ePassport Protection Profile V2.1

June 2010

National Intelligence Service IT Security Certification Center

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

Protection Profile Title

ePassport Protection Profile V2.1

Evaluation Criteria Version

This Protection Profile has been prepared in conformance to the Common Criteria V3.1r3.

Developer

This Protection Profile has been developed by KISA(Korea Internet & Security Agency

Tables of Contents

List of Tables

List of Figures

1 Protection Profile Introduction

1.1 PP Reference

1   Title : ePassport Protection Profile

2   Protection Profile Version : V2.1

3   Evaluation Criteria : Common Criteria for Information Security System (Ministry of Public Administration and Security Notice No. 2009-52)

4   Common Criteria Version : V3.1r3

5   Evaluation Assurance Level : EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)

6   Developer: KISA(Korea Internet & Security Agency)

7   Certification Body : IT Security Certification Center

8   Certification Number : KECS-PP-0163a-2009, June 10, 2010

9   Validation Result : This Protection Profile is certified to be compatible with Common Criteria

10   Keywords : ePassport, COS, MRTD, ICAO

1.2 TOE Overview

1.2.1 TOE Type

11   The TOE that defined in this protection profile is 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).

12   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 V1.11 2008.02 [2] (EAC specification).

13   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.

1.2.2 ePassport System

14   The [Figure 1] shows the overall configuration of the ePassport system.
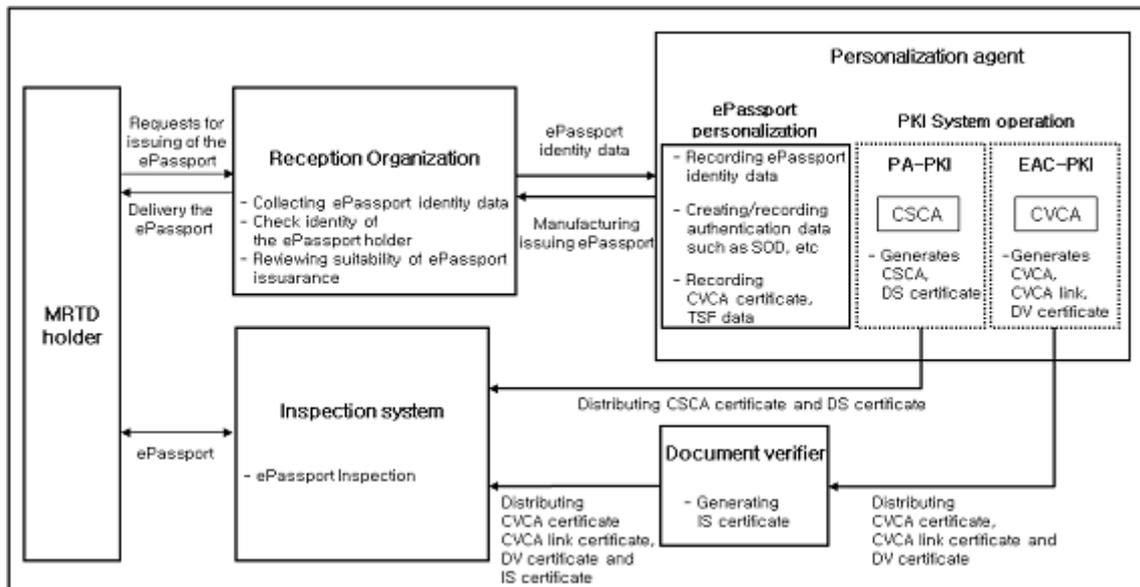
[Figure 1] Overall Configuration of the ePassport System

15   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.

16   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.

17   The Personalization agent generates document security object('SOD' hereinafter) by digital signature on the user data (identity and authentication data) and records it in the MRTD chip with the ePassport identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the personalization agent manufactures and issues the ePassport embedded the MRTD chip to the passport. Details of data recorded in the ePassport will be described in [Table 3] of 1.2.3.3 Logical Scope of the TOE.

18   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.

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

20   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.

1.2.3 TOE Scope

21   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.

1.2.3.1 Life Cycle and Environment of the TOE

The Life Cycle of the MRTD Chip and the TOE

22   [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

23　[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.
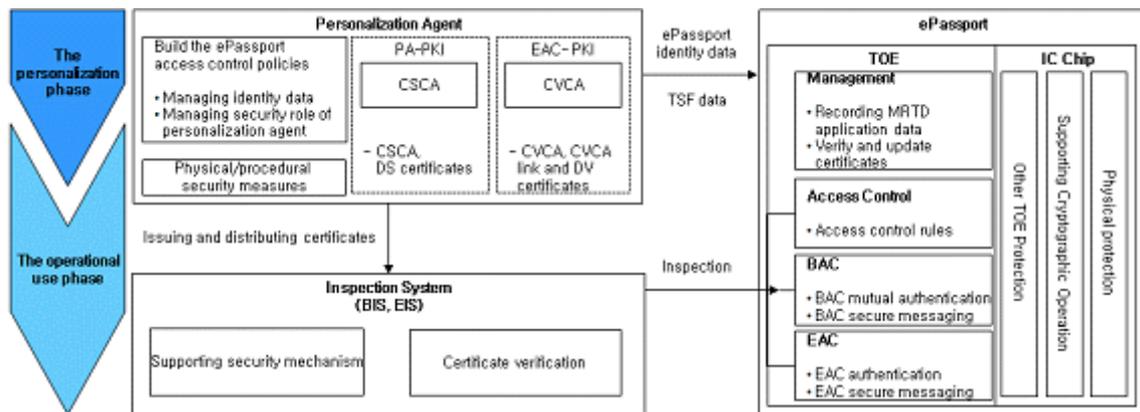
[Figure 2] TOE Operational Environment

1.2.3.2 Physical Scope of the TOE

24　[Figure 3] shows the scope of the TOE.
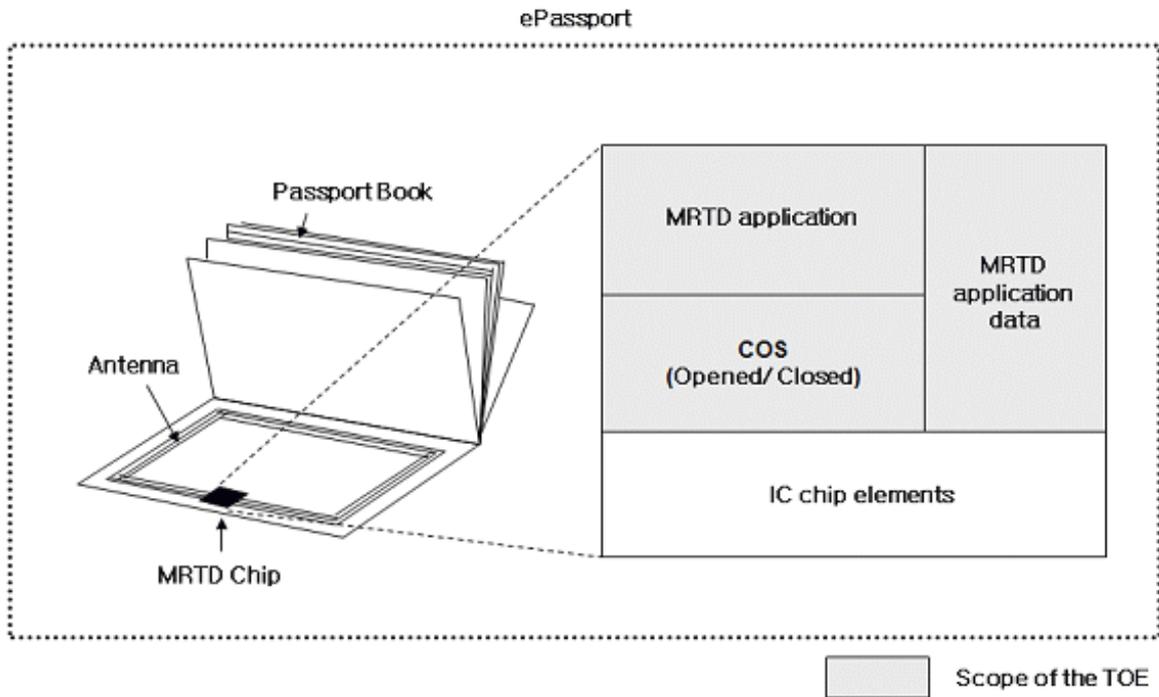
Scope of the TOE

[Figure 3] Scope of the TOE

25   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.

26   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.

27   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.

28   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.

29   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.

30   TOE may require the IC chip elements and additional hardware, software or firmware for operation. This protection profile was developed to reflect TOE that was implemented in various forms. When one ST claims this protection profile, all hardware, software or firmware which are not part of TOE but are need to perform TOE function should be described in ST.

1.2.3.3 Logical Scope of the TOE

31   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 protection, such as the TSF self-testing, preservation of a secure state, etc.

Assets

32   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.

33   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] Contents of the LDS in which the User Data are Stored

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

		Date	
		Check Digit DOE/VUD	
		Composite Check Digit	
Encoded Identification Features	DG2	Encoded face	
	DG3	Encoded finger(s)	
	DG4	Encoded Eye(s)	
Others	DG5	Displayed Portrait	
	DG6	-	
	DG7	Displayed Signature	
	DG8	-	
	DG9	-	
	DG10	-	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	-	
	DG14	EAC Chip Authentication Public Key	
	DG15	AA Digital Signature Verification Key (optional)	
	DG16	Person(s) to Notify	

1.2.4 TOE Security Characteristics

1.2.4.1 Security Mechanism

34   The TOE provides security characteristics 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 characteristics 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 >

35   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.

36   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.

37   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 >

38   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.

39   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.

40   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.

41   [Table 5] summarized the ePassport security mechanisms.

[Table 5] The ePassport Security Mechanisms

The ePassport Security Mechanisms				IT Security characteristic of the TOE
Security Mechanism	Security characteristic	cryptography	Cryptographic Key/Certificate Type	
PA	User Data Authentication	N/A	N/A	Access control to the SOD - Read-rights: BIS, EIS -Write-rights: Personalization agent
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.

		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 Key Distribution			
	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

1.2.4.2 TOE Access Control and Security Management

42 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.

43 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.

44 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.

1.2.4.3 Other TOE Protection

45 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 TSF. 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).

46 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.).

1.3 Conventions

47   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").

48   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.

Iteration

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

Selection

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

Refinement

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

Assignment

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

49   "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.

1.4 Protection Profile Organization

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

51   Section 2 provides the conformance claim that declares conformance for common criteria, protection profile, and packages, and describes rationale of conformance claim and conformance statement.

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

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

54   Section 5 defines extended components that are not based on common criteria part 2 and part 3.

55   Section 6 contains the IT security requirements including the functional and assurance requirements and rationale of security requirements intended to satisfy security objectives.

56   Section 7 describes Application Notes which deserve notice in applying the PP herein.

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

58 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.

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

2 Conformance Claim

60   Conformance claim contains common criteria, protection profile and package for this protection profile, and methods for other protection profiles and security targets to conform to this protection file.

2.1 Common Criteria Conformance Claim

61   This protection profile claims conformance to

    ・ Common Criteria for Information Technology Security Evaluation, part 1 : Introduction and general model, Version 3.1r3, July. 2009, CCMB-2009-07-001

    ・ Common Criteria for Information Technology Security Evaluation, part 2 : Security functional requirements, Version 3.1r3, July. 2009, CCMB-2009-07-002

    ・ Common Criteria for Information Technology Security Evaluation, part 3 : Security assurance requirements, Version 3.1r3, July. 2009, CCMB-2009-07-003

as follows

    ・ Part 2 Conformant

    ・ Part 3 Conformant

2.2 Protection Profile Claim

62   This protection profile doesn't claims conformance to any other Protection Profiles.

2.3 Package Claim

63   This protection profile is conforming to assurance package as follows

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

2.4 Conformance Rationale

64   Since this protection profile is not claiming conformance to any other protection profile, no rationale is necessary here.

2.5 Conformance Statement

65   This protection profile requires "demonstrable conformance of any ST or PP, which claims conformance to this PP".

3 Security Problem Definition

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

3.1 Threats

67   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.

68   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.

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

<Threats to the TOE in the Personalization phase>

T.TSF_Data_Modification

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

<BAC-related Threats in the TOE Use phase>

T.Eavesdropping

71   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_Corruption_ Personal_ Data

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

T.BAC_Authentication_Key_Disclose

73   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_Info').

T.BAC_ReplayAttack

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

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

<EAC-related Threats in the Operational Use phase>

T. Damage_to_Biometric_Data

75   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

76   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

77   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.SessionData_Reuse

78   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

79   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

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

<Other Threats in the Operational Use phase>

T.Leakage_CryptographicKey_Info

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

T.ePassport_Reproduction

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

T.Residual_Info

83   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.

3.2 Organizational Security Policies

84   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.International_Compatibility

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

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

P.Security_Mechanism_Application_Procedures

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

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

P.Application_Program_Install

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

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

P.Personalization_Agent

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

P.ePassport_Access_Control

89 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 Subjects	Security Attribute	Security Attributes	Personal data of the ePassport holder		Biometric data of the ePassport holder		ePassport Authentication data		EF.CVCA		EF.COM	
			Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	BIS	BAC Authorization	Allow	Deny	Deny	Deny	Allow	Deny	Allow	Deny	Allow	Deny
	EIS	BAC Authorization	Allow	Deny	Deny	Deny	Allow	Deny	Allow	Deny	Allow	Deny
		EAC Authorization	Allow	Deny	Allow	Deny	Allow	Deny	Allow	Deny	Allow	Deny
	Personalization Agent	Personalization Authorization	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow

P.PKI

90   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.

91   Also, The Issuing State of the ePassport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System. When the EAC-TA provides the TOE with CVCA link certificate, DV certificate and IS certificate after the Inspection System obtaining information from EF.CVCA stored in the TOE, the TOE shall internally update certificates by verifying validity of the certificates.

P.Range_RF_Communication

92   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.

3.3 Assumptions

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

A.Certificate_Verification

94   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.

95   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.Inspection_System

96   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.

97   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.IC_Chip

98   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.MRZ_Entropy

99   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.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

O.Management

102 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.Security_Mechanism_Application_Procedures

103 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.Session_Termination

104   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.

O.Secure_Messaging

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

O.Certificate_Verification

106   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.Secure_State

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

O.Deleting_Residua_Info

108   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.Replay_Prevention

109　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.Access_Control

110　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.Handling_Info_Leakage

111　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.BAC

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

O.EAC

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

4.2 Security Objectives for the Environment

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

OE.ePassport_Manufacturing_Security

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

OE.Procedures_of_ePassport_holder_Check

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

OE.Application_Program_Install

117 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

118 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.

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

OE.Personalization_Agent

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.Inspection_System

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

OE.IC_Chip

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

OE.MRZ_Entropy

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

OE.PKI

124　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.

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

OE.Range_RF_Communication

126　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.

4.3 Security Objectives Rationale

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

128　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.

129   [Table 7] shows the mapping between Security Problem Definition and Security Objectives.

[Table 7] The mapping between Security Problem Definition and Security Objectives

Security Problem Definition \ Security Objectives	TOE Security Objective												Security Objective for Environment									
	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_Residua_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.BAC	O.EAC	OE.ePassport_Manufacturing_Security	OE.Procedures_of_ePassport_Holder_Check	OE.Application_Program_Install	OE.Certificate_Verification	OE.Personalization_Agent	OE.Inspection_System	OE.IC_Chip	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Communication
T.TSF_Data_ Modification	×		×						×								×					
T.Eavesdropping				×														×				
T. Forgery_Corruption_Personal Data			×						×		×							×				
T.BAC_Authentication_Key_Disclose	×		×			×			×							×						
T.BAC_ReplayAttack								×														
T.Damage_to_Biometric_Data			×	×	×				×			×				×		×			×	
T. EAC-CA_Bypass		×														×	×	×				
T. IS_Certificate_Forgery	×				×												×					
T. SessionData_Reuse								×										×				
T. Skimming									×		×	×						×				×
T.Malfunction						×													×			
T.Leakage_CryptographicKey_Info										×												
T. ePassport_Reproduction													×	×								
T.Residual_Info							×															
P.International_Compatibility																	×					
P.Security_Mechanism_Application_Procedures		×															×					
P.Application_Program_Install															×							
P.Personalization_Agent	×																×					
P.ePassport_Access_Control	×								×		×	×					×	×				
P. PKI				×																	×	

-42-

P.Range_RF_Communication																		×
A.Certificate_Verification												×	×				X	
A.Inspection System														×				
A.IC_Chip															×			
A.MRZ_Entropy																×		

4.3.1 Security Objective Rationale for the TOE

O.Management

130   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.

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

O.Security_Mechanism_Application_Procedures

132   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.

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

O.Session_Termination.

134   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_Corruption_Personal Data, T.Damage_to_Biometric_Data, T.BAC_Authentication_Key_Disclose and T.TSF_Data_Modification.

O.Secure_Messaging

135 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.

O.Certificate_Verification

136 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.

137 This security objective is required to counter the threats of T.Damage_to_Biometric_Data and T.IS_Certificate_Forgery by determining the status of forgery as the TOE verifies validity of the CVCA link certificate, DV certificate and IS certificate in the EAC-TA.

O.Secure_State

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

O.Deleting_Residua_Info

139 This security objective is required to counter the threat of T.Residual_Infoby 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.

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

O.Replay_Prevention

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

O.Access_Control

142 This security objective is required to counter the threats of T. Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data and T.Skimming and enforce the organizational security 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.

143   This security objective is required to counter the threats of T.TSF_Data_Modification and T.BAC_Authentication_Key_Disclose as it allows the authorized personalization agent has the write-rights of the MRTD application data in the Personalization phase and denies the access by Personalization agent in the Operational Use phase.

O.Handling_Info_Leakage

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

O.BAC

145   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.

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

the BAC mutual authentication and denies access by the Inspection System that does not have the read-rights.

O.EAC

147　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.

148　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.

4.3.2 Security Objective Rationale for Operating Environment

OE.ePassport_Manufacturing_Security

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

OE.Procedures_of_ePassport_Holder_Check

150 This security objective for environment is required to counter the threats of T.ePassport_Reproduction, T.BAC_Authentication_Key_Disclose and T.EAC-CA_Bypass by implementing procedural security measures in immigration process, such as procedures to check the printed identify information page of the ePassport and to determine the forgery status of the ePassport book, etc.

OE.Application_Program_Install

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

OE.Certificate_Verification

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

T.IS_Certificate_Forgery and support the assumption of A.Certificate_Verification.

OE.Personalization_Agent

153   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.

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

OE.Inspection_System

155   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.

156 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.

157 This security objective for environment is required to counter the threats of T. Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data, T.Skimming and T.EAC-CA_Bypass as the Inspection System supports the BAC mutual authentication, EAC and PA.

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

OE.IC_Chip

159 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.

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

OE.MRZ_Entropy

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

OE.PKI

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

OE.Range_RF_Communication

163   This security objective for environment is required to counter the threat of T.Skimming and enforce the organizational security policies of P.Range_RF_Communication by ensuring that RF communication distance between the MRTD chip and the Inspection System is less than

5cm and that RF communication channel is not established if the page of the ePassport attached with the IC chip is not opened.

5 Definition of Extended Component

164　This protection profile does not define extended component.

6 Security Requirements

165 Security requirements specify security functional and assurance requirements that must be satisfied by the TOE that claims this Protection Profile.

166 In this Protection Profile, the external entities specified in security requirements include Personalization agent, BIS, EIS, ePassport IC chip.

167 This Protection Profile defines all subjects, objects, operation, security attributes employed in security requirements as [Table 8]. Also, it defines SSC(Send Sequence Counter) with session security attributes related to establishing secure messaging.

[Table 8] Definition of Subject, Object, related Security Attributes and Operation

Subject	Subject Security Attributes	Object		Object Security Attributes		Operation
			Security attributes			- Read
		Objects	Security attributes of object's operation	Security attributes of object's access-rights		- Write
		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		

Inner subject table:

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

168   ST author should precisely define subjects, objects, operation, security attributes, external entities when they are not explicitly explained in this Protection Profile.

6.1 Security Functional Requirements

169   The security functional requirements for this Protection Profile consist of the following components from Part2 of the CC in order to satisfy security

requirements identified in chapter 4, summarized in the following [Table 9].

[Table 9] 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_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes

(FMT)	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Info.)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialization)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy (FPR)	FPR_UNO.1	Unobservability
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_TST.1	TSF testing

6.1.1 Cryptographic Support

FCS_CKM.1 Cryptographic key generation(Key Derivation Mechanism)

Hierarchical to : No other components.

Dependencies : [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

170 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

171   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

172 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]

173 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 list of standard 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

174   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 cannot implement this requirement, this requirement can be supported in the TOE environment (the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip).

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

175   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 cannot implement this requirement, this requirement can

be supported in the TOE environment (the co-processor of the certified

IC chip or cryptographic libraries loaded in the certified IC chip).

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

176   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 cannot implement this requirement, this requirement can be supported in the TOE environment (the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip).

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

177   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 10] so that to respond to   attackers possessing moderate attack potential required by AVA_VAN.4. However, in case the TOE cannot implement this requirement, this requirement can be supported in the TOE environment (the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip).

[Table 10] 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

6.1.2 User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to : No other components.

Dependencies : FDP_ACF.1 Security attribute based access control

178 FDP_ACC.1.1 The TSF shall enforce 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) 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

179   FDP_ACF.1.1 The TSF shall enforce the [ePassport access control

policy] to objects based on the following: [[Table 11], [Table 12],

[assignment : *security attributes relevant to additional assigned lists of objects, subjects and operations in FDP_ACC.1*]].

[Table 11] Subject-relevant Security Attributes

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

[Table 12] 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.

-66-

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.

180   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.

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

182   FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

   a) Explicitly deny access of subjects to objects if instructions order of the inspection system is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specifications

   b Explicitly deny read of subjects to biometric data if there is no the read-rights of biometric data in IS certificate of the EIS that has the EAC authorization

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

   d) [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.

183 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]

184 FDP_UCT.1.1 The TSF shall enforce the [ePassport access control policy] to *transmit, receive* **object** 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]

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

186 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.

6.1.3 Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components.

Dependencies : FIA_UAU.1 Timing of authentication

187   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*]

].

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

<u>Application Notes</u> : 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

189   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.

190 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)**

191 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.

192 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.

193 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.

194   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.

195   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.

196 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.

197 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.

6.1.4 Security Management

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

198 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

199 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

200 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.

201   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

202   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

203 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 : FMT_MTD.1 Management of TSF data

204 FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [assignment : _list of TSF data_].

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

FMT_SMF.1 Specification of Management Functions
Hierarchical to : No other components.
Dependencies : No dependencies.

205 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

206   FMT_SMR.1.1 The TSF shall maintain the roles [

a) Personalization agent

b) [assignment : *other roles*].

207   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.

6.1.5 Privacy

FPR_UNO.1 Unobservability

Hierarchical to : No other components.

Dependencies : No dependencies.

208 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 measures to handle attacks, such as DPA and SPA,.etc do not be implemented completely by TOE, it can be provided from TOE environment(the certified IC chip or cryptographic libraries loaded in the certified IC chip).

6.1.6 TSF Protection

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to : No other components.
Dependencies : No dependencies.

209   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.

210   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].

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

] if modifications are detected.

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

FPT_TST.1 TSF testing
Hierarchical to : No other components.
Dependencies : No dependencies

212 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 authorized 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*].

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

214 FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].

6.2 Security Assurance Requirements

215 The security assurance requirements for this Protection Profile consist of the following components from Part 3 of the CC, summarized in the

following [Table 13] and evaluation assurance level is EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VAN.4).

216 The assurance components are augmented follows:

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

[Table 13] Security Assurance Requirements

Assurance class	Assurance component	
Security target evaluation	ASE_INT.1	ST Introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedure

	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: Security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability analysis	AVA_VAN.4	Methodical vulnerability analysis

6.2.1 Security target

ASE_INT.1 ST Introduction

Dependencies : No dependencies.

Developer action elements :

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

Content and presentation elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

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

ASE_CCL.1 Conformance claim
Dependencies : ASE_INT.1 ST Introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements :

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

Evaluator action elements:

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

ASE_SPD.1 Security problem definition
Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

242 ASE_SPD.1.1C The security problem definition shall describe the threats.
243 ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.
244 ASE_SPD.1.3C The security problem definition shall describe the OSPs.
245 ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

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

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

Evaluator action elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

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

ASE_REQ.2 Derived security requirements
Dependencies : ASE_OBJ.2 Security objectives
                      ASE_ECD.1 Extended components definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

270 ASE_REQ.2.4C All operations shall be performed correctly.

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

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

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

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

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

Evaluator action elements:

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

ASE_TSS.1 TOE summary specification
Dependencies : ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

6.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies : ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

ADV_FSP.4 Complete functional specification
Dependencies: ADV_TDS.1 Basic design

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

Evaluator action elements:

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

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

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

Dependencies: ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

ALC_CMC.5 Advanced support

Developer action elements:

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

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

Content and presentation elements:

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

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

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

Evaluator action elements:

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

ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

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

315   ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces,

interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

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

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

Evaluator action elements:

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

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

6.2.3 Guidance Documents

AGD_OPE.1 Operational user guidance
Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

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

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

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

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

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

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

Evaluator action elements:

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

AGD_PRE.1 Preparative procedures
Dependencies: No dependencies.
Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

6.2.4 Life-cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies : ALC_CMS.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

ALC_LCD.1 Developer defined life-cycle model

Objectives

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

Evaluator action elements:

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

ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

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

Evaluator action elements:

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

ALC_DEL.1 Delivery procedures
Dependencies: No dependencies.
Developer action elements:

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

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

Content and presentation elements:

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

Evaluator action elements:

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

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

360   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:

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

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

Content and presentation elements:

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

364   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:

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

ALC_TAT.1 Well-defined development tools
Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

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

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

Content and presentation elements:

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

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

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

Evaluator action elements:

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

6.2.5 Testing

ATE_COV.2 Analysis of coverage
Dependencies : ADV_FSP.2 Security-enforcing functional specification
                    ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

ATE_DPT.2 Testing: Security enforcing modules
Dependencies : ADV_ARC.1 Security architecture description
                ADV_TDS.3 Basic modular design
                ATE_FUN.1 Functional testing
Developer action elements:

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

Content and presentation elements:

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

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

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

Evaluator action elements:

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

ATE_FUN.1 Functional testing
Dependencies: ATE_COV.1 Evidence of coverage
Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

390   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:

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

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

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

6.2.6 Vulnerability analysis

AVA_VAN.4 Methodical vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.4 Complete functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_DPT.1 Testing: basic design

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

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

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

6.3 Security Requirements Rationale

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

6.3.1 Security Functional Requirements Rationale

401   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.

402   [Table 14] presents the mapping between the security objectives and the security functional requirements.

[Table 14] Summary of Mappings between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	TOE Security Objectives											
	O.Management	O.Security_Mechanism_Application_Procedures	O.Session Termination	O.Secure_Messaging	O.Certificate Verification	O.Secure State	O.Deleting_Residua_Info	O.Replay Prevention	O.Access_Control	O.Handling_Info_Leakage	O.BAC	O.EAC
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_TST.1						X						

FCS_CKM.1 Cryptographic key generation (Key Derivation Mechanism)

403 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)

404 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).

405   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)

406   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).

407   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

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

409   This   component   satisfies   the   security   objective   of O.Deleting_Residua_Info 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)

410 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.

411 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.

412 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)

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

414 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.

415 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)

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

417 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)

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

419 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

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

421 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

422 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.

423 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.

424 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.

425 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

426 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.

427 This component satisfies the security objective of O.Deleting_Residua_Info as it ensures that previous information of the BAC authentication key, BAC session key and EAC session key is not available when destroying these keys according to the method of destruction defined in FCS_CKM.4. Also, this component satisfies the security objective of O.Replay_Prevention by ensuring that previous information of random numbers used for the BAC mutual authentication, TAC-TA and generation of session key is not available.

FDP_UCT.1 Basic data exchange confidentiality

428 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.

429 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.

430 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

431   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.

432   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.

433   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

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

435   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.

436 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)

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

438 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)

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

440 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

441 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.

442 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

443 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.

444 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

445   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.

446   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 behavior

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

448   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

449   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.

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

FMT_MSA.3 Static attribute Initialization

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

452   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.)

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

454   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)

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

456   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

457   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.

458   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.

459   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

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

461 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.

462 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

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

464 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

465 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.

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

FPT_FLS.1 Failure with preservation of secure state

467 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.

468 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 TSF 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

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

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

FPT_TST.1 TSF testing

471   This component requires self-testing to detect loss of the TSF 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. 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 stored in the TOE, therefore detecting loss of the TSF data.

6.3.2 Security Assurance Requirements Rationale

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

474   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.

475   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.

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

477   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.

478   The TOE is developed by using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to design and operation of the TOE. Also, TOE is easily accessed as it is used in open environment and it is difficult to trace an attack. However, since the IC chip is not included in the scope of the TOE, it does not require understanding on hardware structure and advanced specialized equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing

moderate attack potential. EAL4 includes AVA_VLA.3 that resistant the enhanced-basic attack potential. Therefore, AVA_VLA.4 is augmented to require execution of 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.

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

6.3.3 Rationale of Dependency

6.3.3.1 Dependency of TOE Security Functional Requirements

480   [Table 15] shows dependency of TOE functional components

[Table 15] 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	2, 3 4
2	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 4

3	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 4
4	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	1
5	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
6	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
7	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
8	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 4
9	FDP_ACC.1	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	21
		FMT_SMR.1	27
23	FMT_MTD.1(1)	FMT_SMF.1	26
		FMT_SMR.1	27
24	FMT_MTD.1(2)	FMT_SMF.1	26
		FMT_SMR.1	27
25	FMT_MTD.3	FMT_MTD.1	23
26	FMT_SMF.1	-	-
27	FMT_SMR.1	FIA_UID.1	19
28	FPR_UNO.1	-	-
29	FPT_FLS.1	-	-
30	FPT_ITI.1	-	-
31	FPT_TST.1	-	-

481   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 included. FDP_UCT.1 and FDP_UIT.1 require secure messaging between the Inspection System and the TOE. Since the secure messaging between Inspection System and TOE is the unique channel, it is not necessary to be logically separated from other communicational channels. Therefore, in this protection profile, requirements of FTP_ITC.1 are not defined.

482   FIA_UAU.1(2) shall have dependency with FIA_UID.1, but the dependency   changed to FIA_UAU.1(1) by refinement operation. Since the EAC-TA is executed after the BAC mutual authentication, FIA_UAU.1(2) depends on FIA_UAU.1(1) and FIA_UAU.1(1) depends on FIA_UID.1. Therefore, indirectly, the dependency is satisfied.

6.3.3.2 Dependency of TOE Security Assurance Requirements

483   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 16].

484   ADV_IMP.2 shall have dependency with ALC_CMC.5 but, ADV_IMP.2 is augmented to enable analysis on the entire implementation representation in order to check if the TSF is accurately implemented and defect code does not exist. And ADV_IMP.2 is not augmented in this protection file because CM at ALC_CMC.5 level which provides automated measure to identify if the changes in configuration items affect other configuration items is determined to be not necessarily required.

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

[Table 16] Dependency of the Augmented Assurance Components

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

		ADV_IMP.1	1
		AGD_OPE.1	EAL4
		AGD_PRE.1	EAL4
		ATE_DPT.1	2

6.3.4 Rationale of Mutual Support and Internal Consistency

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

487   In '6.3.3.1 Dependency of TOE security functional requirements' and '6.3.3.2 Dependency of TOE security assurance requirements', the dependency is analyzed as a supportive relationship among security requirements of which it is necessary to depend on other security requirements in order to achieve a security objective because a security requirement is insufficient. In case the dependency was not satisfied, additional rationale is provided.

488   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.

489   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).

490 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.

491 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.

492 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.

493 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.

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

7 Protection Profile Application Notes

495 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 ST author shall define additional security problem definition, security objectives and security requirements.

496 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.

497 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 problem definiton, security objectives and security requirements.

498 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 overview, security problem definition, security objectives and security requirements by considering these details.

8 Terms and Definitions

499   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

REFERENCE

[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 1.11, TR-03110, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2008. 2

[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 3.1r3, CCMB, 2009. 7

[6] Common Methodology for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7

[7] Smart Card Open Platform Protection Profile V2.1, IT Security Certification Center, 2010.6

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

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

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

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

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

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

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

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

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

[17] ISO/IEC 18033-3:2005, Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers

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

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

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

[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 Verifying 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
SPA	Simple Power Analysis
SSC	Send Sequence Counter
ST	Security Target
TA	Terminal Authentication
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functionality