Ref.: SKEPSV10-ASE-LITE-V1.6

Security Target Lite

SK e-Pass V1.0

Version 1.6

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target defines security functional requirements and security assurance requirements for SK e-Pass V1.0, IC chip operating system (COS) and the application of machine readable travel documents (MRTD Application) manufactured by SK C&C, with the exception of hardware elements of the chip of machine readable travel documents (MRTD chip).

1.1 ST and ST-Lite Identification

The information required for identifying the Security Target and the Security Target Lite for the TOE is shown in the following table.

ST	SK e-Pass V1.0 Security Target(SKEPSV10-ASE-V1.6)
Version	V1.6
Publication Date	2010.06.18
ST-Lite	SK e-Pass V1.0 Security Target Lite(SKEPSV10-ASE-LITE-V1.6)
Version	V1.6
Publication Date	2010.07.20
Author	SK C&C

Table 1 ST Identification

1.2 TOE Identification

The information required for identifying the TOE is shown in the following table.

TOE	SK e-Pass V1.0
IC Chip	S3CC9LC, Samsung Electronics
Release Date	To be determined
Manufacturer	SK C&C

Table 2 TOE Identification

1.3 CC and PP Conformance

This Security Target claims conformance with the Common Criteria, Protection Profile and Assurance Package shown in the following table.

Common Criteria	Common Criteria for Information Security Evaluation V3.1 (Ministry of

	Public Administration and Security, Public Notice No. 2009-52
CC Version	CC V3.1 R3
Assurance Package	EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)
Protection Profile	ePassport Protection Profile V2.1 (KECS-PP-0163a-2009, 2010. 6. 10)

Table 3 CC and PP Conformance

1.4 Conventions

The notation, formatting and conventions used in this Security Target 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 Security Target.

Assignment

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

Iteration

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

Refinement

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

Selection

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

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

1.5 Security Target Organization

Section 1 provides the introductory material for the Security Target.

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

Section 3 defines the operational environment for the TOE and the logical and physical scope of the TOE.

Section 4 defines the conformance claims for the Security Target.

Section 5 describes the TOE security environment and includes security problems of the TOE and its IT environment from such as assumptions, threats and organizational security policies.

Section 6 defines the security objectives for the TOE and its IT environment to counter the identified threats and support the assumptions and organizational security policies along with the rationale to demonstrate that the security objectives for the TOE and its IT environment address the defined security problems appropriately

Section 7 defines the extended components which are not defined in the Common Criteria Part 2 or Part 3.

Section 8 contains the IT security requirements including the functional and assurance requirements intended to satisfy security objectives along with the rationale to demonstrate that the IT security requirements are adequate and complete to satisfy the security objectives.

Section 9 provides the TOE Summary Specification for the security functions of the TOE.

Section 10 defines the terms which is used in this Security Target. References contain references to noteworthy background and/or supporting materials or prospective users of the ST who may be interested in knowing more than what is specified herein. Acronym is an acronym list that defines frequently used acronyms.

2 TOE Description

2.1 TOE Overview

The ePassport is the passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO). The contactless IC chip used in the ePassport is referred to as MRTD chip. The MRTD chip is loaded with the MRTD Application and IC chip operating system (COS) to support IT and information security technology for electronic storage, processing and handling of the ePassport identity data.

The TOE consists of the SK COS (IC chip operating system), the MRTD Application and the MRTD Application Data which are loaded in the Samsung S3CC9LC IC chip. The IC chip elements and the antenna are excluded from the scope of the TOE. The Samsung S3CC9LC IC chip is a CCRA EAL5+ certified product with the certification number of 'BSI-DSZ-CC-0624-2010-MA-01'.

The TOE was developed based on the international standards shown in the following table

TOE	International Standards	Standard Organization	Conformation Claim
SK COS	- Javacard Specification(Java Card 2.2.2 Virtual Machine Specification[1], Java Card 2.2.2 Runtime Environment Specification[2], Java Card 2.2.2 Application Programming Interfaces[3], hereafter referred to as "Javacard Specification")	SUN	Conforms except particular functions (e.g. Loading, Installing and Deleting of an Application, Firewall etc.)
	- GlobalPlatform Specification(GlobalPlatform Card Specification 2.1.1[4], hereafter referred to as "GP Specification")	GlobalPlatform	
	- Visa GlobalPlatform - Configuration 2 Specification (Visa GlobalPlatform 2.1.1 Card Implementation Requirements[5] - Configuration 2, hereafter referred to as "VGP Specification")	VISA	
MRTD Application	- ICAO MRTD Specification (ICAO Machine Readable Travel Documents, Doc	ICAO	Conforms

	9303 Part 1 Volume 2[6], hereafter referred to as “MRTD Specification”)		
	- BSI EAC Specification(BSI, Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.11(2008.2) [7], hereafter referred to as “EAC Specification”)	BSI	
	- ISO/IEC 14443-4:2001, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol[8] - ISO/IEC 9798-2:1999, Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms[9] - ISO/IEC 11770-2:1996, Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques[10] - ISO/IEC 10118-3:2004, Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions[11] - ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher[12] - ISO/IEC 15946-3:2002, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 3: Key establishment[13] - ISO/IEC 15946-2:2002, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures[14]	ISO	

Table 4 International Standards for the TOE Development

2.2 ePassport System

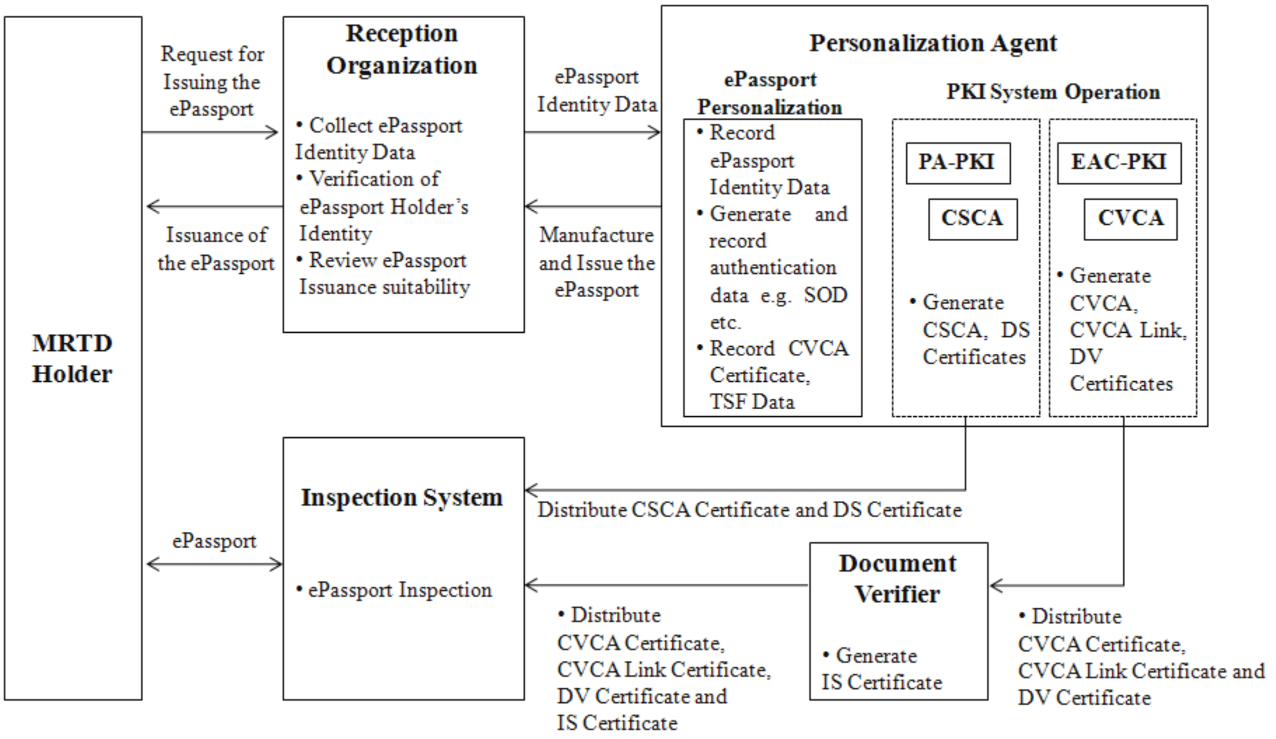

MRTD Holder
Request for Issuing the ePassport
Issuance of the ePassport
Reception Organization
• Collect ePassport Identity Data
• Verification of ePassport Holder's Identity
• Review ePassport Issuance suitability
ePassport Identity Data
Manufacture and Issue the ePassport
Personalization Agent
ePassport Personalization
• Record ePassport Identity Data
• Generate and record authentication data e.g. SOD etc.
• Record CVCA Certificate, TSF Data
PKI System Operation
PA-PKI
CSCA
• Generate CSCA, DS Certificates
EAC-PKI
CVCA
• Generate CVCA, CVCA Link, DV Certificates
ePassport
Inspection System
• ePassport Inspection
Distribute CSCA Certificate and DS Certificate
Document Verifier
• Generate IS Certificate
• Distribute CVCA Certificate, CVCA Link Certificate, DV Certificate and IS Certificate
• Distribute CVCA Certificate, CVCA Link Certificate and DV Certificate

Figure 1 Overall Configuration of the ePassport System

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

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

The Personalization agent generates document security object ('SOD' hereinafter) by digital signature on the user data (identity and authentication data) and records it in the MRTD chip with the ePassport identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the personalization agent is manufactures and issues the ePassport embedded the MRTD chip to the passport. Details of data recorded in the ePassport will be described in Table 10 of 3.3 Logical Scope of the TOE.

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

The Document verifier generates IS certificate by using CVCA and DV certificates, and then provides these certificates to Inspection System. Types of certificates used in the ePassport system are as shown in the following table.

Usage	ePassport PKI Systems	Subjects	Certificates
Verifying the user data against forgery or corruption	PA-PKI	CSCA	CSCA Certificate
		Personalization Agent	DS Certificate
Verifying the access control rights of ePassport holder’s biometric data	EAC-PKI	CVCA	CVCA Certificate
			CVCA Link Certificate
		Document Verifier	DV Certificate
		EAC Supporting Inspection System	IS Certificate

Table 5 Types of Certificates

2.3 Security Mechanisms

The TOE provides security functions such as the confidentiality, the integrity, the access control and the authentication, in order to protect the TSF data and the user data of the ePassport identity data and the ePassport Authentication Data, etc. These security functions are implemented with the SCP02 mechanism of the GP Specification, the BAC mechanism of the ICAO document, the EAC mechanism of the EAC specifications and the AA mechanism. Also, the TOE provides the SOD for the BIS and the EIS and the Inspection System to detect forgery and corruption of the user data through the verification of the digital signature of the SOD by using the PA mechanism.

<SCP02>

The SCP02 (Secure Channel Protocol ’02) is to provide the confidentiality and the 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 Personalization Agent with read-rights and/or write-rights. The SCP02 includes the SCP02 Mutual Authentication, the SCP02 key distribution and the SCP02 Secure Messaging.

The SCP02 Secure Channel is initiated by the Personalization Agent by transmitting a “host” challenge (random data unique to this session) to the TOE. The TOE generates its own “card” challenge (random data unique to this session) when the TOE receives the “host” challenge. The TOE creates the new secret session key using its internal Sequence Counter and the SCP02 Authentication Key and generates a first cryptographic value (card cryptogram) using the newly created session key. The card cryptogram is transmitted back to the Personalization Agent with the Sequence Counter, the card challenge, and other information. As the Personalization Agent now has all the data that the TOE used to generate the card cryptogram, it should be able to generate the same session key and the same card cryptogram and the

Personalization Agent can authenticate the TOE by comparing them.

The Personalization Agent executes a similar process to create another cryptographic value (host cryptogram) to be transmitted back to the TOE. As the TOE has all the data that the Personalization Agent used to generate the host cryptogram, it should be able to generate the same cryptogram and, the TOE is able to authenticate the Personalization Agent by comparing them.

The TOE, in order to secure the transmission of the personal data of the ePassport holder after checking the read-rights and/or write-rights of the Personalization Agent for the personal data of the ePassport holder through the SCP02 Mutual Authentication, establishes the SCP02 Secure Messaging by encrypting with the SCP02 Session Key shared through the SCP02 key distribution and generating the MAC.

<BAC>

The BAC (Basic Access Control) is to provide the confidentiality and the 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 generates random values by either generate the BAC Authentication Key from the MRZ data of DG1 or using the stored BAC Authentication Key and the BAC-supporting Inspection System by using BAC Authentication Key generated from reading optically the MRZ. Then, the TOE and the Inspection System perform encryption the generated random number and exchange them. 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 the mutual authentication failure.

The TOE, in order 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 the BAC Secure Messaging by encrypting with the BAC Session Key shared through the BAC Key Distribution and generating the MAC.

<EAC>

The EAC (Extended Access Control) is to provide 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 is to implement 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 key distribution protocol by using temporary public key received from the Inspection System. The session is ended in case of the EAC-CA failure. In case of the successful EAC-CA, the TOE establishes the EAC Secure Messaging by using the EAC session key.

The EAC-TA is for the TOE to implement 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 temporary public key used for the EAC-CA, by 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 by using the CVCA Digital signature Verification Key in secure memory. Then, by checking 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 the EAC Secure Messaging.

<AA>

The AA (Active Authentication) is to provide the verification of the authenticity of the MRTD Chip for the Inspection System. The AA security mechanism is the authentication protocol based on the Digital signature. The Inspection System transmits the random number to the TOE. The TOE signs the random number by the AA Chip Authentication Private Key and sends it back to the Inspection system. The Inspection System authenticates the TOE by verifying the received data with the AA Public Key.

<PA>

The PA (Passive Authentication) is to provide the verification of the authenticity of the personal data of the ePassport holder for the Inspection System. The Inspection System with the DS Certificate verifies the digital signature of the SOD and the hash value of the MRTD User Data according to the ePassport Access Policy.

The following table summarizes the ePassport security mechanisms provided by the TOE.

TOE Security Mechanisms				TOE Security Features Security Features
Security Features	Cryptography	Security Features	Cryptography	
User Data Authentication	N/A	User Data Authentication	N/A	User Data Authentication
BAC Mutual Authentication, BAC Key Distribution, BAC Secure Messaging	Symmetric Key Based Entity Authentication Protocol - TDES-CBC - SHA - Retail MAC	BAC Mutual Authentication	Symmetric Key Based Entity Authentication Protocol - TDES-CBC - SHA - Retail MAC	BAC Mutual Authentication
	Symmetric Key Based Key Distribution Protocol - TDES-CBC	BAC Key Distribution	Symmetric Key Based Key Distribution Protocol - TDES-CBC - SHA - Retail MAC	BAC Key Distribution

	- SHA Retail MAC			
	Secure Messaging	BAC Secure Messaging	Secure Messaging	BAC Secure Messaging
EAC-CA, EAC Secure Messaging, EAC-TA	ECDH Key Distribution Protocol	EAC-CA	ECDH Key Distribution Protocol	EAC-CA
	Secure Messaging	EAC Secure Messaging	Secure Messaging	EAC Secure Messaging
	- ECDSA-SHA-1 - ECDSA-SHA-224 ECDSA-SHA-256	EAC-TA	- ECDSA-SHA-1 - ECDSA-SHA-224 - ECDSA-SHA-256	EAC-TA
Verifying Illegal Chip	- RSA-SHA-1	Verifying Illegal Chip	- RSA-SHA-1	Verifying Illegal Chip
SCP02 Mutual Authentication, SCP02 Secure Messaging	Secure Channel Protocol ‘02’ - Single DES plus Final Triple DES. - TDES-CBC	SCP02 Mutual Authentication	Secure Channel Protocol ‘02’ - Single DES plus Final Triple DES. - TDES-CBC	SCP02 Mutual Authentication
	SCP02 Secure Messaging - TDES-CBC - TDES-ECB - Single DES plus Final Triple DES. Single DES	SCP02 Secure Messaging	SCP02 Secure Messaging - TDES-CBC - TDES-ECB - Single DES plus Final Triple DES. - Single DES	SCP02 Secure Messaging

Table 6 TOE Security Mechanisms

2.4 Non-TOE Hardware/ Software/ Firmware

The Non-TOE hardware and software required by for the operation of the TOE consists of the passport booklet, the antenna, the crypto library and the IC Chip. There is no firmware required by the TOE. The configuration of the passport booklet, the antenna and the IC Chip is as follows.

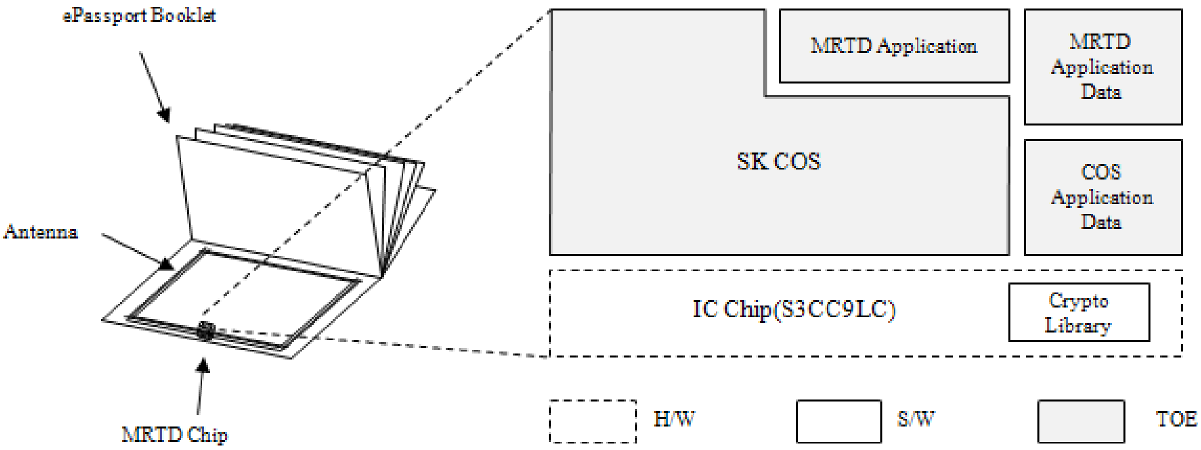


Figure 2 The Configuration of the ePassport

- **The passport booklet and the antenna (H/W)**
  The MRZ data is physically printed on the passport booklet in which the MRTD chip and the antenna are integrated to enable the contactless communication.

- **Crypto Library(S/W)**
  The RSA and ECC crypto library is embedded in the IC Chip to support cryptographic operations.

- **IC Chip(H/W)**
  The IC Chip is the lower platform of the TOE that supports TOE security functions providing random number generation, cryptographic operations etc.

The specifications of the IC Chip, Samsung S3CC9LC, are shown in the following table. Samsung S3CC9LC is certified with CCRA EAL5+ and the certification number is 'BSI-DSZ-CC-0624-2010-MA-01'.

Components	Specifications
CPU ROM EEPROM	16Bit CalmRISC16 core, Executes code of the TOE 256 Kbytes, Stores execution code of the TOE 72 Kbytes, Stores TSF data of the SK COS and the ePassport
RAM	4 Kbytes, Memory required to operate the SK COS
Contactless Interface	Supports ISO 14443-4 Type A
Cryptographic Support	RNG(Random Number Generator), Hardware DES/ TDES , Tornado Crypto Co-processor, RSA Cryptographic Library (Version 3.7s) and ECC Cryptographic Library (Version 2.4s)

Table 7 Samsung S3CC9LC Specification

The configuration of Samsung S3CC9LC is show in Figure 3.

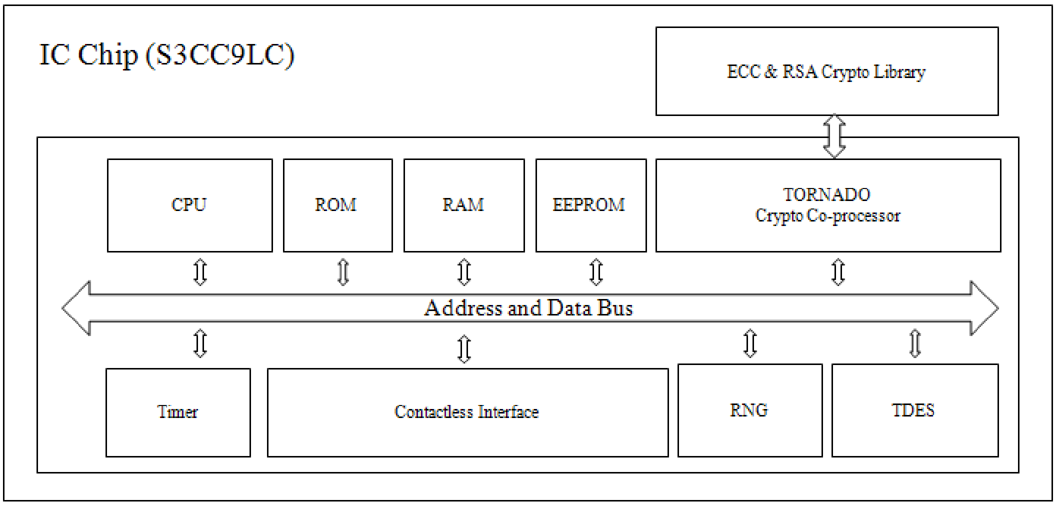


Figure 3 IC Chip Configurations

3 TOE Definition

3.1 Lifecycle and Environment of the TOE

The following table shows the lifecycle of the MRTD chip and the TOE. In the lifecycle shown in the following table, TOE development process corresponds to phase 1 (Development) and phase 2 (Manufacturing), while TOE operational environment corresponds to phase 3 (Personalization), phase 4 (Operational Use) and phase 5 (Termination).

Phase	Lifecycle of the MRTD Chip	Lifecycle of the TOE
Phase 1 (Development)	The IC chip developer designs the IC chip and develops the IC chip Dedicated S/W	
		- The S/W developer develops the TOE (COS, MRTD Application) by using the IC chip and the Dedicated S/W
Phase 2 (Manufacturing)	The IC chip manufacturer masks the TOE in the ROM, records the IC chip identifier and produces the IC chip	
		The ePassport manufacturer creates user data storage space according to the LDS format or the ICAO document and records it in EEPROM - The ePassport manufacturer to embed the IC chip in the passport book
Phase 3 (Personalization)		The Personalization Agent records identification and authentication information of the ePassport Personalization Agent in the EEPROM The Personalization Agent creates SOD by a digital signature on the ePassport identity data The Personalization Agent records the ePassport identity data, the authentication data (including SOD) and the TSF data in the TOE
Phase 4 (Operational Use)		The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE
Phase 5 (Terminating)		The Personalization Agent terminates the ePassport

		- The Personalization Agent terminates the TOE to prohibit further use.

Table 8 Lifecycle of the MRTD Chip and the TOE

Figure 4 shows the operational environment of the TOE in the phases of the ePassport Personalization and Operational Use through the relationship with major security functions of TOE and external entities (the Personalization Agent, the Inspection System) that interact with TOE.

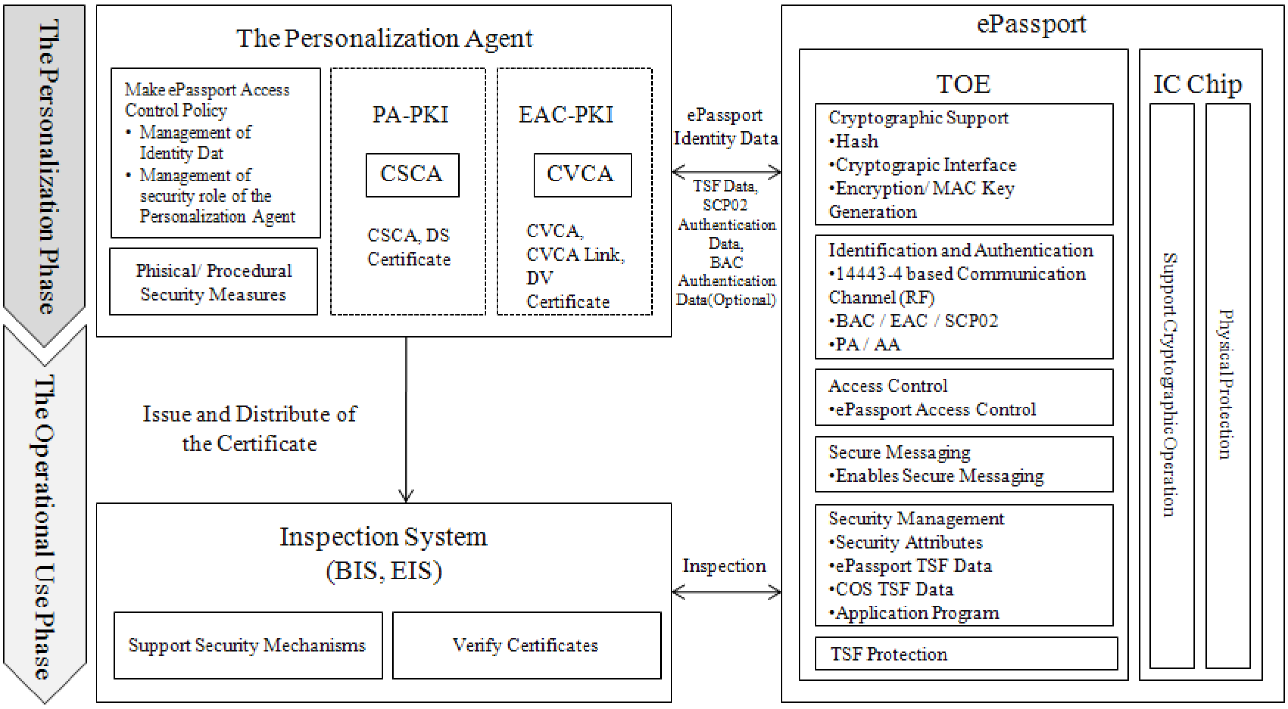

The Personalization Phase
The Operational Use Phase
The Personalization Agent
Make ePassport Access Control Policy
• Management of Identity Dat
• Management of security role of the Personalization Agent
Phisical/ Procedural Security Measures
PA-PKI
CSCA
CSCA, DS Certificate
EAC-PKI
CVCA
CVCA, CVCA Link, DV Certificate
Issue and Distribute of the Certificate
Inspection System (BIS, EIS)
Support Security Mechanisms
Verify Certificates
ePassport Identity Data
TSF Data, SCP02 Authentication Data, BAC Authentication Data(Optional)
Inspection
ePassport
TOE
Cryptographic Support
•Hash
•Cryptograpic Interface
•Encryption/ MAC Key Generation
Identification and Authentication
•14443-4 based Communication Channel (RF)
•BAC / EAC / SCP02
•PA / AA
Access Control
•ePassport Access Control
Secure Messaging
•Enables Secure Messaging
Security Management
•Security Attributes
•ePassport TSF Data
•COS TSF Data
•Application Program
TSF Protection
IC Chip
Support Cryptographic Operation
Physical Protection

Figure 4 TOE Operational Environment

3.2 Physical Scope of the TOE

The ePassport refers to the passport booklet and the MRTD chip and the antenna embedded in the cover of the passport book. The MRTD chip includes the IC chip operating system, the MRTD Application, the MRTD Application Data and the IC chip elements. The IC chip elements consist of CPU, co-processor, I/O port, memory (RAM, ROM, and EEPROM) and contactless interface, etc. The IC chip supports the operation of the TOE which consists of the SK COS and the MRTD Application. The SK COS is a chip operating system based on the Javacard Specification and the GP Specification. The SK COS consists of Javacard Platform, Kernel, Cryptographic Module and Card Manager. The SK COS does not allow removal of the MRTD Application. The physical scope of the TOE is shown in the following figure.

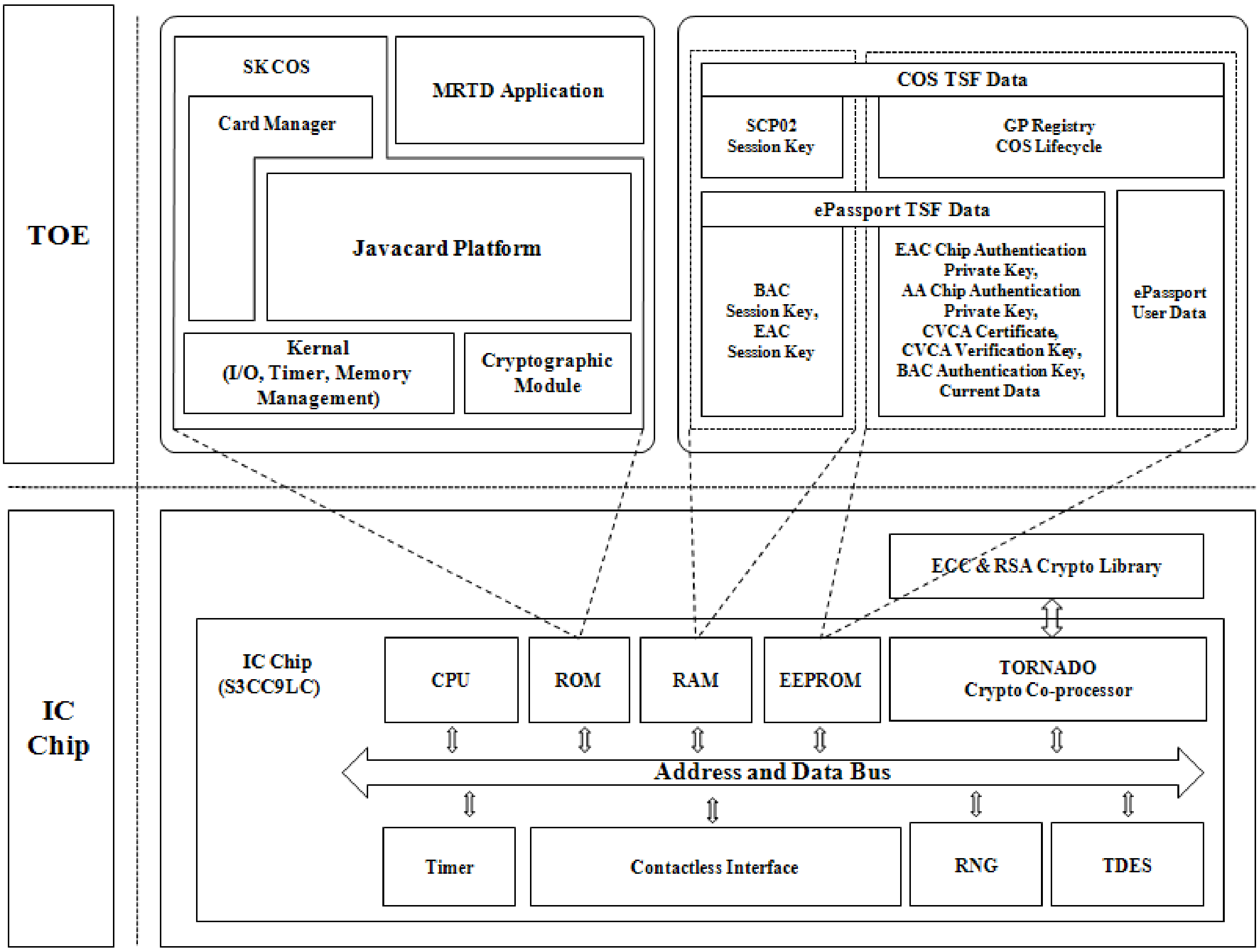

TOE
SK COS
Card Manager
MRTD Application
Javacard Platform
Kernal (I/O, Timer, Memory Management)
Cryptographic Module
COS TSF Data
SCP02 Session Key
GP Registry COS Lifecycle
ePassport TSF Data
BAC Session Key, EAC Session Key
EAC Chip Authentication Private Key, AA Chip Authentication Private Key, CVCA Certificate, CVCA Verification Key, BAC Authentication Key, Current Data
ePassport User Data
IC Chip
ECC & RSA Crypto Library
IC Chip (S3CC9LC)
CPU
ROM
RAM
EEPROM
TORNADO Crypto Co-processor
Address and Data Bus
Timer
Contactless Interface
RNG
TDES

Figure 5 Physical Scope of the TOE

The physical scope of the TOE consists of following components.

Components	Identifier	Version	Type
SK COS and MRTD Application	SK e-Pass	V1.0	Software Stored in ROM
ePassport Data	ePassport Data	-	Data Stored in RAM and/or EEPROM
COS Data	COS Data	-	Data Stored in RAM and/or EEPROM
Guidance	SK e-Pass V1.0 Personalization Guide	V1.1	Document
	SK e-Pass V1.0 Inspection Guide	V1.1	Document

Table 9 TOE Configuration

- **MRTD Application**

The MRTD Application is a Javacard application program 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 and security mechanism to securely protect the function. The MRTD Application Data consists of the user data, such as the ePassport identity data, etc., and the TSF data required in the security mechanism. After the Personalization, only read access to the ePassport identity data is allowed.

The MRTD Application implements the security mechanisms to protect the MRTD Application Data. The BAC security mechanism is used to control the access to the personal data of the ePassport holder. Also, the MRTD Application is added the EAC security mechanism by the EAC specifications, because the biometric data of the ePassport holder is included in the ePassport identity data. The SCP02 security mechanism is used to authenticate the Personalization Agent.

- **Card Manager**

  The Card Manager analyzes the commands received from the Personalization Agent or the Inspection System, and then it processes the instructions or forwards it to the MRTD Application for processing. Also, the Card Manager provides functions developed according to GP Specifications such as the SCP02 Mutual Authentication and the COS lifecycle management etc. to the MRTD Application.

- **Javacard Platform**

  The Javacard Platform consists of the JCRE (Javacard Run-Time Environment), the JCVM (Javacard Virtual Machine) and the JCAPI (Javacard Application Programming Interface) stored in ROM of the IC Chip. The JCRE configures the operational environment that the MRTD Application executes. The JCVM consists of On-Card VM and Off-Card VM. The JCAPI consists of Javacard Framework and Extended Javacard Package used for application program development.

- **Kernel**

  The Kernel manages the hardware I/O between the IC Chip and the Javacard Platform. Also, the Kernel controls functions such as the timer management, the contactless interface based on ISO 14443 Type A/ Type B and the EEPROM read/ write etc.

- **Cryptographic Module**

  The Cryptographic Module uses the cryptographic functions of the IC chip to provides the interfaces such as the random number generator, hardware DES/TDES, RSA and ECC (ECDH, ECDSA) to the Javacard Platform. The hash functions of SHA-1, SHA-224 and SHA-256 are implemented as software by the TOE.

- **MRTD Application Data**

  The MRTD Application Data is stored in EEPROM and RAM of the IC Chip and consists of the MRTD User Data and the MRTD TSF Data.

- **COS Application Data**

  The COS Application Data is stored in EEPROM and RAM of the IC Chip and consists of the COS TSF Data.

- **User Guidance**

  The user guidance of SK e-Pass V1.0 consists of the Administration Guidance and the Inspection Guidance. The Administration Guidance and the Inspection Guidance provide guidelines for the personalization and the inspection of SK e-Pass V1.0, respectively.

3.3 Logical Scope of the TOE

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

- **Cryptographic Support**

The TOE provides cryptographic features related to generation of random numbers, encryption keys, MAC keys, hash values, digital signatures and performing cryptographic operations on the data.

- **Identification and Authentication**

The TOE provides methods to identify and authenticate the users attempt to access the TOE using security mechanisms such as the SCP02 Mutual Authentication, the BAC Mutual Authentication, EAC-TA, PA and AA.

When an authentication failure is detected, the TOE terminates the secure channel and destroys the resources related to the authentication to prevent the replay. If the authentication failure was detected during the EAC-TA, the EAC-CA shall be performed before the execution of EAC-TA.

- **ePassport Access Control**

The TOE makes ePassport Access Control Policy to protect the MRTD Application Data. The TOE grants the Personalization Agent Issuing Authorization only to the Personalization Agent authenticated through the SCP02 Mutual Authentication in the Personalization Phase. In the Operational Use Phase, the Inspection System is required to gain the BAC Authorization or the EAC Authorization authenticated by the BAC Mutual Authentication or the EAC-CA/ EAC-TA, respectively, to read the MRTD Application Data. No write access to the MRTD Application Data is allowed after the Personalization of the ePassport.

- **Secure Messaging**

The TOE provides the Secure Messaging based on the BAC and the EAC security mechanisms to protect the confidentiality and integrity of the data transmitted between the TOE and the Inspection System. Also, the TOE provides the function for the Personalization Agent to enable the protection of confidentiality and/or integrity of the data. If the Personalization Agent enables the protection of confidentiality and/or integrity of the data transmitted between the TOE and the Personalization Agent, the transmitted data is protected using the Secure Messaging based on the SCP02 security mechanism.

- **Security Management**

The TOE provides security management features for the MRTD Application and the COS such as application program management, lifecycle management, TSF data management and security attributes management.

- **Protection of the TSF**

The TOE provides functions to protect the TOE such as the preservation of the secure state, detection of modification of transmitted TSF data and self-testing of the TOE.

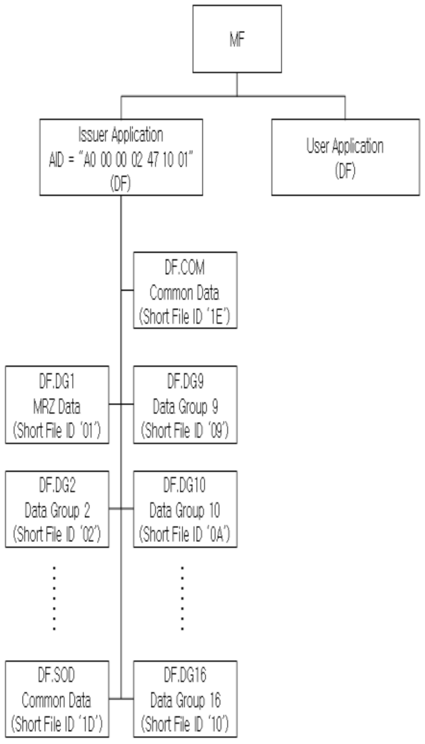
In order to protect the TOE assets in the following table, the TOE provides security functions, such as the confidentiality, the integrity, the authentication and the access control, etc.

Category			Description	Storage
MRTD User Data	ePassport Identity Data	Personal Data of the ePassport Holder	Data stored in EF.DG1, EF.DG2, EF.DG5 ~ EF.DG13, EF.DG16	ePassport Identity Data
		Biometric Data of the ePassport Holder	Data stored in EF.DG3, EF.DG4	
	ePassport Authentication Data		EF.SOD, EAC Chip Authentication Public Key (EF.DG15)	
	EF.CVCA		The CVCA Digital signature Verification Key identifier list used by the TOE to authenticate the Inspection System using EAC-TA	
	EF.COM		LDS version information., tag list of DG used	
MRTD TSF Data	EAC Chip Authentication Private Key		The Chip Private key used by the TOE to verify the authenticity of the MRTD chip using EAC-CA.	Secure Memory
	AA Chip Authentication Private Key		The Chip Private key used by the TOE to verify the authenticity of the MRTD chip using AA	
	CVCA Certificate		The Root CA Certificate issued in EAC-PKI during the personalization phase.	
	CVCA Digital signature Verification Key		The CVCA Certificate Public key created by certificate update after personalization phase.	
	Current Date		Date of issuing the ePassport is recorded during personalization phase. The TOE, However, internally updates it as the latest date among issuing dates of CVCA Link Certificate, DV certificate or Issuing State IS certificate during operational use phase.	

	BAC Authentication Key	BAC authentication encryption key BAC authentication MAC key	
	BAC Session Key	BAC session encryption key BAC session MAC key,	Temporary Memory
	EAC Session Key	EAC session encryption key EAC session MAC key,	
COS TSF Data	SCP02 Authentication Key	SCP02 authentication encryption key SCP02 authentication MAC key SCP02 authentication DEK key	Secure Memory
	COS Lifecycle	COS Lifecycle Status	
	SCP02 Session Key	SCP02 session encryption key SCP02 session MAC key	Temporary Memory

Table 10 TOE Assets

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

Category	DG	Contents	LDS Structure
MRZ Data	DG1	Document Type	 MF Issuer Application AID = "A0 00 00 02 47 10 01" (DF) User Application (DF) DF.COM Common Data (Short File ID '1E') DF.DG1 MRZ Data (Short File ID '01') DF.DG9 Data Group 9 (Short File ID '09') DF.DG2 Data Group 2 (Short File ID '02') DF.DG10 Data Group 10 (Short File ID '0A') DF.SOD Common Data (Short File ID '1D') DF.DG16 Data Group 16 (Short File ID '10')
		Issuing State	
		Name of the Holder	
		Document Number	
		Check Digit of Document Number	
		Nationality	
		Date of Birth	
		Check Digit of DOB	
		Sex	
		Date of Expiry	
		Check digit of DOE	
		Composite Check Digit	
Biometric Data	DG2	Encoded Face Info	
	DG3	Encoded Fingerprint Info	
	DG4	Encoded Iris Info	
Others	DG5	Display Portrait	
	DG6		
	DG7	Display Signature	
	DG8		
	DG9		
	DG10		

	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13		
	DG14	EAC Chip Authentication Public Key	
	DG15	AA Digital signature Verification Key (optional)	
	DG16	Person(s) to Notify	

Table 11 Contents of LDS

4 Conformance Claims

This Security Target claims conformance with the Common Criteria, Protection Profile and Assurance Package.

4.1 Conformance with the Common Criteria

This Security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, part 1 : Introduction and general model, Version 3.1r3, 2009. 7, CCMB-2009-97-001
- Common Criteria for Information Technology Security Evaluation, part 2 : Security functional requirements, Version 3.1r3, 2009. 7, CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation, part 3 : Security assurance requirements, Version 3.1r3, 2009. 7, CCMB-2009-07-003

As follows

- Part 2 Conformant
- Part3 Conformant

4.2 Conformance with the Protection Profile

This Security Target claims demonstrable conformance to

- Protection Profile : ePassport Protection Profile V2.1(KECS-PP-0163a-2009, 2010. 6)

4.3 Conformance with the Assurance Package

This Security Target claims conformance to

- Assurance Package EAL4 augmented with ADV_IMP.2, ATE_DPT.2, AVA_VAN.

4.4 Conformance Claims Rationale

4.4.1 TOE Type

The TOE type defined in this ST is equivalent with the one defined in the PP. Therefore, this ST demonstrably conforms to the PP.

	Protection Profile	Security Target
TOE Type	The TOE is the IC chip operating system (COS), the MRTD Application and the MRTD Application Data. The IC chip elements are excluded from the scope of the TOE.	The TOE consists of the SK COS (IC chip operating system), the MRTD Application and the MRTD Application Data which are loaded in the Samsung S3CC9LC IC chip. The IC chip elements are excluded from the scope of the TOE.

Table 12 TOE Definition

4.4.2 TOE Security Environment

The Security Environment defined in this ST is equivalent with those defined in the PP. This ST added T. SCP02 Replay Attack to the Threats. Also, this ST modified T. BAC Authentication Key Disclose, T. Session Data Reuse, T. Residual Information, P. Application Program Loading, P. ePassport Access Control and A. Inspection System to be equivalent or more restrictive than the Protection Profile. Therefore, this ST demonstrably conforms to the PP.

Security Environment	PP	ST (+) : Added, (*): Modified	Rationale
Threats		T. SCP02 Replay Attack(+)	The TOE authenticates the Personalization Agent using SCP02 Mutual Authentication which is not defined in the PP. T. SCP02 Replay Attack is added in that the threat agent may bypass SCP02 Mutual Authentication. It makes the authentication function of the ST more restrictive than the PP without damaging the Threats defined in the PP. Therefore, this ST is demonstrably conformant to the PP.
	T. TSF Data Modification T. Eavesdropping T. Forgery and Corruption of Personal Data	T. TSF Data Modification T. Eavesdropping T. Forgery and Corruption of Personal Data	Identical to the PP.

	T. BAC Authentication Key Disclose	T. BAC Authentication Key Disclose(*)	The ST modified the application note of T. BAC Authentication Key Disclose to be equivalent to the PP. Therefore, this ST is demonstrably conformant to the PP.
	T. BAC Replay Attack T. Damage to Biometric Data T. EAC-CA Bypass T. IS Certificate Forgery	T. BAC Replay Attack T. Damage to Biometric Data T. EAC-CA Bypass T. IS Certificate Forgery	Identical to the PP.
	T. Session Data Reuse	T. Session Data Reuse(*)	AA and SCP02 might be vulnerable to ciphertext only attack. Therefore, the ST adds AA and SCP02 to T. Session Data Reuse. It makes the ST more restrictive than the PP to add AA and SCP02 to T. Session Data Reuse without damaging the Threats defined in the PP. Therefore, this ST is demonstrably conformant to the PP.
	T. Skimming T. Malfunction T. Leakage to Cryptographic Key Information T. ePassport Reproduction	T. Skimming T. Malfunction T. Leakage to Cryptographic Key Information T. ePassport Reproduction	Identical to the PP.
	T. Residual Information	T. Residual Information(*)	The threat agent may disclose to critical information using SCP02 Session Key remaining in the temporary memory. Therefore, the ST adds SCP02 to T. Residual Information. It makes the ST more restrictive than the PP to add SCP02 to T. Residual Information without damaging the Threats defined in the PP. Therefore, this ST is demonstrably conformant to the PP.
OSP	P. International Compatibility P. Security Mechanism Application Procedures	P. International Compatibility P. Security Mechanism Application Procedures	Identical to the PP.

	P. Application Program Loading	P. Application Program Loading(*)	The ST prevents the TOE from loading application program other than the MRTD Application while the PP allows application program loading which makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	P. Personalization Agent	P. Personalization Agent	Identical to the PP.
	P. ePassport Access Control	P. ePassport Access Control(*)	The ST categorizes the Personalization Agent Authorization into two; the Personalization Agent Issuing Authorization and the Personalization Agent Management Authorization. The Personalization Agent cannot accesses the personal data of the ePassport holder when the Personalization Agent acquires the Personalization Agent Management Authorization It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	P. PKI P. Range of RF Communication	P. PKI P. Range of RF Communication	Identical to the PP.
Assumptions	A. Certificate Verification	A. Certificate Verification	Identical to the PP.
	A. Inspection System	A. Inspection System(*)	The ST defines that the Inspection System may implement AA security mechanism in addition to the security mechanisms defined in the PP. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	A. IC Chip A. MRZ Entropy	A. IC Chip A. MRZ Entropy	Identical to the PP.

Table 13 Security Environments

4.4.3 TOE Security Objectives

The Security Objectives defined in this ST are equivalent with those defined in the PP. This ST added O. SCP02 and

O. AA. Also, this ST modified the Security Objectives for the TOE O. Management, O. Session Termination, O. Secure Messaging, O. Deleting Residual Information, O. Replay Prevention and the Security Objectives for the Environment OE. Application Program Loading, OE. Handling Information Leakage to be equivalent or more restrictive than those defined in the PP. Therefore, this ST demonstrably conforms to the PP.

Security Objectives	PP	ST (+) : Added, (*): Modified	Rationale
Security Objectives for the TOE	O. Management	O. Management(*)	The TOE provides means to manage the COS TSF Data along with the MRTD Application Data in the Personalization phase to the authorized Personalization Agent. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	O. Security Mechanism Application Procedures	O. Security Mechanism Application Procedures	Identical to the PP.
	O. Session Termination	O. Session Termination(*)	The TOE terminates the session in case of failure of the SCP02 Mutual Authentication. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	O. Secure Messaging	O. Secure Messaging(*)	The TOE provides means to protect transmitted COS TSF Data. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	O. Certificate Verification O. Self-protection	O. Certificate Verification O. Self-protection	Identical to the PP.
	O. Deleting Residual Information	O. Deleting Residual Information(*)	The TOE provides means to delete residual information such as the SCP02 Session Key, the random numbers, the DV certificate, the IS certificate. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	O. Replay Prevention	O. Replay Prevention(*)	The TOE provides means to prevent replay attack during SCP02 Mutual Authentication and AA authentication.

			It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	O. Access Control	O. Access Control	Identical to the PP.
	O. Handling Information Leakage		The ST defines O. Handling Information Leakage as a Security Objectives for the Environment according to the application note in the PP. Therefore, this ST is demonstrably conformant to the PP.
	O. BAC	O. BAC	Identical to the PP.
	O. EAC	O. EAC	Identical to the PP.
		O. SCP02(+)	The TOE authenticates the Personalization Agent using SCP02 Mutual Authentication to allow the Personalization Agent Management Authority only to successfully authenticated Personalization Agent. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
		O. AA(+)	The TOE implements the AA security mechanism to provide means to authenticate the TOE for the Inspection System. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
Security Objectives for the Environment	OE. Passport Book Manufacturing Security OE. Procedures of ePassport holder Check	OE. Passport Book Manufacturing Security OE. Procedures of ePassport holder Check	Identical to the PP.
	OE. Application Program Loading	OE. Application Program Loading(*)	This ST only allows the MRTD Application to be loaded on the MRTD Chip. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.

	OE. Certificate Verification OE. Personalization Agent OE. Inspection System OE. IC Chip OE. MRZ Entropy OE. PKI OE. Range of RF Communication	OE. Certificate Verification OE. Personalization Agent OE. Inspection System OE. IC Chip OE. MRZ Entropy OE. PKI OE. Range of RF Communication	Identical to the PP.
		OE. Handling Information Leakage(*)	The ST defines O. Handling Information Leakage as a Security Objectives for the Environment according to the application note in the PP. Therefore, this ST is demonstrably conformant to the PP.

Table 14 Security Objectives

4.4.4 Security Functional Requirements

The Security Functional Requirements defined in this ST are equivalent with those defined in the PP. This ST added FCS_CKM.1(2), FDP_DAU.1, FIA_UAU.2, FMT_MOF.1(2), FMT_MTD.1(3), FMT_MTD.1(4), FMT_MTD.1(5) and modified FDP_ACF.1, FDP_UCT.1, FDP_UIT.1, FMT_MOF.1(1), FMT_MSA.3, FMT_MTD.1(1), FMT_SMR.1, FPT_TST.1. Additionally, Security Functional Requirements FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4), FPR_UNO.1 were removed from the ST according to the application notes from the PP. The TOE satisfies these requirements by using the co-processor of the certified IC chip and cryptographic libraries loaded in the certified IC chip.

	PP	ST (+) : Added, (*): Modified	Rationale
SFR	FCS_CKM.1	FCS_CKM.1(1)	Identical to the PP.
		FCS_CKM.1(2)(+)	The TOE generates SCP02 Session Key when the Personalization Agent is authenticated using SCP02 Mutual Authentication. The ST added this SFR using Iteration Operation defined in the PP. It makes the ST more restrictive than the PP. Therefore,

			this ST is demonstrably conformant to the PP.

	FCS_CKM.2(1)
	FCS_CKM.2(2)
		FCS_CKM.2(1)
		FCS_CKM.2(2)
			The Selection Operation defined in the PP was used to state the requirements.
			Therefore, this ST is demonstrably conformant to the PP.

	FCS_CKM.4	FCS_CKM.4	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.

	FCS_COP.1(1)
	FCS_COP.1(2)
			These SFRs were removed from the ST in that the TOE satisfies these requirements by using the IC chip. Additionally, the SFR dependencies related to these SFRs are no longer relevant. Therefore, this ST is equivalent with the PP and is demonstrably conformant to the PP.

	FCS_COP.1(3)	FCS_COP.1	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.
	FCS_COP.1(4)		This SFR was removed from the ST in that the TOE satisfies these requirements by using the IC chip. Additionally, the SFR dependencies related to this SFR is no longer relevant. Therefore, this ST is equivalent with the PP and is demonstrably conformant to the PP.
	FDP_ACC.1	FDP_ACC.1	Identical to the PP.
	FDP_ACF.1	FDP_ACF.1(*)	The ST categorizes the Personalization Agent Authorization into two; the Personalization Agent Issuing Authorization and the Personalization Agent Management Authorization. The Personalization Agent cannot accesses the personal data of the ePassport holder when the Personalization Agent acquires the Personalization Agent Management Authorization It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
		FDP_DAU.1(+)	This ST defines AA security mechanism to provide means to authenticate the TOE for the Inspection System which is not in the PP. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FDP_RIP.1	FDP_RIP.1	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.

	FDP_UCT.1	FDP_UCT.1(*)	This ST adds SCP02 security mechanism to the application notes of the SFR. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FDP_UIT.1	FDP_UIT.1(*)	The Selection Operation defined in the PP was used to state the requirements and the usage of the MAC key for SCP02 session is added to the application notes as a mean to protect integrity of transmitted data. Therefore, this ST is demonstrably conformant to the PP.
	FIA_AFL.1	FIA_AFL.1	The Selection Operation and the Assignment Operation defined in the PP was used to state the requirements. Also, the Refinement Operation was used to define the 'user session termination' in the PP. Therefore, this ST is demonstrably conformant to the PP.
	FIA_UAU.1(1)	FIA_UAU.1(1)	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.
	FIA_UAU.1(2)	FIA_UAU.1(2)	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.
		FIA_UAU.2(+)	This ST defines SCP02 security mechanism to authenticate the Personalization Agent. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FIA_UAU.4 FIA_UAU.5	FIA_UAU.4 FIA_UAU.5	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.
	FIA_UID.1	FIA_UID.1	The ST defines means to identify the Personalization Agent. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FMT_MOF.1	FMT_MOF.1(1)(*)	This ST refines the 'Personalization Agent in the Personalization phase' to 'Personalization Agent with Personalization Agent Issuing Authority in the Personalization phase' using the Refinement Operation defined in the PP. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
		FMT_MOF.1(2)(+)	This ST defines that the Personalization Agent and the

			TOE can manage the COS lifecycle. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FMT_MSA.1	FMT_MSA.1	Identical to the PP.
	FMT_MSA.3	FMT_MSA.3(*)	This ST modifies FMT_MSA.3 using the Refinement Operation to make the TOE perform static attribute initialization instead of the Personalization Agent. The initial values of the static attribute are always the same and it does not damage the TSF for the TOE to generate the initial values. It makes the ST equivalent with the PP. Therefore, this ST is demonstrably conformant to the PP.
	FMT_MTD.1(1)	FMT_MTD.1(1)(*)	This ST modifies the 'Personalization Agent in the Personalization Phase' to 'Personalization Agent with the Personalization Agent Issuing Authority in the Personalization Phase' using the Refinement Operation. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FMT_MTD.1(2)	FMT_MTD.1(2)	Identical to the PP.
		FMT_MTD.1(3)(+)	This ST restricts the ability to modify GP registry to the Personalization Agent with the Personalization Agent Issuing Authority. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
		FMT_MTD.1(4)(+)	This ST restricts the ability to write the BAC Authentication Key in the secure memory to the TOE and the Personalization Agent with the Personalization Agent Issuing Authority. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
		FMT_MTD.1(5)(+)	This ST restricts the ability to write the SCP02 Authentication Key in the secure memory to the Personalization Agent with the Personalization Agent Issuing Authority. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FMT_MTD.3 FMT_SMF.1	FMT_MTD.3 FMT_SMF.1	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.

	FMT_SMR.1	FMT_SMR.1(*)	This ST defines the authorities of the Personalization Agent in the PP more specifically using the Refinement Operation. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.
	FPR_UNO.1		This SFR was removed from the ST in that the TOE satisfies these requirements by using the IC chip. Additionally, the SFR dependencies related to this SFR is no longer relevant. Therefore, this ST is equivalent with the PP and is demonstrably conformant to the PP.
	FPT_FLS.1 FPT_ITI.1	FPT_FLS.1 FPT_ITI.1	The Assignment Operation defined in the PP was used to state the requirements. Therefore, this ST is demonstrably conformant to the PP.
	FPT_TST.1	FPT_TST.1(*)	This ST modifies the authorized users to the authorized Personalization Agent in the Personalization Phase using the Refinement Operation. It makes the ST more restrictive than the PP. Therefore, this ST is demonstrably conformant to the PP.

Table 15 Security Functional Requirements

4.4.5 Security Assurance Requirements

The Security Assurance Requirements defined in this ST is identical to the one defined in the PP. Therefore, this ST demonstrably conforms to the PP.

	PP	ST	Rationale
SAR	ASE_INT.1 ASE_CCL.1 ASE_SPD.1 ASE_OBJ.2 ASE_ECD.1 ASE_REQ.2 ASE_TSS.1 ADV_ARC.1 ADV_FSP.4 ADV_IMP.2 ADV_TDS.3 AGD_OPE.1	ASE_INT.1 ASE_CCL.1 ASE_SPD.1 ASE_OBJ.2 ASE_ECD.1 ASE_REQ.2 ASE_TSS.1 ADV_ARC.1 ADV_FSP.4 ADV_IMP.2 ADV_TDS.3 AGD_OPE.1	Identical to the PP.

	AGD_PRE.1	AGD_PRE.1	
	ALC_CMC.4	ALC_CMC.4	
	ALC_CMS.4	ALC_CMS.4	
	ALC_DEL.1	ALC_DEL.1	
	ALC_DVS.1	ALC_DVS.1	
	ALC_LCD.1	ALC_LCD.1	
	ALC_TAT.1	ALC_TAT.1	
	ATE_COV.2	ATE_COV.2	
	ATE_DPT.2	ATE_DPT.2	
	ATE_FUN.1	ATE_FUN.1	
	ATE_IND.2	ATE_IND.2	
	AVA_VAN.4	AVA_VAN.4	

Table 16 Security Assurance Requirements

5 TOE Security Environment

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

5.1 Threats

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

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

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

<Threats in the Personalization Phase>

T. TSF Data Modification

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

T. SCP02 Replay Attack

The threat agent may bypass the SCP02 Mutual Authentication by replay data transmitted by the TOE and the Personalization Agent in the initial phase of the SCP02 Mutual Authentication.

Application Notes : The Personalization Agent receives the information required for the authentication according to 'Initialize Update' instruction and delivers the response data to the TOE according to 'External Authentication' instruction. Therefore, the threat agent can bypass the SCP02 Mutual Authentication by acquiring the authentication information and the response data of the Personalization Agent and re-transmitting the data to the Personalization Agent.

<BAC-related Threats in the Operational Use Phase>

T. Eavesdropping

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

T. Forgery and Corruption of Personal Data

In order to forge and corrupt the personal data of the ePassport holder stored in the MRTD chip, the threat agent may attempt access to read the user data by using the unauthorized Inspection System.

T. BAC Authentication Key Disclose

In order to find out the personal data of the ePassport holder, the threat agent may obtain the read-rights of the BAC Authentication Key located inside the TOE and disclose the related information.

Application Notes : The BAC Authentication Key may be generated by Personalization Agent in the Personalization phase or by the TOE in the Personalization Phase. If the Personalization Agent does not provide the BAC Authentication Key in the Personalization phase the TOE produces the BAC Authentication Key and stores the key in the secure memory of the MRTD Chip.

T. BAC Replay Attack

The threat agent may bypass the BAC Mutual Authentication by replay after intercepting data transmitted by the TOE and the Inspection System in the initial phase of the BAC Mutual Authentication.

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

<EAC-related Threats in the Operational Use Phase>

T. Damage to Biometric Data

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

Application Notes : Only the EIS that succeeded the EAC-TA can access the read-rights the biometric data of the ePassport holder. Therefore, the threat agent may attempt to obtain the biometric data by using the unauthorized Inspection System and BIS, etc.

T. EAC-CA Bypass

The threat agent may bypass the authentication of the Inspection System so that to go through EAC-CA by using the threat agent generated EAC Chip Authentication Public Key.

T. IS Certificate Forgery

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

<BAC, EAC, AA and SCP02 –related Threats in the Operational Use Phase >

T. Session Data Reuse

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

Application Notes : When the TOE and Inspection System use the BAC Authentication Key as the BAC Session Key, they are vulnerable to ciphertext only attack as the same session key is used in each BAC session. When the BAC Session Key is generated with the same random number used in the BAC Mutual Authentication, critical information necessary in deriving the session key may be provided to an attacker as the first random number of the TOE is transmitted as plaintext. In case the EIS transmits temporary public key in the EAC-CA and random number in the EAC-TA and AA to other sessions in the same way and the TOE continues to use them, they may be vulnerable to ciphertext only attack. Additionally, if the TOE transmits the SCP02 Session Key used in the previous sessions without generating a new SCP02 Session Key, it might be vulnerable to ciphertext only attack.

T. Skimming

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

<IC Chip-related Threats>

T. Malfunction

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

<Other Threats in the Operational Use Phase>

T. Leakage to Cryptographic Key Information

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

T. ePassport Reproduction

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

T. Residual Information

The threat agent may disclose to critical information by using residual information remaining while the TSF data, such as BAC Authentication Key, BAC Session Key, EAC Session Key, SCP02 Session Key, DV certificate and IS certificate, etc., are recorded and used in temporary memory.

5.2 Organizational Security Policies

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

P. International Compatibility

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

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

P. Security Mechanism Application Procedure

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

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

P. Application Program Loading

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

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

P. Personalization Agent

The Personalization Agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational Use phase after verifying that the data inside MRTD chip are operating normally after issuing. The Personalization Agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.

P. ePassport Access Control

The Personalization Agent and TOE shall build the ePassport access control policies in order to protect the MRTD Application Data. Also, the TOE shall regulate the roles of user.

Application Notes : The TOE shall build access control policies as of the following according to the ICAO document and EAC specifications. The Personalization Agent acquires the Personalization Agent Issuing Authorization and the Personalization Agent Management Authorization when successfully authenticated as the Personalization Agent in the Personalization Phase and in the Operational Use Phase, respectively.

		List of Objects	**Objects**									
			Personal data of the ePassport holder		**Personal data of the ePassport holder**		**Personal data of the ePassport holder**		**Personal data of the ePassport holder**		**Personal data of the ePassport holder**	
List of Subjects		**Security Attributes**	**Read Right**	**Write Right**	**Read Right**	**Write Right**	**Read Right**	**Write Right**	**Read Right**	**Write Right**	**Read Right**	**Write Right**
Subjects	**BIS**	**BAC Authorization**	*Allow*	*Deny*	*Deny*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*
	EIS	**BAC Authorization**	*Allow*	*Deny*	*Deny*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*
		EAC Authorization	*Allow*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*	*Allow*	*Deny*
	Personalization Agent	**Personalization Agent Issuing Authorization**	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*	*Allow*
		Personalization Agent Management Authorization	*Deny*	*Deny*	*Deny*	*Deny*	*Deny*	*Deny*	*Deny*	*Deny*	*Deny*	*Deny*

Table 17 TOE Access Control Policies

P. PKI

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

P. Range of RF Communication

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

5.3 Assumptions

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

A. Certificate Verification

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

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

Application Note : The BIS shall periodically verify the CSCA Certificate according to the ICAO PKD or the diplomatic channel of the issuing country. EIS shall periodically verify the CVCA Certificate and the CVCA Link Certificate according to the diplomatic channel of the issuing country.

A. Inspection System

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

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

Application Notes : The TOE denies the request to access EF.SOD by the Inspection System that failed the BAC Mutual Authentication.

As the BIS support the BAC and PA security mechanisms, it obtains the read-rights for the personal and authentication data of the ePassport holder if the BAC Mutual Authentication using the BAC Authentication Key succeeds. Then, by establishing the BAC Secure Messaging with the BAC Session Key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the BAC. Then, by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder.

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

Additionally, the Inspection System may implement the AA security mechanism. If the Inspection System supports the AA security mechanism, the Inspection System can authenticate the TOE using the AA security mechanism.

A. I C Chip

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

Application Notes : Samsung S3CC9LC, the IC Chip on which the TOE operates, is a CCRA EAL5+ certified product. S3CC9LC supports cryptographic functions such as Random Number Generation and Hardware DES/TDES. It also provides RSA Cryptographic Library (version 3.7s) and ECC Cryptographic Library (version 2.4s). Additionally, S3CC9LC provides security features that protect the TOE from the physical attack.

A. MRZ Entropy

The BAC Authentication Key seed takes the MRZ entropy to ensure the secure BAC Authentication Key.

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

6 TOE 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.

6.1 Security Objectives for the TOE

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

O. Management

The TOE shall provide the means to manage the MRTD Application Data and the COS TSF Data in the Personalization phase to the authorized Personalization Agent.

Application Notes : In the Personalization phase, the Personalization Agent shall deactivate the writing function after recording the MRTD Application Data.

O. Security Mechanism Application Procedures

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

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

O. Session Termination

The TOE shall terminate the session in case of failure of the SCP02 Mutual Authentication, the BAC Mutual Authentication, failure of the EAC-TA or detecting modification in the transmitted TSF data.

O. Secure Messaging

The TOE shall ensure confidentiality and integrity to protect the transmitted user data, MRTD TSF Data and COS TSF Data.

Application Notes : The Personalization Agent can set the TOE to ensure confidentiality and integrity to protect the transmitted user and TSF data in the personalization phase.

O. Certificate Verification

The TOE shall automatically update the certificate and Current Date by checking valid date on the basis of the CVCA

Link Certificate provided by the Inspection System.

O. Self-protection

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

O. Deleting Residual Information

When allocating resources, the TOE shall provide means to ensure that previous security-related information (Ex.: BAC Session Key, EAC Session Key, SCP02 Session Key, random numbers, DV certificate, IS certificate etc.) is not included.

O. Replay Prevention

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

Application Notes : The TOE generates the transmitted data to the Inspection System in the SCP02 Mutual Authentication, BAC Mutual Authentication and EAC-TA to be different per session and does not use the BAC Authentication Key as the BAC Session Key. Also, the TOE does not provide critical information necessary in deriving session key by generate the BAC Session Key with the same random number used in the BAC Mutual Authentication. Also, the TOE does not use SCP02 Authentication Key as the SCP02 Session Key and does not use the same random number internally during SCP02 Mutual Authentication. After successfully authenticated using SCP02 Mutual Authentication, the TOE increases the Sequence Counter used to generate the session key to prevent session key related information from being disclosed. Additionally, the TOE generates random numbers for the AA security mechanism to be different per session.

O. Access Control

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

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

O. BAC

The TOE executes the BAC Mutual Authentication of the Inspection System with the TOE by implementing the BAC security mechanism in order to allow the read-rights for the personal data of the ePassport holder only to the authorized Inspection System. Also, the TOE generates the BAC Session Key to be used for the BAC Secure Messaging.

O. EAC

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

O. SCP02

The TOE executes the SCP02 Mutual Authentication of the Personalization Agent with the TOE by implementing the SCP02 security mechanism in order to allow the access-rights for the MRTD Application Data and COS TSF Data only to the authorized Personalization Agent. Also, the TOE generates the SCP02 Session Key to be used for the SCP02 Secure Messaging.

O. AA

The TOE implements AA security mechanism in order to allow the Inspection System to validate the authenticity of the TOE.

6.2 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 MRTD chip and attack attempt of the Grandmaster chess, replacement of the portrait and modification of the MRZ data, etc.

OE. Procedures of ePassport holder Check

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

OE. Application Program Loading

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

Application Notes : No application program other than the MRTD Application can be loaded in the MRTD chip.

OE. Certificate Verification

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

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

OE. Personalization Agent

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

OE. Inspection System

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

OE. IC Chip

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

OE. MRZ Entropy

Personalization Agent shall ensure the MRZ entropy to ensure the secure BAC Authentication Key.

OE. PKI

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

OE. Range of RF Communication

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

OE. Handling Information Leakage

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

6.3 Rationale of Security Objectives

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

The rationale of security objectives demonstrates the following:

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

. Each security objective traces to at least one assumption, threat or organizational security policy.

The following table shows the mapping between security environments and security objectives.

Security Objectives / Security Environments	Security Objectives for the TOE													Security Objectives for the Environment										
	O. Management	O. Security Mechanism Application Procedures	O. Session Termination	O. Secure Messaging	O. Certificate Verification	O. Self-protection	O. Deleting Residual Information	O. Replay Prevention	O. Access Control	O. BAC	O. EAC	O.S C P02	O. AA	OE. PASSPORT BOOK MANUFACTURING SECURITY	OE. Procedures of ePassport holder Check	OE. Application Program Loading	OE. Certificate Verification	OE. Personalization Agent	OE. Inspection System	OE. IC Chip	OE. MRZ Entropy	OE. PKI	OE. Range of RF Communication	OE. Handling Information Leakage
T. TSF Data Modification	X		X	X					X									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					
T. IS Certificate Forgery	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

T. ePassport Reproduction													X	X	X									
T. Residual Information							X																	
T. SCP02 Replay Attack								X																
P. International Compatibility																		X						
P. Security Mechanism Application Procedures		X																	X					
P. Application Program Loading																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			

Table 18 Security Environments and Security Objectives Mapping

6.3.1 Rationale of Security Objectives for the TOE

O. Management

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

Also, this security objective provides the Personalization Agent with the means to record CVCA Certificate in secure memory in the Personalization phase, therefore is required to counter the threat of T. IS Certificate Forgery.

O. Security Mechanism Application Procedures

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

Also, this security objective is required to counter the threat of T. EAC-CA Bypass by eliminating the cases of demonstrating the genuine TOE to the unauthorized Inspection System as it ensures the application order of security mechanisms so that to enable the EAC-CA execution by only the Inspection System with access-rights for the EAC Chip Authentication Public Key through the BAC execution.

O. Session Termination

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

O. Secure Messaging

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

O. Certificate Verification

This security objective is required to enforce the organizational security policies of P. PKI as it ensures for the TOE to check the valid date on the basis of the CVCA Link Certificate provided by the Inspection System, therefore to automatically update the certificate and the Current Date.

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

O. Self-protection

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

O. Deleting Residual Information

This security objective is required to counter the threat of T. Residual Information by deleting all of the previous security-related information(SCP02 Session Key, BAC Session Key and EAC Session Key, etc.) so that it is not included when the TOE allocates or deal locates memory resources, therefore ensuring that information is not available.

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

O. Replay Prevention

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

O. Access Control

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

This security objective is required to counter the threats of T. TSF Data Modification and T. BAC Authentication Key Disclose as it allows the authorized Personalization Agent has the write-rights of the MRTD Application Data in the Personalization phase and denies the access by Personalization Agent in the Operational Use phase.

O. BAC

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

This security objective is required to counter the threats of T. Forgery and Corruption of Personal Data and T. Skimming as the TOE allows the read-rights for the personal data of the ePassport holder only to the authorized Inspection System by generating the BAC Session Key during the BAC Mutual Authentication and denies access by the Inspection System that does not have the read-rights.

O. EAC

This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the ePassport holder, therefore gives the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System of which the EAC-TA is successfully completed.

This security objective is required to counter the threats of T. Damage to Biometric Data and T. Skimming as the TOE allows the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System through the EAC-TA by generating the EAC Session Key during the EAC-CA and denies access by the Inspection System that does not have the read-rights.

O. SCP02

This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the SCP02 security mechanism to control access to the MRTD Application Data and COS Application Data. Also, this security objective is required to enforce the P. Personalization Agent as the TOE implements SCP02 security mechanism to control access to the MRTD Application Data, therefore gives the write-rights for the MRTD Application Data only to the authorized Personalization Agent of which the SCP02 Mutual Authentication is successfully completed.

O. AA

This security objective is required to counter the threats of T. ePassport Reproduction as the TOE implements AA security mechanism to validate the authenticity of the TOE.

6.3.2 Rationale of Security Objectives for the Environment

OE. Passport Book Manufacturing Security

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

OE. Procedures of ePassport holder Check

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

OE. Application Program Loading

This security objective for 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.

Application Notes : No application program other than the MRTD Application can be loaded in the MRTD chip.

OE. Certificate Verification

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

OE. Personalization Agent

This security objective for environment is required to enforce the organizational security policies of P. International Compatibility and P. Personalization Agent by ensuring that the TOE is delivered to the Operational Use phase after securely issuing the ePassport so that the Personalization Agent can check that the issuing subject has not been changed, verifying normal operation and compatibility of the ePassport in the Personalization phase and deactivating writing function.

This security objective for environment also is required to enforce the organizational security policies of P. ePassport Access Control as it defines the role of the Personalization Agent. Also, this security objective for environment is required to support the assumption of A. Certificate Verification because the Personalization Agent makes certificates necessary in the PA and EAC support available to the Inspection System.

Additionally, this security objective for the environment is required to counter the threats of T. TSF Data Modification as the Personalization Agent deactivates the writing function to the TSF Data after successfully personalize the ePassport.

OE. Inspection System

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

This security objective for environment is required to counter the threat of T. Eavesdropping as the confidentiality and integrity of the transmitted data are ensured by establishing the BAC Secure Messaging after generating the BAC Session Key through the BAC Key Distribution when the Inspection System communicates with the TOE.

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

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

OE. IC Chip

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

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

OE. MRZ Entropy

This security objective for environment is required to support the assumption of A. MRZ Entropy by providing MRZ entropy necessary for the Personalization Agent to ensure the secure BAC Authentication Key.

OE. PKI

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

OE. Range of RF Communication

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

OE. Handling Information Leakage

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

7 Extended Components Definition

There are no expended components in this Security Target.

8 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.

The external entities defined in this ST are the Personalization Agent, BIS, EIS and the MRTD Chip. The subjects, objects, operations and security attributes used in the security functional requirements are shown in the following table. Additionally, this ST defines SSC (Send Sequence Counter) as a security attribute for the secure messaging.

<table>
<tr><th>Subjects</th><th>Objects</th><th>Operations</th></tr>
<tr>
<td>
<table>
<tr><th>Subjects</th><th>Security Attributes</th></tr>
<tr><td>BIS</td><td>BAC Authorization</td></tr>
<tr><td>EIS</td><td>BAC Authorization,
EAC Authorization</td></tr>
<tr><td>Personalization Agent</td><td>Issuing Authorization,
Management Authorization</td></tr>
</table>
</td>
<td>
<MRTD User Data>
<table>
<tr><th rowspan="2">Objects</th><th colspan="2">Security Attributes</th></tr>
<tr><th>Security Attributes of Object’s Operation</th><th>Security Attributes of Object’s Access-Rights</th></tr>
<tr><td rowspan="2">Personal Data of the ePassport Holder</td><td>Read-Rights</td><td>BAC Authorization,
EAC Authorization,
Personalization Agent Issuing Authorization</td></tr>
<tr><td>Write-Rights</td><td>Personalization Agent Issuing Authorization</td></tr>
<tr><td rowspan="2">Biometric data of the ePassport holder</td><td>Read-Rights</td><td>EAC Authorization,
Personalization Agent Issuing Authorization</td></tr>
<tr><td>Write-Rights</td><td>Personalization Agent Issuing Authorization</td></tr>
<tr><td rowspan="2">ePassport authentication data</td><td>Read-Rights</td><td>BAC Authorization,
EAC Authorization,
Personalization Agent Issuing Authorization</td></tr>
<tr><td>Write-Rights</td><td>Personalization Agent Issuing Authorization</td></tr>
<tr><td rowspan="2">EF.CVCA</td><td>Read-Rights</td><td>BAC Authorization,
EAC Authorization,
Personalization Agent Issuing Authorization</td></tr>
<tr><td>Write-Rights</td><td>Personalization Agent Issuing Authorization</td></tr>
</table>
</td>
<td>· Read
· Write</td>
</tr>
</table>

	EF.COM	Read-Rights	BAC Authorization, EAC Authorization, Personalization Agent Issuing Authorization	
		Write-Rights	Personalization Agent Issuing Authorization	

Table 19 TOE Access Control Policies

8.1 TOE Security Functional Requirements

The security functional requirements for this Security Target consist of the following components from Part2 of the CC, summarized in the following table.

Security Functional Classes	Security Functional Components	
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.1(2)	Cryptographic key generation (SCP02 Session Key Generation)
	FCS_CKM.2(1)	Cryptographic key distribution (KDF Seed Distribution for BAC Session Key generation)
	FCS_CKM.2(2)	Cryptographic key distribution (KDF Seed Distribution for EAC Session Key generation)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	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)	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)
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification

Security Management (FMT)	FMT_MOF.1(1)	Management of security functions behavior (Writing Function)
	FMT_MOF.1(2)	Management of security functions behavior (COS Lifecycle Management)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Info.)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialization)
	FMT_MTD.1(3)	Management of TSF data (COS Management)
	FMT_MTD.1(4)	Management of TSF data (BAC Authentication Key Management)
	FMT_MTD.1(5)	Management of TSF data (SCP02 Authentication Key Management)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Specification of management functions
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_TST.1	TSF testing

Table 20 Security Functional Requirements

8.1.1 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

FCS_CKM.1.1(1) The TSF shall generate **encryption keys and MAC keys** in accordance with a specified cryptographic key generation algorithm [Appendix 5.1 Key Derivation Mechanism] and specified cryptographic key sizes [112bit] that meet the following: [the ICAO document].

Application Notes : The TOE generates the BAC Authentication Key, BAC Session Key and EAC Session Key by using key derivation mechanism. If the Personalization Agent generates BAC Authentication Key and records it in the TOE in the Personalization phase according to the Issuing policy of the ePassport, the TOE does not generate the BAC Authentication Key. Otherwise, the TOE generates the BAC Authentication Key and records it in the secure memory.

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

Hierarchical to : No other components.

Dependencies : [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate **session key** in accordance with a specified cryptographic key generation algorithm [Appendix E.4..1 DES Session Keys] and specified cryptographic key sizes [112bit] that meet the following: [GP Specification].

FCS_CKM.2(1) Cryptographic key distribution (KDF Seed Distribution for BAC Session Key generation)

Hierarchical to : No other components.

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

FCS_CKM.2.1(1) The TSF shall distribute **KDF Seed for the BAC Session Key** generation in accordance with a specified cryptographic key distribution method [*Key Establishment Mechanism 6*] that meets the following : [*ISO/IEC 11770-2*].

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

Hierarchical to : No other components.

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

FCS_CKM.2.1(1) The TSF shall distribute **KDF Seed for the EAC Session Key** generation in accordance with a specified cryptographic key distribution method [*Elliptic Curve Diffie-Hellman Key-agreement Protocol*] that meets the following : [*ISO/IEC 15946-3*].

FCS_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]

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

FCS_COP.1 Cryptographic operation (Hash Function)

Hierarchical to : No other components.

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

FCS_COP.1.1 The TSF shall perform [hash operation] in accordance with a specified cryptographic algorithm [*SHA-1, SHA-224, SHA-256*] and cryptographic key sizes [none] that meet the following: [*ISO/IEC 10118-3*].

Application Notes : In the key derivation mechanism of the ICAO document, the SHA-1 is used as a hash function in order to generate the session key used in the BAC or EAC Secure Messaging. Additionally, the SHA-1 is used to generate AA Digital signature and SHA-1, SHA-224 or SHA-256 is used to verify certificates for EAC-TA.

8.1.2 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 [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 attribute 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 [the ePassport access control policy] to objects based on the following: [Table 21, Table 22, [none]].

Subjects	Security Attributes
BIS	BAC Authorization
EIS	BAC Authorization, EAC Authorization
Personalization Agent	Personalization Agent Issuing Authorization, Personalization Agent Management Authorization

Table 21 Security Attributes for the Subjects

Objects	Security Attributes	
	Security Attributes of Object's Operation	Security Attributes of Object's Access Rights
Personal data of the ePassport holder	Read-Rights	BAC Authorization, EAC Authorization, Personalization Agent Issuing Authorization
	Write-Rights	Personalization Agent Issuing 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

Table 22 Security Attributes for the Objects

Application Notes : The BAC authorization is the right given to the user identified with the Inspection System that supports the MRTD Application by FIA_UID.1 when the BAC Mutual Authentication succeeds. The EAC authorization is the right given when the Inspection System with the BAC authorization succeeds in the EAC-CA and the EAC-TA and the read-rights of the biometric data is included in all of CVCA Certificate, DV certificate and IS certificate held by that Inspection System. Even when the EAC-CA and the EAC-TA succeed, the Inspection System has only the BAC authorization if the certificates do not include the read-rights.

The Personalization Agent Issuing Authorization and the Personalization Agent Management Authorization are the rights given when the Personalization Agent to be successfully authenticated in the Personalization phase and the Operational Use Phase, respectively.

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

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

b) [none].
]

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

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

a) Explicitly deny access of subjects to objects if instructions order of the Inspection System is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specifications
b) Explicitly deny read of subjects to biometric data if there is no the read-rights of biometric data in IS certificate of the EIS that has the EAC authorization
c) Explicitly deny access(read, write, etc.) of the unauthorized Inspection System to all objects
d) [Explicitly deny access(read, write) of the Personalization Agent to the Personal Data of the ePassport holder when the Personalization Agent Management Authorization is acquired]

FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.
Dependencies: No dependencies.
FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [AA Chip Authentication Private Key].
FDP_DAU.1.2 The TSF shall provide [Inspection System] with the ability to verify evidence of the validity of the

indicated information.

FDP_RIP.1 Subset residual information protection

Hierarchical to : No other components.

Dependencies : No dependencies.

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

a) BAC Session Key

b) EAC Session Key

c) BAC Authentication Key

d) [SCP02 Session Key, Random Numbers]

].

Application Notes : After a session termination, the TSF shall not remain the SCP02 Session Key, the BAC Session Key, the EAC Session Key and random numbers, etc. in temporary memory. The SCP02 Session Key, the BAC Session Key, the EAC Session Key and the BAC Authentication Key, etc. can be ensured unavailable by destroying them with the method defined in FCS_CKM.4.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to : No other components.

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

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

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

The Personalization Agent can decide to protect the data by using SCP02 session encryption key from disclosure or not after successfully authenticated using the SCP02 Mutual Authentication.

FDP_UIT.1 Data exchange integrity

Hierarchical to : No other components.

Dependencies : [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

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

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

Application Notes : The TSF protects integrity of the transmitted data by using the MAC key for BAC session or EAC session. This provides the method of protection against modification, deletion and insertion of user data. The Personalization Agent can enable to protect integrity of the transmitted data by using the MAC key for SCP02 session or not after successfully authenticated using the SCP02 Mutual Authentication. Also, the TOE protects the transmitted data form replay using SSC (Send Sequence Counter).

8.1.3 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 [*'Number of Unsuccessful Authentication Attempts' in Table 23*] unsuccessful authentication attempts occur related to [

a) BAC Mutual Authentication

b) EAC-TA

c) [SCP02 Mutual Authentication]

].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**'Actions' in Table 23**].

Security Mechanisms	Number of Unsuccessful Authentication Attempts	Actions
BAC Mutual Authentication	1	User Session Termination
EAC-TA Mutual Authentication	1	User Session Termination (The EAC-CA shall be performed before executing the EAC-TA if the authentication failure was detected during the EAC-TA Mutual Authentication)
SCP02 Mutual Authentication	1	User Session Termination (The lifecycle of the TOE shall be set to Terminated Phase after 255

		times of authentication failure.)

Table 23 Authentication Failure Handling Policies

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(1) The TSF shall allow [

a) indication that support the BAC mechanism

b) [none]

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

FIA_UAU.1.2(1) The TSF shall require each user to be successfully authenticated 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(2) The TSF shall allow [

a) to perform the EAC-CA

b) to read user data except the biometric data of the ePassport holder

c) [to perform the AA]

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

FIA_UAU.1.2(2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action (SCP02 Mutual Authentication)

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to : No other components.

Dependencies : No dependencies.

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

a) BAC Mutual Authentication

b) EAC-TA

c) [SCP02 Mutual Authentication, AA]

].

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to : No other components.

Dependencies : No dependencies.

FIA_UAU.5.1 The TSF shall provide [

a) BAC Mutual Authentication

b) EAC-TA

c) [SCP02 Mutual Authentication]

] to support user authentication.

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

a) The BIS or EIS shall succeed the BAC Mutual Authentication in order to have the
BAC authorization.

b) The EIS, in order to have the EAC authorization, shall succeed the BAC Mutual Authentication, EAC-CA and EAC-TA and include the read-rights of biometric data in all of the CVCA Certificate, DV certificate and IS certificate. For this, the TSF shall provide the EAC-CA.

c) [The Personalization Agent, in order to have the Personalization Agent Issuing Authorization or the Personalization Agent Management Authorization, shall succeed the SCP02 Mutual Authentication.]

FIA_UID.1 Timing of identification

Hierarchical to : No other components.

Dependencies : No dependencies.

FIA_UID.1.1 The TSF shall allow [

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

] on behalf of the user to be performed before the user is identified.

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

Application Notes : If external entities communicated with the TOE request SCP02 Mutual Authentication in the Personalization Phase or in the Operational Use Phase, the TOE identifies it with the Personalization Agent. When external entities communicated with the TOE request the use of the MRTD Application in the Operational Use Phase, the TOE identifies it with the BIS. If the BIS requests EAC authentication, the TOE identifies it with the EIS.

8.1.4 Security Management

FMT_MOF.1(1) Management of security functions behavior (Writing Function)

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

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

FMT_MOF.1(2) Management of security functions behavior (COS Lifecycle Management)

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of* the functions [Managing COS Lifecycle by application program] to [Personalization Agent, TSF].

Application Notes : The MRTD Application sets the COS Lifecycle to Operational Use Phase after recording the MRTD Application Data in the Personalization phase. Also, the MRTD Application sets the COS Lifecycle to Terminated after SCP02 Mutual Authentication fails 255 times. The Personalization Agent can terminate the ePassport when the Personalization Agent Issuing Authorization or the Personalization Agent Management Authorization.

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

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

FMT_MSA.3 Static attribute initialization

Hierarchical to : No other components.

Dependencies : FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

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

FMT_MSA.3.2 The TSF shall allow the [**TSF**] 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, EF.DG2, EF.DG3, EF.DG4, EF.DG5, EF.DG6, EF.DG7, EF.DG8, EF.DG9, EF.DG10, EF.DG11, EF.DG12, EF.DG13, EF.DG14, EF.DG15, EF.DG16, EF.SOD, EF.COM, EF.CVCA) in the Personalization phase, the Personalization Agent shall define security attributes of object's operation and object's access-rights in [Table 22] 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) [AA Chip Authentication Private Key]

] to [**Personalization Agent with the Personalization Agent Issuing Authorization in the Personalization phase**].

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 the EAC Secure Messaging after generating the EAC Session Key.

FMT_MTD.1(3) Management of TSF data (COS 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 *modify* the [GP Registry] to [Personalization Agent with the Personalization Agent Issuing Authorization].

Application Notes : The Personalization Agent with the Personalization Agent Issuing Authorization can modify GP Registry.

FMT_MTD.1(4) Management of TSF data (BAC 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 [*write in secure memory*] the [BAC Authentication Key] to [TSF, Personalization Agent with the Personalization Agent Issuing Authorization].

Application Notes : : The BAC Authentication Key may be generated by Personalization Agent in the Personalization phase or by the TOE in the Personalization phase. If the Personalization Agent does not provide the BAC Authentication Key in the Personalization phase the TOE produces the BAC Authentication Key and stores the key in the secure memory of the MRTD Chip.

FMT_MTD.1(5) Management of TSF data (SCP02 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 [*write in secure memory*] the [SCP02 Authentication Key] to [Personalization Agent with the Personalization Agent Issuing Authorization].

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [EAC Chip Authentication Private Key, Initial Current Date, Initial CVCA Certificate, Initial CVCA Digital signature Verification Key, AA Chip Authentication Private Key, SSC(Send Sequence Counter), GP Registry, BAC Authentication Key, and SCP02 Authentication Key].

Application Notes : The TSF shall use only secure value safe as random numbers against replay attack so that to satisfy the SOF-high. The TSF shall preserve secure values by verifying valid data of the CVCA Link Certificate, DV certificate and IS certificate provided by the EIS when executing the EAC-TA and internally updating the CVCA Certificate, CVCA Digital signature Verification Key, Current Date and EF.CVCA if necessary.

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components.

Dependencies : No dependencies.

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

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

b) Function to verify and update the CVCA Certificate, CVCA Digital signature Verification Key and current data in the Operational Use phase

c) [Function to write SCP02 Authentication Key, BAC Authentication Key and AA Chip Authentication Private Key in the Personalization Phase

d) Function to change COS Lifecycle by the MRTD Application in the Personalization Phase and the Operational Use Phase

e) Function to change COS Lifecycle by the Personalization Agent in the Personalization Phase and the Operational Use Phase

f) Function to initialize the security attributes of the subjects and the SSC.

g) Function to disable writing function and change GP Registry]

].

FMT_SMR.1 Security roles

Hierarchical to : No other components.

Dependencies : FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

a) **Personalization Agent with the Personalization Agent Issuing Authorization, Personalization Agent with the Personalization Agent Management Authorization**

b) [none].

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

Application Notes : The Personalization Agent is defined as the role to execute a), c), e) and g) security management function of FMT_SMF.1. The TSF executes security management functions to FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(2), FMT_MTD.1(4), b) security management function of FMT_SMF.1. However, the TSF is not defined as the role since it is not a user.

8.1.5 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to : No other components.

Dependencies : No dependencies.

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

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

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

c) [Power cut out during the operation of the TSF

].

Application Notes : The TOE preserves a secure state of 'infinite loop' when the failures of a) and b) of FPT_FLS.1 occur. If no failures occur when the next start-up of the TOE, the TOE performs normal operation. Otherwise, the TOE maintains a secure state of 'infinite loop'. When the power cut out during the operation of the TOE, the TOE remains secure by restoring the state before the operation interrupted by the power cut out started: Anti-Tearing.

FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

a) Termination of the BAC Secure Messaging or EAC Secure Messaging

b) Deletion of BAC Session Key or EAC Session Key

c) Management action specified in FMT_MSA.1

d) [Termination of Personalization Agent communication channel

e) Deletion of SCP02 Session Key]

] if modifications are detected.

Application Notes : The Strength of Retail MAC is equivalent to the secure Retail MAC specified in FCS_COP.1(2). Security function of d) is performed only and if only when the integrity of the transmitted data between the Personalization Agent and the TOE is protected.

FPT_TST.1 TSF TSF testing

Hierarchical to : No other components.

Dependencies : No dependencies.

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

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *EAC Chip Authentication Private Key, AA Chip Authentication Private Key, CVCA Certificate*, CVCA Digital signature Verification Key, *BAC Authentication Key, SCP02 Authentication Key, COS lifecycle*.

FPT_TST.1.3 The TSF shall provide authorized **Personalization Agent in the Personalization Phase** with the capability to verify the integrity of *parts of TSF*.

8.2 TOE Security Assurance Requirements

The security assurance requirements for this Protection Profile consist of the following components from Part 3 of the CC, summarized in the following Table 24 and evaluation assurance level is EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.4).

The augmented assurance components are as follows:

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

Assurance Class	Assurance Components	
ASE: Security Target Evaluation	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.2	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance

	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.4	Focused vulnerability analysis

Table 24 Security Assurance Requirements

8.2.1 Security Target Evaluation

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction. Content and presentation elements:

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

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

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

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

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

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

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

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE. Evaluator action elements:

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

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

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

Evaluator action elements:

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

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats. ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

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

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

Evaluator action elements:

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

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

Evaluator action elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

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

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

ASE_REQ.2.4C All operations shall be performed correctly.

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

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

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

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

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

Evaluator action elements:

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

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

8.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification
ADV_TDS.1 Basic design

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

Evaluator action elements:

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

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

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

Dependencies: ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

ALC_CMC.5 Advanced support

Developer action elements:

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

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

Content and presentation elements:

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

ADV_IMP.2.2C The implementation representation shall be in the form used by the development personnel.

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

Evaluator action elements:

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

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

Evaluator action elements:

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

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

8.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance. Content and presentation elements:

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

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

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

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

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

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

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

Evaluator action elements:

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

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

8.2.4 Life-cycle Support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage
ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model

Objectives

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

The use of a CM system increases assurance that the configuration items are maintained in a controlled manner. Providing controls to ensure that unauthorized modifications are not made to the TOE (“CM access control”), and ensuring proper functionality and use of the CM system, helps to maintain the integrity of the TOE.

The purpose of the acceptance procedures is to ensure that the parts of the TOE are of adequate quality and to confirm that any creation or modification of configuration items is authorized. Acceptance procedures are an essential element in integration processes and in the life-cycle management of the TOE.

In development environments where the configuration items are complex, it is difficult to control changes without the support of automated tools. In particular, these automated tools need to be able to support the numerous changes that occur during development and ensure that those changes are authorized. It is an objective of this component to ensure that the configuration items are controlled through automated means. If the TOE is developed by multiple developers, i.e. integration has to take place, the use of automatic tools is adequate.

Production support procedures help to ensure that the generation of the TOE from a managed set of configuration items is correctly performed in an authorized manner, particularly in the case when different developers are involved and integration processes have to be carried out.

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Objectives

A CM system can control changes only to those items that have been placed under CM (i.e., the configuration items identified in the configuration list). Placing the TOE itself, the parts that comprise the TOE, the TOE implementation representation and the evaluation evidence required by the other SARs under CM provides assurance that they have been modified in a controlled manner with proper authorizations.

Placing security flaws under CM ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution.

Application notes

ALC_CMS.4.1C introduces the requirement that security flaws be included in the configuration list and hence be subject to the CM requirements of CM capabilities (ALC_CMC). This requires that information regarding previous security flaws and their resolution be maintained, as well as details regarding current security flaws.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE. Content and presentation elements:

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

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

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

Evaluator action elements:

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

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

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

ALC_DEL.1.2D The developer shall use the delivery procedures. Content and presentation elements:

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

Evaluator action elements:

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

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

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

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation. Content and presentation elements:

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

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

Evaluator action elements:

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

ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

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

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

Content and presentation elements:

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

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

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

Evaluator action elements:

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

8.2.5 Tests

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Objectives

The objective of this component is to confirm that all of the TSFIs have been tested.

Application notes

In this component the developer confirms that tests in the test documentation correspond to all of the TSFIs in the functional specification. This can be achieved by a statement of correspondence, perhaps using a table, but the developer also provides an analysis of the test coverage.

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage. Content and presentation elements:

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

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

Evaluator action elements:

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

ATE_DPT.2 Testing: security enforcing modules

Dependencies: ADV_ARC.1 Security architecture description
ADV_TDS.3 Basic modular design
ATE_FUN.1 Functional testing

Objectives

The subsystem and module descriptions of the TSF provide a high-level description of the internal workings, and a description of the interfaces of the SFR-enforcing modules, of the TSF. Testing at this level of TOE description provides assurance that the TSF subsystems and SFR-enforcing modules behave and interact as described in the TOE design and the security architecture description.

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing. Content and presentation elements:

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

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

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

Evaluator action elements:

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

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Objectives

The objective is for the developer to demonstrate that the tests in the test documentation are performed and documented correctly.

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation. Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing

Objectives

In this component, the objective is to demonstrate that the TOE operates in accordance with its design representations and guidance documents. Evaluator testing confirms that the developer performed some tests of some interfaces in the functional specification.

Application notes

The intent is that the developer should provide the evaluator with materials necessary for the efficient reproduction of developer tests. This may include such things as machine-readable test documentation, test programs, etc.

This component contains a requirement that the evaluator has available test results from the developer to supplement the programme of testing. The evaluator will repeat a sample of the developer's tests to gain confidence in the results obtained. Having established such confidence the evaluator will build upon the developer's testing by conducting additional tests that exercise the TOE in a different manner. By using a platform of validated developer test results the evaluator is able to gain confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. Having gained confidence that the developer has tested the TOE, the evaluator will also have more freedom, where appropriate, to concentrate testing in areas where examination of documentation or specialist knowledge has raised particular concerns.

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing. Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

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

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

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

8.2.6 Vulnerability Assessment

AVA_VAN.4 Methodical vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description
ADV_FSP.4 Complete functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures
ATE_DPT.1 Testing: basic design

Objectives

A methodical vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities. The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Moderate.

Developer action elements:

AVA_VAN.4.1D The developer shall provide the TOE for testing. Content and presentation elements:

AVA_VAN.4.1C The TOE shall be suitable for testing. Evaluator action elements:

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

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

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

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

8.3 Rationale for Security Requirements

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

8.3.1 Rationale of Security Functional Requirements

The rationale of TOE security functional requirements demonstrates the followings :

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

Table 25 presents the mapping between the security objectives and the security functional requirements.

Security Objectives Security Functional Requirements	TOE Security Objectives												
	O. Management	O. Security Mechanism Application Procedures	O. Session Termination	O. Secure Messaging	O. Certificate Verification	O. Self-protection	O. Deleting Residual Information	O. Replay Prevention	O. Access Control	O. BAC	O. EAC	O. SCP02	O. AA
FCS_CKM.1(1)										X	X		
FCS_CKM.1(2)												X	
FCS_CKM.2(1)								X		X			
FCS_CKM.2(2)											X		

FCS_CKM.4							X						
FCS_COP.1										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.2			X						X			X	
FIA_UAU.4								X		X	X	X	X
FIA_UAU.5		X							X	X	X	X	
FIA_UID.1										X	X	X	
FMT_MOF.1(1)	X								X				
FMT_MOF.1(2)	X								X				
FMT_MSA.1				X					X				
FMT_MSA.3	X								X				
FMT_MTD.1(1)	X								X				
FMT_MTD.1(2)		X											
FMT_MTD.1(3)	X												
FMT_MTD.1(4)	X								X				
FMT_MTD.1(5)	X												
FMT_MTD.3					X			X			X		
FMT_SMF.1	X				X								
FMT_SMR.1	X												
FPT_FLS.1						X							
FPT_ITI.1			X	X									
FPT_TST.1						X							

Table 25 Security Functional Requirements and Security Objectives Mapping

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

This component requires the TOE to generate the 112 bit BAC Authentication Key, BAC and EAC Session Keys according to the cryptographic key generation algorithm specified in the ICAO document.

Through this, the BAC Authentication Key is generated for use in the BAC Mutual Authentication and BAC/EAC Session Key is generated for use in the BAC/ EAC Secure Messaging. Therefore, this component satisfies the security objectives of O. BAC and O. EAC.

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

This component requires the TOE to generate the SCP02 Session Key according to the session key generation algorithm specified in the GlobalPlatform Card Specification, Version 2.1.1[5].

Through this, the SCP02 Session Key is generated for use in the SCP02 Secure Messaging. Therefore, this component satisfies the security objectives of O. SCP02

FCS_CKM.2(1) Cryptographic key distribution (KDF Seed Distribution for BAC Session Key generation)

This component defines the method to distribute seed of key derivation mechanism necessary in generating the BAC Session Key to the Inspection System (ISO/IEC 11770-2 Key Establishment Mechanism 6).

The distribution method defined in this component satisfies the security objective of O. Replay Prevention as it uses random numbers and O. BAC as it enables to generate the BAC Session Key of FCS_CKM.1 by generating KDF seed.

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

This component defines the method to distribute seed of key derivation mechanism necessary in generating the EAC Session Key to the Inspection System (DH or ECDH key distribution protocol of PKCS#3, ANSI X9.42, ISO/IEC 15946-3).

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

FCS_CKM.4 Cryptographic key destruction

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

This component satisfies the security objective of O. Deleting Residual Information as it provides the method of destroying the key generated by the TSF and remained in temporary memory by overwriting with ‘0’.

FCS_COP.1 Cryptographic operation (Hash Function)

This component defines SHA-1, SHA-224 and SHA-256 hash function necessary in KDF implementation according to FCS_CKM.1. The hash function defined in this component satisfies the security objective of O.AA, O. BAC and O. EAC as it generates AA Digital signature and it enables the KDF to generate the BAC and EAC Session Key.

FDP_ACC.1 Subset access control

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

FDP_ACF.1 Security attributes based access control

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

Security attributes and the ePassport access control rules defined in this component satisfy the security objectives of O. Management and O. Access Control as only the authorized Personalization Agent with the Personalization Agent

Issuing Authorization can perform management functions.

Also, this component satisfies the security objectives of O. BAC, O. EAC and O. Access Control because the read-rights for the personal data of the ePassport holder and ePassport Authentication Data etc. is allowed only to the subjects holding the BAC authorization and the read-rights for the biometric data of the ePassport holder is allowed only to the subjects holding the EAC authorization.

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

Additionally, this component satisfies the security objectives of O. SCP02 because the read-rights for the personal data of the ePassport holder, ePassport Authentication Data and the read-rights for the biometric data of the ePassport holder is allowed only to the subjects holding the Personalization Agent Issuing Authorization.

FDP_DAU.1 Basic Data Authentication

This component defines the method to validate the AA Chip Authentication Private Key used to verify the authenticity of the MRTD Chip. Therefore, this component satisfies the security objectives 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 SCP02 Session Key, BAC Authentication Key, BAC Session Key, EAC Session Key and random numbers.

This component satisfies the security objective of O. Deleting Residual Information as it ensures that previous information of the SCP02 Session Key, the BAC Authentication Key, BAC Session Key and EAC Session Key is not available when destroying these keys according to the method of destruction defined in FCS_CKM.4. Also, this component satisfies the security objective of O. Replay Prevention by ensuring that previous information of random numbers used for the BAC Mutual Authentication, EAC-TA and generation of session key is not available.

FDP_UCT.1 Basic data exchange confidentiality

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

This component establishes the BAC or EAC Secure Messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session encryption key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session encryption key. Additionally, in case the Personalization Agent protects the confidentiality of the transmitted data between the TOE and the Personalization Agent, the transmitted data is protected using SCP02 Secure Messaging by performing cryptographic operations with the SCP02 Session Encryption Key. Therefore, this component satisfies the security objective of O. Secure Messaging as the confidentiality of user data is ensured.

This component satisfies the security objective of O. Replay Prevention by ensuring that the BAC session encryption key is not same as the BAC Authentication Key when establishing the BAC Secure Messaging and the SCP02 Session

Encryption Key is not same as the SCP02 Authentication Key when establishing the SCP02 Secure Messaging..

FDP_UIT.1 Data exchange integrity

This component defines the method to protect from modification, deletion, insertion, replay when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies. This component establishes the BAC or EAC Secure Messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session MAC key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session MAC key. Additionally, in case the Personalization Agent protects the integrity of the transmitted data between the TOE and the Personalization Agent, the transmitted data is protected using SCP02 Secure Messaging by performing cryptographic operations with the SCP02 Session MAC Key. Therefore, this component satisfies the security objective of O. Secure Messaging as the integrity of user data is ensured.

This component satisfies the security objective of O. Replay Prevention by ensuring that the BAC session MAC key is not same as the BAC Authentication Key when establishing the BAC Secure Messaging and the SCP02 Session MAC Key is not same as the SCP02 Authentication Key when establishing the SCP02 Secure Messaging..

FIA_AFL.1 Authentication failure handling

If the authentication attempt failure number defined in the table 26 is surpassed, this component detects it and requires terminating a user session.

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

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

FIA_UAU.1(1) Timing of authentication (BAC Mutual Authentication)

This component defines the functions the user to be performed before the BAC Mutual Authentication and executes the BAC Mutual Authentication for user.

In this component, the BAC Mutual Authentication is executed in order to enable the Inspection System identified in FIA_UID.1 to execute the indication function to support the BAC mechanism and to read the personal data of the ePassport holder. This component satisfies the security objectives of O. Session Termination, O. BAC and O. Access Control as it enables detection by FIA_AFL.1 if the authentication fails and allows the read-rights for the personal data of the ePassport holder if the authentication succeeds.

FIA_UAU.1(2) Timing of authentication (EAC-TA)

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

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

FIA_UAU.2 User authentication before any action (SCP02 Mutual Authentication)

This component requires the Personalization Agent to be successfully authenticated using SCP02 Mutual Authentication before allowing the Personalization Agent any other TSF-mediated action such as access to the MRTD Application Data and the COS TSF Data. This component satisfies the security objectives of O. Session Termination, O. SCP02, O. Access Control as it enables detection by FIA_AFL.1 if authentication fails and allows the access to the MRTD Application Data and the COS TSF Data if authentication succeeds..

FIA_UAU.4 Single-use authentication mechanisms

This component requires that authentication-related information sent by the TSF to the Inspection System in the SCP02 Mutual Authentication, the BAC Mutual Authentication and the EAC-TA, is not replay.

This component satisfies the security objectives of O. Replay Prevention, O.SCP02, O. BAC and O. EAC as the TSF executes the SCP02 Mutual Authentication, the BAC Mutual Authentication and EAC-TA by generating different random numbers used in the SCP02 Mutual Authentication, the BAC Mutual Authentication and EAC-TA per session and transmitting them to the Inspection System.

FIA_UAU.5 Multiple authentication mechanisms

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

This component satisfies the security objectives of O. Security Mechanism Application Procedures, O. Access Control, O. BAC and O. EAC as the Inspection System holds the BAC authorization by succeeding in BAC Mutual Authentication and the EAC authorization by succeeding in the EAC-CA, EAC-TA and certificate verification after the BAC Mutual Authentication according to authentication mechanism application rules. Additionally, this component satisfies O. SCP02 as the Personalization Agent holds the Personalization Agent Issuing Authorization or the Personalization Agent Management Authorization by succeeding in the SCP02 Mutual Authentication.

FIA_UID.1 Timing of identification

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

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

FMT_MOF.1(1) Management of security functions behavior (Writing Function)

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

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

FMT_MOF.1(2) Management of security functions behavior (COS Lifecycle Management)

This component defines that the ability to manage COS Lifecycle is given only to the Personalization Agent.

This component satisfies the security objectives of O. Management by allowing the management function of the COS Lifecycle to the Personalization Agent.

FMT_MSA.1 Management of security attributes

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

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

FMT_MSA.3 Static attribute Initialization

This component requires the TSF to specify initial values in order to restrict default values for security attributes when an object is created

This component satisfies the security objectives of O. Management and O. Access Control as only the authorized Personalization Agent generates user data in order to enforce the ePassport access control policies in the Personalization phase and the TOE specifies initial values to restrict security attributes of the data.

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

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

This component satisfies the security objectives of O. Management and O. Access Control by enabling only the authorized Personalization Agent to have the ability to write TSF data, such as the EAC Chip Authentication Private Key, current data, CVCA Certificate and CVCA Digital signature Verification Key, etc., in secure memory in the Personalization phase

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

This component requires terminating BAC Secure Messaging before the EAC Secure Messaging is established.

This component satisfies the security objective of O. Security Mechanism Application Procedures by initializing SSC (send Sequence Counter) to ‘0’ in order to terminate the BAC Secure Messaging after generating the EAC Session Key and newly establishing the EAC Secure Messaging.

FMT_MTD.1(3) Management of TSF data (COS Management)

This component restricts that only authorized Personalization Agent modifies GP Registry of the COS.

This component satisfies the security objective of O. Management as only authorized Personalization Agent modifies GP Registry.

FMT_MTD.1(4) Management of TSF data (BAC Authentication Key Management)

This component defines that the BAC Authentication Key can be generated by Personalization Agent in the Personalization phase or by the TSF in the Personalization Phase.

This component satisfies the security objective of O. Management and O. Access Control as only authorized Personalization Agent or the TSF can generate and store the BAC Authentication Key in the secure memory.

FMT_MTD.1(5) Management of TSF data (SCP02 Authentication Key Management)

This component restricts that only authorized Personalization Agent writes the SCP02 Authentication Key in the secure memory.

This component satisfies the security objective of O. Management as only authorized Personalization Agent stores the SCP02 Authentication Key in the secure memory.

FMT_MTD.3 Secure TSF data

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

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

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

FMT_SMF.1 Specification of management functions

This component provides the means to manage the MRTD Application Data in the Personalization phase.

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

Also, this component satisfies the security objective of O. Certificate Verification as it provides the function for the TSF to update the CVCA Certificate, the CVCA Digital signature Verification Key and Current Dates, etc. by itself in the Operational Use phase.

FMT_SMR.1 Security roles

This component defines the role of the Personalization Agent to manage the MRTD Application Data.

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

FPT_FLS.1 Failure with preservation of secure state

This component requires preserving a secure state when the types of failures occur, such as the failure detected from the self-testing and abnormal operating conditions detected by the IC chip, etc.

This component satisfies the security objective of O. Self-protection as it preserves a secure state to prevent the malfunction of the TSF when the modification of integrity of the TSF data or executable code from the self-testing of FPT_TST.1 is detected or the IC chip detects abnormal operating conditions.

FPT_ITI.1 Inter-TSF detection of modification

This component requires detecting modification in the transmitted TSF data and defines an action to be taken if modifications are detected.

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

FPT_TST.1 TSF testing

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

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

8.3.2 Rationale of Security Assurance Requirements

The EAL(Evaluation Assurance Level) of this Protection Profile was selected as EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.4) by considering the value of assets protected by the TOE and level of threats, etc.

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

This Protection Profile partially selected assurance components that are higher than

EAL4. The rationale of the augmented with assurance components are as follows.

ADV_IMP.2 Implementation of the TSF, ATE_DPT.2 Testing: low-level design, AVA_VLA.4 Focused vulnerability analysis

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

The TOE is developed by using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to design and operation of the TOE. Also, TOE is easily accessed as it is used in open environment and it is difficult to trace an attack. However, since the IC chip is not included in the scope of the TOE, it does not require understanding on hardware structure and advanced specialized equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing moderate attack potential. EAL4 includes AVA_VLA.3 that resistant the enhanced-basic attack potential. Therefore, AVA_VLA.4 is augmented to require execution of focused vulnerability analysis and resistant to attackers possessing moderate attack potential. However, there still exists direct attack potential to the IC chip by threat agent possessing high attack potential and evaluation and verification for this may be assigned to the IC chip manufacturer.

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

8.3.3 Rationale of Dependency

8.3.3.1 Dependency of TOE Security Functional Requirements

Table 26 shows dependency of TOE functional components.

No.	Functional Components	Dependencies	Reference Numbers
1	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	3, 6 5
2	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	3, 6 5
3	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 5

4	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 5
5	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	1
6	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 5
7	FDP_ACC.1	FDP_ACF.1	8
8	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	7 23
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
14	FIA_UAU.1(1)	FIA_UID.1	19
15	FIA_UAU.1(2)	FIA_UAU.1(1)	14
16	FIA_UAU.2	FIA_UID.1	19
17	FIA_UAU.4	-	-
18	FIA_UAU.5	-	-
19	FIA_UID.1	-	-
20	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	30 31
21	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	30 31
22	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	7 30 31
23	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	22 31
24	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	30 31
25	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	30 31
26	FMT_MTD.1(3)	FMT_SMF.1	30

		FMT_SMR.1	31
27	FMT_MTD.1(4)	FMT_SMF.1 FMT_SMR.1	30 31
28	FMT_MTD.1(5)	FMT_SMF.1 FMT_SMR.1	30 31
29	FMT_MTD.3	FMT_MTD.1	24,25,26,27,28
30	FMT_SMF.1	-	-
31	FMT_SMR.1	FIA_UID.1	19
32	FPT_FLS.1	-	-
33	FPT_ITI.1	-	-
34	FPT_TST.1	-	-

Table 26 Security Functional Requirements Dependency

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

FIA_UAU.1(2) has dependency with FIA_UID.1, but the dependency has changed to FIA_UAU.1(1) according to the Refinement Operation. Since the EAC-TA is executed after the BAC Mutual Authentication, FIA_UAU.1(2) depends on FIA_UAU.1(1) and FIA_UAU.1(1) depends on FIA_UID.1. Therefore, indirectly, the dependency is satisfied.

8.3.3.2 Dependency of TOE Security Assurance Requirements

The dependency of EAL4 provided in Common Criteria is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in Table 27.

ALC_CMC.5 has dependency with ADV_IMP.2, however, ALC_CMC.5 is not included in this ST. ADV_IMP.2 is included in order to ensure that the TSF is implemented correctly and no defective code exists. Therefore, the configuration management according to ALC_CMC.5 is not necessary for the TOE and ALC_CMC.5 is excluded from this ST

.

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

No.	Assurance Components	Dependencies	Reference Numbers
1	ADV_IMP.2	ADV_TDS.3 ALC_TAT.1 ALC_CMC.5	EAL4 EAL4 None
2	ATE_DPT.2	ADV_ATC.1 ADV_TDS.3 ATE_FUN.1	EAL4 EAL4 EAL4
3	AVA_VAN.4	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	EAL4 EAL4 EAL4 1 EAL4 EAL4 2

Table 27 Security Assurance Requirements Dependency

8.3.3.3 Rationale of Mutual Support and Internal Consistency

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

In the Personalization phase, the Personalization Agent records the MRTD Application Data (FMT_MTD.1(1), FMT_MSA.3) and deactivates writing function so that the TOE is not modified by external entities when delivering the TOE to the Operational Use phase(FMT_MOF.1, 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).

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

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

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

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

9 TOE Summary Specification

This section explains the TOE security functions that satisfy the security functional requirements defined in this ST.

9.1 Cryptographic Support

This security function provides cryptographic features related to generation of random numbers, hash values, digital signatures and performing cryptographic operations on the data.

The TOE generates the 112 bit BAC Authentication Key, BAC and EAC Session Keys according to the cryptographic key generation algorithm specified in the ICAO document to satisfy FCS_CKM.1(1). The BAC Authentication Key is generated for use in the BAC Mutual Authentication and BAC/EAC Session Key is generated for use in the BAC/ EAC Secure Messaging. Also, the TOE generates SCP02 Session Key according to the session key generation algorithm specified in the GlobalPlatform Card Specification to satisfy FCS_CKM.1(2)

The TOE generates and distributes the BAC Session Key and the EAC Session Key to the Inspection System according to the key derivation mechanisms defined in this ST to satisfy FCS_CKM.2(1) and FCS_CKM.2(2).; ISO/IEC 11770-2 Key Establishment Mechanism 6 for the BAC Session Key and DH or ECDH Key Distribution Protocol of PKCS#3, ANSI X9.42, ISO/IEC 15946-2 for the EAC Session Key.

The TOE securely destroys the keys generated in the temporary memory by overwriting them with ‘0’s to satisfy FCS_CKM.4.

The TOE uses SHA-1, SHA-224 and SHA-256 has functions to implement key distribution functions according to FCS_CKM.1(1) and FCS_CKM.1(2) to satisfy FCS_COP.1.

9.2 User Data Protection

This security function provides the access control and the secure messaging to protect the personal data of the ePassport holder when the external entities attempt to access the data.

The TOE enforces the ePassport Access Control Policies according to the list of subjects, objects and operations in order to protect the personal data and biometric data of the ePassport holder and ePassport Authentication Data etc. to satisfy FDP_ACC.1 and FDP_ACF.1.

The TOE provides the means to validate the AA Chip Authentication Private Key used to verify the authenticity of the MRTD Chip to satisfy FDP_DAU.1.

The TOE destroys the SCP02 Session Key, the BAC Authentication Key, BAC Session Key and EAC Session Key in the temporary memory to ensure that previous information does not reside in the memory when the TSF allocates or deallocates memory resources. The TOE removes the information according to the method defined in FCS_CKM.4 to satisfy FDP_RIP.1.

The TOE protects the confidentiality of the transmitted data such as the personal data and the biometric data of the ePassport holder by establishing the BAC or the EAC Secure Messaging by performing cryptographic operations using the BAC Session Encryption Key or the EAC Session Encryption Key for the data transmitting between the TOE and the Inspection System. Additionally, in case the Personalization Agent protects the confidentiality of the transmitted data between the TOE and the Personalization Agent, the SCP02 Secure Messaging is established between the TOE and the Personalization Agent by performing cryptographic operation using SCP02 Session Encryption Key. This satisfies FDP_UCT.1.

The TOE protects the integrity of the transmitted data such as the personal data and the biometric data of the ePassport holder by establishing the BAC or the EAC Secure Messaging by performing cryptographic operations using the BAC Session MAC Key or the EAC Session MAC Key for the data transmitting between the TOE and the Inspection System. Additionally, in case the Personalization Agent protects the integrity of the transmitted data between the TOE and the Personalization Agent, the SCP02 Secure Messaging is established between the TOE and the Personalization Agent by performing cryptographic operation using SCP02 Session MAC Key. This satisfies FDP_UIT.1.

9.3 Identification and Authentication

This security function provides methods to identify and authenticate the users attempt to access the TOE using security mechanisms such as the SCP02 Mutual Authentication, the BAC Mutual Authentication, EAC-TA, PA and AA.

The TOE terminates the user session when the number of authentication attempt failure of the SCP02 Mutual Authentication, the BAC Mutual Authentication and the EAC-TA surpassed ‘Number of Unsuccessful Authentication Attempts’ defined in the table 26. Also, the lifecycle of the TOE is set to Terminated Phase when the authentication attempts of the SCP02 Mutual Authentication fails 255 times. This satisfies FIA_AFL.1.

The TOE satisfies FIA_UAU.1(1) as it defines the functions available for the users before the BAC Mutual Authentication and executes the BAC Mutual Authentication in order to enable the Inspection System identified in FIA_UID.1 to execute the indication function to support the BAC mechanism and to read the personal data of the ePassport holder.

The TOE satisfies FIA_UAU.1(2) as it the functions available for the users before the EAC-TA and executes the EAC-TA for users. Only the Inspection System of which the BAC Mutual Authentication succeeded in FIA_UAU.1(1) can execute EAC-CA and reading of user data(exception of the biometric data of the ePassport holder). To read the biometric data of the ePassport holder, the EAC-TA shall be executed.

The TOE satisfies FIA_UAU.2 as it does not allow any action for the Personalization Agent before successfully authenticated using SCP02 Mutual Authentication.

The TOE ensures that authentication-related information sent by the TSF to the Inspection System in the SCP02 Mutual Authentication, the BAC Mutual Authentication and the EAC-TA, is not replay as it executes the SCP02 Mutual Authentication, the BAC Mutual Authentication and EAC-TA by generating different random numbers used in the BAC Mutual Authentication and EAC-TA per session and transmitting them to the Inspection System. This satisfies FIA_UAU.4.

The TOE authenticates the users with different authentication mechanisms and the rules of applying authentication mechanism according to type of user data to be accessed by the Inspection System to satisfy FIA_UAU.5. The Inspection System holds the BAC authorization by succeeding in BAC Mutual Authentication and the EAC authorization by succeeding in the EAC-CA, EAC-TA and certificate verification after the BAC Mutual Authentication according to authentication mechanism application rules. Additionally, the Personalization Agent holds the Personalization Agent Issuing Authorization or the Personalization Agent Management Authorization by succeeding in the SCP02 Mutual Authentication.

The TOE satisfies FIA_UID.1 as it establishes the communication channel based on contactless IC card transmission protocol (ISO/ IEC 14443-4) before the identification and to identify the user. If external entities communicated with the TOE request SCP02 Mutual Authentication in the Personalization Phase or in the Operational Use Phase, the TOE identifies it with the Personalization Agent. When external entities communicated with the TOE request the use of the MRTD Application in the Operational Use Phase, the TOE identifies it with the BIS. If the BIS requests EAC authentication, the TOE identifies it with the EIS.

9.4 Security Management

This security function provides security management features for the MRTD Application and the COS such as application program management, lifecycle management, TSF data management etc.

The TOE restricts the ability to disable writing function only to the Personalization Agent in the Personalization Phase to satisfy FMT_MOF.1(1). After the Personalization of the TOE the Personalization Agent deactivates the writing function so that the TOE in the Operational Use phase cannot record any data.

The TOE restricts the ability to manage COS Lifecycle only to the Personalization Agent to satisfy FMT_MOF.1(2). The Personalization Agent is able to manage COS Lifecycle after authenticated by using SCP02 Mutual Authentication.

The TOE restricts the ability of initializing user security attributes only to the TSF as an action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1. The TOE ensures integrity of the MRTD Application Data and blocks access to the MRTD Application Data 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. This satisfies FMT_MSA.1.

The TOE specifies the initial values for the security attributes when an object is created. Only the authorized Personalization Agent generates user data in order to enforce the ePassport access control policies in the Personalization phase and the TOE specifies initial values to restrict security attributes of the data. This satisfies FMT_MSA.3.

The TOE satisfies FMT_MTD.1(1) as it restricts that only the Personalization Agent in the Personalization phase writes certificate verification information necessary for the EAC-TA in secure memory. Only the authorized Personalization Agent has the ability to write TSF data, such as the EAC Chip Authentication Private Key, current data, CVCA Certificate and CVCA Digital signature Verification Key, etc., in secure memory in the Personalization phase

The TOE satisfies FMT_MTD.1(2) as it terminates BAC Secure Messaging before the EAC Secure Messaging is established. The TOE initializes SSC (send Sequence Counter) to ‘0’ in order to terminate the BAC Secure Messaging after generating the EAC Session Key and newly establishing the EAC Secure Messaging.

The TOE satisfies FMT_MTD.1(3) as it restricts that only authorized Personalization Agent through the SCP02 Mutual Authentication can modify GP Registry of the COS.

The TOE satisfies FMT_MTD.1(4) as it restricts that the BAC Authentication Key can be generated by Personalization Agent in the Personalization phase or by the TSF in the Personalization Phase.

The TOE satisfies FMT_MTD.1(5) as it restricts that only authorized Personalization Agent writes the SCP02 Authentication Key in the secure memory.

The TOE allows only secure values as the TSF data in order to ensure the secure random numbers and to ensure that valid date of certificates used in EAC-TA has not expired. Only the secure random numbers are used in order to prevent a replay attack when the TSF generates session key. Also, the TSF compares the CVCA Link Certificate provided by the Inspection System with the CVCA Certificate stored in the TOE in order for verification of the IS certificate used in the EAC-TA. If the CVCA Certificate update is necessary, the TSF internally updates the CVCA Certificate, CVCA Digital signature Verification Key, Current Dates and EF.CVCA, therefore maintains the TSF data as secure values. The EAC-TA can be successfully executed by verifying the DV certificate and IS certificate with the secure CVCA Certificate. This satisfies FMT_MTD.3.

The TOE satisfies FMT_SMF.1 as it provides the means to manage the MRTD Application Data in the Personalization phase. The TOD defines the writing function of user data and TSF data in the Personalization phase. Also, the TOE provides the function for the TSF to update the CVCA Certificate, the CVCA Digital signature Verification Key and Current Dates, etc. by itself in the Operational Use phase.

The TOE satisfies FMT_SMR.1 as it defines the role of the Personalization Agent that executes the writing function of user data and TSF data in the Personalization phase.

9.5 Protection of the TSF

This security function provides functions to protect the TOE such as the preservation of the secure state, detection of modification of transmitted TSF data and self-testing of the TOE. The TOE

The TOE satisfies FPT_FLS.1 as it preserves a secure state when the types of failures occur, such as the failure detected from the self-testing and abnormal operating conditions detected by the IC chip, etc. The TOE prevents the malfunction of the TSF when the modification of integrity of the TSF data or executable code from the self-testing of FPT_TST.1 is detected or the IC chip detects abnormal operating conditions.

The TOE satisfies FPT_ITI.1 as it detects modification in the transmitted TSF data and defines an action to be taken if modifications are detected. The TOE detects modification of the transmitted TSF data in the Personalization and Operational Use phases and by performing an action to be taken, such as terminating the related communication channels, deleting the related session key and management actions specified in FMT_MSA.1, etc., if modifications are detected

The TOE satisfies FPT_ TST.1 as it self-tests to detect loss of the TSF executable code and the TSF data by various failure (unexpected failure mode, lack of the IC chip design and intentionally damage to the TSF, etc.). The TOE runs self-testing under the self-testing execution conditions for TSF parts, therefore demonstrating the correct operation of the TSF. Also, the TOE verifies the integrity of TSF data parts and the TSF executable code stored in the TOE, therefore detecting loss of the TSF data and the executable code.

9.6 TOE Summary Specification Rationale

This section explains the rationale for the TOE Summary Specification. The mapping between the security functions and the security functional requirements is show in the following table.

Security Functions Security Functional Requirements	TOE Security Functions				
	Cryptographic Support	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF
FCS_CKM.1(1)	X				
FCS_CKM.1(2)	X				
FCS_CKM.2(1)	X				
FCS_CKM.2(2)	X				
FCS_CKM.4	X	X			
FCS_COP.1	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FDP_DAU.1		X			
FDP_RIP.1		X			
FDP_UCT.1		X			
FDP_UIT.1		X			
FIA_AFL.1			X		
FIA_UAU.1(1)			X		
FIA_UAU.1(2)			X		
FIA_UAU.2			X		
FIA_UAU.4			X		
FIA_UAU.5			X		
FIA_UID.1			X		
FMT_MOF.1(1)				X	
FMT_MOF.1(2)				X	
FMT_MSA.1				X	
FMT_MSA.3				X	
FMT_MTD.1(1)				X	
FMT_MTD.1(2)				X	
FMT_MTD.1(3)				X	
FMT_MTD.1(4)				X	
FMT_MTD.1(5)				X	

FMT_MTD.3				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_FLS.1					X
FPT_ITI.1					X
FPT_TST.1					X

Table 28 TOE Security Functional Requirements and TOE Security Function Mapping

10 Terms and Definitions

AA (Active Authentication)

The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values

BAC (Basic Access Control)

The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the secure messaging for the MRTD chip and the IS

BAC Authentication Key

The BAC authentication encryption key and the BAC authentication MAC key generated by using the KDM from the MRZ (passport No., passport No. check digit, date of birth, date of birth check digit, valid date, valid date check digit) for mutual authentication of the MRTD chip and the IS

BAC Mutual Authentication

The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol

BAC Secure Messaging

The communication channel to provide the confidentiality and the integrity of transmitted data by encryption the transmitted data with the BAC session encryption key and generating, therefore transmitting after generating message authentication value with the BAC session MAC key

BAC Session Key

The BAC session encryption key and the BAC session MAC key for generated by using the KDM from random numbers for generating session keys shared in the BAC Mutual Authentication

Biometric data of the ePassport holder

Fingerprint and/ or iris data of ePassport holder stored in the MRTD chip in the LDS structure

BIS (BAC Inspection System)

The IS implemented with the BAC and the PA security mechanisms

Certificate

The electronic data by a digital signature on the digital signature verification key by the CA in order to check and demonstrate that the digital signature generation key belongs only to the person who holds the key

Ciphertext Only Attack

Attack by the threat agent to attempt decryption based on the collected ciphertext

CSCA (Country Signing Certification Authority)

The root CA that generates and issues the CSCA certificate and the DV certificate by securely generating the digital signature key in the PA-PKI to support the PA security mechanisms

CSCA Certificate

The certificate to demonstrate validity of the digital signature verification key for the digital signature generation key of the PA-PKI root CA by signature on the digital signature verification key with digital signature generation key of the PA-PKI root CA CVCA (Country Verifying Certification Authority) The root CA that generates and issues the CVCA Certificate, the CVCA Link Certificate and the DV certificate by securely generating digital signature key in the EAC-PKI to support the EAC security mechanisms

CVCA Certificate

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

CVCA Link Certificate

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

DS (Document Signer) Certificate

The certificate of the Personalization Agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism

DV (Document Verifier)

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

DV Certificate

The certificate that includes digital signature value on the digital signature verification key of the IS with the digital signature generation key of the DV in order to demonstrate validity of the digital signature verification key of the IS

EAC-CA (EAC-chip Authentication)

The security mechanism to implement the Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) to enable the MRTD chip authentication by the EIS through key checking for the EAC Chip Authentication Public Key and private key of the MRTD chip and temporary public key and private key of the EIS

EAC-TA (EAC-terminal Authentication)

The security mechanism that The EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS.

EAC (Extended Access Control)

The security mechanisms consisted with the EAC-CA for chip authentication and the EAC-TA for the IS authentication in order to enable only the EAC supporting Inspection System (EIS) to read the biometric data of the ePassport holder for access control to the biometric data of the ePassport holder stored in the MRTD chip

EAC Chip Authentication Public Key and EAC Chip Authentication Private Key

Set of the DH keys used by the MRTD chip to authenticate itself to the EAC supporting IS in the EAC-CA that contain data recorded by the Personalization Agent in the Personalization phase.

EAC Inspection System (EIS: EAC Inspection System)

The IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option

EAC Session Key

The session key used to establishing secure messaging to protect transmission of the biometric data of the ePassport holder that consist of the EAC session encryption key and the EAC session MAC key generated by using the KDF of which keys shared with the EIS through the Ephemeral-Static DH key distribution protocol in the EAC-CA are used as Seed

EF.COM

Including the LDS version info. Data Groups tag information

EF.CVCA

The EF format file to specify the read-right and the list of the CVCA Digital signature Verification Key identifier necessary in verification of the CVCA Certificate validity in the EAC-TA

Encryption Key

Key used in the symmetric cryptographic algorithm for data encryption in order to prevent the data disclosure

ePassport

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

ePassport Authentication Data

The data stored in the MRTD chip with the LDS format to support ePassport security mechanisms that includes the PA SOD, the EAC Chip Authentication Public Key and the AA chip authentication public key, etc.

ePassport identity data

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

ePassport PKI

Unique data signed on the ePassport by the Personalization Agent with digital signature generation key issued in the ePassport PKI System in order to issuance and check of the electronically processed passport

ePassport PKI System

System to provide certification practice such as issuance of certificates necessary in passport's digital signature and management of certification-related records, etc.

Grandmaster Chess Attack

Attack by masquerading as the MRTD chip using the IC chip to hookup the communication channel between the MRTD chip and the IS

ICAO-PKD

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

Inspection

Procedure in which immigration office checks identity of the ePassport holder by inspecting the MRTD chip presented by the ePassport holder, therefore verifying genuine of the MRTD chip

IS (Inspection System)

As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands.

IS Certificate

Certificate used by the MRTD chip to verify the digital signature transmitted by the IS in the EAC-TA. The DV performs a digital signature on the digital signature verification key of the EIS with the digital signature generation key.

KDF (Key Derivation Function)

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

KDM (Key Derivation Mechanism)

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

LDS (Logical Data Structure)

Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip

MAC Key (Key for Message Authentic Code)

Key used by symmetric cryptographic algorithm according to ISO9797 to generate the message authentication code in order to prevent data forgery and corruption

MRTD

Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes

MRTD Application

Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc.

MRTD Application Data

Including user data and TSF data of the MRTD

MRTD Chip

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

PA (Passive Authentication)

The security mechanism to demonstrate that identity data recorded in the ePassport has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the ePassport access control policy.

Personal data of the ePassport holder

Visually identifiable data printed on identity information page of the of ePassport and other identity data stored in the MRTD chip in the LDS structure

Personalization Agent

The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the Personalization Agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI. Probing Attack to search data by inserting probing pin in the IC chip

Reverse Engineering

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

SCP02 (Secure Channel Protocol 02) Mutual Authentication

The mutual authentication of the MRTD chip used to authenticate the Personalization Agent according to GlobalPlatform Card Specification, Version 2.1.1

SCP02 Session Key

The SCP02 session encryption key and the SCP02 session MAC key for generated by using the KDM from random numbers for generating session keys shared in the SCP02 Mutual Authentication

SOD (Document Security Object)

The SOD refers to the ePassport identity data and the ePassport Authentication Data recorded in the Personalization phase by the Personalization Agent that is signed by the Personalization Agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and encoded with DER method.

TSF Data

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

User Data

Including the ePassport identity data and the ePassport Authentication Data

[Acronyms]

AA	Active Authentication
BAC	Basic Access Control
BIS	BAC Inspection System
CA	Chip Authentication
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
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EIS	EAC Inspection System
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IS	Inspection System
ISO	International Organization for Standardization
IT	Information Technology
KDM	Key Derivation Mechanism
KDF	Key Derivation Function
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PA	Passive Authentication
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory

RF	Radio Frequency
ROM	Read Only Memory
SCP	Secure Channel Protocol
SOD	Security Object of Document
SPA	Simple Power Analysis
SSC	Send Sequence Counter
TA	Terminal Authentication
TDES	Triple-DES

Table 29 Abbreviation

[References]

[1] Java Card Platform 2.2.1, Virtual Machine Specification, Sun Microsystems, October 2003

[2] Java Card Platform 2.2.1, Runtime Environment Specification, Sun Microsystems, October 2003

[3] Java Card Platform 2.2.1, Application Programming Interface, Sun Microsystems, October 2003

[4] GlobalPlatform Card Specification, Version 2.1.1, GlobalPlatform Inc., March 2003

[5] VISA GlobalPlatform 2.1.1 Card Implementation Requirements, Version 1.0, VISA, May 2003

[6] Doc 9303 "Machine Readable Travel Documents" Part 1 "Machine Readable Passports" Volume 2 "Specification for Electronically Enabled Passports with Biometric Identification Capability" Sixth Edition, International Civil Aviation Organization(ICAO), 2006. 8

[7] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Version 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2008. 2

[8] ISO/IEC 14443-4:2001, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol

[9] ISO/IEC 9798-2:1999, Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms

[10] ISO/IEC 11770-2:1996, Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques

[11] ISO/IEC 10118-3:2004, Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions

[12] ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher

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

[14] ISO/IEC 15946-2:2002, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures

[15] ePassport Protection Profile V2.1, National Intelligence Service IT Security Certification Center, Korea Internet Security Agency, 2010. 6

[16] VISA GlobalPlatform 2.1.1 Card Production Guide, Version 1.0, VISA, February 2004

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

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

[19] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB

[20] Common Methodology for Information Technology Security Evaluation, Version 3.1, CCMB, 2007. 9.

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

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