ePassport Protection Profile V1.0

2008. 1.

National Intelligence Service

IT Security Certification Center

(This page left blank on purpose for double-side printing)

Protection Profile Title

ePassport Protection Profile

Evaluation Criteria Version

This Protection Profile has been prepared in conformance to the Common Criteria for Information Technology Security Evaluation (Ministry of Information & Communication Public Notice No. 2005-25).

Developer

This Protection Profile has been developed by the following developers:

Wan S. Yi, JunHo Lee, YounJung Yu, JaeDuk Ji,
NamHo Oh, WonSoon Hong, JaeHo Jeong
Korea Information Security Agency (KISA)

(This page left blank on purpose for double-side printing)

Table of Contents

List of Tables

List of Figures

1. Protection Profile(PP) Introduction

1.1 PP Identification

1 Title : ePassport Protection Profile

2 Protection Profile Version : V1.0

3 Evaluation Criteria : Common Criteria for Information Security Evaluation (Ministry of Information and Communication Public Notice No. 2005-25)

4 Common Criteria Version : V2.3

5 Evaluation Assurance Level : EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.3)

6 Sponsor : KISA

7 Developer: IT Security Evaluation Division, Evaluation Planning Team, KISA

8 Certification Body : IT Security Certification Center, National Intelligence Service

9 Certification Number : KECS-PP-0084-2008, Jan. 2008

10 Validation Result : Validated under the KECS(Korea IT Security Evaluation and Certification Scheme)

11 Keywords : ePassport, COS, MRTD, ICAO

1.2 PP Overview

12 This protection profile defines security functional requirements and security assurance requirements for IC chip operating system (COS) and the application of machine readable travel documents(MRTD application) with the exception of hardware elements of the chip of machine readable travel documents(MRTD chip).

13 The MRTD application satisfies the ICAO's Machine Readable Travel Documents, DOC 9303 Part 1 Volume 2[1] (ICAO document) and the BSI's Advanced Security Mechanisms Machine Readable Travel Documents – Extended Access Control V1.1 2007.08 [2] (EAC specification).

1.3 Conformance Claim

14 This protection profile claims conformance to

- Common Criteria for Information Technology Security Evaluation, part 1 : Introduction and general model, Version 2.3, Aug. 2005, CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation, part 2 : Security functional requirements, Version 2.3, Aug. 2005, CCMB-2005-08-002

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

as follows

- Part 2 Conformant
- Part 3 Conformant
- Package Conformant to EAL4 augmented with ADV_IMP2, ATE_DPT2 and AVA_VLA.3

1.4 Conventions

15 The notation, formatting and conventions used in this Protection Profile are consistent with the Common Criteria for Information Technology Security Evaluation (hereafter referred to as “CC”).

16 The CC allows several operations to be performed on functional requirements;, assignment, iteration, refinement and selection. Each of these operations is used in this Protection Profile.

Assignment

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

Iteration

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

Refinement

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

Selection

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

17 “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 Protection Profile Organisation

18 Section 1 provides the introductory material for the Protection Profile.

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

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

21 Section 4 defines the security objectives for the TOE and its IT environment to counter to identified threats and support the assumptions and organisational security policies.

22 Section 5 contains the IT security requirements including the functional and assurance requirements intended to satisfy security objectives.

23 Section 6 describes Application Notes which deserve notice in applying the PP herein.

24 Section 7 provides a rationale to demonstrate that the security objectives for the TOE and its IT environment address the defined security problems appropriately and the IT security requirements are adequate and complete to satisfy the security objectives.

25 Section 8 defines the terms which is used in this protection profile.

26 References contain references to noteworthy background and/or supporting materials for prospective users of the PP who may be interested in knowing more than what is specified herein.

27 Acronym is an acronym list that defines frequently used acronyms.

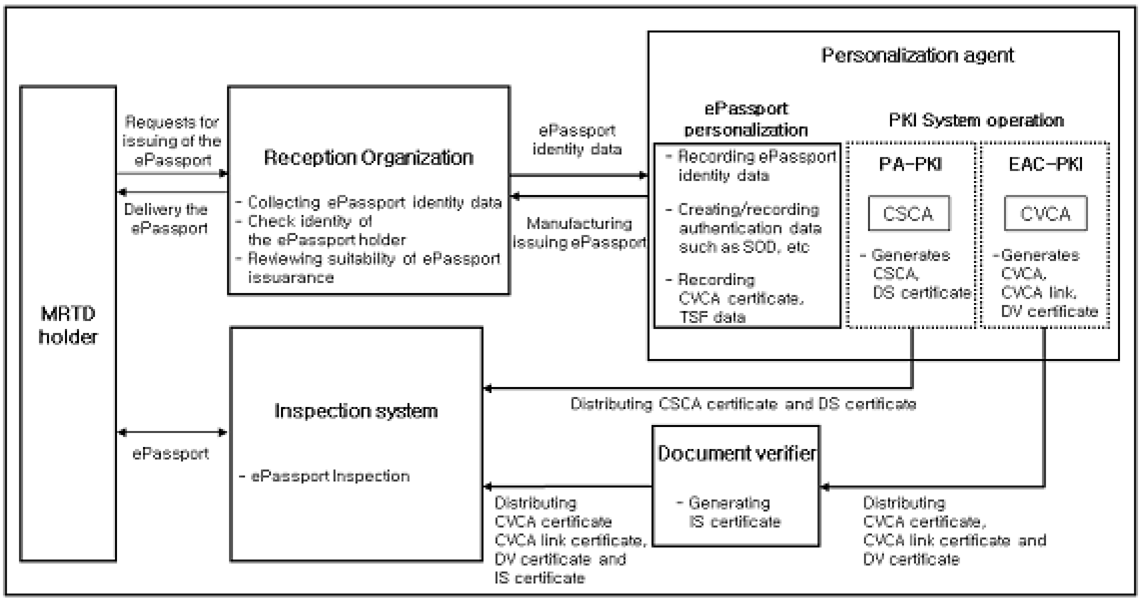
2. TOE Description

2.1 ePassport Overview

28 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.

ePassport System

29 The (Figure 1) shows the overall configuration of the ePassport system.



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

(Figure 1) Overall Configuration of the ePassport System

30 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.

31 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.

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

33 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.

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

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

[Table 1] Types of Certificates

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

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

2.2 TOE Scope

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

2.2.1 Life Cycle and Environment of the TOE

The Life Cycle of the MRTD Chip and the TOE

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

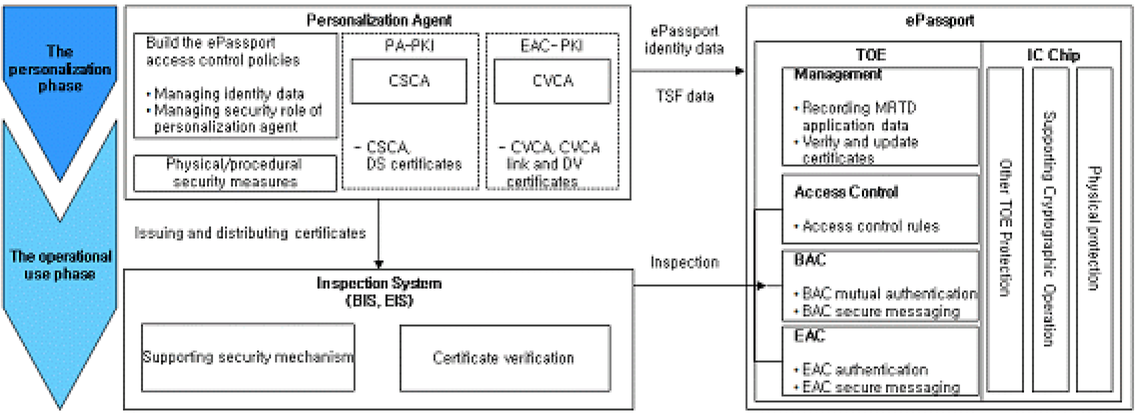
[Table 2] Life Cycle of the MRTD Chip and the TOE

Phase	Life Cycle of the MRTD Chip	Life Cycle of the TOE
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W	
		② The S/W developer to develop the TOE (COS, MRTD application) by using the IC chip and the Dedicated S/W
Phase 2 (Manufacturing)	③ The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier and to produce the IC chip	
		④ The ePassport manufacturer to create user data storage space according to the LDS format or the ICAO document and to record it in EEPROM ⑤ The ePassport manufacturer to record identification and authentication information of the ePassport Personalization agent in the EEPROM ⑥ The ePassport manufacturer to embed the IC chip in the passport book

Phase 3 (personalization)		⑦ The Personalization agent to create SOD by a digital signature on the ePassport identity data ⑧ The Personalization agent to record the ePassport identity data, the authentication data (including SOD) and the TSF data in the TOE
Phase 4 (Operational Use)		⑨ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE

TOE Operational Environment

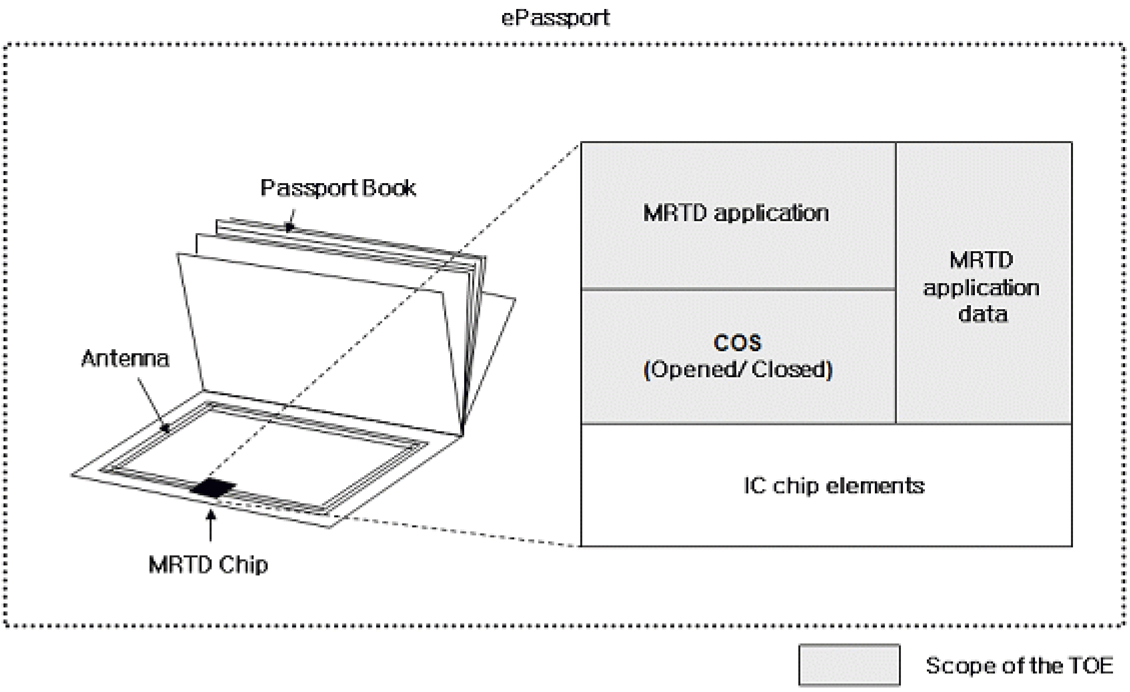
38 (Figure 2) shows the operational environment of the TOE in the phases of the ePassport Personalization and Operational Use through the relationship with major security functions of TOE and external entities (the Personalization agent, the Inspection System) that interact with TOE.


The personalization phase
The operational use phase
Personalization Agent
Build the ePassport access control policies
• Managing identity data
• Managing security role of personalization agent
Physical/procedural security measures
PA-PKI
CSCA
- CSCA, DS certificates
EAC-PKI
CVCA
- CVCA, CVCA link and DV certificates
ePassport identity data
TSF data
Issuing and distributing certificates
Inspection
Inspection System (BIS, EIS)
Supporting security mechanism
Certificate verification
ePassport
TOE
Management
• Recording MRTD application data
• Verify and update certificates
Access Control
• Access control rules
BAC
• BAC mutual authentication
• BAC secure messaging
EAC
• EAC authentication
• EAC secure messaging
IC Chip
Other TOE Protection
Supporting Cryptographic Operation
Physical protection

(Figure 2) TOE Operation Environment

2.2.2 Physical Scope of the TOE

39 (Figure 3) shows the scope of the TOE.



(Figure 3) Scope of the TOE

40 The ePassport refers to the passport book 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, EEPROM) and contactless interface, etc.

41 In this protection profile, TOE is defined with 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.

42 The COS provides functions for execution of MRTD application and management of the MRTD application data, such as commands processing and files management, etc. defined in ISO/ IEC 7816-4, 8 and 9. In this protection profile accepts both opened or closed IC chip operating systems.

43 The MRTD chip application is IC chip application that implements the function to store and process the ePassport identity data according to LDS(Logical Data Structure) format

defined in the ICAO document and security mechanism to securely protect the function. Also, the MRTD application is added the EAC security mechanism by the EAC specifications, because the biometric data of the ePassport holder is included in the ePassport identity data.

44 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.

2.2.3 Logical Scope of the TOE

45 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.

Assets

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

[Table 3] TOE Assets

Category			Description	Storage Space
User Data	ePassport Identity Data	Personal Data of the ePassport holder	Data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13 and EF.DG16	EF file
		Biometric Data of the ePassport holder	Data stored in EF.DG3 and EF.DG4	
	ePassport Authentication Data		SOD, EAC chip authentication public key, etc.	
	EF.CVCA		In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System	
	EF.COM		LDS version info., tag list of DG used, etc.	
TSF Data	EAC Chip Authentication Private Key		In EAC-CA, Chip Private key used by the TOE to demonstrate Not forged MRTD chip	Secure memory
	CVCA Certificate		In personalization phase, Root CA Certificate issued in EAC-PKI	
	CVCA Digital Signature Verification Key		After personalization phase, CVCA certificate Public key newly created by certificate update	
	Current Date		In personalization phase, Date of issuing the ePassport is recorded. However, In operational use phase, the TOE internally updates it as the latest date among issuing dates of CVCA link certificate, DV certificate or Issuing State IS certificate.	
	BAC Authentication Key		BAC authentication encryption key, BAC authentication MAC key	
	BAC Session Key		BAC session encryption key, BAC session MAC key	Temporary memory
	EAC Session Key		EAC session encryption key, EAC session MAC key	

Application Notes : The biometric data obtained from an ePassport holder include the face, the fingerprint and the iris. The face information is contained mandatory according to the ICAO document. The Fingerprint and iris information is contained optionally according to the Issuing policy of the ePassport. This protection profile includes security functional requirements for the EAC specifications by assuming fingerprint information to be contained. The security target author may additionally define iris information in DG4.

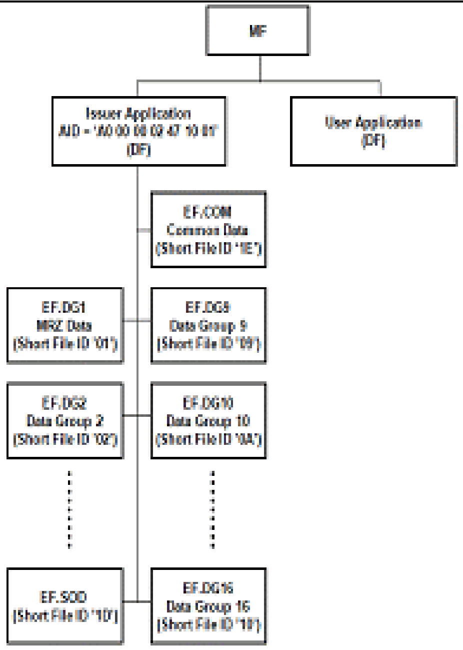
Application Notes : The BAC authentication key is already generated in the personalization phase by MRTD chip implementation method and recorded in secure memory of the MRTD chip or the TOE generates the key itself in the BAC of the operational use phase.

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

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

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

Category	DG	Content	LDS Structure
Detail(s) in MRZ	DG1	Document(Passport) Type	
		Issuing State	
		Name (of Holder)	
		Document Number	
		Check Digit (of Doc Number)	
		Nationality	
		Date of Birth	
		Check Digit (of DOB)	
		Sex	
		Data of Expiry of Valid Until Date	

		Check Digit (of DOE/VUD)	 MF Issuer Application AID = 'A0 00 00 02 47 10 01' (DF) User Application (DF) EF.COM Common Data (Short File ID '1E') EF.DG1 MRZ Data (Short File ID '01') EF.DG9 Data Group 9 (Short File ID '09') EF.DG2 Data Group 2 (Short File ID '02') EF.DG10 Data Group 10 (Short File ID '0A') EF.SOD (Short File ID '1D') EF.DG16 Data Group 16 (Short File ID '10')
		Composite Check Digit	
Biometric Data	DG2	Encoded face info.	
	DG3	Encoded fingerprint info.	
	DG4	Encoded iris info. (optional)	
Others	DG5	Display Portrait	
	DG6	-	
	DG7	Displayed Signature	
	DG8	-	
	DG9	-	
	DG10	-	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	-	
	DG14	EAC Chip Authentication Public Key	
	DG15	AA Digital Signature Verification Key (optional)	
	DG16	Person(s) to Notify	

Security Mechanism

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

<BAC>

49 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.

50 The TOE generate 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.

51 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>

52 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.

53 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.

54 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.

55 [Table 5] summarized the ePassport security mechanisms.

[Table 5] The ePassport Security Mechanisms

The ePassport Security Mechanisms				IT Security Function of the TOE
Security Mechanism	Function	cryptography	Cryptographic Key/ Certificate Type	
PA	User Data Authentication	N/A	N/A	Access control to the SOD - Read-rights: BIS, EIS - Write-rights: Personalization agent
BAC	BAC Mutual authentication	Symmetric key-based entity authentication protocol TDES-CBC SHA MAC	BAC Authentication Key (encryption key, MAC key)	The TOE verifies if the Inspection System has access-rights, by decryption and MAC operation for the transmitted value of the Inspection System. The TOE transmits the value to the Inspection System after encryption and MAC operation for authentication.
	BAC Key Distribution	Symmetric key-based key distribution protocol TDES-CBC SHA MAC	BAC Session Key (encryption key, MAC key)	Generating BAC session key by using KDF from the exchanged key-sharing random number on the basis of the TDES-based key distribution protocol
	BAC Secure messaging	Secure Messaging	BAC Session Key (encryption key, MAC key)	Transmitting messages by creating the MAC after encryption with the BAC session key Receiving messages by decryption it after verifying the MAC with the

				BAC session key
EAC	EAC-CA	DH key distribution protocol ECDH key distribution protocol	EAC Chip Authentication Public Key EAC Chip Authentication Private Key	The TOE executes the ephemeral-static DH key distribution protocol
	EAC Secure messaging	Secure messaging	EAC Session Key (cryptographic key, MAC key)	Secure messaging by using the EAC session key shared in the EAC-CA
	EAC-TA	RSAPSS ECDSA	CVCA certificate CVCA link certificate DV certificate IS certificate	Verifying the IS certificate by using the certificate chain and the link certificate Verifying the digital signature for transmitted messages of the EIS for the EIS authentication

TOE Access Control and Security Management

56 The TOE provides access control rules and management functions for the MRTD application data based on security attributes of the user in the phases of the Personalization and the Operational Use.

57 The TOE provides only the authorized personalization agent to writing function on the user data and TSF data in the Personalization phase. Also, the TOE provides the access control function on the read-rights of the user data based on the access-rights of the Inspection System given through execution of security mechanisms in the Operational Use phase.

58 The TOE allows only the authorized personalization agent to manage the security attributes of user, user data and TSF data in the phases of the Personalization and the Operational Use and defines it as security role. Also, the TSF executes itself some security management functions, such as updating the CVCA certificate and the current date and initializing the identifier for secure messaging, etc.

Other TOE Protection

59 The TOE, in order to protect the TSF from interference and tampering by untrusted subjects, ensures that the access control function is always invoked without bypassing

and separates between domain used by untrusted subjects, such as other application programs, etc., and domain in which the MRTD application program is executed.

60 The TOE executes the functions to detect and handle for modification of the TSF data transmitted and run self-testing to verify the integrity of the stored TSF data and executable code. Also, if detecting failures through self-testing or abnormal operation in the IC chip, the TOE preserves a secure state so that to prevent the types of failures in the TSF(malfunction).

61 The TOE ensures not to obtain the cryptographic-related data by exploiting physical phenomena of the cryptographic operation (change of current, voltage and electromagnetic, etc.).

3. TOE Security Environment

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

3.1 Assumptions

63 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

64 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.

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

Application Notes : The methods of the Inspection System to verify the certificate chain for the PA and to distribute the IS certificate and the digital signature generation key may depend on the Issuing policy of the ePassport. Therefore, the ST author can define security environment according to the Issuing policy of the ePassport.

A. IC Chip

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

Application Notes : To ensure the secure TOE environment, the IC chip shall be a certified product of CCRA EAL4+(SOF-high) or higher level. The cryptographic operation supported by the IC chip may be provided in the co-processor of the IC chip or cryptographic libraries loaded in the IC chip.

A. Inspection System

67 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.

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

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

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

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

A. MRZ Entropy

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

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

3.2 Threats

70 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.

71 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.

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

<Threats to the TOE in the Personalization phase>

T. Application Program Interference

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

T. TSF Data Modification

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

<BAC-related Threats in the Operational Use phase>

T. BAC Authentication Key Disclose

75 In order to find out the personal data of the ePassport holder, the threat agent may obtain the read-rights of the BAC authentication key located inside the TOE and disclose

the related information.

Application Notes : The BAC authentication key may be generated by Personalization agent in the Personalization phase or by the TOE in the Operational Use phase. According to the method to generate the BAC authentication key, the ST author shall consider the threat of disclose of the BAC authentication key stored in secure and temporary memory of the MRTD chip in the former case. In the latter case, the ST author shall consider the threat of disclose of the BAC authentication key from the residual information remaining in temporary memory (Refer to ‘T. Residual Information’.).

T. BAC Replay Attack

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

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

T. Eavesdropping

77 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

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

<EAC-related Threats in the Operational Use phase>

T. Damage to Biometric Data

79 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

80 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

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

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

T. Session Data Reuse

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

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

T. Skimming

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

holder realizing it.

<Threats related to IC Chip Support>

T. Malfunction

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

<Other Threats in the Operational Use phase>

T. ePassport Reproduction

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

T. Leakage to Cryptographic Key Information

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

T. Residual Information

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

3.3 Organisational Security Policies

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

P. Application Program Loading

89 The Personalization agent shall approve application program loading after checking that

application programs loaded in the MRTD chip does not affect the secure TOE.

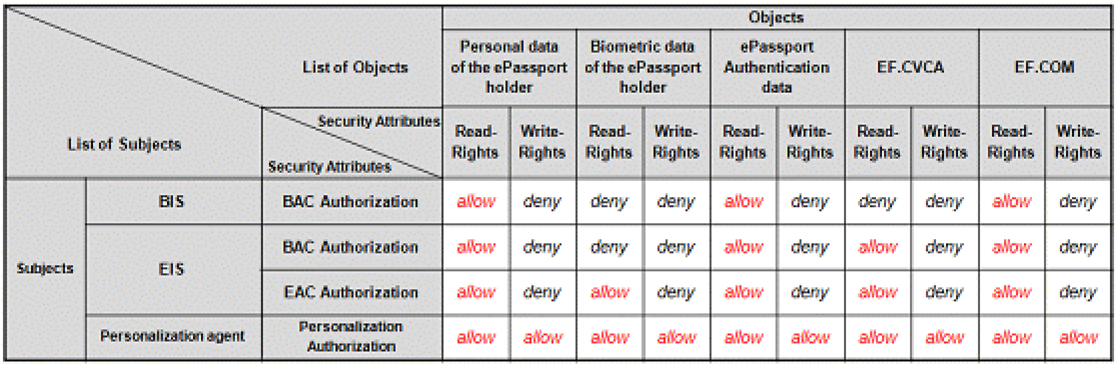
Application notes : The application program loading can only be done by organizations holding the same authority as the Personalization agent.

P. ePassport Access Control

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

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

[Table 6] ePassport Access Control Policies



		List of Objects	Objects									
			Personal data of the ePassport holder		Biometric data of the ePassport holder		ePassport Authentication data		EF.CVCA		EF.COM	
List of Subjects		Security Attributes Security Attributes	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	BIS	BAC Authorization	allow	deny	deny	deny	allow	deny	deny	deny	allow	deny
	EIS	BAC Authorization	allow	deny	deny	deny	allow	deny	allow	deny	allow	deny
		EAC Authorization	allow	deny	allow	deny	allow	deny	allow	deny	allow	deny
	Personalization agent	Personalization Authorization	allow	allow	allow	allow	allow	allow	allow	allow	allow	allow

P. International Compatibility

91 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. PKI

92 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.

93 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. Personalization Agent

94 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. Range of RF Communication

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

P. Security Mechanism Application Procedures

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

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

4. Security Objectives

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

4.1 Security Objectives for the TOE

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

O.Access Control

99 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

100 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.Certificate Verification

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

O.Deleting Residual Information

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

O.Domain Separation

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

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

O.EAC

104 The TOE authenticate 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.Handling Information Leakage

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

Application Notes : In case the co-processor of the IC chip or cryptographic libraries loaded in the IC chip provide countermeasures to satisfy this security objective, the ST author shall specify it as a security objective for environment.

O.Management

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

Application Notes : In the Personalization phase, the Personalization agent shall deactivate the writing function after recording the MRTD application data.

O.Replay Prevention

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

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

O.Secure Messaging

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

O.Security Mechanism Application Procedures

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

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

O.Self-protection

110 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.Session Termination

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

4.2 Security Objectives for the Environment

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

OE. Application Program Loading

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

OE. Certificate Verification

114 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.

115 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. IC Chip

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

OE. Inspection System

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

OE. MRZ Entropy

118 Personalization agent shall ensure the MRZ entropy to ensure the secure BAC authentication key.

OE. Passport Book Manufacturing Security

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

OE. Personalization Agent

120 The personalization agent shall issue the ePassport in the secure manner so that to

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

OE. PKI

121 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.

122 Also, The Issuing State of the ePassport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System.

OE. Range of RF Communication

123 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. Procedures of ePassport holder Check

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

5. IT Security Requirements

125 IT security requirements specify security functional and assurance requirements that must be satisfied by the TOE that conforms to this Protection Profile.

5.1 TOE Security Functional Requirements

126 The security functional requirements for this Protection Profile consist of the following components from Part2 of the CC, summarized in the following [Table 7].

127 This Protection Profile provides Application Notes together with relevant requirements to clarify the intent of a requirement, identify implementation choices or to define "Pass/Fail" criteria for a requirement.

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

[Table 7] Security Functional Requirements

Security functional class	Security functional component	
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.2(1)	Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)
	FCS_CKM.2(2)	Cryptographic key distribution (KDF Seed Distribution for EAC session key generation)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (Symmetric Key Cryptographic Operation)
	FCS_COP.1(2)	Cryptographic operation (MAC)
	FCS_COP.1(3)	Cryptographic operation (Hash Function)
	FCS_COP.1(4)	Cryptographic operation (Digital signature Verification for Certificates Verification)
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	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.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Info.)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialisation)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy (FPR)	FPR_UNO.1	Unobservability
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_TST.1	TSF testing

5.1.1 Cryptographic Support

FCS_CKM.1 Cryptographic key generation(Key Derivation Mechanism)

Hierarchical to : No other components.

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

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

Application Notes : The TOE generates the BAC authentication key, BAC session key and EAC session key by using key derivation mechanism. If the Personalization agent generates BAC authentication key and records it in TOE in the Personalization phase according to the Issuing policy of the ePassport, TOE does not generate the BAC authentication key.

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

Hierarchical to : No other components.

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

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

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

Hierarchical to : No other components.

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

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

131 FCS_CKM.2.1 The TSF shall distribute **KDF Seed for the EAC session key generation** in accordance with a specified cryptographic key distribution method [[selection : *Diffie-Hellman key-agreement protocol, Elliptic Curve Diffie-Hellman key-agreement protocol, [assignment : other cryptographic key distribution method]*]] that meets the following : [[selection : *PKCS#3, ANSI X9.42, ISO/IEC 15946-3, [assignment : other standards]*]].

FCS_CKM.4 Cryptographic key destruction

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

132 FCS_CKM.4.1 The TSF shall destroy **encryption keys and MAC keys** in accordance with a specified cryptographic key destruction method [assignment : *cryptographic key destruction method*] that meets the following: [assignment : *list of standards*].

Application Notes : The ST author shall specify the method to securely destroy the keys generated by the key derivation mechanism. It can be assigned as ‘none’ if there is no standard list for reference.

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

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

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

Application Notes : The TOE uses the TDES cryptographic algorithm for the confidentiality protection of the transmitted data of the BAC or EAC secure messaging, for the BAC mutual authentication and for the BAC key distribution. For operation mode of the cryptographic algorithm used, the CBC mode with IV=0 as defined in ISO/IEC 10116 is used. However, in case the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement can be changed as a requirement for the IT environment.

FCS_COP.1(2) Cryptographic operation (MAC)

Hierarchical to : No other components.

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

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

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

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

Hierarchical to : No other components.

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

135 FCS_COP.1.1 The TSF shall perform [hash operation] in accordance with a specified cryptographic algorithm [[select : *SHA-1, [assignment : other cryptographic algorithm]*]]

and cryptographic key sizes [none] that meet the following: [[selection : *ISO/IEC 10118-3, [assignment : other standards]*]].

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. However, in case the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement can be changed as a requirement for the IT environment.

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

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

136 FCS_COP.1.1 The TSF shall perform [assignment : *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [[selection : *RSASSA-PKCS1-v1.5-SHA-256, RSASSA-PSS-SHA-256, ECDSA-SHA-224, ECDSA-SHA-256, [assignment : other cryptographic algorithm]*]] and cryptographic key sizes [assignment : *cryptographic key sizes*] that meet the following: [[select : *PKCS#1, ISO/IEC 15946-2*]].

Application Notes : In Appendix A.3 Terminal Authentication of the EAC specifications, the digital signature algorithm, hash algorithm and digital signature key sizes are defined as of the following. The ST author shall specify the cryptographic key sizes by referring to [Table 8] so that to satisfy the SOF-high. However, in case the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement can be changed as a requirement for the IT environment.

[Table 8] Details of Digital Signature in the EAC Specifications

Digital Signature Algorithm	Hash Algorithm	Digital Signature Key Sizes
RSASSA-PKCS1-v1.5	SHA-1, SHA-256	1024, 1280, 1536, 2048, 3072 bits
RSASSA-PSS	SHA-1, SHA-256	1024, 1280, 1536, 2048, 3072 bits
ECDSA	SHA-1, SHA-224/ SHA-256	160, 192, 224, 256 bits

5.1.2 User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to : No other components.

Dependencies : FDP_ACF.1 Security attribute based access control

137 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) [Assignment : *list of other subjects*]

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) [Assignment : *list of other objects*]

c) Operations

(1) Read

(2) Write

(3) [Assignment : *list of other operations*]

]

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 initialisation

138 FDP_ACF.1.1 The TSF shall enforce the [the ePassport access control policy] to objects based on the following: [[Table 9], [Table 10], [assignment : *security attributes relevant to additional assigned lists of objects, subjects and operations in FDP_ACC.1*]].

[Table 9] Subject-relevant Security Attributes

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

[Table 10] Object-relevant Security Attributes

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

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

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

The Personalization agent issuing authorization is the right given when the

Personalization agent to be successfully authenticated in the Personalization phase.

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

]

Application Notes : The ST author shall implement access control rules by referring to [Table 6] of P. ePassport Access Control in order to enforce the ePassport access control policies.

140 FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment : *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

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

FDP_RIP.1 Subset residual information protection

Hierarchical to : No other components.

Dependencies : No dependencies.

142 FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource

is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [

a) BAC session key

b) EAC session key

c) BAC authentication key

d) [assignment : *list of other objects*]

].

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

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]

143 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 unauthorised disclosure.

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

FDP_UIT.1 Data exchange integrity

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

144 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 [selection : *modification, deletion, insertion, replay*] errors.

145 FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection : *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 ST author shall implement additional security mechanism in case of selecting 'replay' in selection operation.

5.1.3 Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components.
Dependencies : FIA_UAU.1 Timing of authentication

146 FIA_AFL.1.1 The TSF shall detect when [selection : *[assignment : positive integer number], an administrator configurable positive integer within[assignment : range of acceptable values]*] unsuccessful authentication attempts occur related to [

a) BAC mutual authentication
b) EAC-TA
c) [assignment : *list of other authentication events*]

].

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

Application Notes : In case of a failure of the BAC mutual authentication or EAC-TA, it is recommended to terminate the BAC or EAC secure messaging. However, the ST author can replace it with another equivalent mechanism. The ST author shall assign the number of unsuccessful authentication attempts by agreeing with the Personalization agent.

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

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

148 FIA_UAU.1.1 The TSF shall allow [

a) indication that support the BAC mechanism
b) [assignment : *list of other TSF mediated actions*]

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

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

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)

150 FIA_UAU.1.1 The TSF shall allow [

a) to perform the EAC-CA

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

c) [assignment: *list of other TSF mediated actions*]

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

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to : No other components.

Dependencies : No dependencies.

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

a) BAC mutual authentication

b) EAC-TA

c) [assignment : *other authentication mechanism(s)*]

].

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to : No other components.

Dependencies : No dependencies.

153 FIA_UAU.5.1 The TSF shall provide [

a) BAC mutual authentication

b) EAC-TA

c) [assignment : *other authentication mechanism(s)*]

] to support user authentication.

154 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) [assignment : *other rules of authentication mechanism(s)*]

].

FIA_UID.1 Timing of identification

Hierarchical to : No other components.

Dependencies : No dependencies.

155 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.

156 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 : When external entities communicated with the TOE request the use of the MRTD application, the TOE identifies it with the Inspection System.

5.1.4 Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

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

FMT_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

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

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

FMT_MSA.3 Static attribute initialisation

Hierarchical to : No other components.
Dependencies : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

159 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.

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

Application Notes : When generating user data (EF.DG1~16, 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 10] of FDP_ACF.1.1.

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

Hierarchical to : No other components.
Dependencies : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

161 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) [assignment : *list of other TSF data*]

] to [Personalization agent in the Personalization phase].

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

Hierarchical to : No other components.

Dependencies : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

162 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.3 Secure TSF data

Hierarchical to : No other components.

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

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components.

Dependencies : No dependencies.

164 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) [assignment : *other security management functions*]

].

FMT_SMR.1 Security roles

Hierarchical to : No other components.

Dependencies : FIA_UID.1 Timing of identification

165 FMT_SMR.1.1 The TSF shall maintain the roles [

a) Personalization agent

b) [assignment : *other roles*].

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

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

5.1.5 Privacy

FPR_UNO.1 Unobservability

Hierarchical to : No other components.

Dependencies : No dependencies.

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

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

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

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

d) [assignment : *list of other operations*]

] on [

a) BAC authentication key

b) BAC session key

c) EAC session key

d) EAC chip authentication private key

e) [assignment: *list of other objects*] by [TSF].

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

5.1.6 TSF Protection

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to : No other components.

Dependencies : ADV_SPM.1 Informal TOE security policy model

168 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) [assignment: *list of types of other failures in the TSF*]

].

FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components.

Dependencies: No dependencies.

169 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].

170 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) [assignment : *other action to be taken*]

] if modifications are detected.

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

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to : No other components.

Dependencies : No dependencies.

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

FPT_SEP.1 TSF domain separation

Hierarchical to : No other components.

Dependencies : No dependencies.

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

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

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

FPT_TST.1 TSF testing

Hierarchical to : No other components.

Dependencies : FPT_AMT.1 Abstract machine testing

174 FPT_TST.1.1 The TSF shall run a suite of self tests [selection : *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment : conditions under which self test should occur]*] to demonstrate the correct operation of [selection : *[assignment : parts of TSF], the TSF*].

175 FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection : *[assignment : parts of TSF data], TSF data*].

176 FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.2 Security Assurance Requirements

177 The security assurance requirements for this Protection Profile consist of the following components from Part 3 of the CC, summarized in the following [Table 11] and evaluation assurance level is EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.3).

178 The assurance components are augmented follows:

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

[Table 11] Security Assurance Requirements

Assurance class	Assurance component	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.3	Moderately resistant

5.2.1 Configuration Management

ACM_AUT.1 Partial CM automation

Dependencies :

ACM_CAP.3 Authorisation controls

Developer action elements :

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

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

Content and presentation of evidence elements :

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

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

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

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

Evaluator action elements :

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

ACM_CAP.4 Generation support and acceptance procedures

Dependencies :

ALC_DVS.1 Identification of security measures

Developer action elements :

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

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

188 ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements :

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

190 ACM_CAP.4.2C The TOE shall be labelled with its reference.

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

192 ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that

comprise the TOE.

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

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

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

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

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

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

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

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

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

Evaluator action elements :

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

ACM_SCP.2 Problem tracking CM coverage

Dependencies :

ACM_CAP.3 Authorisation controls

Developer action elements :

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

5.2.2 Delivery and Operation

ADO_DEL.2 Detection of modification

Dependencies :

ACM_CAP.3 Authorisation controls

Developer action elements :

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

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

Content and presentation of evidence elements :

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

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

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

Evaluator action elements :

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

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

Dependencies :

AGD_ADM.1 Administrator guidance

Developer action elements :

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

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

5.2.3 Development

ADV_FSP.2 Fully defined external interfaces

Dependencies :

ADV_RCR.1 Informal correspondence demonstration

Developer action elements :

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

Content and presentation of evidence elements :

217 ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

218 ADV_FSP.2.2C The functional specification shall be internally consistent.

219 ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

220 ADV_FSP.2.4C The functional specification shall completely represent the TSF.

221 ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements :

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

223 ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies :

ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements :

224 ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements :

225 ADV_HLD.2.1C The presentation of the high-level design shall be informal.

226 ADV_HLD.2.2C The high-level design shall be internally consistent.

227 ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

228 ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

229 ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

230 ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

231 ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

232 ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

233 ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements :

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

235 ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.2 Implementation of the TSF

Dependencies :

ADV_LLD.1 Descriptive low-level design
ALC_TAT.1 Well-defined development tools

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

Evaluator action elements :

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

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

ADV_LLD.1 Descriptive low-level design

Dependencies :

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

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

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

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

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

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

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

252 ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements :

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

requirements for content and presentation of evidence.

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

ADV_RCR.1 Informal correspondence demonstration

Dependencies :

No dependencies.

Developer action elements :

255 ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements :

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

Evaluator action elements :

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

ADV_SPM.1 Informal TOE security policy model

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements :

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

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

Content and presentation of evidence elements :

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

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

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

263 ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional

specification are consistent and complete with respect to the TSP model.

Evaluator action elements :

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

5.2.4 Guidance Documents

AGD_ADM.1 Administrator guidance

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements :

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

Content and presentation of evidence elements :

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

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

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

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

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

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

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

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

Evaluator action elements :

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

AGD_USR.1 User guidance

Dependencies :

ADV_FSP.1 Informal functional specification

Developer action elements :

275 AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements :

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

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

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

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

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

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

Evaluator action elements :

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

5.2.5 Life Cycle Support

ALC_DVS.1 Identification of security measures

Dependencies :

No dependencies.

Developer action elements :

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

Content and presentation of evidence elements :

284 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.

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

Evaluator action elements :

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

287 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 :

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

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

Content and presentation of evidence elements :

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

291 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 :

292 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 Subset of the implementation of the TSF

Developer action elements :

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

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

Content and presentation of evidence elements :

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

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

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

Evaluator action elements :

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

5.2.6 Tests

ATE_COV.2 Analysis of coverage

Dependencies :

ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

Developer action elements :

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

Content and presentation of evidence elements :

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

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

Evaluator action elements :

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

ATE_DPT.2 Testing: low-level design

Dependencies :

ADV_HLD.2 Security enforcing high-level design

ADV_LLD.1 Descriptive low-level design

ATE_FUN.1 Functional testing

Developer action elements :

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

Content and presentation of evidence elements :

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

Evaluator action elements :

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

ATE_FUN.1 Functional testing

Dependencies :

No dependencies.

Developer action elements :

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

307 ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements :

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

309 ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

310 ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

311 ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

312 ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements :

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

ATE_IND.2 Independent testing - sample

Dependencies :

ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
ATE_FUN.1 Functional testing

Developer action elements :

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

Content and presentation of evidence elements :

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

316 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 :

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

318 ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

319 ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 Vulnerability Assessment

AVA_MSU.2 Validation of analysis

Dependencies :

ADO_IGS.1 Installation, generation, and start-up procedures
ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements :

320 AVA_MSU.2.1D The developer shall provide guidance documentation.

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

Content and presentation of evidence elements :

322 AVA_MSU.2.1C The guidance documentation shall identify all possible modes of

operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

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

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

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

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

Evaluator action elements :

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

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

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

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

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies :

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

Developer action elements :

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

Content and presentation of evidence elements :

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

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

the specific strength of function metric defined in the PP/ST.

Evaluator action elements :

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

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

AVA_VLA.3 Moderately resistant

Dependencies :

ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements :

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

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

Content and presentation of evidence elements :

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

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

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

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

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

Evaluator action elements :

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

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

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

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

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

6. Protection Profile Application Notes

348 This protection profile includes the minimum security requirements and does not make definition on implementation model of the TOE. In relation to security problems possible to occur according to the TOE implementation model, the developer shall define additional security environments, security objectives and security requirements.

349 Product developers or marketers can draw up the Security Target by conforming all contents defined in this protection profile and users can utilize them for selection, operation and management of the product.

350 The AA (active authentication) is optional in the EAC specifications. Therefore, the ST author can add the AA security mechanism according to the Issuing policy of the ePassport. In case of adding AA security mechanism, the ST author shall additionally define security environments, security objectives and security requirements.

351 The TOE life cycle and Personalization agent authentication mechanism, etc. may differ according to the Issuing policy of the ePassport. Therefore, the ST author may add or modify TOE description, security environments, security objectives and security requirements by considering these details.

7. Rationale

352 This chapter describes the rationale of security objectives and rationale of security requirements.

7.1 Rationale of Security Objectives

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

354 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.

355 [Table 12] shows the mapping between security environments and security objectives.

[Table 12] Summary of Mappings between Security Environments and Security Objectives

Security Objectives Security Objectives	TOE Security Objectives													Security Objectives for Environment									
	O.Access Control	O.BAC	O.Certificate Verification	O.Deleting Residual Information	O.Domain Separation	O.EAC	O.Handling Information Leakage	O.Management	O.Replay Prevention	O.Secure Messaging	O.Security Mechanism Application Procedures	O.Self-protection	O.Session Termination	OE. Application Program Loading	OE. Certificate Verification	OE. IC Chip	OE. Inspection System	OE. MRZ Entropy	OE. Passport Book Manufacturing Security	OE. Personalization Agent	OE. PKI	OE. Procedures of Passport Holder Check	OE. Range of RF Communication
T. Application Program Interference					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. Eavesdropping										X							X						
T. ePassport Reproduction					X														X			X	

T. Forgery and Corruption of Personal Data	X	X											X				X						
T. IS Certificate Forgery			X		X			X							X								
T. Leakage to Cryptographic Key Information							X																
T. Malfunction												X				X							
T. Residual Information				X																			
T. Session Data Reuse									X								X						
T. Skimming	X	X				X											X						X
T. TSF Data Modification	X				X			X		X			X							X			
P. Application Program Loading														X									
P. ePassport Access Control	X	X				X		X									X			X			
P. International Compatibility																				X			
P. Personalization Agent								X												X			
P. PKI			X																		X		
P. Range of RF Communication																							X
P. Security Mechanism Application Procedures											X						X						
A. Certificate Verification															X					X	X		
A. IC Chip																X							
A. Inspection System																	X						
A. MRZ Entropy																		X					

7.1.1 Rationale of TOE Security Objective

O.Access Control

356 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.

357 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

358 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.

359 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.Certificate Verification

360 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.

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

O.Deleting Residual Information

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

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

O.Domain Separation

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

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

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

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

O.EAC

368 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.

369 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.Handling Information Leakage

370 This security objective 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.

O.Management

371 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

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

O.Replay Prevention

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

O.Secure Messaging

374 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.Security Mechanism Application Procedures

375 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.

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

O.Self-protection

377 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.Session Termination

378 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

7.1.2 Rationale of Security Objective for Environment

OE. Application Program Loading

379 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.

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

OE. Certificate Verification

381 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. IC Chip

382 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.

383 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. Inspection System

384 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.

385 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.

386 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.

387 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. MRZ Entropy

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

OE. Passport Book Manufacturing Security

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

OE. Personalization Agent

390 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.

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

OE. PKI

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

OE. Procedures of Passport Holder Check

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

OE. Range of RF Communication

394 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.

7.2 Rationale for Security Requirements

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

7.2.1 Rationale for Security Functional Requirements of the TOE

396 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.

397 [Table 13] presents the mapping between the security objectives and the security functional requirements.

[Table 13] Summary of Mappings between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	TOE Security Objectives												
	O.Access Control	O.BAC	O.Certificate Verification	O.Deleting Residual Information	O.Domain Separation	O.EAC	O.Handling Information Leakage	O.Management	O.Replay Prevention	O.Secure Messaging	O.Security Mechanism Application Procedures	O.Self-protection	O.Session Termination
FCS_CKM.1		X				X							
FCS_CKM.2(1)		X							X				
FCS_CKM.2(2)						X							
FCS_CKM.4				X									
FCS_COP.1(1)		X								X			
FCS_COP.1(2)		X								X			
FCS_COP.1(3)		X				X							
FCS_COP.1(4)			X			X							

FDP_ACC.1	X												
FDP_ACF.1	X	X				X		X			X		
FDP_RIP.1				X					X				
FDP_UCT.1									X	X			
FDP_UIT.1									X	X			
FIA_AFL.1	X	X				X					X		X
FIA_UAU.1(1)	X	X											X
FIA_UAU.1(2)	X					X					X		X
FIA_UAU.4		X				X			X				
FIA_UAU.5	X	X				X					X		
FIA_UID.1		X				X							
FMT_MOF.1	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.3			X			X			X				
FMT_SMF.1			X					X					
FMT_SMR.1								X					
FPR_UNO.1							X						
FPT_FLS.1												X	
FPT_ITI.1										X			X
FPT_RVM.1	X											X	
FPT_SEP.1	X				X								
FPT_TST.1												X	

FCS_CKM.1 Cryptographic key generation (Key Derivation Mechanism)

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

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

399 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).

400 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)

401 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).

402 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

403 This component ensures the ST author to define the method to securely destroy the key generated by key derivation mechanism of FCS_CKM.1.

404 This component satisfies the security objective of O. Deleting Residual Information as it provides the method of destroying the key generated by the TSF and remained in temporary memory with the method defined by the ST author.

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

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

406 The cryptographic operation defined in this component satisfies the security objective of O. Secure Messaging as it ensures confidentiality of user data transmitted between the TOE and the Inspection System by using cryptographic algorithm.

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

FCS_COP.1(2) Cryptographic operation (MAC)

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

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

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

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

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

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

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

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

414 The digital signature verification method defined in this component satisfies the security objective of O. Certificate Verification as it verifies the CVCS link certificate, DV certificate and IS certificate provided by the Inspection System to the TOE. Also, this

component satisfies the security objective of O. EAC as it provides the digital signature verification method necessary in the EAC-TA in order to check the access-rights for the biometric data of the ePassport holder.

FDP_ACC.1 Subset access control

415 This component defines list of subjects, objects and operations in order to decide a scope of control for the ePassport access control policies.

416 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

417 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.

418 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.

419 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.

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

FDP_RIP.1 Subset residual information protection

421 This component ensures that previous information is not included when the TSF allocates or deallocates memory resources for the BAC authentication key, BAC session

key, EAC session key and random numbers.

422 This component satisfies the security objective of O. Deleting Residual Information as it ensures that previous information of the BAC authentication key, BAC session key 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, TAC-TA and generation of session key is not available.

FDP_UCT.1 Basic data exchange confidentiality

423 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.

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

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

FDP_UIT.1 Data exchange integrity

426 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.

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

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

FIA_AFL.1 Authentication failure handling

429 If the authentication attempt failure number defined by the ST author is surpassed, this component detects it and requires to terminate a user session.

430 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.

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

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

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

433 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)

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

435 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.4 Single-use authentication mechanisms

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

437 This component satisfies the security objectives of O. Replay Prevention, O. BAC and O. EAC as the TSF executes 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.

FIA_UAU.5 Multiple authentication mechanisms

438 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.

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

FIA_UID.1 Timing of identification

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

441 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 Management of security functions behaviour

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

443 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_MSA.1 Management of security attributes

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

445 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 Initialisation

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

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

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

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

449 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)

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

451 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.3 Secure TSF Data

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

453 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.

454 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

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

456 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.

457 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

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

459 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.

FPR_UNO.1 Unobservability

460 This component ensures that external entities are unable to observe the cryptographic-related data, such as the BAC authentication key, BAC session key, EAC session key and EAC chip authentication private key, etc. when the TSF performs a cryptographic operation.

461 This component satisfies the security objective of O. Handling Information Leakage as it ensures that external entities cannot find out any cryptographic-related data by exploiting physical phenomena (change of current, voltage and electromagnetic, etc.) occurred when the TSF performs cryptographic operation of TDES, MAC and digital signature verification, etc.

FPT_FLS.1 Failure with preservation of secure state

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

463 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 TPT_TST.1 is detected or the IC chip detects abnormal operating conditions.

FPT_ITI.1 Inter-TSF detection of modification

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

465 This component satisfies the security objectives of O. Secure Messaging and O. Session Termination by detecting modification of the transmitted TSF data in the Personalization and Operational Use phases and by performing an action to be taken, such as terminating the related communication channels, deleting the related session key and

management actions specified in FMT_MSA.1, etc., if modifications are detected

FPT_RVM.1 Non-bypassability of the TSP

466 This component requires to always invoke the ePassport access control function as a reference monitor to protect the TSF from manipulating operation and bypassing access control policy, etc. by untrusted subjects.

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

FPT_SEP.1 TSF Domain Separation

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

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

470 Also, this component satisfies the security objective of O. Domain Separation by separating secure memory domain from other memory domains, therefore protecting the TSF data from external IT entities.

FPT_TST.1 TSF testing

471 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.).

472 This component satisfies the security objective of O. Self-protection by running self-testing under the self-testing execution conditions for TSF parts defined by the ST author, therefore demonstrating the correct operation of the TSF.

473 Also, this component satisfies the security objective of O. Self-protection by verifying the integrity of TSF data parts defined by the ST author and the TSF executable code stored in the TOE, therefore detecting loss of the TSF data and the executable code.

7.2.2 Rationale of Assurance Requirements

474 The EAL(Evaluation Assurance Level) of this Protection Profile was selected as EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) by considering the value of assets protected by the TOE and level of threats, etc.

475 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.

476 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.

477 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.3 Moderately resistant

478 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.

479 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 specialised equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing moderate attack potential. EAL4 includes AVA_VLA.2 that resistant the low attack potential. Therefore, AVA_VLA.3 is augmented to require execution of systematic vulnerability analysis and resistant to attackers possessing moderate attack potential. However, there still exists direct attack potential to the IC chip by threat agent possessing high attack potential and evaluation and verification for this may be assigned to the IC chip manufacturer.

480 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.

7.3 Rationale of Dependency

7.3.1 Dependency of TOE Security Functional Requirements

481 [Table 14] shows dependency of TOE functional components

[Table 14] Dependency of TOE Functional Components

No.	Functional Component	Dependency	Ref. No.
1	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4 FMT_MSA.2	2, 3 4 None
2	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4 FMT_MSA.2	1 4 None
3	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4 FMT_MSA.2	1 4 None
4	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_MSA.2	1 None
5	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 4 None
6	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 4 None
7	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 4 None
8	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 4 None
9	FDP_ACC.1	FDP_ACF.1	10
10	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	9 22
11	FDP_RIP.1	-	-
12	FDP_UCT.1	[FPT_ITC.1 or FPT_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	None 9

13	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	9 None
14	FIA_AFL.1	FIA_UAU.1	15, 16
15	FIA_UAU.1(1)	FIA_UID.1	19
16	FIA_UAU.1(2)	FIA_UAU.1(1)	15
17	FIA_UAU.4	-	-
18	FIA_UAU.5	-	-
19	FIA_UID.1	-	-
20	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	26 27
21	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	9 26 27
22	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	21 27
23	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	26 27
24	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	26 27
25	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	EAL4 23
26	FMT_SMF.1	-	-
27	FMT_SMR.1	FIA_UID.1	19
28	FPR_UNO.1	-	-
29	FPT_FLS.1	ADV_SPM.1	EAL4
30	FPT_ITI.1	-	-
31	FPT_RVM.1	-	-
32	FPT_SEP.1	-	-
33	FPT_TST.1	FPT_AMT.1	None

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

483 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.

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

485 FPT_TST.1 has dependency with FPT_AMT.1, but the dependency in this PP is not satisfied. FPT_AMT.1 is executed by the IC chip, the TSF underlying abstract machine rather than by the TOE. Therefore, testing if the IC chip is operating normally to support security functions of the TOE is satisfied by security objective for environment of OE. IC Chip.

7.3.2 Dependency of TOE Security Assurance Requirements

486 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 15].

487 AVA_VLA.3 has dependency with ADV_FSP.1 and ADV_IMP.1. This is satisfied by ADV_FSP.2 and ADV_IMP.2 in hierarchical relationship with ADV_FSP.1 and ADV_IMP.1

[Table 15] Dependency of the Added Assurance Components

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

7.4 Rationale of the Extended Security Requirements

488 There are no expended security requirements in this protection profile.

7.5 Rationale of Strength of Function

489 This protection profile requires ‘SOF-high’ for security functional requirements of FCS_CKM.1, FCS_COP.1(1), FCS_COP.1(2), FIA_UAU.4 and FMT_MTD.3.

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

selected to handle this situation. Therefore, SOF-high is claimed.

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

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

7.6 Rationale of Mutual Support and Internal Consistency

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

494 In '7.3.1 Dependency of TOE security functional requirements' and '7.3.2 Dependency of TOE security assurance requirements', the dependency is analyzed as a supportive relationship among security requirements of which it is necessary to depend on other security requirements in order to achieve a security objective because a security requirement is insufficient. In case the dependency was not satisfied, additional rationale is provided.

495 Also, security functional requirements, although there is no dependency among security functional requirements, are mutually supportive and internally consistency in relation to the TSF operations as of the following.

496 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). It is separated the execution domain of subjects and objects within the scope of control of the ePassport access control policies from other domains (FPT_SEP.1) and ensured to invoke the access control function at all times as a reference monitor to protect these subjects and objects(FPT_RVM.1). Therefore, these security requirements are mutually supportive and internally consistent.

497 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.

498 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.

499 The TSF must ensure that physical phenomena of current, voltage and electromagnetic waves, etc. occurred when the TSF performs cryptographic operations (FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4)) are not exploited by the threat agents (FPR_UNO.1). the cryptographic-related data created in temporary memory after cryptographic operations must be destroyed to prevent reuse (FCS_CKM.4, FDP_RIP.1). Therefore, these security requirements are mutually supportive and internally consistent.

500 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.

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

8. Terms and Definitions

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

Terms	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
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

REFERENCES

[1] 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

[2] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Version 1.1, TR-03110, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2007. 9

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

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

[5] Common Criteria for Information Technology Security Evaluation, Version 2.3, CCMB, 2005. 8.

[6] Common Methodology for Information Technology Security Evaluation, Version 2.3, CCMB, 2005. 8.

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

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

[9] ISO/IEC 7816-4:2005, Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange

[10] ISO/IEC 7816-8:2004, Identification cards - Integrated circuit cards - Part 8: Commands for security operations

[11] ISO/IEC 7816-9:2004, Identification cards - Integrated circuit cards - Part 9: Commands for card management

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

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

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

[15] ISO/IEC 10116:2006, Information technology - Security techniques - Modes of operation for an n-bit block cipher

[16] ISO/IEC 18033-3:2005, Information technology - Security techniques - Encryption

algorithms - Part 3: Block ciphers

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

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

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

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

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

ACRONYMS

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

IT	Information Technology
KDM	Key Derivation Mechanism
KDF	Key Derivation Function
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PA	Passive Authentication
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read Only Memory
SFP	Security Function Policy
SOD	Security Object of Document
SOF	Strength of Function
SPA	Simple Power Analysis
SSC	Send Sequence Counter
ST	Security Target
TA	Terminal Authentication
TDES	Triple-DES
TSC	TSF Scope of Control
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy