification key	MAC key for making integrity value TSF	
	BAC Session Key	BAC session encryption key BAC session MAC key	Temporary memory
	EAC Session Key	EAC session encryption key EAC session MAC key	
	PAC Session Key	PAC session encryption key PAC session MAC key	

Application Notes: The biometric data obtained from an ePassport holder include the face, the fingerprint and the iris scan. It is mandatory to contain the face information according to the ICAO document. The fingerprint and iris information is included optionally according to the issuing policy of the ePassport. This security target includes security functional requirements for the EAC

specifications by assuming the fingerprint information to be contained.

Application Notes: A BAC authentication key is generated and saved in the secure memory of the IC chip in the personalization phase by the command of the Personalization agent

Application Notes: To support the 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 the secure memory of the MRTD chip during the personalization phase. When the CVCA digital signature verification key is updated, the TOE overwrites at the existing CVCA digital signature verification key.

Application Notes: The Personalization agent generates the SOD through a digital signature on the ePassport identity data.

The LDS in which the user data are stored defines the MF, DF and EF file structure. (Table 5) shows the content of EF.DG1~EF.DG16, in which parts of the user data is stored.

(Table 5) Content of the LDS in which the User Data are Stored

Category	DG	Contents
Detail(s) in MRZ	DG1	Document (Passport) Type
		Issuing State
		Name (of Holder)
		Document Number
		Check Digit (of Doc Number)
		Nationality
		Date of Birth
		Check Digit (of DOB)
		Sex
		Data of Expiry of Valid Until Date
		Check Digit (of DOE/VUD)
		Composite Check Digit
Biometric	DG2	Encoded face info.

Category	DG	Contents
Data		
Biometric Data	DG3	Encoded fingerprint info.
ePassport authentication information	DG5	Photo image
	DG7	Signature image
	DG11	Personalization additional information
	DG12	ePassport additional information
	DG14	EAC Chip Authentication Public Key
	DG15	AA Digital Signature Verification Key
	EF.COM	LDS version info., tag list of DG used, etc.
	EF.SOD	Document of security
	EF.CVCA	In EAC-TA, CVCA digital signature verification key identifier list

Security Mechanisms

The TOE provides security functions such as confidentiality, integrity, access control and authentication to protect the TSF data and the user data of the ePassport identity data and the ePassport authentication data. These security functions are implemented with the PAC, the BAC mechanism of the ICAO document and the EAC mechanism of the EAC specifications. Additionally, the TOE provides the SOD to the BIS and the EIS, and the Inspection System detects forgery and corruption of the user data through verification of the digital signature of the SOD.

< PAC (Personalization Access Control) >

The TOE provides a PAC (Personalization Access Control) security mechanism to control the access-rights of the security role of the Personalization agent. The PAC is divided into PAC mutual authentication, PAC session key generation and PAC personalization and management authentication.

PAC mutual authentication is a TDES-based entity authentication protocol that modifies the BAC security mechanism to authenticate between the Personalization agent and the TOE mutually in the personalization phase.

PAC session key generation is implemented using the TDES-based key distribution protocol, which is the function that generates the PAC session key (the PAC session encryption key and PAC session MAC key) that is used to create the PAC secure messaging between the TOE and the Personalization agent. This protocol is implemented by modifying the standard symmetric key-based key distribution protocol.

PAC personalization and management authentication is operated after TSF checks the operational mode of the TOE when the Personalization agent requests the TOE security management or the TSF data management. The Personalization agent issuing authorization is obtained when the Personalization agent successfully establishes with the security management functions it will use. The personalization right consists of the PAC authentication key update, operational mode transition, executable code and data path, and the Unblock function.

< BAC (Basic Access Control) >

The BAC (Basic Access Control) provides confidentiality and integrity for the personal data of the ePassport holder by secure messaging when controlling access to the personal data of the ePassport holder stored in the TOE and transmitting it to the Inspection System with read-rights. The BAC includes the BAC mutual authentication, the BAC key distribution and the BAC secure messaging.

The TOE uses the BAC authentication key stored in secure memory and the BAC-supporting Inspection System using the BAC authentication key generated from reading optically the MRZ. The TOE and the Inspection System then perform encryption by a generated random number and exchange the numbers. The TOE and the BAC-supporting Inspection System execute the BAC mutual authentication by checking the exchanged random number. The session is ended in case of a mutual authentication failure.

The TOE, to secure transmission of the personal data of the ePassport holder after checking the read-rights of the Inspection System for the personal data of the ePassport holder through the BAC mutual authentication, establishes BAC secure messaging through encryption of the BAC session key shared by the BAC key distribution. It also generates the MAC.

< AA (Active Authentication) >

The AA security mechanism is implemented to prove the authenticity of the TOE to the inspection system. The TOE generates and transmits the digital signature generated by the AA private key on the random number transmitted by the inspection system. The inspection system then

authenticates the TOE by verifying the digital signature using the AA public key. Therefore, AA is the security mechanism that prevents the substitution of the MRTD IC chip onto which the TOE is loaded.

< EAC (Extended Access Control) >

The EAC (Extended Access Control) provides the confidentiality and the integrity for the biometric data of the ePassport holder by secure messaging when controlling access to the biometric data of the ePassport holder stored in the TOE and transmitting it to the Inspection System with read-rights. The EAC includes the EAC-CA, the EAC secure messaging and the EAC-TA.

The EAC-CA implements the ephemeral-static DH key distribution protocol for the EAC session key distribution and the chip authentication. The TOE transmits the EAC chip authentication public key so that the Inspection System authenticates itself and executes the key distribution protocol by using a temporary public key received from the Inspection System. The session is ended if the EAC-CA fails. When the EAC-CA is successful, the TOE establishes the EAC secure messaging using the EAC session key.

The EAC-TA is used by the TOE to implement the challenge-response authentication protocol based on the digital signature in order to authenticate the EAC-supporting Inspection System. The TOE authenticates the Inspection System, verifying the value of the digital signature by the Inspection System in the temporary public key used for the EAC-CA using the IS Certificate. The TOE, when receiving the CVCA Link Certificate, the DV Certificate and the IS Certificate from the EAC-supporting Inspection System, verifies the CVCA Link Certificate using the CVCA digital signature verification key in secure memory. Then, by verifying a valid date of the CVCA Link Certificate, the TOE updates the CVCA digital signature verification key and the current date if necessary. After verifying the IS Certificate and checking that it is a suitable certificate, the TOE allows access of the EAC-supporting Inspection System to read the biometric data of the ePassport holder and transmits the data through EAC secure messaging.

TOE Access Control and Security Management

The TOE Access control and Security Management is divided into the access control of the Personalization, the access control of the IS, the personalization management of the Personalization agent and the TOE self protection management.

< Access control of the Personalization agent>

The access control of the Personalization agent provides the Personalization agent with the access control rules for the User Data and the TSF Data. If the Personalization agent has the issuing authorization as the security property, the TOE allows read and writes operations for the personal data and biometric data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM.

< Access control of the IS >

In the Operational phase, the TOE provides the access control rules and management functions for the User Data based on the security properties of the user.

In addition, in the Operational phase, the TOE provides the access control functions for the read right of the User Data based on the access right of the IS, which is authenticated through performance of the security mechanisms.

Therefore, if the IS succeeds with the BAC authentication, the TOE grants a BAC authorization (the read-rights for the personal data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM). If the IS also succeeds with the EAC authentication and the CVCA Certificate, DV Certificate and IS Certificate that the IS has included with the read-rights for the biometric data, the TOE then grants the EAC authorization (the read-rights for the personal data of ePassport holder, the biometric data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM).

< Personalization management of the Personalization agent >

For the personalization management of the Personalization agent, the TOE provides the Personalization agent with the EEPROM initialization, the operational mode transition, the executable code, the data patch, the Unblock, the PAC authentication key update, and the BAC authentication key generation and save functions.

< TOE self protection management >

The TOE initializes security attributes of the subject for preserving the inter-operational state when detecting modifications to TSF data. When successfully generating the EAC session key, the TOE initializes the SSC to shift from BAC secure messaging to EAC secure messaging.

Other TOE Protection

The TOE, in order to protect the TSF from interference and tampering by untrusted subjects, ensures that the access control function is always invoked without bypassing and maintains separation of the secure memory area where the TSF data is stored and the memory area where the User Data is stored. The TOE only allows an authorized Personalization agent to use the writing function for TSF data and does not allow use of the reading function for the TSF data. Therefore, TSF data is protected against external interferences.

The TOE executes the functions to detect modifications of the transmitted TSF data using the MAC function of the IC chip. When detecting a modification, the TOE performs the function of session termination. Loading the TSF data from temporary memory to perform the security mechanism, the TOE provides the integrity measure for the TSF data.

The IC chip provides the functions that consider countermeasures to the DPA/SPA, which is an attack technique, by analyzing the physical phenomena (electric current, voltage, an electromagnetism change) during the cryptographic algorithm (random number, TDES, Retail MAC, RSA, ECC) for the TOE. If the IC chip detects an abnormal operation, it notifies the TSF and then maintains a safe state which prevents the abnormal operation from occurring.

2.4.3 IT environment (a chip)

The IC Chip(S3CC9LC/GC/GW) provides the TDES cryptographic algorithm, Retail MAC algorithm and RSA, only S3CC9LC provides additional Hash algorithm and ECC cryptographic algorithm

Thus, the TOE is provided CRC function for memory integrity.

The IC Chip provides functions that consider countermeasures to the DPA/SPA, which is an attack technique, by analyzing physical phenomena (electric current, voltage, an electromagnetism change) during the cryptographic algorithm (random number, TDES, Retail MAC, RSA, ECC) for the TOE.

In addition the IC Chip provides an inspect mechanism as to whether the TOE departs from the normal operational range of the TSF with an ActiveShield and sensor test function for the TOE.

2.4.4 External IT

The ePassport PKI System provides certification functions that include the issuance of the necessary certificates in the digital signature of ePassport and the management of certification-related records.

PA-PKI

PA (Passive Authentication) demonstrates that the identity data recorded in the ePassport has not been forged of corrupted as the IS with the DS Certificate verifies the digital signature in the SOD and the hash value of user data according to read-right of the ePassport access control policy.

CSCA (Country Signing Certification Authority) is 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

The DS (Document Signer) Certificate is the certificate of the Personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism. The DS Certificate may be saved in EF.SOD of TOE for PA.

EAC-PKI

EAC-TA (EAC-Terminal Authentication) is the security mechanism implementing the digital signature-based Challenge-Response authentication protocol with which the TOE authenticates the EIS through verification of the digital signature with the IS Certificate. The digital signature is the value with which the EIS takes e-signature temporary public key used in the EAC-CA using its own digital signature key and transmits it to the TOE.

CVCA (Country Verifying Certification Authority) is the certificate that includes the digital signature value by the EAC-PKI root CA with the digital signature generation key of the EAC-PKI root CA on the digital signature verification key to demonstrate the validity of the CVCA Link Certificate and the DV Certificate.

The DV (Document Verifier) generates and issues the IS Certificate.

3. TOE Security Environment

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

3.1 Assumptions

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

A. Certificate Verification

The Inspection System of the BIS and the EIS verifies the SOD after verifying the validity of the certificate chain for the PA (CSCA Certificate → DS Certificate) to guard against forgery and corruption of the ePassport identity data recorded in the TOE. To do this, the DS Certificate and CRL shall be verified periodically.

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

Application Notes: The distribution process of the certificates follows the ICAO PKD or diplomatic policy of the country in which the ePassport is issued.

A. Inspection System

The Inspection System shall implement the 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.

Additionally, after the 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 the session information.

Application Notes: The TOE denies the request to access EF.SOD by the Inspection System when it fails the BAC mutual authentication procedure.

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. Subsequently, 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, and by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it then conforms the absence of forgery or corruption of the personal and authentication data of the ePassport holder.

As the EIS supports the BAC, EAC and PA security mechanisms, it obtains the read-rights for the personal, authentication and biometric data of the ePassport holder. The EIS, when the BAC mutual authentication and secure messaging succeed, executes the EAC-CA using the EAC chip authentication public key read in the BAC to verify the authenticity of the TOE. It then executes the PA to verify the EAC chip authentication public key. When the EAC-CA succeeds, the BAC secure messaging ends, the EAC secure messaging with the EAC session key starts, and the EAC-TA with which the TOE authenticates the Inspection System is executed. When the EAC-TA succeeds, the EIS obtains the read-rights for the biometric data of the ePassport holder and the TOE provides the biometric data to EIS.

A. IC Chip

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

Application Notes: The cryptographic processor of an IC chip provides TDES, the Retail MAC to support the security function of TOE. The cryptographic library provides the RSA and the ECC cryptographic algorithm, and the RNG provides the random number. The CRC of an IC chip provides the CRC algorithm, and the TOE executes the hash algorithm. The IC chip onto which the TOE is loaded is an Samsung Electronics S3CC9LC / S3CC9GC/ S3CC9GW EAL4+.

A. MRZ Entropy

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

Application Notes: In order to provide resistance against a high-level threat agent and the

entropy of the passport number, the date of birth and the date of expiry and the check digit used as the BAC authentication key seed in the MRZ in the current technological level shall be at least 56 bits.

3.2 Threats

The ePassport is used in the possession of individuals without the need for physically controlled devices; therefore, both logical and physical threats can occur. A threat agent is an external entity that attempts illegal access to assets protected by the TOE using physical or logical methods outside the TOE.

In this document, the IC chip provides physical protection of the TOE according to the A.IC Chip. Therefore, a physical threat to the IC chip itself by a high-level threat agent is not considered.

Consequently, a threat agent to the TOE requires the high-level of expertise, resources and motivation.

<Threats to the TOE in the Personalization phase>

T. Application Program Interference

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

T. TSF Data Modification

The threat agent can modify the transmitted TSF data when the Personalization agent records the TSF data or attempts access to the stored TSF data using the external interface through the Inspection System.

T. Personal Agent Camouflage

A threat can attempt to personalize the ePassport using the write and management methods of ePassport application data to forge the ePassport.

T. Issue organization forgery

A threat can attempt to write to the electronic passport application data; management in this case refers to electronic passport forgery.

<BAC-related Threats in the Operational Use phase>

T. Eavesdropping

To determine the personal data of an ePassport holder, the threat agent may eavesdrop on the transmitted data using a terminal capable of RF communication.

T. Forgery and Corruption of Personal Data

To forge and corrupt the personal data of the ePassport holder stored in the MRTD chip, a threat agent may attempt to read the user data using an unauthorized Inspection System.

T. BAC Authentication Key Disclose

To determine the personal data of the ePassport holder, a threat agent may obtain read-rights of the BAC authentication key located inside the TOE and disclose related information.

Application Notes: The BAC authentication key is generated by the Personalization agent in the Personalization phase and saved in secure memory. A threat can attempt to access the BAC authentication key that is saved in secure or in the temporary memory of the MRTD IC Chip.

T. BAC Replay Attack

The threat agent can bypass the BAC mutual authentication by replaying the data after intercepting it as it is transmitted by the TOE and the Inspection System in the initial phase of the BAC mutual authentication.

Application Notes: The TOE delivers a random number of plain text to the Inspection System according to the 'et_challenge' instruction of the Inspection System in the BAC. Therefore, a 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. Moreover, the threat agent can find the transmission data, as the threat agent can generate the BAC session key after obtaining the BAC authentication key through the T. BAC Authentication Key Disclose function.

<EAC-related Threats in the Operational Use phase>

T. Damage to Biometric Data

The threat agent can disclose, forge and corrupt the biometric data of the ePassport holder using a terminal capable of unauthorized RF communications.

Application Notes: Only the EIS that succeeds with the EAC-TA can access the read-rights regarding the biometric data of the ePassport holder. Therefore, a threat agent can attempt to obtain the biometric data through such means as an unauthorized Inspection System and the BIS.

T. EAC-CA Bypass

A threat agent can bypass the authentication of the Inspection System and go through the EAC-CA using the EAC chip authentication public key generated by the threat agent.

T. IS Certificate Forgery

To obtain access rights to the biometric data of the ePassport holder, a threat agent can attempt to bypass the EAC-TA by forging the CVCA Link Certificate, DV Certificate and IS Certificate and requesting verification of the certificates by the TOE.

Application Notes: Instead of storing the CVCA Certificate, TOE stores the information(CVCA Certifcate public key paramaters)related to CVCA Certificate public key to the secured memory and verifies the CVCA Certificate. TOE can verify CVCA linked Certificate, DV Certificate, IS Certificate with the information related to CVCA Certificate public key stored in the secured memory.

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

T. Session Data Reuse

To access the data transmitted through secure messaging, a threat agent can derive session keys from a number of cryptographic communication texts collected using a 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 a cipher-text-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 process, the critical information necessary in deriving the session key can be provided to an attacker because the first random number of the TOE is transmitted as plain text. In case the EIS transmits a temporary public key in the EAC-CA and a random number in the EAC-TA to other sessions in the same way and if the TOE continues to use these data items, they may be vulnerable to cipher-text only attacks.

T. Skimming

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

<Threats related to IC Chip Support>

T. Malfunction

To bypass security functions or to damage the TOE executable code and the TSF data stored in the TOE, a threat agent can instigate a malfunction of the TOE in the environmental stress outside the normal operating conditions.

<Other Threats in the Operational Use phase>

T. Leakage of the Cryptographic Key Information

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

T. ePassport Reproduction

A threat agent can masquerade as the ePassport holder by reproducing the MRTD application data stored in the TOE and forging the identity information page of the ePassport.

T. ePassport IC chip Replacement

A threat can forge an electronic passport and write the data onto another passport IC chip.

T. Residual Information

A threat agent can disclose the critical information using the residual information remaining while the TSF data, such as the BAC authentication key, BAC session key, EAC session key, DV Certificate and IS Certificate, are recorded and used in temporary memory.

3.3 Organizational Security Policies

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

P. International Compatibility

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

Application Notes: International compatibility shall be ensured according to the ICAO document and EAC specifications

P. Security Mechanism Application Procedures

The TOE shall ensure the order of the security mechanism application according to the type of Inspection System so as 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 the Standard ePassport Inspection Procedure described in 2.1.1 and Advanced ePassport Procedure in 2.1.2 in the EAC specifications.

P. Application Program Loading

The Personalization agent shall approve the loading application program after checking that the application programs loaded in the MRTD chip does not affect the security of the TOE.

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

P. Personalization Agent

The personalization agent shall issue the ePassport in a secure manner 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 they are issued. 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 the TOE shall formulate the ePassport access control policies to protect the MRTD application data. Additionally, the TOE shall regulate the roles of user.

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

(Table 6) ePassport Access Control Policies in the Operational Use phase

Subjects List		Objects List	Objects									
		Objects List	Personal data of the ePassport holder		The biometric data of the ePassport holder		ePassport authentication data		EF.CVCA		EF.COM	
		Security Attributes / Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	BIS	BAC Rights	allow	deny	deny	deny	allow	deny	allow	deny	allow	deny
	EIS	BAC Rights	allow	deny	deny	deny	allow	deny	allow	deny	allow	deny
	EIS	EAC Rights	allow	deny	allow	deny	allow	deny	allow	deny	allow	deny

(Table 7) Personalization Phase ePassport Access Control Policies

	Objects List	Objects

Subjects List		Objects List	Personal data of the ePassport holder		The biometric data of the ePassport holder		ePassport authentication data		EF.CVCA		EF.COM	
		Security Attributes / Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	Personal Agent	Issuing Rights	allow	allow	allow	allow	allow	allow	allow	allow	allow	allow

Subjects		Objects	Objects									
		Objects	EAC Chip Authentication private key		CVCA Authentication and CVCA Digital Signature verification of the Key current date		BAC Authentication Key		AA private key		PAC Authentication Key	
		Security Attributes / Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	Personal Agent	Issuing Rights	deny	allow	deny	allow	deny	allow	deny	allow	deny	allow

P. PKI

The Issuing State of the ePassport shall implement the PA-PKI and EAC-PKI security mechanism according to the ePassport PKI System and execute the practice of certification (creating, issuing, operating and destroying the certificates) by securely generating and managing digital signature keys in accordance with the Certification Practice Statement (CPS)

In addition, the Issuing State of the ePassport shall update certificates according to the policies to maintain a valid date of the certificates and securely delivery them to the Verifying State and Inspection System. When the EAC-TA provides the TOE with a CVCA Link Certificate, a 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 the validity of the certificates.

P. Range of RF Communication

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

This page left blank on purpose for double-side printing

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 in relation to IT fields or by non-technical/process-related means.

4.1 Security Objectives for the TOE

The following items are security objectives that are handled directly by the TOE.

O. Management

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

Application Note: In the Personalization phase, the TOE shall provide the personalization and management functions (lifecycle change, execution code patch, PAC authentication key update, and Unblock, among others) to the authorized Personalization agent.

The TOE divides EEPROM for the user data and the TSF data and manages the memory area of each user separately. The Personalization agent deactivates the writing function by modifying the lifecycle of the TOE after the Personalization agent writes the ePassport applicable data in the Personalization phase. This operation is performed before the lifecycle of the TOE is transferred to the Operational phase. The TOE stores the BAC authentication key in secure memory after it is generated by request of the Personalization agent in the Personalization phase.

O. Security Mechanism Application Procedures

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

Application note: The TOE shall ensure that the application order of the PA, AA, BAC and EAC security mechanisms conforms to the 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specification. In addition, it shall not allow requests from the Inspection System that does not correspond to the security mechanism application order.

O. Session Termination

The TOE shall terminate the session if the BAC mutual authentication or the EAC-TA fails or if a modification is detected in the transmitted TSF data.

O. Secure Messaging

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

Application Note: The TOE forms a secure communication channel using a PAC Session key during the Personalization Phase. The TOE forms the secure communication channel using the BAC Session key and the EAC Session key during the Operation Phase.

O. Domain Separation

The TOE shall provide the means to prevent interference and tampering of the TSF and TSF data through external IT entities.

Application Note: The TOE is not infringed due to interference from other application programs due to the closed-type COS. The TOE managing the storage scope is sectioned into user data on the TSF data, and the TSF data are stored in the COS controls so that they cannot approach the interface of the external IT and breach the area of the protective memory scope.

O. Certificate Verification

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

O. Self-protection

The TOE shall protect itself so as to preserve a secure state from attempts to bypass and modify the TSF executable code and data upon start-up.

O. Deleting Residual Information

When allocating resources, the TOE shall provide the means to ensure that previous security-related information (e.g., the BAC session key, the EAC session key) is not included.

O. Replay Prevention

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

Application Note: The TOE shall generate the transmitted data to the Inspection System in the BAC mutual authentication and EAC-TA, ensuring that it is different with every session. In addition, it shall not use the BAC authentication key as the BAC session key. The TOE also shall not provide the critical information necessary in deriving the session key by generating the BAC session key with the same random number used in the BAC mutual authentication. The TOE shall generate the data transmitted to the personalization agent in the PAC mutual authentication so that it is different per each session. Additionally, it shall not use the PAC authentication key as the PAC session key. The TOE shall not provide the critical information necessary in deriving the session key by generating the PAC session key with the same random number used in the PAC mutual authentication. The TOE shall not generate the RSA digital signature value with the Single-use random number mechanisms used in the AA.

O. Access Control

The TOE shall provide an access control function so that access to the ePassport application data is allowed only to external entities granted with access rights according to the ePassport access control policies of the Personalization agent.

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

O. AA

The TOE implements the AA mechanism to prove the authenticity of the TOE to the inspection components. The TOE generates and transmits the digital signature by the AA private key on the random number transmitted by the inspection system. The inspection system authenticates the

TOE by verifying the digital signature using the AA public key.

O. BAC

The TOE executes the BAC mutual authentication of the Inspection System with the TOE by implementing a BAC security mechanism to allow read-rights for the personal data of the ePassport holder only to the authorized Inspection System. The TOE generates the BAC session key that is 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) to allow read-rights for the biometric data of the ePassport holder only to the authorized Inspection System. The TOE generates the EAC session key that is used for the EAC secure messaging.

O. PAC

The TOE carries out PAC mutual authentication and PAC personalization and management authentication to provide a means of management for electronic passport issue (EF file creation, PAC authentication Key Update, lifecycle change, an execution code and data patch, Unblock, and TSF data management) to only an authorized Personalization agent.

4.2 Security Objectives for the Environment

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

OE. Passport Book Manufacturing Security

Physical security measures (security printing, etc.) for the ePassport shall be prepared to detect reproduction of the ePassport chip and attack attempts against such factors as Grandmaster chess, replacement of the portrait, or modification of the MRZ data.

OE. Procedures of the ePassport holder Check

The Immigration officer shall prepare for procedures to check the identity of the ePassport holder against the printed identity information page of the ePassport.

OE. Application Program Loading

The Personalization agent shall approve application program loading after checking that the application programs loaded in the ePassport chip do not affect the secure TOE.

OE. Certificate Verification

The Inspection System, including the BIS and the EIS, verifies the SOD after verifying the validity of the certificate chain for the PA (CSCA Certificate → DS Certificate) to verify that forgery and corruption of the ePassport identity data recorded in the TOE has not occurred. To do 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 a CVCA Link Certificate, a DV Certificate and an IS Certificate in the EAC-TA.

OE. Personalization Agent

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

OE. Handling Information Leakage

The TOE shall implement countermeasures to prevent the exploitation of leaked information during the cryptographic operation for the TSF.

Application Note: The IC chip of the TOE support functions as a countermeasure of the DPA/SPA prevents the exploitation of leaked information (electric current, electric pressure, electromagnetism etc) during crypto graphic operation.

OE. Inspection System

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

OE. IC Chip

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

Application Note: The IC chip support TDES, Retail MAC, the random number, RSA, ECC and IC chip support functions that act as a countermeasure for the DPA/SPA to the TOE. The IC chip supports an inspection mechanism that determines whether the TOE deviates from its normal operational range of TSF via an ActiveShield and sensor test function of the TOE.

OE. MRZ Entropy

The Personalization agent shall ensure the MRZ entropy to ensure the security of the BAC authentication key.

OE. PKI

The Issuing State of the ePassport shall execute certification procedures that securely generate and manage a digital signature key and generate, issue, operate and destroy certificates according to the CPS by implementing the PA-PKI and EAC-PKI according to the ePassport PKI System.

The Issuing State of the ePassport shall also update the certificates according to the policies to maintain a valid date for certificates and securely deliver them to the Verifying State and Inspection System.

OE. Range of RF Communication

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

This page left blank on purpose for double-side printing

5. IT Security Requirements

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

5.1 TOE Security Functional Requirements

The security functional requirements for this Security Target consist of the following components from Part 2 of the CC and additional components, as summarized below (Table 8).

The strength of function (SOF) for security functional requirements of FCS_CKM.1(1), FDP_DAU.1, FIA_UAU.5(1), FIA_UAU.5(2), FCS_COP.1(3) FPT_TST.1 in this ST is “SOF-high”.

(Table 8) Security Functional Requirements

Security functional class	Security functional component	
Cryptographic Support (FCS)	FCS_CKM.1(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)
	FCS_CKM.2(3)	Cryptographic key distribution (Seed Distribution for PAC session key generation)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(3)	Cryptographic operation (Hash Function)
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based 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_AFL.1	Authentication failure handling
	FIA_UAU.1(1)	Timing of authentication(BAC Mutual Authentication)
	FIA_UAU.1(2)	Timing of authentication(EAC-TA)

Security functional class	Security functional component	
(FIA)	FIA_UAU.1(3)	Timing of authentication(PAC Mutual Authentication)
	FIA_UAU.1(4)	Timing of authentication(PAC Personalization management Authentication)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5(1)	Multiple authentication mechanisms
	FIA_UAU.5(2)	Multiple authentication mechanisms(PAC Mutual Authentication and PAC personalization and management Authentication)
	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(initialization)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Information)
	FMT_MTD.1(2)	Management of TSF data (SSC initialization)
	FMT_MTD.1(3)	Management of TSF data (Key Write)
	FMT_MTD.1(4)	Management of TSF data(TOE lifecycle and PAC Authentication key management)
	FMT_MTD.1(5)	Management of TSF data (TOE lifecycle change)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure to preserve a secure state
	FPT_ITC.1	Inter-TSF Confidentiality
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_TST.1	TSF Self-testing

5.1.1 Cryptographic Support

FCS_CKM.1(1) Cryptographic key generation (Key Derivation Mechanism)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

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

Application Notes: The TOE generates the BAC authentication key, BAC session key and EAC session key using a key derivation mechanism. The BAC authentication key, which is generated by the TOE, is stored in protected memory during the Personalization 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

FMT_MSA.2 Secure security attributes

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

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

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

Application Notes: DH protocol is used to generate EAC session key for GC/GW/LC chip and ECDH protocol is used to generate EAC session key for LC chip. This process is included in the IT environment because the TOE uses the ECC algorithm and modular arithmetic to generate the EAC session key.

FCS_CKM.2(3) Cryptographic key distribution (Seed Distribution for PAC session key generation)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

The TSF shall distribute **the Seed for the PAC session key generation** in accordance with a specified cryptographic key distribution method [none] that meets the following: [none].

Application Notes: The PAC session key generation Seed value distribution procedures are implemented by modifying a standard symmetric key distribution protocol (ISO/IEC 11770-2).

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FMT_MSA.2 Secure security attributes

FCS_CKM.4.1. The TSF shall destroy **authentication keys, encryption keys and MAC keys** in accordance with a specified cryptographic key destruction method [none] that meets the following: [delete by writing '0' in memory].

Application Notes: The TOE deletes the BAC authentication key, BAC session key, EAC session key, PAC authentication key, PAC session key, AA private key, EAC chip authentication private key, CVCA digital signature verification key and domain information in temporary memory by writing '0' in the memory.

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

FMT_MSA.2 Secure security attributes

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

Application Notes: In the key derivation mechanism of the ICAO document, the SHA-1 is used as a hash function to generate the session key used in the BAC or EAC. In addition, the SHA-1 is used as a hash function to generate the BAC authentication key, generate the EAC temporary public key and verify the initial CVCA. The SHA-256 is used for EAC-TA and AA.

5.1.2 User Data Protection

FDP_ACC.1 Subset 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) The biometric data of the ePassport holder

: EF.DG3, EF.DG4

(3) ePassport authentication data

: EF.DG14, EF.DG15, EF.SOD

(4) EF.CVCA

(5) EF.COM

(6) [None]

c) Operations

(1) Read

(2) Write

(3) [None]

]

FDP_ACF.1 Security attributes based 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] on objects based on the following: (Table 9), (Table 10).

(Table 9) Subject-relevant Security Attributes

Subjects	Security attributes
BIS	BAC authorization
EIS	BAC authorization, EAC authorization
Personalization agent	Personalization agent issuing authorization

(Table 10) Object-relevant Security Attributes

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

Objects	Security attributes	
	Security attributes of object' operation	Security attributes of object' access-rights
		authorization
Biometric data of the ePassport holder	Read-rights	EAC authorization, Personalization agent issuing authorization
	Write-rights	Personalization agent issuing authorization
ePassport authentication data	Read-rights	BAC authorization, EAC authorization, Personalization agent issuing authorization
	Write-rights	Personalization agent issuing authorization
EF.CVCA	Read-rights	BAC authorization, EAC authorization, Personalization agent issuing authorization
	Write-rights	Personalization agent issuing authorization
EF.COM	Read-rights	BAC authorization, EAC authorization, Personalization agent issuing authorization
	Write-rights	Personalization agent issuing authorization

Operation	Security attributes
Read	none
Write	

Application Notes: The BAC authorization is the right given to the user identified with the Inspection System that supports the ePassport 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

the CVCA certificate, the DV certificate and the IS certificate held by that Inspection System. Even when the EAC-CA and the EAC-TA succeed, the Inspection System comprises only the BAC authorization if the certificates do not include the read-rights.

Issuing authorization is the right given when PAC mutual authentication and PAC personalization and management authentication succeed due to the personalization agent.

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 the security attributes of the subjects are included in the security attributes of the object's access-rights and if the operations correspond to security attributes of the object's operation.

b) [none]

Application Notes: The TSF shall enforce the following ePassport access control policies: (Table 7), (Table 8):

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

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

a) Explicitly deny access for subjects to objects, if the 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 specification

b) Explicitly deny reading for subjects to biometric data if there are no read-rights of biometric data in the 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) [The TOE consists of eight lifecycles (Empty, Unissue, InitAuth, SecondAuth, StartIssue, Issued, Block, and Discard), and Access to the object is explicitly rejected for the commands that cannot be executed in each lifecycle of the TOE].

FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.

Dependencies: No other components.

FDP_DAU.1.1. The TSF shall provide the capability to generate evidence that can be used as a guarantee of the validity of [the AA 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 shall perform the 1024bit or 2048 bit RSASSA-PKCS-V1.5 digital signature algorithm in AA.

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 from* the following objects:[

a) BAC session key

b) EAC session key

c) BAC authentication key

d) [PAC session key,

e) PAC authentication key,

f) AA private key,

g) EAC chip authentication private key,

h) CVCA digital signature verification key and domain information,

i) TOE integrity verification key]

Application Notes: After the termination of the session, the TSF deletes the BAC authentication key, BAC session key, EAC session key, PAC authentication key, PAC session key, AA private key, EAC chip authentication key, CVCA digital signature verification key and domain information in temporary memory by writing '0' in the memory. EAC-CA private key for RSA is not loaded into the temporary memory. After finished the issuance and a status of TOE is Issued, PAC authentication key and TOE integrity verification key are physically deleted by writing '0' in the memory.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1. The TSF shall enforce [the ePassport access control policy] so that it can *transmit, and receive* objects in a manner protected from unauthorized disclosure.

Application Notes: When the Inspection System successfully completes the BAC mutual authentication, the TSF protects from disclosure using the BAC session encryption key. When the EAC-CA is successfully executed, the data transmitted thereafter are protected from disclosure using the EAC session encryption key. In addition, when the PAC mutual authentication is successfully executed, data transmitted thereafter are protected from disclosure using the PAC session encryption key.

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

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

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

Application Notes: The TSF protects the integrity of the transmitted data using the MAC key for the BAC session, the EAC session or the PAC session. This provides a method for protecting against modification, deletion and insertion of user data.

5.1.3 Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1. The TSF shall detect when [a certain number of times (see table below)] unsuccessful authentication attempts occur related to the following:

a) BAC mutual authentication

b) EAC-TA

c) [PAC mutual authentication,

d) PAC management authentication]

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

(Table 11) Authentication failure handling

Assignment: Number of unsuccessful authentication attempts	Assignment: Specified Authentication events	Assignment: Actions
3	Unsuccessful PAC Mutual authentication PAC personalization and management authentication	Session Termination and operational mode transition

1	Unsuccessful BAC Mutual authentication	Function halt for 1 sec after session termination
3	Unsuccessful EAC-TA authentication	Session Termination

Application Notes: The TSF halts all functions for 1 sec after terminating the session when BAC mutual authentication failed.

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 that supports the BAC mechanism

b) [None]

These are done 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 authenticated successfully before allowing any other TSF-mediated actions on behalf of that user.

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) performance of the EAC-CA

b) reading user data except for the biometric data of the ePassport holder

c) [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 authenticated successfully before allowing

any other TSF-mediated actions on behalf of that user except for actions indicated in FIA_UAU.1.1.

FIA_UAU.1(3) authentications (PAC Mutual Authentication)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 identification

FIA_UAU.1.1. The TSF shall allow [

a) TOE Personalization initialization of the Personalization phase

b) transmission of a crypto CSN and Ticket

c) transmission of a random number

] *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 for actions indicated in FIA_UAU.1.1.

Application Notes: TOE personalization initialization of the personalization phase can be only performed once.

FIA_UAU.1(4) authentication (PAC personalization and management authentication)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 identification

FIA_UAU.1.1. The TSF shall allow [

a) transmission of crypto CSN and Ticket

b) transmission of random number

c) PAC Mutual authentication

d) creating of EF

] *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 authenticated successfully before allowing any other TSF-mediated actions on behalf of that user except for actions indicated in FIA_UAU.1.1.

Application Notes: According to the lifecycle of the TOE, some actions that the TSF of b), c), d) listed in FIA_UAU.1.1 mediates may or may not be performed. When the lifecycle of the TOE is StartIssue or Block (d), PAC personalization and management authentication can be only performed and PAC mutual authentication not performed. And when the lifecycle of the TOE is SecondAuth, b) or c) is not performed since CSN, Ticket and random number are used obtained in the previous lifecycle, InitAuth.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) BAC mutual authentication

b) EAC-TA

c) [PAC Mutual authentication,

d) PAC personalization and management authentication]]

FIA_UAU.5(1) 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) [None]

] to support user authentication.

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

a) The BIS or EIS shall succeed with BAC mutual authentication to allow BAC authorization.

b) The EIS, to succeed with EAC authorization, shall succeed with BAC mutual authentication, EAC-CA, and EAC-TA, and shall include the read-rights of biometric data in the CVCA Certificate, DV Certificate and IS Certificate. To do this, the TSF shall provide the EAC-CA.

c) [None]]

Application Notes: In case of GC/GW chips, the TSF shall perform 1024 bit or 2048 bit RSASSA-PKCS-v1.5 digital signature algorithm. And in case of LC chip, the TSF shall perform 1024 bits, 2048 bits RSASSA-PKCS-v1.5 digital signature algorithms or 224 bit ECDSA digital signature algorithm in EAC-TA.

FIA_UAU.5(2) Multiple authentication mechanisms (PAC Mutual Authentication and PAC personalization and management authentication)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1. The TSF shall provide [

a) PAC mutual authentication

b) PAC personalization and management authentication (PAC-LifeCycle authentication, PAC-Patch authentication, PAC-KeyUpdate authentication, and PAC-Unblock authentication)

to support user authentication.

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

a) In case the lifecycle of the TOE in Personalization phase is in Unissue status, PAC mutual authentication has to be performed to generate EF.

b) When the lifecycle of the TOE in the Personalization phase is in InitAuth status, PAC personalization and management authentication has to be performed to update the function of the PAC authentication key.

c) When the lifecycle of the TOE in the Personalization phase is in InitAuth status, one of

the PAC personalization and management authentications, such as PAC-LifeCycle, PAC-Patch, or PAC-KeyUpdate, has to be performed to activate the writing function of the TSF.

d) In case the lifecycle of TOE in Personalization phase is in SecondAuth status and the issuing right for updating the PAC authentication key is not obtained, PAC personalization and management authentication along with PAC-KeyUpdate authentication have to be performed successfully to update the PAC authentication key.

e) In case the lifecycle of the TOE in the Personalization phase is in SecondAuth status and the issuing right for patching the execution code and data is not obtained, PAC personalization and management authentication along with PAC-Patch authentication have to be performed successfully to patch the execution code and data.

f) When the lifecycle of the TOE in the Personalization phase is in StartIssue status, PAC-LifeCycle authentication has to be performed to change the function of the lifecycle.

g) When the lifecycle of the TOE in the Personalization phase is in Block status, PAC-Unblock authentication has to be performed to unblock it.

]

Application Notes: The lifecycle of the TOE is changed to InitAuth status and the TOE has the right to create EF if PAC mutual authentication was performed successfully. If PAC personalization and management authentication was performed successfully in InitAuth status, the lifecycle of the TOE is changed to SecondAuth status and the TOE can change the lifecycle to the other lifecycle. The personalization right of the personalization agent includes that the personalization agent can assign the rights of reading or writing for user data and the TSF and the lifecycle is changed InitAuth to SecondAuth, from SecondAuth to StartIssue or Issued.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1. The TSF shall allow [

a) the establishment of a 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 identified successfully before allowing any

other TSF-mediated actions on behalf of that user except for actions indicated in FIA_UAU.1.1.

Application Notes: When external entities that communicate with the TOE request the use of the ePassport application, the TOE identifies it with the Inspection System. In addition, when external entities that communicate with the TOE request the use of the personalization program, the TOE identifies it with the personalization agent.

5.1.4 Security Management

FMT_MOF.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 [the Personalization agent in the Personalization phase].

Application Notes: After changing the lifecycle to Issued, the write function is deactivated.

FMT_MOF.1(2) Management of security functions behavior(initialization)

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 *open* [the functions (see table below] to [roles (see table below)].

(Table 12) Security Attributes

Assignment: Functions	Assignment: Roles
Initialization of the TOE personalization	Personalization agent
Initialization of the TOE re-personalization	Personalization agent with personalization authority
Initialization of LDS file system	Personalization agent with personalization authority

Application Notes: TOE personalization initialization means the initialization of user data storage and the transmission of PAC authentication stored in ROM to EEPROM.

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_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1. The TSF shall enforce [the ePassport access control policy] to restrict the ability to [*initialize*] the security attributes [*security attributes of the subjects defined in FDP_ACF.1*] to [*TSF*].

Application Notes: As the action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1, the TSF shall reset the security attributes of the 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 the security attributes that are used to enforce the SFP.

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

Application Notes: When generating user data (EF.DG1~16, EF.SOD, EF.COM, EF.CVCA) in the Personalization phase, the Personalization agent shall define the security attributes of object's operation and object's access-rights in (Table 10) of FDP_ACF.1.1.

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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 public key info.

d) initial CVCA digital signature verification key

e) [None]

to [**the Personalization agent in the Personalization phase**].

Application Notes: After the TSF stores the first CVCA Certificates and the first CVCA digital signature verification key in secure memory, the Personalization agent sends the command for verifying the validity of the first CVCA public key to the TOE. The TOE then verifies the signature of the first CVCA certificate using the first CVCA digital signature verification key. The trust point used in EAC-TA authentication consists of a CVCA digital signature verification key and the first CVCA Certificates.

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

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

FMT_MTD.1(3) Management of TSF data(Key Write)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to [*write in secure memory*] the [TSF data (see table below)] by [**the restrictions (see table below)**].

(Table 13) Security Attributes

Assignment: TSF data	Assignment: Restrictions
AA private key	Authorized Personalization agent according to FIA_UAU.5(2).2 in the Personalization phase
TSF execution code and IC chip setting the value for the patch	Authorized Personalization agent according to FIA_UAU.5(2).2 in the Personalization phase
BAC authentication key	TSF

Application Notes: TOE creates BAC authentication key using the commands of the authorized personalization phase according to FIA_UAU.5(2).2 and BAC authentication key is stored into secure memory area of IC chip. And the read functionality is not allowed for TSF of the personalization agent.

FMT_MTD.1(4) Management of TSF data (lifecycle of TOE and PAC authentication key management)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to *change* the [PAC authentication key, lifecycle of TOE in the Personalization Phase] to [**Authorized Personalization agent FIA_UAU.5(2).2**]

Application Notes: The initial PAC authentication key is stored in ROM during the Manufacturing phase. And the read functionality is not allowed for PAC authentication key of the personalization agent.

FMT_MTD.1(5) Management of TSF data(internal change of lifecycle)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to *change* the [lifecycle of the TOE in the Personalization phase] to [TSF].

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

b) A function to verify and update the CVCA Certificate, CVCA digital signature verification key and current data in the Operational Use phase

c) [A function to manage the TSF security: a function to verify the Security Attributes and SSC initialization, random number reuse,

d) A function to initialize personalization EEPROM in the Personalization phase,

e) A function to manage personalization and management: a function to change the lifecycle, function to patch the execution code and data, a function to unblock, a function to update the PAC key, and a function to inactivate writing in the Personalization phase]]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1. The TSF shall maintain the following roles: [

a) Authorized Personalization agent to update the PAC authentication key of the PAC in the Personalization phase

Authorized Personalization agent to change the lifecycle in the Personalization phase

Authorized Personalization agent for Unblock operations in the Personalization phase

Authorized Personalization agent for patching of the execution code and data patch in the Personalization phase

b) [None]]

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

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

5.1.4 Security Management

FMT_MOF.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 [the Personalization agent in the Personalization phase].

Application Notes: To change the lifecycle, the write function is deactivated.

FMT_MOF.1(2) Management of security functions behavior(initialization)

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 *open* [the functions (see table below] to [roles (see table below)].

(Table 144) Security Attributes

Assignment: Functions	Assignment: Roles
Initialization of the TOE personalization	Personalization agent
Initialization of the TOE re-personalization	Personalization agent with personalization authority
Initialization of LDS file system	Personalization agent with personalization authority

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_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1. The TSF shall enforce [the ePassport access control policy] to restrict the

ability to [*initialize*] the security attributes [security attributes of the subjects defined in FDP_ACF.1] to [TSF].

Application Notes: As the action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1, the TSF shall reset the security attributes of the 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 the security attributes that are used to enforce the SFP.

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

Application Notes: When generating user data (EF.DG1~16, EF.SOD, EF.COM, EF.CVCA) in the Personalization phase, the Personalization agent shall define the security attributes of object's operation and object's access-rights in (Table 10) of FDP_ACF.1.1.

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

a) EAC chip authentication private key

b) initial current date

c) initial CVCA Certificate

d) initial CVCA digital signature verification key

e) [None]

to [**the Personalization agent in the Personalization phase**].

Application Notes: After the TSF stores the first CVCA Certificates and the first CVCA digital signature verification key in secure memory, the Personalization agent sends the command for verifying the validity of the first CVCA public key to the TOE. The TOE then verifies the signature of the first CVCA certificate using the first CVCA digital signature verification key. The trust point used in EAC-TA authentication consists of a CVCA digital signature verification key and the first CVCA Certificates.

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

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

FMT_MTD.1(3) Management of TSF data(Key Write)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to [*write in secure memory*] the [TSF data (see table below)] by [**the restrictions (see table below)**].

(Table 155) Security Attributes

Assignment: TSF data	Assignment: Restrictions
AA private key	Authorized Personalization agent according to

Assignment: TSF data	Assignment: Restrictions
	FIA_UAU.5(2) in the Personalization phase
TSF execution code and IC chip setting the value for the patch	Authorized Personalization agent according to FIA_UAU.5(2) in the Personalization phase
BAC authentication key	TSF

FMT_MTD.1(4) Management of TSF data (lifecycle of TOE and PAC authentication key management)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to *change* the [PAC authentication key, lifecycle of TOE in the Personalization Phase] to [**Authorized Personalization agent FIA_UAU.5(2).2**]

Application Notes: The initial PAC authentication key is stored in ROM during the Manufacturing phase.

FMT_MTD.1(5) Management of TSF data(internal change of lifecycle)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to *change* the [lifecycle of the TOE in the Personalization phase] to [TSF].

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

b) A function to verify and update the CVCA Certificate, CVCA digital signature verification key and current data in the Operational Use phase

c) [A function to manage the TSF security: a function to verify the Security Attributes and SSC initialization, random number reuse,

d) A function to initialize personalization EEPROM in the Personalization phase,

e) A function to manage personalization and management: a function to change the lifecycle, function to patch the execution code and data, a function to unblock, a function to update the PAC key, and a function to inactivate writing in the Personalization phase]]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1. The TSF shall maintain the following roles: [

a) **Authorized Personalization agent to update the PAC authentication key of the PAC in the Personalization phase**

Authorized Personalization agent to change the lifecycle in the Personalization phase

Authorized Personalization agent for Unblock operations in the Personalization phase

Authorized Personalization agent for patching of the execution code and data patch in the Personalization phase

b) [None]]

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

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

5.1.5 TSF Protection

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model

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

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

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

c) [When the Operational mode is in InitAuth or SecondAuth mode and when the PAC secure channel is terminated]

]

FPT_ITC.1 Confidentiality of Inter-TSF

Hierarchical to: No other components.

Dependencies: No other components.

FPT_ITI.1.1. The TSF shall protect against the unauthorized disclosures for all TSF transmitted between TSF and reliable IT products.

Application Notes: All TSF transmitted between TOE and the external agents have to be encrypted.

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 the 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 BAC secure messaging or EAC secure messaging

b) Deletion of the BAC session key or the EAC session key

c) Management action specified in FMT_MSA.1

d) Termination of the PAC secure messaging and deletion of the PAC session key

e) [None]

] if modifications are detected

Application Notes: The strength of the Retail MAC is equivalent to the secure Retail MAC specified in FCS_COP.1(2).

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Application Notes: The TOE consists of eight lifecycles, and each lifecycle consists of a suitable command.

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: FPT_AMT.1 Abstract machine testing

FPT_TST.1.1. The TSF shall run a suite of self tests [*before executing the TSF*] 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 **an authorized Personalization agent** with the capability to verify the integrity of stored TSF executable code.

5.2 Security Requirements for the IT environment

This section describes the security functional requirements for the IT environment.

(Table 166) Security requirements for the IT environment

Security functional class	Security functional component	
Cryptographic Support (FCS)	FCS_CKM.1(2)	Cryptographic key generation (PAC session key)
	FCS_COP.1(1)	Cryptographic operation (Symmetric Key Cryptographic Operation)
	FCS_COP.1(2)	Cryptographic operation (MAC)
	FCS_COP.1(3)	Cryptographic operation (HSAH Function)
	FCS_COP.1(4)	Cryptographic operation (Digital signature Verification for Certificates Verification)
	FCS_COP.1(5)	Cryptographic operation (Digital signature generation)
Privacy (FPR)	FPR_UNO.1	Unobservable

FCS_CKM.1(2) Cryptographic key generation (PAC session key)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_CKM.1.1. The TSF shall generate **PAC encryption keys and MAC keys** in accordance with a specified cryptographic key generation algorithm [none] with a specified cryptographic key size [112 bits] that meets the following: [none].

Application Notes: According to FCS_CKM.2(3) encryption key distribution, the TSF performs TDES-based encryption after distributing seed values. And the TSF then generates PAC session encryption key and MAC key.

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

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

Application Notes: The TOE uses the TDES cryptographic algorithm of Certified IC chip for the confidentiality protection of the transmitted data of the BAC or EAC secure messaging, for the BAC mutual authentication, and for the BAC key distribution. For the operation mode of the cryptographic algorithm used, the CBC mode with IV=0 as defined in ISO/IEC 10116 is used.

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

FMT_MSA.2 Secure security attributes

FCS_COP.1.1. The TSF shall perform [a MAC operation] in accordance with a specified cryptographic algorithm [*Retail MAC*] with a cryptographic key size [*112 bits*] that meets the

following: [*ISO/IEC 9797-1*].

Application Notes: The TOE uses the Retail MAC algorithm of the Certified IC chip to protect the integrity of the transmitted data of the PAC, BAC or EAC secure messaging and for BAC mutual authentication.

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

FMT_MSA.2 Secure security attributes

FCS_COP.1.1. The TSF shall perform [a HASH operation] in accordance with a specified cryptographic algorithm [*SHA-1, SHA-224, SHA-256*] with a cryptographic key size [*none*] that meets the following: [*FIPS PUB 180-2*].

Application Notes: In case of LC chip, the TOE utilizes SHA-1, SHA-224 or SHA-256 algorithms supported by IC chip during ECDSA operation of EAC-TA authentication.

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1. The TSF shall perform [Digital signature Verification] in accordance with a

specified cryptographic algorithm [*ECDSA-SHA-1, ECDSA-SHA-224, ECDSA-SHA-256 / RSASSA-PKCS1-V1.5-SHA-1, RSASSA-PKCS1-V1.5-SHA-256*] with a cryptographic key size [224 bits, 256 bits / 1024 bits, 2048 bits] that meets the following: [*ISO/IEC 15946-2 / PKCS#1*].

Application Notes: The TOE utilizes the RSA library if RSA algorithm is used for EAC security mechanism. In case of LC chip, the TOE utilizes the ECC library if ECC algorithm is used for EAC security mechanism.

FCS_COP.1(5) Cryptographic operation (Digital Signature Generation)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1. The TSF shall perform [Digital signature generation] in accordance with a specified cryptographic algorithm [*RSASSA-PKCS1-v1.5-SHA-256*] and cryptographic key size [1024 bits, 2048 bits] that meets the following: [*PKCS#1*]

Application Notes: The TOE utilizes the RSA library for the AA digital signature algorithm and the algorithms specified in the RSA library are used for the AA security mechanism.

FPR_UNO.1 Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) FCS_COP.1(1) A cryptographic operation (Symmetric Key Cryptographic Operation)

b) FCS_COP.1(2) A Cryptographic operation (MAC)

c) FCS_COP.1(4) A cryptographic operation (Digital signature Verification for Certificates Verification)

d) FCS_COP.1(5) A cryptographic operation (Digital signature Generation)

] on the following:[

a) BAC authentication key

b) BAC session key

c) EAC session key

d) EAC chip authentication private key

e) [AA Private key

PAC authentication key

PAC session key]]

Application Notes: An external entity may discover and exploit the cryptographic-related data from physical phenomena (change of current, voltage and electromagnetic, etc.) that occur when the TSF performs cryptographic operations. The TSF provides the means to handle attacks such as DPA and SPA.

5.3 Security Assurance Requirements

The security assurance requirements for this Security Target consist of the components from Part 3 of the CC summarized in (Table 16). The evaluation assurance level is EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.4).

The assurance components are augmented follows:

- ADV_IMP.2 Implementation of the TSF
- ATE_DPT.2 Testing: low-level design
- AVA_VLA.4 High-level resistant

(Table 177) Security Assurance Requirements

Assurance class	Assurance component	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	N/A ※ Installation, generation, and start-up procedures for this TOE are not required.
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	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: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.4	High-level resistant

This page left blank on purpose for double-side printing

6. TOE Summary Specification

This chapter describes the TOE Security Functions and the Assurance Measures covering the requirements of the previous chapter.

6.1 Security Functions

This chapter gives an overview of the TOE Security Functions composing the TSF.

In the following table, all TOE Security Functions are listed and if appropriate, a SOF claim is stated.

(Table 188) TOE security functions

Security Functions	SOF	Description
SF.MUT_AUTH	high	PAC mutual authentication, PAC session key generation, PAC personalization and management authentication, BAC mutual authentication
SF.CHIP_AUTH	high	EAC-CA authentication
SF.TERMINAL_AUTH	high	EAC-TA authentication
SF.SEC_MESSAGE	-	Secure messaging structure, Secure communication channel mechanism.
SF.ACTIVE_AUTH	high	AA authentication
SF.ACC_CONTROL	high	Personalization Agent access control, Personalization Agent personalization and management Inspection System access Control
SF.RELIABILITY	high	Residual Information management, Vulnerability countermeasure, TSF self test, Data integrity, TSF domain separation

6.2 SF.MUT_AUTH (PAC security mechanism, BAC security mechanism)

This security function includes a PAC security mechanism for the Personalization agent and a BAC security mechanism for the Inspection System.

The PAC security mechanism provides authority control of the security role to the Personalization

agent in the issue stage. This security function is composed of PAC mutual authentication, PAC session Key generation, and PAC personalization and management authentication.

The BAC security mechanism (Basic Access Control) provides confidentiality and integrity for the personal data of the ePassport holder via secure messaging when controlling access to the personal data of the ePassport holder records in the TOE and transmitting it to the Inspection System with read-rights. This security function is composed of BAC mutual authentication and session Key generation.

6.3 SF.CHIP_AUTH

This security function implements EAC-CA authentication. It includes the ephemeral-static EC Diffie-Hellman key distribution protocol which provides the Inspection System with the generation of the EAC session key for a secure communication channel between the TOE and the Inspection System.

6.4 SF.TERMINAL_AUTH

This security function implements EAC-TA authentication. The EAC-TA is used by the TOE to implement a challenge-response authentication protocol based on the digital signature to authenticate the EAC-supporting Inspection System.

6.5 SF.SEC_MESSAGE

This security function provides a secure communication channel to protect the command message (C-APDU) and response message (R-APDU) between the TOE and the Personalization agent or the Inspection System.

6.6 SF.ACC_CONTROL

This security function provides access control and management of the TOE. The TOE provides access control rules and management functions for the MRTD application data based on security.

6.7 SF.ACTIVE_AUTH

This security function provides an AA mechanism with which the TOE verifies that the MRTD chip is genuine to the IS by signing the random number transmitted from the IS; the IS verifies the authenticity of the MRTD chip through verification with the signed values.

6.8 SF.RELIABILITY

This security function executes the residual information management and vulnerability countermeasures of the TOE, TSF self-test, data integrity and TSF domain separation.

6.9 Assurance Measures

(Table 199) Assurance Measures

Assurance component		Assurance Measures
ACM_AUT.1	Partial CM automation	EPS-02-QT-ACM-1.2
ACM_CAP.4	Generation support and acceptance procedures	EPS-02-QT-ACM-1.2
ACM_SCP.2	Problem tracking CM coverage	EPS-02-QT-ACM-1.2
ADO_DEL.2	Detection of modification	EPS-02-QT-ADO-1.1
ADO_IGS.1	Installation, generation, and start-up procedures	N/A ※ Installation, generation, and start-up procedures for this TOE are not required.
ADV_FSP.2	Fully defined external interfaces	EPS-02-DG-FSP-1.4
ADV_HLD.2	Security enforcing high-level design	EPS-02-DG-HLD-1.3
ADV_IMP.2	Implementation of the TSF	EPS-02-IM-IMP-1.2
ADV_LLD.1	Descriptive low-level design	EPS-02-DG-LLD-1.2
ADV_RCR.1	Informal correspondence demonstration	EPS-02-AN-ST-1.4 EPS-02-DG-FSP-1.4 EPS-02-DG-HLD-1.3 EPS-02-IM-IMP-1.2 EPS-02-DG-LLD-1.2

Assurance component		Assurance Measures
ADV_SPM.1	Informal TOE security policy model	EPS-02-AN-SPM-1.1
AGD_ADM.1	Administrator guidance	EPS-02-QT-AGD_ADM-1.2
AGD_USR.1	User guidance	EPS-02-QT-AGD_USR-1.2
ALC_DVS.1	Identification of security measures	EPS-02-QT-ALC-1.2
ALC_LCD.1	Developer defined life-cycle model	EPS-02-QT-ALC-1.2
ALC_TAT.1	Well-defined development tools	EPS-02-QT-ALC-1.2
ATE_COV.2	Analysis of coverage	EPS-02-TS-ATE-1.2
ATE_DPT.2	Testing: low-level design	EPS-02-TS-ATE-1.2
ATE_FUN.1	Functional testing	EPS-02-TS-ATE-1.2
ATE_IND.2	Independent testing - sample	N/A
AVA_MSU.2	Validation of analysis	EPS-02-TS-MSU-1.1 EPS-02-QT-AGD_USR-1.2 EPS-02-QT-AGD_ADM-1.2
AVA_SOF.1	Strength of TOE security function evaluation	EPS-02-TS-SOF-1.1
AVA_VLA.4	High-level resistant	EPS-02-TS-VLA-1.1

7. Acceptance of Protection Profile

This chapter describes the Protection Profile accepted in the Security Target, reconstruction, and additional articles.

7.1 Reference of Protection Profile

This Security Target accepts the security and assurance requirements of the Protection Profile, as follows:

- "Protection Profile V1.0"(KECS-PP-0084-2008)

7.2 Reconstruction of Protection Profile

This Security Target contains the reconstructed T.Residual Information and A.Inspection System, the security objectives O.Session Terminate and O.Handling Information Leakage, and the security objective for environment OE.ePassport Personalization agent. The security functional requirements are reconstructed.

7.3 Additional components of Protection Profile

This Security Target has added the following security environments, security objectives and security functional requirements to supplement the PAC and AA authentication function in ePassport Protection Profile V1.0.

This page left blank on purpose for double-side printing

8. Rationale

This chapter describes the rationale of Security Objectives and Security Requirements based on Security Environments (Assumptions, Threats, and Organizational Security Policies). The rationale demonstrates that the TOE supports efficient IT Security Countermeasures in Security Environments.

8.1 Rationale of Security Objectives

The Rationale of the Security Objectives demonstrates that the specified Security Objectives are appropriate, and that they can sufficiently trace security problems. It also shows that they are essential and not excessive.

The Rationale of the 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 20) shows the mapping between security environments and security objectives.

(Table 20) Mapping between Security Environments and Security Objectives

Security Objectives / Security Environment	TOE Security Objectives	Security Objectives for Environment

Security Objectives / Security Environment	O.Management	O.Security Mechanism Application Procedures	O.Session Termination	O.Secure Messaging	O.Domain Separation	O.Certificate Verification	O.Self protection	O.Deleting residual Information	O.Replay Prevention	O.Access Control	O. A A	O. B A C	O. E A C	O. P A C	OE.Passport Book Manufacturing Security	OE.Procedures of Passport Holder Check	OE.Application Program Loading	OE.Certificate Verification	OE.Personalization Agent	OE.Handling Residual Information	OE.Inspection System	OE.IC Chip	OE.MRZ Entropy	OE.PKI	OE.Range of RF Communication
T.Application Program Interference					X												X								
T.TSF Data Modification	X		X	X	X					X				X					X						
T.Disguise of Personalization Agent														X											
T.Eavesdropping				X																	X				
T.Forgery and Corruption of Personal Data			X							X		X									X				
T.BAC Authentication Key Disclose	X		X					X		X						X									
T.BAC Replay Attack									X																
T.Damage to Biometric Data			X	X		X				X			X					X			X			X	
T.EAC-CA Bypass		X				X										X		X			X				
T.IS Certificate Forgery	X				X	X												X							
T.Session Data Reuse									X												X				
T.Skimming										X		X	X								X				X
T.Malfunction							X															X			
T.Leakage to Cryptographic Key Information																				X		X			
T.ePassport Reproduction					X										X	X									
T.Replacement of ePassport IC Chip					X						X														
T.Residual Information								X																	
P.International Compatibility																			X						
P.Security Mechanism Application Procedures		X																			X				
P.Application ProgramLoading																	X								
P.Personalization Agent	X													X					X						
P.ePassport Access Control	X									X		X	X	X					X		X				
P.PKI						X																		X	
P.Range of RF Communication																									X
A.Certificate Verification																		X	X					X	
A.Inspection System																					X				
A.IC Chip																						X			
A.MRZ Entropy																							X		

8.1.1 Rationale of TOE Security Objectives

O. Management

This security objective ensures that the TOE provides the means to write user data in the EF domain, the means to write TSF data in secure memory, and the means to store the BAC authentication key in secure memory only to the authorized Personalization agent in the Personalization phase. It also prevents unauthorized access using an external interface by deactivating the MRTD application data writing function of the Personalization agent in the Operational Use phase. Therefore, this Security Objective is required to counter the threats of T. TSF Data Modification and T. BAC Authentication Key Disclose. It enforces the organizational security policies of P. ePassport Access Control and P. Personalization Agent to prevent the forgery and corruption of the user data and the Security Function through abuse of the functions related to personalization.

In addition, this security objective provides the Personalization agent with the means to record the CVCA Certificate in secure memory in the Personalization phase. Therefore, this objective is required to counter the threat of T. IS Certificate Forgery.

O. Security Mechanism Application Procedures

This security objective is required to enforce the organizational security policies of the P.Security Mechanism Application Procedures, as the TOE ensures that the application order of the PA, AA, BAC and EAC security mechanisms according to the 2.1.1 Standard ePassport Inspection Procedure and the 2.1.2 Advanced ePassport Procedure of the EAC specification by not allowing requests from the Inspection System that does not correspond to the security mechanism application order.

In addition, this security objective is required to counter T. EAC-CA Bypass threats by eliminating cases in which the genuine TOE is shown to an unauthorized Inspection System, as it ensures the application order of security mechanisms so as to enable EAC-CA executions by only an Inspection System with access rights to the EAC chip authentication public key through the BAC execution.

O.Session Termination

This security objective prevents the attacker to attempt continuous authentication who tries to forge and corrupt the personal or biometric data of the ePassport holder. In addition, the TOE

terminates the session when it detects any modification of the transmitted TSF data. Therefore, this security objective is required to counter the threats T. Forgery and the Corruption of Personal Data, T. Damage to Biometric Data, T. BAC Authentication Key Disclosure and T. TSF Data Modification. Moreover, this security objective is required to counter the threat of T. Eavesdropping and T. Damage to the Biometric Information, as the user data for ePassport Personalization is transmitted using the PAC secure channel when it is written in the TOE.

O. Secure Messaging

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

O. Domain Separation

This security objective is required to counter the threat of T. Application Program Interference because the TOE provides the means to prevent interference and tampering by the external IT entities through the separation of the execution domains between the TSF loaded in the MRTD chip and other application programs.

This security objective is required to counter the threat of T. TSF Data Modification by preventing TSF data modification, as the COS blocks access by the external entities when the TOE records the TSF data in secure memory.

This security objective is required to counter the threat of T. IS Certificate Forgery by protecting the CVCA certificate recorded by the Personalization agent in secure memory to detect forgery of the CVCA link certificate via external interference and tampering.

This security objective is required to counter the threat of T. ePassport Reproduction and T. Replacement of the ePassport IC Chip because reproduction of the TSF data stored in secure memory is not possible, even when an attacker reproduces the user data in the EF domain by manufacturing an illegal chip.

O. Certificate Verification

This security objective is required to enforce the organizational security policies of P. PKI as it enables the TOE to check for a valid date on the basis of the CVCA link certificate provided by the Inspection System and therefore to update the certificate and the current date automatically.

This security objective is required to counter the threats of T. Damage to Biometric Data and T. IS Certificate Forgery by determining the presence of forgery as the TOE verifies the validity of the CVCA Link Certificate, the DV Certificate and the IS Certificate in the EAC-TA.

O. Self-protection

This security objective is required to counter the threat of T. Malfunction as the TOE detects modification of the TOE executable code and data through self-testing. It also provides the means to prevent TOE security function bypassing attempts and protects the TOE itself by preserving a secure state so that malfunction of the TSF does not occur.

O. Deleting Residual Information

This security objective is required to counter the threat of T. Residual Information, as the TOE deletes all the previous security-related information (including the BAC session key and the EAC session key) so that this information is not included and becomes unavailable when allocating or deallocating memory resources.

This security objective is required to counter the threat of T. BAC Authentication Key Disclosure by providing the means to ensure that the residual information remaining in the temporary memory is not available.

O. Replay Prevention

This security objective is required to counter the threat of T. BAC Replay Attack by ensuring that the TOE generates different values per session when the values are transmitted to the Inspection System during the BAC mutual authentication process. This security objective is also required to counter the threat of T. Session Data Reuse by ensuring that the different random numbers are generated and used for each session of the security mechanism, as the TOE ensures that the BAC authentication key is not used as the BAC session key during the BAC mutual authentication process. It also ensures that the BAC session key is not generated with the same random number

used in the BAC mutual authentication process and checks the replay status of the random number transmitted by the EIS in the EAC.

O. Access Control

This security objective is required to counter the threats of T. Forgery and Corruption of Personal Data, T. Damage to Biometric Data and T. Skimming and enforce the organizational security policies of P. ePassport Access Control by implementing the rules of allowing or denying the Inspection System to read user data in accordance with the ePassport access control policies by the Personalization agent.

This security objective allows read-rights and write-rights of ePassport user data in the Personalization phase and enforces the organizational security policies of P. ePassport Access Control by simply approving specific functions according to the Security role of the Personalization agent.

This security objective enforces the organizational security policies of P. ePassport Access Control by controlling each issuing management function after departmentalizing the role of the Personalization agent in accordance with the PAC authentication key in the Personalization phase.

O. AA

This security objective is required to counter the threats of T. Replacement of the ePassport IC Chip by implementing the AA security mechanism so that the Inspection System can verify the genuineness of the IC chip TOE is embedded.

O. BAC

This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the BAC security mechanism to control access to the personal data of the ePassport holder. It thus gives read-rights of the personal data of the ePassport holder only to an authorized Inspection System for which the BAC mutual authentication is successfully completed.

This security objective is required to counter the threats of T. Forgery and Corruption of Personal Data and T. Skimming as the TOE allows read-rights of the personal data of the ePassport holder only to an authorized Inspection System by generating the BAC session key during the BAC

mutual authentication. It also denies access for an Inspection System that does not have read-rights.

O. EAC

This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the ePassport holder. It therefore gives read-rights of the biometric data of the ePassport holder only to an authorized Inspection System for 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 read-rights of the biometric data of the ePassport holder only to an authorized Inspection System through the EAC-TA by generating the EAC session key during the EAC-CA and denies access by an Inspection System that does not have read-rights.

This security objective enforces the organizational security policies of P. ePassport Access Control as the access right is assigned in accordance with the PAC authentication key; specific functions can only be performed by an authorized Personalization agent for which PAC is successfully completed.

O. PAC

This security objective is required to enforce the organizational security policies of the P. ePassport Access Control and P. Personalization Agent as the TOE implements PAC mutual authentication and PAC issuing management authentication to assign the ePassport issuing functionality to the authorized Personalization agent only and the issuing right regarding each functionality of the Personalization agent, such as updating of the PAC authentication key, modification of the life cycle, patch, and unblocking in accordance with the PAC authentication key.

This security objective is required to counter the threats of T. modification of the TSF data and T. Disguise of the Personalization Agent, as the TOE only allows access for an authorized Personalization Agent for which PAC mutual authentication is successfully completed. Secure communication between the TOE and the Personalization Agent is performed using the PAC session key generated.

8.1.2 Rationale of Security Objective for Environment

OE. Passport Book Manufacturing Security

This security objective for the 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 attempts of the Grandmaster chess, replacement of the portrait, and modification of the MRZ data, among others.

OE. Procedures of Passport Holder Check

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

OE. Application Program Loading

This security objective for the environment is required to enforce the organizational security policies of P. Application program loading by ensuring that only the application programs are loaded to the MRTD chip in a secure manner by the Personalization agent.

This security objective for the environment is required to counter the threat of T. Application Program Interference by providing the means to prevent interference and tampering with the TSF as an attacker loads any application program onto the IC chip through the restriction that stipulates that only the authorized Personalization agent can load application programs.

OE. Certificate Verification

This security objective for the environment verifies the SOD after regularly verifying the DS certificate and CRL so that the Inspection System of the BIS and EIS can verify against forgery and corruption of the ePassport identity data recorded in the TOE. This security objective for the environment also ensures that the EIS securely maintains the digital signature generation key that corresponds to the IS certificate and provides the TOE with the CVCA Link Certificate, DV Certificate and IS Certificate in the EAC-TA. Therefore, this security objective for the environment is required to counter the threats of T. Damage to Biometric Data, T. EAC-CA Bypass and T. IS

Certificate Forgery and is required to 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 the writing function. This security objective for the environment also is required to enforce the organizational security policies of P. ePassport Access Control as it defines the role of the Personalization agent. It is also required to support the assumption of A. Certificate Verification because the Personalization agent makes certificates necessary for PA and EAC support available to the Inspection System.

This security objective for the environment is required to counter the threat of T. TSF Data Modification because the Personalization agent deactivates the writing function in the Operational Use phase, thereby disabling the writing function for modification of the TSF data.

OE.Handling Information Leakage

This security objective for the environment is required to counter the threat of T. Leakage of the Cryptographic Key Information as the TOE provides the means to prevent the analysis of the leakage information (electric power, wave, and other information) during cryptographic operations and prevents the key information from being obtained.

OE. Inspection System

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

This security objective for the environment is required to counter the threat of T. Eavesdropping, as the confidentiality and integrity of the transmitted data are ensured by establishing BAC secure

messaging after the generation of the BAC session key through the BAC key distribution when the Inspection System communicates with the TOE.

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

This security objective for the environment is required to counter the threat of T. Session Data Reuse as the Inspection System generates a different temporary public key per session and transmits it to the TOE in the EAC-CA.

OE. IC Chip

This security objective for the environment is required to support the assumption of the A. IC Chip as it uses the EAL5+ IC chip that generates the random number and provides the cryptographic operation to support the security functions of the TOE. This also provides the malfunction detection and physical protection other operations.

This security objective for the environment is also required to counter the threat of T. Malfunction as the IC chip detects malfunctions outside the normal operating conditions.

It is also required to counter the threat of T. Leakage of the Cryptographic Key Information as the IC chip performs the TDES, Retail MAC, and ECC cryptographic operations and supports DPA/SPA countermeasures.

OE. MRZ Entropy

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

OE. PKI

This security objective for the environment is required to enforce the organizational security policies of P. PKI and supports the assumption of A. Certificate Verification by implementing and operating the ePassport PKI System that executes the certification practice according to the Certification Practice Statement (CPS). These operations include generating a digital signature

key and generating, issuing, and distributing the certificates necessary in support of the PA and EAC security mechanisms.

This security objective for the environment is also required to counter the threat of T. Damage to Biometric Data by generating, issuing and distributing the certificates necessary in the EAC through implementation of the EAC-PKI.

OE. Range of RF Communication

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

8.2 Rationale of Security Requirements

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

8.2.1 Rationale of Security Functional Requirements

The rationale of the security functional requirements demonstrates the following:

• 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 21) presents the mapping between the security objectives and the security functional requirements.

(Table 21) Mapping between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	O.Management	O.Security Mechanism Application Procedures	O.Session Termination	O.Secure Messaging	O.Domain Separation	O.Certificate Verification	O.Self Protection	O.Deleting Residual Information	O.Replay Prevention	O.Access Control	O.AA	O. BAC	O. EAC	O. PAC
FCS_CKM.1(1)												X	X	
FCS_CKM.2(1)									X			X		
FCS_CKM.2(2)													X	
FCS_CKM.2(3)									X					X
FCS_CKM.4								X						
FCS_COP.1(3)							X				X	X	X	
FDP_ACC.1										X				
FDP_ACF.1	X	X								X		X	X	X
FDP_DAU.1											X			
FDP_RIP.1								X	X					
FDP_UCT.1				X					X					
FDP_UIT.1				X					X					
FIA_AFL.1		X	X							X		X	X	X
FIA_UAU.1(1)			X							X		X		
FIA_UAU.1(2)		X	X							X			X	
FIA_UAU.1(3)			X							X				X
FIA_UAU.1(4)			X							X				X
FIA_UAU.4									X		X	X	X	X
FIA_UAU.5(1)		X								X		X	X	
FIA_UAU.5(2)										X				X
FIA_UID.1											X	X	X	X
FMT_MOF.1(1)	X									X				X
FMT_MOF.1(2)	X									X				X
FMT_MSA.1				X						X				
FMT_MSA.3	X									X				X
FMT_MTD.1(1)	X									X				X
FMT_MTD.1(2)		X												
FMT_MTD.1(3)	X									X				
FMT_MTD.1(4)	X									X				X
FMT_MTD.1(5)	X									X				X
FMT_MTD.3						X			X				X	
FMT_SMF.1	X					X								
FMT_SMR.1	X													
FPT_AMT.1							X							
FPT_FLS.1							X							
FPT_ITI.1			X	X										
FPT_SEP.1					X					X				
FPT_TST.1							X							

FCS_CKM.1(1) Cryptographic Key Generation (Key Derivation Mechanism)

This component requires generation of the 112-bit BAC authentication key, the 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 process, and the BAC/EAC session key is generated for use in the BAC/EAC secure messaging. Therefore, this component satisfies the security objectives of O.BAC and O.EAC.

FCS_CKM.2(1) Cryptographic Key Distribution (KDF Seed Distribution for BAC Session Key Generation)

This component defines the method to distribute the seed of the 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 generation of the BAC session key of FCS_CKM.1(1) by generating the KDF seed.

FCS_CKM.2(2) Cryptographic Key Distribution (KDF Seed Distribution for EAC Session Key Generation)

This component defines the method of distributing the seed of the key derivation mechanism necessary in generating the EAC session key to the Inspection System (ECDH key distribution protocol).

The distribution method defined in this component satisfies the security objective of O.EAC as it enables the generation of the EAC session key of FCS_CKM.1(1) by generating the KDF seed.

FCS_CKM.2(3) Cryptographic Key Distribution (Seed Distribution for PAC Session Key Generation)

This component is an additional key derivation mechanism and defines the method to distribute the seed of the key derivation mechanism necessary in generating the PAC session key to the Inspection System.

This component defines a method to distribute the seed values necessary to generate the PAC session key to the Personalization Agent as a key-derivation mechanism is developed by itself.

The distribution method defined in this component satisfies the security objective of O.Replay Prevention as it uses random numbers and O. PAC as it enables the generation of the PAC session key of FCS_CKM.1(2) by generating the seed.

FCS_CKM.4 Cryptographic Key Destruction

This component defines the method to destroy the key generated by key derivation mechanism of FCS_CKM.1(1) and FCS_CKM.1(2) securely.

This component satisfies the security objective of O. Deleting Residual Information as it provides the method of destroying the key generated by the TSF and that which remains in temporary memory via its defined method.

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

This component defines the SHA-1 hash function necessary in KDF implementation according to FCS_CKM.1(1) and the SHA-256 hash function necessary in RSA digital signature algorithm implementation according to FCS_COP.1(5). This component also defines the SHA-224 hash function necessary in the ECDSA digital signature algorithm implementation according to FCS_COP.1(4) and the SHA-1 hash function necessary in generating the BAC authentication key and verifying the integrity of the executable code.

The hash function defined in this component satisfies the security objective of O. BAC, O. EAC, and O. AA as it enables the KDF to generate the BAC authentication key, the BAC and the EAC session key. It also supports the RSA digital signature necessary in the AA authentication process and the ECDSA digital signature necessary in the EAC-TA authentication process.

FDP_ACC.1 Subset Access Control

This component defines the list of subjects, objects and operations to determine the scope of control for the ePassport access control policies.

The ePassport access control policies defined in this component satisfy the security objective of O. Access Control because they define the Personalization agent, BIS and EIS as subjects and the personal data and biometric data of the ePassport holder and ePassport authentication data objects. They also define their relationships as operations.

FDP_ACF.1 Security Attributes based Access Control

To enforce the ePassport access control policies, this component defines the security attributes of the subjects and objects defined in FDP_ACC.1 and specifies the ePassport access control rules.

The security attributes and the ePassport access control rules defined in this component satisfy the security objectives of O. Management and O. Access Control because only an authorized Personalization agent with a Personalization agent issuing authorization can perform management functions.

This component also satisfies the security objectives of O. BAC, O. EAC, O. PAC and O. Access Control because the read-rights of the personal data of the ePassport holder and ePassport authentication data are allowed only to subjects holding BAC authorization, read-rights of the biometric data of the ePassport holder are allowed only to subjects holding EAC authorization, and the issuing rights for ePassport personalization are allowed only to subjects holding PAC authorization.

The explicit deny rules of FDP_ACF.1.4 defined in this component satisfy the security objective of the O. Security Mechanism Application Procedures because the application order of the security mechanisms is ensured; access by the Inspection System is denied when the order of the transmitted instructions specified in the Inspection Procedures in 2.1 of the EAC specifications are violated.

FDP_DAU.1 Basic Data Authentication

This component supports the ability to generate the evidence used for ensuring the validity of the genuineness of the MRTD IC chip and stipulates that it has to be supported to the BIS and EIS, which can verify the validity of the indicated information.

To demonstrate to the Inspection System that this ePassport was justifiably issued by the Personalization Agent, the TOE provides proof of the genuineness of the MRTD IC chip by verifying that the AA security mechanism is implemented and the validity of the AA private key is guaranteed. Therefore, this component satisfies the security objective of O. AA.

FDP_RIP.1 Subset Residual Information Protection

This component ensures that previous information is not included when the TSF allocates or deallocates memory resources for the BAC authentication key, BAC session key, EAC session key, PAC session key, PAC authentication key, AA private key, EAC chip authentication private key, CVCA digital signature verification key, and domain information.

This component satisfies the security objective of O. Deleting Residual Information as it ensures that previous information of the BAC authentication key, BAC session key, EAC session key, PAC session key, PAC authentication key, AA private key, EAC chip authentication private key, CVCA

digital signature verification key, and domain information are not available when these keys are destroyed according to the method of destruction defined in FCS_CKM.4. This component also satisfies the security objective of O. Replay Prevention by ensuring that the previous information pertaining to the random numbers used for the PAC mutual authentication, PAC issuing management authentication, BAC mutual authentication, AA authentication, EAC-TA, and generation of the session key is not available.

FDP_UCT.1 Basic Data Exchange Confidentiality

This component defines the method to protect from disclosure when transmitting objects information 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 as it is transmitted between the TOE and the Inspection System with the BAC session encryption key. This is also done for the biometric data of the ePassport holder as it is transmitted between the TOE and the Inspection System with the EAC session encryption key. This component also establishes PAC secure messaging by performing cryptographic operations for data such as the ePassport applicable data as it is transmitted between the TOE and the Inspection System with the PAC session encryption key. Therefore, this component satisfies the security objective of O. Secure Messaging as the confidentiality of user data is ensured.

This component satisfies the security objective of O. Replay Prevention both by ensuring that the BAC session encryption key used is not identical to the BAC authentication key when BAC secure messaging is established and by ensuring that the PAC session encryption key used is not identical to the PAC authentication key when PAC secure messaging is established.

FDP_UIT.1 Data Exchange Integrity

This component defines the protection method against modification, deletion, and insertion when transmitting information 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 BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder as it is transmitted between the TOE and the Inspection System with the BAC session MAC key. This is also done for the biometric data of the ePassport holder as it is transmitted between the TOE and the Inspection System with the

EAC session MAC key. This component also establishes PAC secure messaging by performing cryptographic operations for the ePassport applicable data as it is transmitted between the TOE and the Inspection System with the PAC 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 both by ensuring that the BAC session MAC key used is not identical to the BAC authentication key when BAC secure messaging is established and by ensuring that the PAC session MAC key used is not identical to the PAC authentication key when PAC secure messaging is established.

FIA_AFL.1 Authentication Failure Handling

If the authentication attempt failure number of the BAC mutual authentication, PAC mutual authentication, PAC issuing management authentication and EAC-TA is surpassed, this component detects it and requires termination of the user session and modification of the life cycle.

This component satisfies the security objective of O. Session Termination as the session is terminated if the authentication attempt failure number of the BAC mutual authentication, PAC mutual authentication, PAC issuing management authentication and EAC-TA integrity verification is surpassed. This component also satisfies the security objective of the O. Security Mechanism Application Procedures by preventing the unauthorized external entity from moving to the next phase of the inspection procedures by terminating the session if the BAC mutual authentication fails.

This component satisfies the security objective of O. PAC as the session is terminated. The life cycle is modified if the authentication attempt failure number of the PAC mutual authentication and PAC issuing management authentication is surpassed.

In addition, this component satisfies the security objectives of O. BAC, O. EAC and O. Access Control because access to user data is denied by session termination as BAC mutual authentication or EAC-TA failure indicates no access rights for user data.

FIA_UAU.1(1) Authentication (BAC Mutual Authentication)

This component defines the user functions to be performed before BAC mutual authentication and executes BAC mutual authentication for the user.

In this component, BAC mutual authentication is executed to enable the Inspection System identified in FIA_UID.1 to execute the indication function to support the BAC mechanism and to

read the personal data of the ePassport holder. This component satisfies the security objectives of O. Session Termination, O. BAC and O. Access Control, as it enables detection of whether authentication fails through FIA_AFL. 1 and allows read-rights to the personal data of the ePassport holder if authentication succeeds.

FIA_UAU.1(2) Authentication (EAC-TA)

This component defines the user functions to be performed before the EAC-TA and executes the EAC-TA for user.

In this component, only the Inspection System for which BAC mutual authentication succeeds in FIA_UAU.1(1) can execute EAC-CA and the reading of the 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 Termination, O. EAC and O. Access Control, as it enables detection of whether authentication fails through FIA_AFL. 1 and allows read-rights to the biometric data of the ePassport holder if authentication succeeds.

FIA_UAU.1(3) Authentication (PAC Mutual Authentication)

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

In this component, the Personalization Agent must be allowed to obtain the CSN and Ticket before the PAC mutual authentication process. This component satisfies the security objectives of O. Session Termination, O. Access Control, and O. PAC, as it enables detection of whether authentication fails through FIA_AFL. 1 and allows the environment for PAC secure messaging if authentication succeeds.

FIA_UAU.1(4) Authentication (PAC Issuing Management Authentication)

This component defines the user functions to be performed before the PAC issuing management authentication process and executes PAC issuing management authentication for the Personalization Agent.

In this component, the Personalization Agent must be allowed to transmit a random number and execute PAC mutual authentication before the PAC issuing management authentication process.

This component satisfies the security objectives of O. Session Termination, O. Access Control, and O. PAC, as it enables detection of whether authentication fails through FIA_AFL.1 and allows issuing rights if authentication succeeds.

FIA_UAU.4 Single-use Authentication Mechanisms

This component requires that the authentication-related information sent by the TSF to the Inspection System during the PAC mutual authentication and the PAC issuing management authentication process is not replayed. It also requires that the authentication-related information sent by the TSF to the Inspection System during the BAC mutual authentication, the AA, and the EAC-TA process is not replayed.

This component satisfies the security objectives of O.Replay Prevention and O.PAC by performing PAC mutual authentication with a mechanism that prevents a replay of the random number used in PAC mutual authentication and the PAC personalization and management authentication processes.

This component satisfies the security objectives of O. Replay Prevention, O. BAC, O. AA, and O. EAC as the TSF executes BAC mutual authentication, AA, and EAC-TA by generating different random numbers that are used in BAC mutual authentication, AA and EAC-TA for each session and transmitting them to the Inspection System.

FIA_UAU.5(1) Multiple Authentication Mechanisms

This component defines multiple authentication mechanisms and the rules of applying the authentication mechanisms according to type of user data to be accessed by the Inspection System.

This component satisfies the security objectives of the O. Security Mechanism Application Procedures, O. Access Control, O. BAC and O. EAC as the Inspection System holds the BAC authorization process by succeeding in BAC mutual authentication and the EAC authorization process by succeeding in EAC-CA, EAC-TA and certificate verification after BAC mutual authentication according to the application rules of the authentication mechanism.

FIA_UAU.5(2) Multiple Authentication Mechanisms (PAC Mutual Authentication and PAC Issuing Management Authentication)

This component defines the PAC mutual authentication and PAC issuing management authentication mechanisms and the rules of applying the authentication mechanisms according to the type of issuing rights to be accessed by the Personalization agent.

This component satisfies the security objectives of O. Access Control and O. PAC as the Personalization Agent holds the issuing authorization by succeeding in the PAC mutual authentication and PAC issuing management authentication processes.

FIA_UID.1 Identification

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

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

FMT_MOF.1(1) Management of Security Functions Behavior

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

This component satisfies the security objectives of O. Management, O. Access Control and O. PAC by deactivating the writing function of the Personalization Agent in the Personalization phase and by modifying the life cycle to the Operational Use phase so that the TOE in the Operational Use phase cannot record any data. The writing function can be performed when the lifecycle of the TOE is in SecondAuth status. By performing PAC personalization and management (PAC-LifeCycle) authentication, the lifecycle of the TOE moves into StartIssue status to test the written data. After finishing the test, the lifecycle moves into Issued status to deactivate the writing function of the Personalization agent by performing PAC personalization and management (PAC-LifeCycle) authentication.

FMT_MOF.1(2) Management of Security Functions Behavior (Initialization)

This component stipulates that the initialization of TOE issuance, TOE re-issuance, and LDS file

system are performed only by an authorized Personalization Agent with issuing rights and that the initialization of the variables is performed only by TSF.

This component satisfies the security objectives of O.Access Control, O.Management, and O.PAC by ensuring that a file table and a data pointer are initialized and the lifecycle of the TOE, Empty status, moves into Unissue status by performing TOE issuance initialization. Additionally, the LDS file system and temporary memories are initialized.

FMT_MSA.1 Management of Security Attributes

This component requires restriction of the ability to initialize 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, O. Access Control, and O. PAC as only the authorized Personalization agent generates user data to enforce the ePassport access control policies in the Personalization phase. It also specifies the initial values to restrict the security attributes of the data.

FMT_MTD.1(1) TSF Management of TSF Data (Certification Verification Information)

This component stipulates the restriction in which only Personalization agents in the Personalization phase write the certificate verification information necessary for the EAC-TA in secure memory.

This component satisfies the security objectives of O. Management, O. Access Control, and O. PAC by enabling only an authorized Personalization agent to have the ability to write TSF data such as the EAC chip authentication private key, current data, CVCA Certificate and CVCA digital

signature verification key in secure memory in the Personalization phase.

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

This component requires termination of BAC secure messaging before EAC secure messaging is established.

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

FMT_MTD.1(3) Management of TSF Data (Writing Key)

This component stipulates a restriction in which only an authorized Personalization agent in the Personalization phase writes the AA private key, TSF executable code and IC chip RF settings in secure memory and that only the TSF writes the BAC authentication key in secure memory.

This component satisfies the security objective of O.Management and O.Access Control by stipulating a restriction in which only an authorized Personalization agent in the Personalization phase writes the AA private key, TSF executable code and IC chip RF settings in secure memory.

This component satisfies the security objective of O.Management and O.Access Control by stipulating a restriction in which only the TSF writes the BAC authentication key in secure memory.

FMT_MTD.1(4) Management of TSF Data (TOE Lifecycle and PAC Authentication Key Management)

This component stipulates a restriction in which only an authorized Personalization agent in the Personalization phase modifies the lifecycle of the TOE.

This component satisfies the security objective of O.Management, O.Access Control and O.PAC by stipulating a restriction in which only authorized Personalization agents in the Personalization phase modify the PAC authentication key and the TOE lifecycle.

FMT_MTD.1(5) Management of TSF Data (Internal Modification of TOE Lifecycle)

This component stipulates a restriction in which only the TSF modifies the lifecycle of the TOE.

This component satisfies the security objective of O.Management, O.Access Control and O.PAC by stipulating a restriction in which only the TSF modifies the lifecycle of the TOE according to the result after PAC mutual authentication, PAC issuing management authentication and the TOE initialization for personalization.

If the initialization command for personalization is performed by the Personalization agent, the lifecycle of the TOE moves from the Empty status to the Unissue status. If verification of the integrity of the executable code fails, the lifecycle of the TOE moves from Empty status to Discard status via the TSF. When the lifecycle of the TOE is InitAuth or SecondAuth status in the personalization phase, the lifecycle moves to Unissue status if a communication channel between the TOE and the inspection system becomes disconnected. The lifecycle changes from Unissue status into InitAuth status by the TSF, if PAC mutual authentication is performed successfully, and the lifecycle changes from InitAuth status to SecondAuth status if PAC personalization and management (PAC-KeyUpdate, PAC-LifeCycle, PAC-Patch) authentication is performed successfully in the personalization phase. If PAC mutual authentication or PAC personalization and management authentication fails three times, the lifecycle changes into Block status; if PAC-Unblock authentication fails three times, the lifecycle changes from Block status to Discard status.

FMT_MTD.3 Secure TSF Data

This component requires allowing only secure values as the TSF data to ensure secure random numbers by preventing replay of the random numbers and ensuring that certificates with valid and unexpired dates are used in EAC-TA. This component satisfies the security objective of O.Replay Prevention because only secure random numbers are used, which prevents a replay attack when the TSF generates the session key.

This component satisfies the security objective of O.Replay Prevention because the TSF uses only secure random numbers when performing PAC, BAC, EAC and AA authentication.

Additionally, the TSF compares the CVCA Link Certificate provided by the Inspection System with the CVCA Certificate stored in the TOE for verification of the IS Certificate used in the EAC-TA. If CVCA Certificate updating is necessary, the TSF internally updates the CVCA Certificate, the CVCA digital signature verification key, the current dates and EF.CVCA. Thus, it 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 executed successfully 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 the user data and the TSF data in the Personalization phase and the security management function of the TOE.

This component also 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 the current dates by itself in the Operational Use phase.

FMT_SMR.1 Security roles

This component defines the role of the Personalization agent to manage the MRTD application data.

This component satisfies the security objective of O. Management as it defines the role of the Personalization agent that has the rights for updating the PAC authentication key, modifying the lifecycle, unblocking and patching the executable code and the data in the Personalization phase.

FPT_FLS.1 Failure with preservation of the secure state

This component must preserve a secure state when different types of failure occur, such as the failure detected from the self-testing, abnormal operating conditions detected by the IC chip, or the condition in which the PAC secure channel disengages during the InitAuth or SecondAuth phase.

In this component, the TOE is safely preserved by changing the operational mode to a safe mode if the PAC secure channel is terminated when the operational mode of the TSF is in InitAuth or SecondAuth mode. The TOE initializes RAM and falls into ‘panic’ status if any failures of the TSF are detected by the IC chip. Additionally, the TOE is safely preserved by changing the operational mode to a safe mode if verification of the integrity of the executable code fails. Therefore, this component satisfies the security objective of O.Self-protection.

FPT_ITI.1 Inter-TSF detection of modification

This component requires detection modification of the transmitted TSF data and defines an action

to be taken if modifications are detected.

This component satisfies the security objectives of O. Secure Messaging and O. Session Termination by detecting modification of the transmitted TSF data in the Personalization and Operational Use phases and by performing a specified action, such as terminating the related communication channels, deleting the related session key and modifying the previous condition of PAC mutual authentication or PAC issuing management authentication while deleting the Personalization rights of the Personalization agent if modifications are detected.

FPT_RVM.1 Non-bypassability of the TSP

This component always requires invocation of the ePassport access control function as a reference monitor to protect the TSF from manipulating the operation and bypassing access control policy with untrusted subjects.

This component satisfies the security objectives of O. Self-protection and O. Access Control together with FPT_SEP.1 as the ePassport access control function is always invoked; therefore, it serves as a reference monitor to protect all subjects, objects and operations included within the scope of control of the ePassport access control policies defined in FDP_ACC.1.

FPT_SEP.1 TSF Domain Separation

This component defines the security domains to protect subjects, objects, operations and the TSF data included within the scope of control of the ePassport access control policies from external interference and tampering by untrusted subjects.

As this COS is native, this component satisfies the security objectives of O. Access Control and O. Domain Separation by separating the domains used by untrusted subjects, such as other application programs, from the domain in which the ePassport access control function is executed.

This component also satisfies the security objective of O. Domain Separation by separating the secure memory domain from other memory domains and therefore protecting the TSF data from external IT entities.

FPT_TST.1 TSF testing

This component requires self-testing to detect a loss of the TSF executable code and the TSF

data by various failures (such as an unexpected failure mode, lack of an IC chip design or intentional damage to the TSF).

This component satisfies the security objective of O.Self-protection because the TOE checks the patch status of the TSF. To demonstrate the correct operation of the TSF, each TSF does a self-test and ensures correct operation before it runs the TSF. If the TSF is patched, the patched code is executed.

This component satisfies the security objective of O.Self-protection by verifying the integrity of the TSF data with using a 16-bit checksum generated by the CRC function of the IC chip when the TSF data is internally used.

To verify the integrity of the TSF execution code, the TOE compares a previously saved Retail MAC value and another Retail MAC value in which the ROM area is calculated in Unissue status. Therefore, this component satisfies the security objective of O.Self-protection by verifying the integrity of the TSF execution code.

8.2.2 Rationale of IT Environment Security Requirements

(Table 22) presents the mapping between the security objectives and the security functional requirements for the IT environment.

(Table 22) Mapping of Security Objectives for the IT environment by SFR

Security objectives for the IT environment / Security functional requirements for the IT environment	OE. Passport Book Manufacturing Security	OE. Procedures of ePassport holder Check	OE. Application Program Loading	OE. Certificate Verification	OE. Personalization Agent	O.Handling Information Leakage	OE. Inspection System	OE. IC Chip	OE. MRZ Entropy	OE. PKI	OE. Range of RF Communication
FCS_CKM.1(2)								X			
FCS_COP.1(1)								X			
FCS_COP.1(2)								X			
FCS_COP.1(3)								X			
FCS_COP.1(4)								X			
FCS_COP.1(5)								X			
FPR_UNO.1						X		X			

FCS_CKM.1(2) Cryptographic key generation (PAC Session Key)

FCS_CKM.1(2) requires the generation of a 112-bit PAC authentication key according to the cryptographic key generation algorithm specified in the PAC.

This component satisfies the security objectives of OE.IC chip by performing the cryptographic operations defined in this component using the functions supported in the IC chip.

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

This component defines the TDES cryptographic operation used to authenticate the Inspection System that supports the PAC and BAC or to protect the transmitted user data from disclosure.

This component satisfies the security objectives of the OE.IC chip by performing the cryptographic operations defined in this component using the functions supported in the IC chip.

FCS_COP.1(2) Cryptographic operation (MAC)

This component defines the Retail MAC (ISO/IEC 9797-1) used to authenticate the Inspection System that supports the PAC and BAC or to detect modification of the transmitted user data.

This component satisfies the security objectives of the OE.IC chip by performing the cryptographic operations defined in this component using the functions supported in the IC chip.

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

This component defines the hash algorithm (SHA-1, SHA-224, SHA-256) used to digital signature.

This component satisfies the security objectives of the OE.IC chip by performing the cryptographic operations defined in this component using the functions supported in the IC chip.

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

This component defines the method of digital signature verification (RSASSA- PKCS1- v1.5 -SHA-1, RSASSA- PKCS1- v1.5 -SHA-256 and ECDSA-SHA-1, ECDSA-SHA-224, ECDSA-SHA-256) necessary in the EAC-TA.

This component satisfies the security objectives of the OE.IC chip by performing the cryptographic operations defined in this component using the functions supported in the IC chip and RSA library.

FCS_COP.1(5) Cryptographic operation (Digital signature Generation)

This component defines the method of digital signature generation (RSASSA- PKCS1- v1.5 -SHA-256) necessary in the AA authentication mechanism.

This component satisfies the security objectives of the OE.IC chip by performing the cryptographic operations defined in this component using the functions supported in the IC chip and ECC cryptographic library.

FPR_UNO.1 Unobservability

This component ensures that external entities are unable to observe the cryptographic-related data, such as the PAC authentication key, PAC Session key, BAC authentication key, BAC session key, EAC session key and EAC chip authentication private key, AA private key and CVCA digital signature verification key when the TSF performs a cryptographic operation.

This component satisfies the security objectives of the OE.IC chip by providing countermeasures for DPA/SPA in the IC chip.

This component satisfies the security objectives of OE.Handling Information Leakages by providing the means to prevent extrusion of the key information in the IC chip.

8.2.3 Rationale of Assurance Requirements

The EAL (Evaluation Assurance Level) of this Security Target was selected as EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.4) after considering factors such as the value of the assets protected by the TOE and the level of the threats.

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 or 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 with assurance components are given below.

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

The TOE is an operating system and application program that operates in the MRTD chip. Therefore, it largely depends on the IC chip in terms of a cryptographic operation function and physical security. To ensure a 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 using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to the design and operation of the TOE. Moreover, the TOE is easily accessible, as it is used in an open environment, making it difficult to trace an attack. However, as the IC chip is not included in the scope of the TOE, it does not require understanding of the hardware structure or any advanced specialized equipments. Therefore, considering the resources, motivation and expertise of attackers, the TOE must counter attackers possessing moderate attack potential. EAL4 includes AVA_VLA.2, which is resistant to low-level attack potential. Therefore, AVA_VLA.3 is augmented to require execution of systematic vulnerability analysis and is resistant to attackers possessing moderate attack potential. However, there still exists direct attack potential to the IC chip by a threat agent possessing a high level of attack potential. Evaluation and verification of this may be assigned to the IC chip manufacturer.

It is difficult to correct defects, even if they occur after the ePassport loaded with the IC chip is issued. This can be exploited by attackers. Therefore, ADV_IMP.2 is augmented to enable analysis of the entire implementation representation in order to check if the TSF is accurately implemented and that defective code does not exist. Additionally, ATE_DPT.2 is augmented to enable detection of defects not discovered while the TOE is developed through testing of the subsystems and modules closely related to the internal structure of the TSF.

8.3 Rationale of Dependency

8.3.1 Dependency of TOE Security Functional Requirements

(Table 23) shows the dependency of the TOE functional components.

(Table 23) Dependency of TOE Functional Components

No.	Functional Component	Dependency	Ref. No.
1	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4 FMT_MSA.2	2, (Table 23) 2 5 None
2	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 orFCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 5 None
3	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 orFCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 5 None
4	FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 orFCS_CKM.1] FMT_CKM.4 FMT_MSA.2	(Table 23) 1 5 None
5	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 orFCS_CKM.1] FMT_MSA.2	1, (Table 23) 1 None
6	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 orFCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 5 None
7	FDP_ACC.1	FDP_ACF.1	8
8	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	7 25
9	FDP_DAU.1	-	-
10	FDP_RIP.1	-	-
11	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	None 7
12	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	7 None
13	FIA_AFL.1	FIA_UAU.1	14,15,16,17
14	FIA_UAU.1(1)	FIA_UID.1	21
15	FIA_UAU.1(2)	FIA_UAU.1(1)	14
16	FIA_UAU.1(3)	FIA_UID.1	21

No.	Functional Component	Dependency	Ref. No.
17	FIA_UAU.1(4)	FIA_UID.1	21
18	FIA_UAU.4	-	-
19	FIA_UAU.5(1)	-	-
20	FIA_UAU.5(2)	-	-
21	FIA_UID.1	-	-
22	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	32 33
23	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	32 33
24	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	7 32 33
25	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	24 33
26	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	32 33
27	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	32 33
28	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	32 33
29	FMT_MTD.1(4)	FMT_SMF.1 FMT_SMR.1	32 33
30	FMT_MTD.1(5)	FMT_SMF.1 FMT_SMR.1	32 33
31	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	EAL4 26
32	FMT_SMF.1	-	-
33	FMT_SMR.1	FIA_UID.1	21
34	FPT_AMT.1	-	-
35	FPT_FLS.1	ADV_SPM.1	EAL4
36	FPT_ITI.1	-	-
37	FPT_RVM.1	-	-

No.	Functional Component	Dependency	Ref. No.
38	FPT_SEP.1	-	-
39	FPT_TST.1	FPT_AMT.1	34

FCS_CKM.1(1), FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM.2(3), FCS_CKM.4 and FCS_COP.1(3) have dependency with FMT_MSA.2, but the dependency in this Security Target is not satisfied. The target of generating, operating and destroying cryptographic key of FCS is the TSF data. Therefore, rather than secure security attributes (FMT_MSA.2), FMT_MTD.3 of the secure TSF data is satisfied.

FDP_UCT.1 and FDP_UIT.1 have dependency with FTP_ITC.1 or FTP_TRP.1, but the dependency in this Security Target is not satisfied. FDP_UCT.1 and FDP_UIT.1 require secure messaging between the Inspection System and the TOE. As secure messaging between the Inspection System and TOE uses an unique channel, it is not necessary for it to be logically separated from other communicational channels. Therefore, in this protection profile, requirements of FTP_ITC.1 are not defined.

FIA_UAU.1(2) has dependency with FIA_UID.1, but the dependency in this Security Target is not satisfied. Since the EAC-TA is executed after the BAC mutual authentication, FIA_UAU.1(2) depends on FIA_UAU.1(1) and FIA_UAU.1(1) depends on FIA_UID.1. Therefore, the dependency is satisfied indirectly.

8.3.2 Dependency of IT Environment Security Functional Requirements

(Table 24) shows the dependency of the IT environment functional components.

(Table 24) Dependency of IT Environment Functional Components

No.	Assurance Component	Dependency	Ref. No.
1	FCS_CKM.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	(Table 22) 1 (Table 22) 5 None

2	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	(Table 22) 1 (Table 22) 5 None
3	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	(Table 22) 1 (Table 22) 5 None
4	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	(Table 22) 1 (Table 22) 5 None
5	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	(Table 22) 1 (Table 22) 5 None
6	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	(Table 22) 1 (Table 22) 5 None
7	FPR_UNO.1	-	-

FCS_CKM.1(2), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4) and FCS_COP.1(5) have dependency with FMT_MSA.2, but the dependency in this Security Target is not satisfied. The target of generating, operating and destroying the cryptographic key of FCS is TSF data. Therefore, rather than secure security attributes (FMT_MSA.2), FMT_MTD.3 of the secure TSF data is satisfied.

8.3.3 Dependency of TOE Security Assurance Requirements

The dependency of EAL4 provided in the 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 25).

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

(Table 25) Dependency of the Added Assurance Components

No.	Assurance Component	Dependency	Ref. No.
1	ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	EAL4 EAL4 EAL4
2	ATE_DPT.2	ADV_HLD.2 ADV_LLD.1 ATE_FUN.1	EAL4 EAL4 EAL4
3	AVA_VLA.4	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	EAL4 EAL4 1 EAL4 EAL4 EAL4

8.4 Rationale of the Extended Security Requirements

There are no expended security requirements in this Security Target.

8.5 Rationale of Assurance Measures

The following table demonstrates the coverage of the Assurance Requirements by the Assurance measures by indicating the correspondence with crosses.

(Table 26) Assurance Measures

Assurance Requirements			Assurance Measures
Assurance class	Assurance component		
Configuration Management	ACM_AUT.1	Partial CM automation	EPS-02-QT-ACM-1.2
Configuration Management	ACM_CAP.4	Generation support and acceptance procedures	EPS-02-QT-ACM-1.2

Assurance Requirements			Assurance Measures
Assurance class	**Assurance component**		
Configuration Management	ACM_SCP.2	Problem tracking CM coverage	EPS-02-QT-ACM-1.2
Delivery and operation	ADO_DEL.2	Detection of modification	EPS-02-QT-ADO-1.1
Delivery and operation	ADO_IGS.1	N/A ※ Does not require Installation, generation, or start-up procedures for this TOE	N/A ※ Installation, generation, and start-up procedures for this TOE are not required.
Development	ADV_FSP.2	Fully defined external interfaces	EPS-02-DG-FSP-1.4
Development	ADV_HLD.2	Security enforcing high-level design	EPS-02-DG-HLD-1.3
Development	ADV_IMP.2	Implementation of the TSF	EPS-02-IM-IMP-1.2
Development	ADV_LLD.1	Descriptive low-level design	EPS-02-DG-LLD-1.2
Development	ADV_RCR.1	Informal correspondence demonstration	EPS-02-AN-ST-1.4 EPS-02-DG-FSP-1.4 EPS-02-DG-HLD-1.3 EPS-02-IM-IMP-1.2 EPS-02-DG-LLD-1.2
Development	ADV_SPM.1	Informal TOE security policy model	EPS-02-AN-SPM-1.1
Guidance documents	AGD_ADM.1	Administrator guidance	EPS-02-QT-AGD_ADM-1.2
Guidance documents	AGD_USR.1	User guidance	EPS-02-QT-AGD_USR-1.2
Life cycle support	ALC_DVS.1	Identification of security measures	EPS-02-QT-ALC-1.2
Life cycle support	ALC_LCD.1	Developer defined life-cycle model	EPS-02-QT-ALC-1.2
Life cycle support	ALC_TAT.1	Well-defined development tools	EPS-02-QT-ALC-1.2
Tests	ATE_COV.2	Analysis of coverage	EPS-02-TS-ATE-1.2

Assurance Requirements			Assurance Measures
Assurance class	Assurance component		
Tests	ATE_DPT.2	Testing: low-level design	EPS-02-TS-ATE-1.2
Tests	ATE_FUN.1	Functional testing	EPS-02-TS-ATE-1.2
Tests	ATE_IND.2	N/A	N/A
Vulnerability assessment	AVA_MSU.2	Validation of analysis	EPS-02-TS-MSU-1.1 EPS-02-QT-AGD_USR-1.2 EPS-02-QT-AGD_ADM-1.2
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation	EPS-02-TS-SOF-1.1
Vulnerability assessment	AVA_VLA.4	Highly resistant.	EPS-02-TS-VLA-1.1

8.6 Rationale of Function Strength

8.6.1 Rationale for function strength of security functional requirements

This Security Target requires ‘SOF-high’ for the security functional requirements of FCS_CKM.1(1), FDP_DAU.1, FIA_UAU.5(1), FIA_UAU.5(2), FCS_COP.1(3) and FPT_TST.1.

(Table 27) Function Strength of Security Functional Requirements

Security Functional Requirements	Strength of Function	Rationale
FCS_CKM.1(1)	SOF-high	FCS_CKM.1(1) has set the length of the encryption key and MAC key to 112 bits to obtain resistance against high-level attacks according to ePassport specification. Therefore, it satisfies 'SOF-high'.
FDP_DAU.1	SOF-high	FDP_DAU.1 has set the key length of RSA digital signature to 1024, 2048 bits to obtain resistance against high-level attacks during AA authentication. . And the attacker is not accessible inside the TOE. Therefore, it satisfies 'SOF-high'.

FIA_UAU.5(1)	SOF-high	1. Case LC : FIA_UAU.5(1) has set the length of the ECDSA digital signature to 224, 256 bits to obtain resistance against high-level attacks during EAC-TA authentication. Therefore, it satisfies 'SOF-high'. 2. Case : GC/GW/LC : FIA_UAU.5(1) has set the length of the RSA digital signature to 1024, 2048 bits to obtain resistance against high-level attacks during EAC-TA authentication. . And the attacker is not accessible inside the TOE. Therefore, it satisfies 'SOF-high'.
FIA_UAU.5(2)	SOF-high	FIA_UAU.5(2) has set the length of PAC key to 112 bits to obtain resistance against high-level attacks in PAC mutual authentication, generating the PAC session key, PAC personalization, and management authentication. Therefore, it satisfies 'SOF-high'.
FCS_COP.1(3)	SOF-high	FCS_COP.1(3) has used 160, 224, 256bit Hash algorithm obtain resistance against high-level attacks in verifying the TSF integrity. And the attacker is not accessible inside the TOE. Therefore, it satisfies 'SOF-high'.
FPT_TST.1	SOF-high	FPT_TST.1 has used 112bit Retail MAC algorithm at the step to verify the integrity of the executable code. Therefore, it satisfies 'SOF-high'. FPT_TST.1 has used 16bit CRC algorithm at the step to verify the integrity of the TSF data and the attacker is not accessible inside the TOE. Therefore, it satisfies 'SOF-high'.

Therefore, if attackers have expert knowledge, resources and the proper motivation, as mentioned in the Security environment, the TOE nonetheless has resistance against their attacks.

8.6.2 Rationale of Strength of Function

This Security Target requires ‘SOF-high’ for the security function of SF.MUT_AUTH, SF.ACTIVE_AUTH, SF.CHIP_AUTH, SF.TERMINAL_AUTH, SF.ACC_CONTROL and SF.RELIABILITY.

(Table 28) Strength of Security Function

Security function	Strength of Function	Rationale
SF.MUT_AUTH	SOF-high	TOE has implemented a TDES-based mutual authentication protocol in the PAC mutual authentication of SF.MUT_AUTH; this satisfies 'SOF-high' because the key length used is 112 bits.

Security function	Strength of Function	Rationale
		TOE has implemented a TDES-based authentication protocol in the PAC personalization and management authentication of SF.MUT_AUTH; this satisfies 'SOF-high' because the key length used is 112 bits.
		TOE has implemented a TDES-based authentication protocol to generate the PAC session key in the PAC mutual authentication of SF.MUT_AUTH; this satisfies 'SOF-high' because the key length used is 112 bits.
		TOE has implemented a TDES-based key distribution protocol to generate the BAC session key in the BAC mutual authentication of SF.MUT_AUTH; this satisfies 'SOF-high' because the key length used is 112 bits and the length of the hash algorithm is 160 bits used and the attacker is not accessible inside the TOE.
SF.CHIP_AUTH	SOF-high	TOE has implemented a 1024, 2048bit DH-based key distribution protocol in the EAC-CA authentication of SF.CHIP_AUTH; this satisfies 'SOF-high' because a 160bit hash algorithm is used at the step to generate the EAC session key and the attacker is not accessible inside the TOE. TOE has implemented a 224, 256 bit ECDH-based key distribution protocol in the EAC-CA authentication of SF.CHIP_AUTH; this satisfies 'SOF-high' because a 160bit hash algorithm is used at the step to generate the EAC session key used and the attacker is not accessible inside the TOE.
SF.TERMINAL_AUTH	SOF-high	TOE has used a 1024, 2048bit RSA digital signature algorithm and a 256bit hash algorithm in EAC-TA authentication of SF.TERMINAL_AUTH so that TOE verifies the inspection system. And the attacker is not accessible inside the TOE. Therefore, it satisfies 'SOF-high'. TOE has used a 224, 256bit ECDSA digital signature algorithm and a 160, 224, 256bit hash algorithm in EAC-TA authentication of SF.TERMINAL_AUTH so that TOE verifies the inspection system. Therefore, it satisfies 'SOF-high'.
SF.ACTIVE_AUTH	SOF-high	TOE has implemented the AA authentication mechanism of SF.ACTIVE_AUTH and it satisfies 'SOF-high' because a 1024, 2048bit RSA algorithm and a 256bit hash algorithm are used and the attacker is not accessible inside the TOE.
SF.ACC_CONTROL	SOF-high	TOE has used a 160bit SHA-1 hash algorithm at the step to generate the BAC session key of SF.ACC_CONTROL. And The attacker is not accessible inside the TOE. Therefore, it satisfies 'SOF-high'.
SF.RELIABILITY	SOF-high	TOE has used a 112bit Retail MAC algorithm at the step to verify the TSF executable code integrity of SF.RELIABILITY. TOE has used a 16bit CRC algorithm at the step to verify the TSF integrity of SF.RELIABILITY. Therefore, it satisfies 'SOF-high'.

Therefore, if the attackers have expert knowledge, resources and the proper motivation, as mentioned in the Security environment, the TOE nonetheless has a resistance against their attacks.

8.7 Rationale of Mutual Support and Internal Consistency

This rationale demonstrates that the TOE security requirements have mutual support and internally consistency.

In "8.3.1 Dependency of TOE security functional requirements" and "8.3.2 Dependency of TOE security assurance requirements"', the dependency is analyzed as a supportive relationship among security requirements in which it is necessary to depend on other security requirements to achieve a security objective when a security requirement is insufficient. In case the dependency was not satisfied, an additional rationale is provided.

Moreover, the security functional requirements, although there is no dependency among security functional requirements, are mutually supportive and have internally consistency in relation to the TSF operations, as shown below.

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

The TSF, after identifying the Inspection System (FIA_UID.1), executes the BAC mutual authentication (FIA_UAU.1(1)) and the EAC-TA (FIA_UAU.1(2)) according to the authentication mechanism application rules (FIA_UAU.5(1)). If the Inspection System fails in authentication, the session is terminated (FIA_AFL.1). Random numbers must be used so as to prevent reuse of authentication-related data used in authentication (FIA_UAU.4). To ensure that secure random numbers are used and that 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)) to indicate the termination of the channel when terminating the BAC secure messaging (FDP_UCT.1, FDP_UIT.1) that was established to protect the transmitted user data. Therefore, these security requirements are mutually supportive and internally consistent.

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

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

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

8.8 Rationale of PP Claims

This security target is conformable to all requirements of the PP (KECS-PP-0084 -2008).

8.8.1 Rationale for Conformance of Security Environment

This Security Target is conformable to all security environments, except that the T. Residual Information, A.Inspection system , P. ePassport Access Control of the ePassport Protection Profile are reconstructed.

T.Residual Information defined in ePassport Protection Profile is reconstructed in this Security Target by adding a PAC authentication key and a Session key to perform PAC authentication functionality to the residual information.

The A.Inspection System defined in the ePassport Protection Profile is reconstructed in this security target by adding the AA authentication functionality of the TOE to the inspection system.

The P. ePassport Access Control defined in the ePassport Protection Profile is reconstructed in this security target by changing to store the relate CVCA Certificates information in secure memory instead to store CVCA Certificates in secure memory.

Therefore, this Security Target is conformable to the security environment of ePassport Protection Profile.

8.8.2 Rationale for Conformance of Security Objective

In this Security Target, Security objectives, O.Session Terminate and OE.ePassport Personalization agent are reconstructed and the O.Handling Information leakage is reconstructed as the OE.Handling Information Leakage because all functions concerning the handling of information leakage are supported in the IC chip. All of the other security objectives are conformable to those of the ePassport Protection Profile, and the O.AA and O.PAC are added to this security target because the AA and PAC authentication functions are added.

O. Session Terminate defined in the ePassport Protection Profile is reconstructed in this security target by adding a function to terminate the PAC session. Therefore, this security target is conformable to the security objectives of the ePassport Protection Profile.

The OE.ePassport Personalization Agent defined in the ePassport Protection Profile is reconstructed in this security target by adding that it has to hold the PAC authentication key necessary to issue the TOE, implement the security mechanism, and guarantee the application order according to the issuing type so as not to violate the access control policy of the personalization agent. Therefore, this security target is conformable to the security objectives of ePassport Protection Profile.

8.8.3 Rationale for Security Functional Requirements

This Security Target is conformable to all security functional requirements of the ePassport Protection Profile and reconstructs the operations according to the allowed rules for the security functional requirements. In addition, the security functional requirements added to this Security Target are related to the PAC and AA function. Therefore, this Security Target is conformable to the security functional requirements of the ePassport Protection Profile.

8.8.4 Rationale for Assurance Requirements

This Security Target is conformable to all the assurance requirements of the EAL 4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) assurance level required in the ePassport Protection Profile. There are

no additionally defined assurance requirements in this Security Target.

[Works Cited]

[1] Doc 9303 "Machine Readable Travel Documents" Part 1 "Machine Readable Passports" Volume 1 "Specification for Electronically Enabled Passports with Biometric Identification Capability" Sixth Edition, International Civil Aviation Organization(ICAO), 2006. 8

[2] Doc 9303 "Machine Readable Travel Documents" Part 1 "Machine Readable Passports" Volume 2 "Passports with Machine Readable Data Stored in Optical Character Recognition Format" Sixth Edition, International Civil Aviation Organization(ICAO), 2006. 8

[3] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Version 1.01, TR-03110, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[4] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01,2004, published by authority of the secretary general, International Civil Aviation Organization

[5] Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, published by authority of the secretary general, International Civil Aviation Organization, LDS 1.7, 2004-05-18

[6] Common Criteria Protection Profile, Machine Readable Travel Document with ICAO Application, Basic Access Control, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2005. 8

[7] Common Criteria Protection Profile, Machine Readable Travel Document with ICAO Application, Extended Access Control, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2006. 9

[8] SHARP Passport Booklet module Security Target - lite, ST Version 1.13-1, SHARP Corporation IC Card Development Dept, 2006. 11

[9] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9.

[10] Common Methodology for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9.

[11] Supporting Document Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.1, CCDB, 2006. 4

[12] Supporting Document Mandatory Technical Document, The Application of CC to Integrated Circuits, Version 2.0, CCDB, 2006. 4

[Abbreviations]

AA	Active Authentication
BAC	Basic Access Control
PAC	Personalization Access Control
BIS	BAC Inspection System
CA	Chip Authentication
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
COS	Card Operating System
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie-Hellman
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman

EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EIS	EAC Inspection System
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IS	Inspection System
ISO	International Organization for Standardization
IT	Information Technology
KDF	Key Derivation Function
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PA	Passive Authentication
PIS	PA Inspection System
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read Only Memory
SFP	Security Function Policy
SOD	Security Object of Document
SOF	Strength of Function

SPA	Simple Power Analysis
SSC	Send Sequence Counter
ST	Security Target
TA	Terminal Authentication
TDES	Triple-DES
TSC	TSF Scope of Control
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy