KOMSCO

Security Target Lite

KCOS e-Passport Version 2.1

S3CT9KW/KC/K9

Version: 1.0

Date: 2013. 01. 17

Filename: EPS-03-AN-ST (Lite-EN)

KOMSCO

Technology Research Institute

IT Research Center

This page left blank on purpose for double-side printing

[Table of Contents]

[List of Tables]

[List of Figures]

1. Introduction

This document is the Security Target (ST) to describe KCOS e-Passport Version 2.1 S3CT9KW/KC/K9 developed by the Korea Minting & Security Printing Corporation (KOMSCO). This chapter identifies the Security Target and TOE and supports the Security Target overview, Common Criteria conformance and other areas.

1.1 ST Reference

- Title: KCOS e-Passport Version 2.1 S3CT9KW/KC/K9 Security Target Lite V1.0 (EPS-03-AN-ST(lite)-1.0)
- ST Version Number : V1.0
- Author: IT Research Center, Technology Research Institute, KOMSCO
- Applicant: Korea Minting & Security Printing Corporation
- Evaluation Criteria: Common Criteria for Information Security Evaluation (Ministry of Public Administration and Security Public Notice No. 2009-52)
- Common Criteria Version: V3.1r3
- Compliant to: ePassport Protection Profile V2.1 (KECS-PP-0163a-2009)
- Evaluation Assurance Level: EAL5+ (ALC_DVS.2, ADV_IMP.2, AVA_VAN.5)
- Keywords: ePassport, COS, MRTD, ICAO, SAC, EAC, BAC

1.2 TOE Reference

- TOE name : KCOS e-Passport Version 2.1 S3CT9KW/KC/K9

  - K2.1.02.01.SS.1420.02(S3CT9KW)
  - K2.1.02.01.SS.140C.02(S3CT9KC)
  - K2.1.02.01.SS.1409.02(S3CT9K9)
    - · K2.1 : KCOS e-Passport Version 2.1

- 02 : Release number (2nd Masking)
- 01 : Patch version (1st Patch)
- SS.140C.02 : IC chip identifier (Samsung S3CT9KC Revision 2)

- TOE Version : Version 2.1

- TOE Components

  - IC chips : S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software (ANSSI-CC-2012/70)
  - Embedded software : KCOS e-Passport Version 2.1
  - Guidance : EPS-03-QT-OPE-1.3(Operational User Guidance), EPS-03-QT-PRE-1.3(Preparative Procedures Guidance)

1.3 TOE Overview

The TOE is the native chip operation system (COS), MRTD application and MRTD application data implemented on the IC chip and additionally includes S3CT9KW/KC/K9 revision 2, which is a contactless IC Chip of Samsung Electronics and is certified according to CC EAL 5+(ANSSI-CC-2012/70). The MRTD application of the TOE follows ICAO document (ICAO, Machine Readable Travel Documents, Doc 9303 Part1 Volume 2[1]), SAC Specification (ICAO, Supplemental Access Control for Machine Readable Travel Documents V1.01 (2010.11.11)) and EAC Specification (BSI, Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.11 (2008.02)).

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

The TOE uses generation of random numbers. TDES, AES, Retail MAC, CMAC, RSA and ECC supported by the MRTD chip. And the TOE can use RSA or ECC operations but the Personalization Agent has to select one cryptographic algorithm needed for EAC operation

Since The TOE is a composite evaluation product, it includes IC chip, COS, application

programs, and etc. There is no non-TOE HW/FW/SW requested to perform TOE security attributes. Note, the RF antenna and the booklet are needed to represent a complete MRTD to ePassport holder, nevertheless these parts are not inevitable for the secure operation of the TOE.

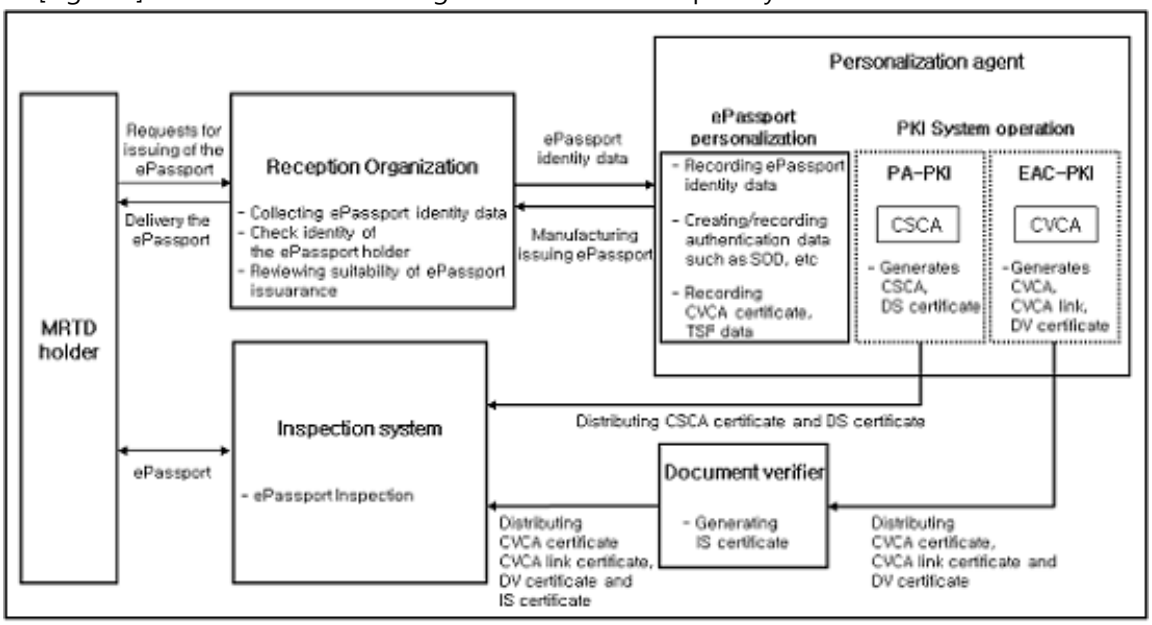
1.3.1 TOE Type

ePassport

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

1.3.2 ePassport System

The [Figure1] shows the overall configuration of the ePassport system.



[Figure 1] Overall Configuration of ePassport System

The ePassport holder requests an issue of the ePassport and receives the ePassport issued according to the Issuing Policy of the ePassport. The ePassport holder presents the ePassport to an immigration officer so that the ePassport can be inspected at immigration

control. For immigration control, the ePassport is verified by an immigration officer or by an automatic Inspection System according to the ePassport immigration control policy for each country.

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

The Personalization agent generates a Document Security Object (''SOD'' hereinafter) using a digital signature on the user data (identity and authentication data) and records it in the MRTD chip with the ePassport identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the Personalization Agent manufactures and issues the ePassport-embedded MRTD chip to the passport. Details of data recorded in the ePassport are described in (Table 6) of 1.4.2.2 Logical Scope of TOE.

The Personalization agent generates a digital signature key to check against forgery and corruption of the user data stored in the MRTD chip. Then, in accordance with the Certification Practice Statement (CPS) of the ePassport PKI System, the Personalization Agent generates, issues, and manages the CSCA Certificate and DS Certificate. According to the Issuing Policy of the ePassport, the Personalization agent generates a digital signature key to verify access-rights to the biometric data of the ePassport holder to support the EAC security mechanism. The Personalization agent then generates, issues, and manages the CVCA Certificate, CVCA Link Certificate and the DV Certificate. Details related to of the ePassport PKI System and certification procedure, including the certification server, key generation devices and the physical and procedural security measures depend on the Issuing Policy of the ePassport.

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

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

(Table 1) Type of Certificates

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

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

1.4 TOE Description

1.4.1 Life Cycle and Environment of TOE

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

ePassport IC chip and Life Cycle of the TOE

The ePassport IC chip is S3CT9KW/KC/K9 revision 2 which is a contactless IC chip product of Samsung Electronics and is certified according to CC EAL 5+(ANSSI-CC-2012/70). The IC chip consists CPU, memory, peripheral unit, crypto-operation S/W library and etc, as follows :

(Table 2) Components of IC chip

components	Details
CPU	· 16bit microprocessor
Memory	· ROM : 384Kbytes · EEPROM : 144Kbytes(KW), 80Kbytes(KC), 36Kbytes(K9) · RAM : 6Kbytes · CRYPTO RAM : 2.5Kbytes
Peripheral unit	· TDES operator, AES operator, · RSA/ECC operator TORNADO 2Mx2 · 16bits random number generator · Abnormal condition detectors · Memory protection unit · 16bits Timer and 20bits watchdog timer · ISO7816 contact interface, ISO14443 contactless interface
S/W library	· ECC library v2.2 : 192bits ~ 512bits

components	Details
	· RSA library v2.2 : 1280bits ~ 2048bits · TRNG random number generator v2.0

Application Notes: The TOE only supports Type B contactless interface.

The TOE includes as following cryptographic algorithms.

(Table 3) Cryptographic Algorithms of TOE

Components	Cryptographic operation	Evaluation scope of IC chip	Evaluation scope of TOE
TDES module	· TDES-based Encryption/Decryption operations · Retail MAC generation/verification operation	112, 168bits	112bits
AES module	· AES-based Encryption/Decryption operations · CMAC generation/verification operation	128, 192, 256bits	128, 192, 256bits
RSA/ECC library	· Key distribution operation for EAC/SAC session key distribution · Digital signature verification operation for EAC certificates · Hash operation using SHA algorithm · Digital signature generation operation for chip authentication private key in AA	[ECC] 192 ~ 512bits [RSA] 1280 ~ 2048bits [SHA] 224, 256, 384, 512bits	[ECC] 192 ~ 512bits [RSA] 1280 ~ 2048bits [SHA] 160, 224, 256, 384, 512bits

Application Notes: The TOE uses higher than 224bits SHA algorithms supported by IC chip and includes 160bits SHA algorithm implemented in KCOS by itself

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

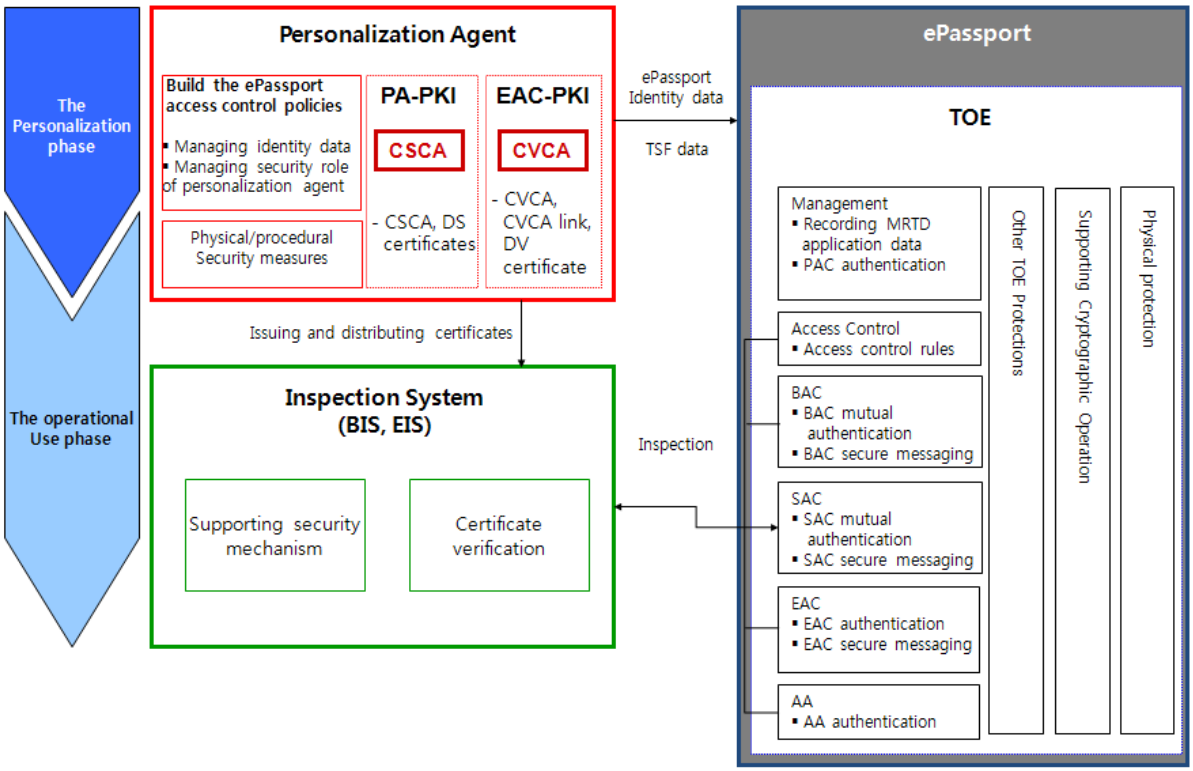
(Table 4) Life Cycle of TOE

Phase	Life Cycle of 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

Phase	Life Cycle of TOE
	the IC chip and the Dedicated S/W. ③ Delivery to IC chip manufacturer the ROM code including the initial PAC authentication key.
Phase 2 (Manufacturing)	④ The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier and to produce the IC chip. ⑤ The ePassport manufacturer to embed the IC chip in the passport book by requesting the Personalization agent.
Phase 3 (Personalization)	⑥ The Personalization agent to operate the functions of the PAC authentication key update and patch. ⑦ The Personalization agent to create a user data storage space according to the LDS format or the ICAO document and to record it in EEPROM. ⑧ The Personalization agent to create a SOD using a digital signature on the ePassport identity data. ⑨ The Personalization agent to record the ePassport identity data, the authentication data (including SOD) and the TSF data (The TOE itself creates the BAC authentication key using the command of the Personalization Agent) in the TOE. ⑩ The Personalization agent to verify the normal operation. ⑪ Issue, discard or re-personalization according to the verifying result.
Phase 4 (Operational Use)	⑫ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE.

TOE Operational Environment

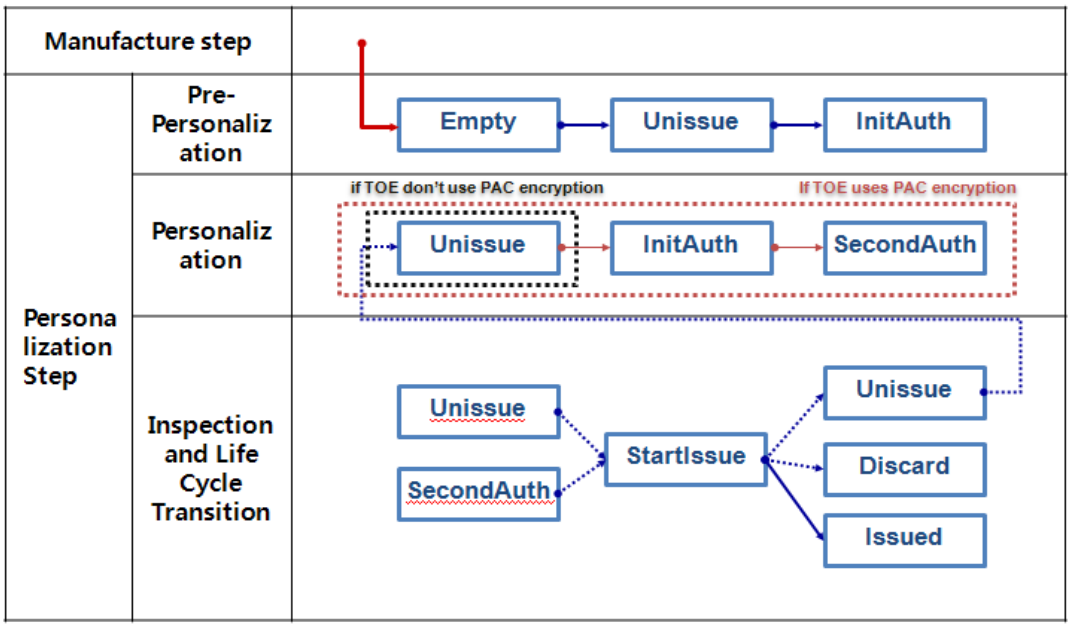
[Figure 2] shows the operational environment of the TOE in the phases of the ePassport Personalization and Operational Use through the relationship with major security functions of the TOE and external entities (the Personalization agent, the Inspection System) that interact with the TOE.



[Figure 2] TOE Operational Environment

TOE Personalization Phase

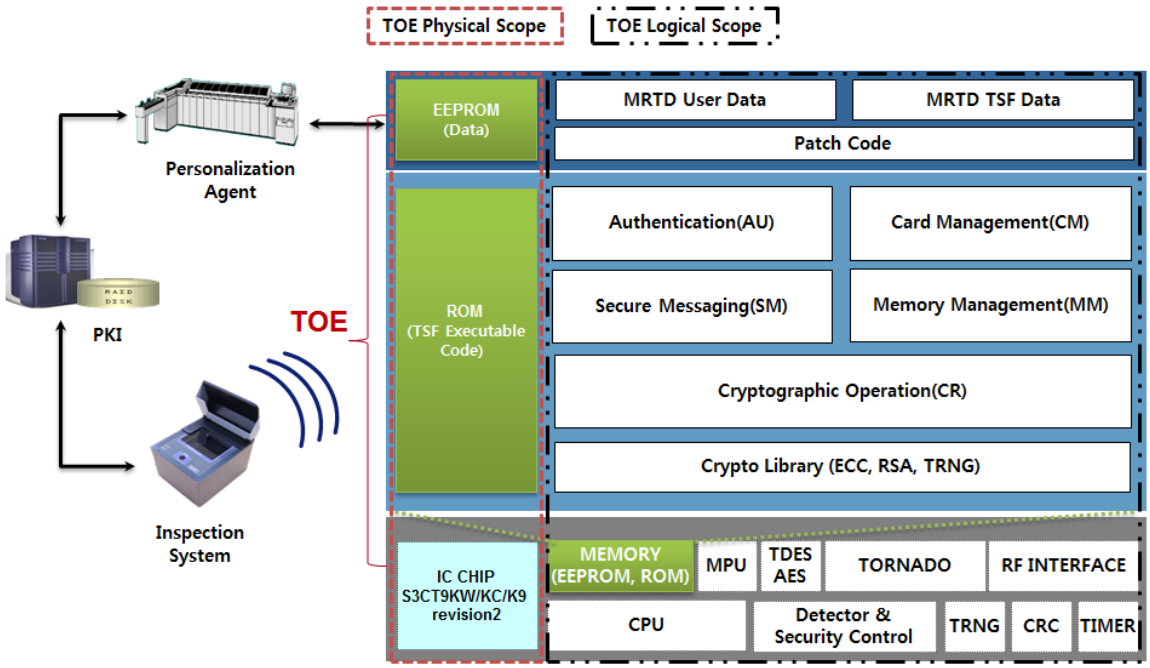
The TOE manages eight statuses as operational modes for secure personalization and management. The personalization phase is divided into pre-personalization, personalization, verification and the operational mode transition.



[Figure 3] Life Cycle Transition according to Personalization

1.4.2 TOE Scope

[Figure 4] shows the physical and logical scope of the TOE.



[Figure 4] Scope of TOE

1.4.2.1 Physical Scope of TOE

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

In the ST, the TOE is defined with IC chip, chip operating system (COS), MRTD application and MRTD application data and etc. The IC chip consists CPU, memory(RAM, ROM, EEPOM), MPU(memory Protection unit), IC chip security features, crypto co-processor, TRNG, timer, RF interface, cryptographic library, HASH function and etc. Additionally, The IC chip supports the contact and contactless(Type A/B) interfaces but the TOE only uses the contactless interface Type B.

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

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

format defined in the ICAO document in addition to the security mechanism to protect the function securely. In addition, the MRTD application is added to the EAC security mechanism by the EAC specifications, as the biometric data of the ePassport holder is included in the ePassport identity data. The MRTD chip application also includes the PAC security mechanism, which is the security mechanism of KCOS for ePassport personalization. The MRTD chip application is stored in the ROM of the MRTD IC chip.

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

The TOE and TOE components are identified in (Table 5).

(Table 5) Identifier of TOE and TOE Components

Type		Identifier	Explanation
TOE	HW+SW	KCOS e-Passport Version 2.1 S3CT9KW/KC/K9	IC Chip + COS + MRTD Application
TOE Components	HW	Samsung S3CT9KW/S3CT9KC/ S3CT9K9	Revision 2
	SW	KCOS e-Passport Version 2.1	
	DOC	Operational User Guidance : EPS-03-QT-OPE-1.3	
		Preparative Procedures Guidance : EPS-03-QT-PRE-1.3	

1.4.2.2 Logical Scope of TOE

The TOE communicates with the Inspection System and Personalization agent according to the transmission protocol defined in ISO/IEC 14443-4. The TOE implements the PAC security mechanism and the security mechanism defined in the ICAO document, EAC specification and SAC specification. It also provides access control and security management functions. In addition, the TOE provides functions of TSF self-protection, such as TSF self-testing, preservation of a secure state.

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

Assets

In order to protect the TOE assets shown in (Table 6), the TOE provides security functions such as the confidentiality, the integrity, the authentication and the access control.

(Table 6) TOE Assets

Category			Description	Storage Space
User Data	ePassport Identity Data	Personal Data of the ePassport holder	EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16	EF File
		Biometric Data of the ePassport holder	EF.DG3, EF.DG4	
	ePassport Authentication Data		EF.SOD, EF.DG14 (EAC chip authentication public key), EF.DG15 (AA public key)	
	EF.CVCA		In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System	
	EF.COM		LDS version info., tag list of DG used, etc.	
TSF Data	EAC Chip Authentication Private Key		In EAC-CA, Chip Private key used by the TOE to demonstrate a non-forged MRTD chip	Secure memory
	CVCA Certificate		In personalization phase, Root CA Certificate issued in EAC-PKI	
	CVCA Digital Signature Verification Key		After the personalization phase, CVCA Certificate Public key is newly created by a certificate update	
	Current Date		In the personalization phase, the date of issue of the ePassport is recorded. However, in the operational use phase, the TOE internally updates it as the latest date among the issuing dates of the CVCA Link Certificate, the DV Certificate or the Issuing State IS Certificate.	
	BAC Authentication Key		BAC authentication encryption key BAC authentication MAC key	
	SAC Authentication Key		SAC authentication key, CAN	
	AA Private Key		Private key of the chip used by the TOE to prove that the chip is not substituted	

Category		Description	Storage Space
	PAC Authentication Key	Symmetric key for PAC mutual authentication and PAC personalization management authentication	
	TSF execute Code for patching	Additional Execute code for improving function	
	TSF integrity verification key	MAC key for making integrity value TSF	
	Other TSF Data	TOE Operational Data, etc.	
	BAC Session Key	BAC session encryption key BAC session MAC key	Temporary memory
	SAC Session Key	SAC session encryption key SAC session MAC key	
	EAC Session Key	EAC session encryption key EAC session MAC key	
	PAC Session Key	PAC session encryption key PAC session MAC key	

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

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

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

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

personalization phase. When the CVCA digital signature verification key is updated, the TOE overwrites at the existing CVCA digital signature verification key.

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

The LDS in which the user data are stored defines the MF, DF and EF file structure. (Table 7) shows the content of EF.DG1~EF.DG16, in which parts of the user data is stored.

(Table 7) LDS Content of User Data

Category	DG	Contents
Detail(s) in MRZ	DG1	Document (Passport) Type
		Issuing State
		Name (of Holder)
		Document Number
		Check Digit (of Doc Number)
		Nationality
		Date of Birth
		Check Digit (of DOB)
		Sex
		Data of Expiry of Valid Until Date
		Check Digit (of DOE/VUD)
		Composite Check Digit
Biometric Data	DG2	Encoded face info.
Biometric Data	DG3	Encoded fingerprint info.
ePassport authentication information	DG5	Photo image
	DG7	Signature image
	DG11	Personalization additional information
	DG12	ePassport additional information
	DG14	EAC Chip Authentication Public Key
	DG15	AA Digital Signature Verification Key

Category	DG	Contents
	DG16	Person(s) to Notify
	EF.CARDACCESS	SAC info
	EF.COM	LDS version info., tag list of DG used, etc.
	EF.SOD	Document of security
	EF.CVCA	In EAC-TA, CVCA digital signature verification key identifier list

Security Mechanisms

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

(Table 8) shows the security mechanisms of TOE.

(Table 8) TOE Security Mechanisms

Security mechanisms			
Mechanism	**Function**	**Cryptographic algorithms**	**Key / Certificate**
AA	Genuineness of IC Chip	RSASSA SHA-256	RSA Digital Signature Key
SAC	SAC Mutual Authentication	AES-CBC TDES-CBC CMAC Retail MAC	SAC Authentication / Session Key
	SAC Key Distribution	ECDH Key Agreement Protocol SHA-1 SHA-256	SAC Session Key (Encryption and MAC Keys)
	SAC Secure Messaging	Secure Messaging	SAC Session key (Encryption and MAC Keys)
BAC	BAC Mutual Authentication	Symmetric Key-based Authentication Protocol TDES-CBC SHA-1 Retail MAC	BAC Authentication Key (Encryption and MAC Keys)
	BAC Key Distribution	Symmetric Key-based Distribution Protocol TDES-CBC SHA-1 Retail MAC	BAC Session Key (Encryption and MAC Keys)

	BAC Secure Messaging	Secure Messaging	BAC Session Key (Encryption and MAC Keys)
EAC	EAC-CA	DH Key Distribution Protocol SHA-1	EAC-CA Public Key EAC-CA Private Key
		ECDH Key Distribution Protocol SHA-1	EAC-CA Public Key EAC-CA Private Key
	EAC Secure Messaging	Secure Messaging	EAC Session Key (Encryption and MAC Keys)
	EAC-TA	RSASSA SHA-256	CVCA, CVCA Link, DV, IS Certificates
		ECDSA SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	CVCA, CVCA Link, DV, IS Certificates
PAC	PAC Mutual Authentication	TDES-CBC Retail MAC	PAC Authentication Keys (K1, K2, K7)
	PAC Personalization Management Authentication		PAC Authentication Keys (K3, K4, K5, K6)
	PAC Key Distribution		PAC Encryption Session Key PAC MAC Session Key
	PAC Secure Messaging		

< PAC (Personalization Access Control) >

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

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

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

key-based key distribution protocol.

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

< SAC (Supplemental Access Control) >

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

If the TOE generates the random number and domain parameters and then transmits them into the Inspection System, then the Inspection System and TOE generate the shared key using anonymous ECDH key distribution algorithm based on the ephemeral domain parameters. The session key is generated from the shared key to the secure messaging. And the authentication token is then generated and verified it after exchanging mutually. The session is ended in case of a mutual authentication failure.

After checking the read-rights of the Inspection System for the personal data of the ePassport holder, the TOE, to secure transmission of the personal data of the ePassport holder through the SAC mutual authentication, establishes SAC secure messaging through encryption of the SAC session key shared by the SAC key distribution and the MAC generated.

< BAC (Basic Access Control) >

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

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

The TOE, to secure transmission of the personal data of the ePassport holder after checking the read-rights of the Inspection System for the personal data of the ePassport holder through

the BAC mutual authentication, establishes BAC secure messaging through encryption of the BAC session key shared by the BAC key distribution and the MAC generated.

< AA (Active Authentication) >

The AA security mechanism is implemented to prove the authenticity of the TOE to the Inspection System. The TOE generates and transmits the digital signature generated by the AA private key on the random number transmitted by the Inspection System. The Inspection System then authenticates the TOE by verifying the digital signature using the AA public key. Therefore, AA is the security mechanism that prevents the substitution of the MRTD IC chip onto which the TOE is loaded.

< EAC (Extended Access Control) >

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

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

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

TOE Access Control and Security Management

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

< Access control of the Personalization agent>

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

< Access control of the IS >

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

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

Therefore, if the IS succeeds with the SAC authentication, the TOE grants a SAC authorization (the read-rights for the personal data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM). If the IS don't perform SAC authentication and succeeds with the BAC authentication, the TOE grants a BAC authorization (the read-rights for the personal data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM). If the IS also succeeds with the EAC authentication and the CVCA Certificate, DV Certificate and IS Certificate that the IS has included with the read-rights for the biometric data, the TOE then grants the EAC authorization (the read-rights for the personal data of ePassport holder, the biometric data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM).

< Personalization management of the Personalization agent >

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

< TOE self protection management >

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

Other TOE Protections

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

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

1.4.3 Functions of IC Chip

The IC Chip supports all functions concerning the RF communication. And it provides the TDES/AES cryptographic algorithm, Retail MAC algorithm, CMAC, TRNG, Hash, ECC/RSA cryptographic algorithm. Thus, the TOE is provided CRC function for memory integrity.
The IC Chip provides functions that consider countermeasures to the DPA/SPA, which is an attack technique, by analyzing the physical phenomena (electric current, voltage, an electromagnetism change) during the cryptographic algorithm. Additionally, the IC Chip provides an inspect mechanism as to whether the TOE departs from the normal operational range of the TSF with an Active-Shield and sensor test function for the TOE.

1.4.4 External Functions of TOE

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

PA-PKI

PA (Passive Authentication) demonstrates that the identity data recorded in the ePassport has not been forged of corrupted as the IS with the DS Certificate verifies the digital signature in the SOD and the hash value of user data according to read-right of the ePassport access control policy.
CSCA (Country Signing Certification Authority) is the root CA that generates and issues the CSCA Certificate and the DV Certificate by securely generating the digital signature key in the PA-PKI to support the PA security mechanisms
The DS (Document Signer) Certificate is the certificate of the Personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism. The DS Certificate may be saved in EF.SOD of TOE for PA.

EAC-PKI

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

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

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

1.5 Conventions

The notation, formatting and conventions used in this Security Target are consistent with the Common Criteria for Information Technology Security Evaluation (hereafter referred to as "CC"). The CC allows several operations to be performed on functional requirements, assignment, iteration, refinement and selection. Each of these operations is used in this Security Target.

Iteration

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

Selection

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

Refinement

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

Assignment

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

Application Notes

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

1.6 Security Target Organization

Chapter 1 provides the introductory material for the Security Target and TOE.

Chapter 2 defines the conformance claim.

Chapter 3 describes the threats, organizational security policies and assumptions for the TOE.
Chapter 4 describes the security objectives of the TOE and environment by supporting the assumptions and organizational security policies to counter the threats.
Chapter 5 describes the extended components that are not based on CC part 2 or part 3.
Chapter 6 describes the security functional requirements and assurance requirements for the security objectives.
Chapter 7 provides the TOE security functionality as the TOE summary.

2. Conformance Claim

2.1 CC Conformance

This Security Target claims conformance to:

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

as follows:

- Common Criteria for Information Technology Security Evaluation, Part 2 Expansion
- Common Criteria for Information Technology Security Evaluation, Part 3 Conformance

2.2 PP Conformance

This Security Target claims conformance to:

- ePassport Protection Profile V2.1 (KECS-PP-0163a-2009)

Application Notes: IC chip, where it is one of TOE components, conforms to "Security IC Platform Protection Profile Version 1.0(BSI-PP-0035-2007)".

2.3 Package Conformance

This Security Target claims conformance to:

- Assurance Package : EAL5 augmented with ALC_DVS.2, ADV_IMP.2 and AVA_VAN.5

3. Security Problem Definition

As the security problems, this chapter defines the threats, organizational security policies and assumptions to determine the scope of the expected operation environment of the TOE.

3.1 Threats

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

<Threats to the TOE in the Personalization phase>

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

T. Personalization_Agent_Forgery
A threat agent can attempt to write to the ePassport application data; management in this case refers to ePassport forgery.

<BAC/SAC-related Threats in the Operational Use phase>

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

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

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

Application Notes: The BAC authentication key is generated by the Personalization agent in

the Personalization phase and saved in secure memory. A threat can attempt to access the BAC authentication key that is saved in secure or in the temporary memory of the MRTD IC Chip.

T. BAC_ReplayAttack

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

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

<EAC-related Threats in the Operational Use phase>

T. Damage_to_Biometric_Data

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

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

T. EAC-CA_Bypass

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

T. IS_Certificate_Forgery

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

<PAC, BAC/SAC and EAC-related Threats>

T. SessionData_Reuse

To access the data transmitted through secure messaging, a threat agent can derive session keys from a number of cryptographic communication texts collected using a terminal capable of wide-ranging RF communication.

Application Notes: In case that the TOE and Inspection System generate the SAC session key with the same random number in the SAC mutual authentication, the critical information necessary in deriving the session key can be provided to an attacker. And when the TOE and Inspection System use the BAC authentication key as the BAC session key, they are vulnerable to a cipher-text-only attack, as the same session key is used in each BAC session. When the BAC session key is generated with the same random number used in the BAC mutual authentication process, the critical information necessary in deriving the session key can be provided to an attacker because the first random number of the TOE is transmitted as plain text. In case the EIS transmits a temporary public key in the EAC-CA and a random number in the EAC-TA to other sessions in the same way and if the TOE continues to use these data items, they may be vulnerable to cipher-text only attacks. And when the TOE and Inspection System use the PAC authentication key as the PAC session key, they are vulnerable to a cipher-text-only attack, as the same session key is used in each PAC session. When the PAC session key is generated with the same random number used in the PAC mutual authentication process, the critical information necessary in deriving the session key can be provided to an attacker because the first random number of the TOE is transmitted as plain text.

T. Skimming

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

<Threats related to IC Chip Support>

T. Malfunction

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

<Other Threats in the Operational Use phase>

T. Leakage_CryptographicKey_Info

By using electric power and wave analysis devices, a threat agent can obtain the key

information used in the cryptographic technique applied to the ePassport security mechanism by analyzing the characteristics of the electric power and the wave emitted in the course of the TOE operation.

T. ePassport_Reproduction

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

T. Residual_Info

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

T. ePassport_ICChip_Replacement

A threat agent can forge an ePassport and write the data onto another MRTD IC chip.

3.2 Organizational Security Policies

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

P. International_Compatibility

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

Application Notes: International compatibility shall be ensured according to the ICAO document, EAC specification and SAC specification.

P. Security_Mechanism_Application_Procedures

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

Application Notes: The operation flow of the TOE differs according to the type of security mechanisms supported by the Inspection System. The basic operation flow of the security mechanisms depends on the Standard ePassport Inspection Procedure and Advanced ePassport Procedure in the EAC specification. In case that both BAC and SAC are implemented

to ensure the international compatibility, the Inspection System has to use the SAC protocol instead of BAC protocol according to the SAC specification.

P. Application_Program_Install

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

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

P. Personalization_Agent

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

P. ePassport_Access_Control

The Personalization agent and the TOE shall formulate the ePassport access control policies to protect the MRTD application data. Additionally, the TOE shall regulate the roles of user.

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

(Table 9) ePassport Access Control Policies in Operational Use Phase

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

(Table 10) ePassport Access Control Policies in the Personalization Phase

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

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

P. PKI

The Issuing State of the ePassport shall implement the PA-PKI and EAC-PKI security mechanism according to the ePassport PKI System and execute the practice of certification (creating, issuing, operating and destroying the certificates) by securely generating and managing digital signature keys in accordance with the Certification Practice Statement (CPS)
In addition, the Issuing State of the ePassport shall update certificates according to the policies to maintain a valid date of the certificates and securely delivery them to the Verifying State and Inspection System. When the EAC-TA provides the TOE with a CVCA Link Certificate, a DV Certificate and IS Certificate after the Inspection System, obtaining information from EF.CVCA stored in the TOE, the TOE shall internally update certificates by verifying the validity of the certificates.

P. Range_RF_Communication

The RF communication distance between the MRTD chip and Inspection System shall be less than 5cm, and the RF communication channel shall not be established if the page of the

ePassport with the IC chip attached is not opened.

P. IC_Chip

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

3.3 Assumptions

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

A. Certificate_Verification

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

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

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

A. Inspection_System

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

Additionally, after the session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the SAC session key, the BAC session key, the EAC session key and the other session information.

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

As the BIS supports the SAC and PA security mechanisms, it obtains the read-rights for the personal and authentication data of the ePassport holder if the SAC mutual authentication using the SAC authentication key succeeds. Subsequently, by establishing the SAC secure

messaging with the SAC session key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the SAC, and by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it then conforms the absence of forgery or corruption of the personal and authentication data of the ePassport holder. The BIS verifies the genuineness of ePassport IC chip by executing the AA after the PA

As the BIS supports the BAC and PA security mechanisms without the SAC security mechanisms, it obtains the read-rights for the personal and authentication data of the ePassport holder if the BAC mutual authentication using the BAC authentication key succeeds. Subsequently, by establishing the BAC secure messaging with the BAC session key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the BAC, and by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it then conforms the absence of forgery or corruption of the personal and authentication data of the ePassport holder. The BIS verifies the genuineness of ePassport IC chip by executing the AA after the PA

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

A. MRZ_Entropy

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

Application Notes: According to the ICAO documents and EAC specifications, the entropy of the passport number, the date of birth and the date of expiry and the check digit used as the BAC authentication key seed shall be sufficient level to ensure the secure BAC authentication key.

<IC chip ST Assumption>

A. Process-Sec-IC Protection during Packaging, Finishing and Personalization

Security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the consumer to maintain confidentiality and integrity of the TOE and of its manufacturing

and test data (to prevent any possible copy, modification, retention, theft or un-authorized use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.

4. Security Objectives

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

4.1 Security Objectives for TOE

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

O. Management

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

Application Note: In the Personalization phase, the TOE shall provide the personalization and management functions (life cycle change, execution code patch, PAC authentication key update, and Unblock, among others) to the authorized Personalization agent.
The TOE divides EEPROM for the user data and the TSF data and manages the memory area of each user separately. The Personalization agent deactivates the writing function by modifying the life cycle of the TOE after the Personalization agent writes the ePassport applicable data in the Personalization phase. This operation is performed before the life cycle of the TOE is transferred to the Operational phase. The TOE stores the BAC authentication key in secure memory after it is generated by request of the Personalization agent in the Personalization phase. According to the Personalization policy, it shall provide the means to manage the deactivation with the PAC secure communication channel.

O. Security_Mechanism_Application_Procedures

The TOE shall ensure the instruction flow according to the ePassport inspection procedures of the EAC specification and the SAC specification.

Application note: The TOE shall ensure that the application order of the PA, AA, BAC and EAC security mechanisms conforms to the Standard ePassport Inspection Procedure and Advanced ePassport Procedure of the EAC specification. In addition, it shall not allow requests from the Inspection System that does not correspond to the security mechanism application order. However, the Inspection System should be used the SAC which suited to the inspection procedures instead of BAC if both BAC and SAC implements in the TOE for international compatibility

O. Session_Termination

The TOE shall terminate the session if the PAC mutual authentication failure, the PAC personalization and management authentication failure, the BAC mutual authentication failure, the SAC mutual authentication failure or the EAC-TA fails or a modification is detected in the transmitted TSF data.

Application Note: The TOE shall terminate the session in case of EAC secure messaging error, but the TOE shall preserve EAC secure channel in case of failure of the EAC-TA Authentication.

O. Secure_Messaging

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

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

O. Certificate_Verification

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

O. Secure_State

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

O. Deleting_Residual_Info

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

O. Replay_Prevention

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

Application Note: The TOE shall generate the transmitted data to the Inspection System in the SAC mutual authentication, the BAC mutual authentication and the EAC-TA authentication, ensuring that it is different with every session. In addition, it shall not use the BAC, SAC authentication key as the BAC, SAC session key. The TOE also shall not provide the critical information necessary in deriving the session key by generating the BAC, SAC session key with

the same random number used in the BAC, SAC mutual authentication. The TOE shall generate the data transmitted to the Personalization Agent in the PAC mutual authentication so that it is different per each session. Additionally, it shall not use the PAC authentication key as the PAC session key. The TOE shall not provide the critical information necessary in deriving the session key by generating the PAC session key with the same random number used in the PAC mutual authentication. The TOE shall not generate the RSA digital signature value with the Single-use random number mechanisms used in the AA.

O. Access_Control

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

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

O. Handling_Info_Leakage

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

Application Note: The TOE activates the protection functions supported by the IC chip and countermeasures the attacks(DPA, SPA) that an external entity may discover and exploit the cryptographic-related data from physical phenomena (change of current, voltage and electromagnetic, etc.) during cryptographic operation.

O. BAC

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

O. EAC

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

O. IC_Chip

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

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

O. SAC

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

Application Note: the Inspection System should be used SAC which suited to the inspection procedures instead of BAC if both BAC and SAC implements in the TOE for international compatibility

O. AA

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

O. PAC

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

4.2 Security Objectives for Operational Environment

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

OE. PassportBook_Manufacturing_Security

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

OE. Procedures_of_ePassport_holder_Check

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

OE. Application_Program_Install

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

OE. Certificate_Verification

The Inspection System, including the BIS and the EIS, verifies the SOD after verifying the validity of the certificate chain for the PA (CSCA Certificate → DS Certificate) to verify that forgery and corruption of the ePassport identity data recorded in the TOE has not occurred. To do this, the DS Certificate and CRL shall be verified periodically.

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

OE. Personalization_Agent

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

OE. Inspection_System

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

OE. MRZ_Entropy

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

authentication key.

OE. PKI

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

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

OE. Range_RF_Communication

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

<Security Objective for the Operational Environment of the IC chip ST >

OE. Process-Sec-IC Protection during Packaging, Finishing and Personalization

The Security procedures shall be used after TOE delivery up to delivery to the "consumer" to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or un-authorized use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.

4.3. Security Objectives Rationale

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

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

The Rationale of the Security Objectives demonstrates the following:

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

security policy.

(Table 11) shows the mapping between Security Problem Definition and Security Objectives.

(Table 11) Mapping between Security Problem Definition and Security Objectives

Security Problem Definition \ Security Objectives	TOE Security Objectives															Security Objectives for Environment								
	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Secure_State	O.Certificate_Verification	O.Deleting_residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.IC_Chip	O.AAA	O.BAC	O.EAC	O.PAC	O.SAC	OE.PassportBook_Manufacturing_Security	OE.Procedures_of_Passport_Holder_Check	OE.Application_Program_Install	OE.Certificate_Verification	OE.Personalization_Agent	OE.Inspection_System	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Communication
T.TSF_Data_Modification	X		X	X					X						X						X				
T.Disguise_of_Personalization_Agent															X										
T.Eavesdropping				X																		X			
T.Forgery_Corruption_Personal_Data			X						X				X			X						X			
T.BAC_ Authentication_Key_Disclose	X		X				X		X									X							
T.BAC_ReplayAttack								X																	
T.Damage_to_Biometric_Data			X	X		X			X					X						X		X		X	
T.EAC-CA_Bypass		X																X		X		X			
T.IS_Certificate_Forgery	X					X														X					
T.SessionData_Reuse								X														X			
T.Skimming									X				X	X		X						X			X
T.Malfunction					X						X														
T.Leakage_CryptographicKey_Info										X	X														
T.ePassport_Reproduction																	X	X							
T.Replacement_of_ePassport_ ICChip												X													
T.Residual_Info							X																		
P.International_Compatibility																					X				
P.Security_Mechanism_Application_Procedures		X																				X			

Security Objectives / Security Problem Definition	TOE Security Objectives															Security Objectives for Environment								
	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Secure_State	O.Certificate_Verification	O.Deleting_residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.IC_Chip	O.AAA	O.BAC	O.EAC	O.PAC	O.SAC	OE.PassportBook_Manufacturing_Security	OE.Procedures_of_Passport_Holder_Check	OE:Application_Program_Install	OE:Certificate_Verification	OE:Personalization_Agent	OE:Inspection_System	OE:MRZ_Entropy	OE:PKI	OE:Range_RF_Communication
P.Application_Program_Install																			X						
P.Personalization_Agent	X														X						X				
P.ePassport_Access_Control	X								X				X	X	X	X					X	X			
P.PKI						X																		X	
P.Range_RF_Communication																									X
P.IC_Chip											X														
A.Certificate_Verification																				X	X			X	
A.Inspection System																						X			
A.MRZ_Entropy																							X		

Security Objectives / Security Problem	Security Objectives for Operational Environment
	OE.Process_Sec_IC
A.Process-Sec-IC	X

For the detailed description of the rationale is referred to the ePassport PP V2.1.

5. Definition of Extended Component

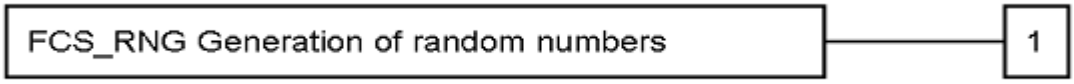
This Security Target defines FCS_RNG that is claimed in the Security Target of the IC Chip.

FCS_RNG Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are i ntended to be used for cryptographic purpose.

Component levelling:



FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hy brid*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a *defined qual ity metric*].

6. Security Requirements

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

In this Security Target, the external entities specified in the security requirements include the Personalization agent, BIS and EIS.

This Security Target defines all subjects, objects, operation, security attributes employed in the security requirements as (Table 12) and (Table 13). Also, it defines SSC(Send Sequence Counter) with session security attributes related to establishing the secure messaging.

(Table 12) Subjects, Security Attributes and Operation

Subjects	Security Attributes	Operation
BIS	SAC Authorization, BAC Authorization	Read
EIS	SAC Authorization, BAC Authorization EAC Authorization	Read
Personalization Agent	Personalization Agent Issuing Authorization	Read, Write

(Table 13) Objectives and Security Attributes

Objects	Security Attributes	
	Security Attributes of Object's Operation	Security Attributes of Object's Access-rights
Personal Data of ePassport Holder	Read-rights	SAC Authorization, BAC Authorization, EAC Authorization
	Write-rights	Personalization Agent Issuing Authorization
Biometric Data of ePassport Holder	Read-rights	EAC Authorization
	Write-rights	Personalization Agent Issuing Authorization
ePassport Authentication Data	Read-rights	SAC Authorization, BAC Authorization, EAC Authorization
	Write-rights	Personalization Agent Issuing Authorization
EF.CVCA	Read-rights	SAC Authorization, BAC Authorization, EAC Authorization
	Write-rights	Personalization Agent Issuing Authorization
EF.COM	Read-rights	SAC Authorization, BAC Authorization, EAC Authorization
	Write-rights	Personalization Agent Issuing Authorization
EF.CARDACCESS	Read-rights	-
	Write-rights	Personalization Agent Issuing Authorization

6.1 Security Functional Requirements

The security functional requirements for this Security Target consist of the following components from Part 2 of the CC and the added components described in chapter 5, as summarized below (Table 14).

(Table 14) Security Functional Requirements

Security functional class	Security functional component	
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.1(2)	Cryptographic key generation (PAC session key)
	FCS_CKM.1(3)	Cryptographic key generation (SAC)
	FCS_CKM.2(1)	Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)
	FCS_CKM.2(2)	Cryptographic key distribution (KDF Seed Distribution for EAC session key generation)
	FCS_CKM.2(3)	Cryptographic key distribution (Seed Distribution for PAC session key generation)
	FCS_CKM.2(4)	Cryptographic key distribution (KDF Seed Distribution for SAC 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)
	FCS_COP.1(5)	Cryptographic operation (Digital signature generation)
	FCS_RNG.1	Random number generation
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_DAU.1	Basic data authentication
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1	Basic data exchange confidentiality

Security functional class	Security functional component	
	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.1(3)	Timing of authentication(PAC Mutual Authentication)
	FIA_UAU.1(4)	Timing of authentication(PAC Personalization management Authentication)
	FIA_UAU.1(5)	Timing of authentication(SAC Mutual Authentication)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5(1)	Multiple authentication mechanisms
	FIA_UAU.5(2)	Multiple authentication mechanisms(PAC Mutual Authentication and PAC personalization and management Authentication)
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1(1)	Management of security functions behavior
	FMT_MOF.1(2)	Management of security functions behavior(initialization)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Information)
	FMT_MTD.1(2)	Management of TSF data (SSC initialization)
	FMT_MTD.1(3)	Management of TSF data (Key Write)
	FMT_MTD.1(4)	Management of TSF data(TOE life cycle and PAC Authentication key management)
	FMT_MTD.1(5)	Management of TSF data (TOE life cycle change)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy(FRP)	FPR_UNO.1	Unobservability
Protection of the TSF	FPT_FLS.1	Failure to preserve a secure state
	FPT_ITI.1	Inter-TSF detection of modification

Security functional class	Security functional component	
(FPT)	FPT_PHP.3	Resistance to physical attack
	FPT_TST.1	TSF Self-testing

6.1.1. Cryptographic Support

FCS_CKM.1(1) Cryptographic key generation (Key Derivation Mechanism)
Hierarchical to: No other components.
Dependencies: [**FCS_CKM.2(1) Cryptographic key distribution (KDF seed distribution for BAC session key generation) and**
FCS_CKM.2(2) Cryptographic key distribution (KDF seed distribution for EAC session key generation) or
FCS_COP.1(3) Cryptographic operation(Hash Function)]
FCS_CKM.4 Cryptographic key destruction

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

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

FCS_CKM.1(2) Cryptographic key generation (PAC Session Key)
Hierarchical to: No other components.
Dependencies: [**FCS_CKM.2(3) Cryptographic key distribution(Seed Distribution for PAC session key generation) or**
FCS_COP.1(1) Cryptographic operation(Symmetric Key Cryptographic Operation)]
FCS_CKM.4 Cryptographic key destruction

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

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

encryption key and MAC key.

FCS_CKM.1(3) Cryptographic key generation (SAC)

Hierarchical to: No other components.

Dependencies: [**FCS_CKM.2(4) Cryptographic key distribution (KDF Seed Distribution for SAC session key generation) or**
FCS_COP.1(3) Cryptographic operation(Hash Function)]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1. The TSF shall generate encryption keys in accordance with a specified cryptographic key generation algorithm [key generation method column in (Table 15)] and specified cryptographic key sizes [key length column in below table] that meets the following: [the SAC specification, ANS X9.62].

(Table 15) SAC Key Generation

SAC key	Encryption key generation method	Encryption key length
Random number encryption key SAC session key(encryption key, MAC key)	SAC specification, 4.2 Key Derivation Function,	112 bit, 128 bit, 192bit, 256 bit
Public/private keys for shared key generation	ANS X9.62, Elliptic Curve Key Generation	192bit ~ 512bit

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(1) Cryptographic key generation(Key Derivation Mechanism)]
FCS_CKM.4 Cryptographic key destruction

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

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

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism)]
FCS_CKM.4 Cryptographic key destruction

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

FCS_CKM.2(3) Cryptographic key distribution (Seed Distribution for PAC session key generation)
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(2) Cryptographic key generation(PAC session key)]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute **the seed for the PAC session key generation** in accordance with a specified cryptographic key distribution method [modified from ISO/IEC 11770-2] that meets the following: [none].

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

FCS_CKM.2(4) Cryptographic key distribution (KDF Seed Distribution for SAC 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(3) Cryptographic key generation(SAC)]
FCS_CKM.4 Cryptographic key destruction

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

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

FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism)
FCS_CKM.1(2) Cryptographic key generation(PAC session key)
FCS_CKM.1(3) Cryptographic key generation(SAC)]

FCS_CKM.4.1. The TSF shall destroy **the encryption keys and the MAC keys** in accordance with a specified cryptographic key destruction method [delete by writing '0x00' or '0xFF' in memory] that meets the following: [none].

Application Notes: The TOE deletes the SAC session key, SAC authentication key, BAC authentication key, BAC session key, EAC session key, PAC authentication key, PAC session key, AA private key, EAC chip authentication private key, CVCA digital signature verification key and domain information in temporary memory by writing '0x00' in the memory and after finishing of personalization, TSF delete by writing '0xFF' PAC authentication key in the EEPROM and also, TOE delete by writing'0xFF' information related to keys in EEPROM if TOE operation mode changed into Discard mode.

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(1) Cryptographic key generation(Key Derivation Mechanism)
FCS_CKM.1(2) Cryptographic key generation(PAC session key)
FCS_CKM.1(3) Cryptographic key generation(SAC)]
FCS_CKM.4 Cryptographic key generation

FCS_COP.1.1. The TSF shall perform [message encryption and decryption operations] in accordance with a specified cryptographic algorithm [*TDES, [AES]*] with a cryptographic key size [*112 bits, [128, 192, 256 bits]*] that meets the following: [*ICAO document, ISO/IEC 18033-3*].

Application Notes: The TOE uses the TDES, AES(CBC mode) cryptographic algorithms of Certified IC chip for the confidentiality protection of the transmitted data of the SAC, BAC or EAC secure messaging, for the PAC mutual authentication, for the SAC or BAC mutual authentication, for the PAC key distribution and for the BAC key distribution.

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(1) Cryptographic key generation(Key Derivation Mechanism)
FCS_CKM.1(2) Cryptographic key generation(PAC session key)
FCS_CKM.1(3) Cryptographic key generation(SAC)]
FCS_CKM.4 Cryptographic key generation

FCS_COP.1.1. The TSF shall perform [a MAC operation] in accordance with a specified cryptographic algorithm [*Retail MAC, [AES-CMAC]*] with a cryptographic key size [*112 bits, [128, 192, 256 bits]*] that meets the following: [*[ICAO document, ISO/IEC 9797-1, NIST SP 800-38B]*].

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

FCS_COP.1(3) Cryptographic operation (HASH function)
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1. The TSF shall perform [a HASH operation] in accordance with a specified cryptographic algorithm [*SHA-1, [SHA-224, SHA-256, SHA-384, SHA-512]*] with a cryptographic key size [none] that meets the following: [*[FIPS PUB 180-3]*].

Application Notes: The TOE uses SHA-1 or SHA-256 as hash function for generating session keys used in the SAC, BAC or EAC secure messaging in KDF mechanism of the ICAO document and SAC Specification. And the TOE uses SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 for EAC-TA, SHA-256 for AA, SHA-1 for BAC authentication key. The TOE uses SHA crypto library for more than SHA-224 and SHA-1 module implemented in KCOS.

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(1) Cryptographic key generation(Key Derivation Mechanism)]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1. The TSF shall perform [Digital signature Verification] in accordance with a specified cryptographic algorithm [*ECDSA-SHA-1, ECDSA-SHA-224, ECDSA-SHA-256, ECDSA-SHA-384, ECDSA-SHA-512 / RSASSA-PKCS1-V1.5-SHA-256*] with a cryptographic key size [*192 bits, 224 bits, 256 bits, 384 bits, 512 bits / 2048 bits*] that meets the following: [*ISO/IEC 15946-2 / PKCS#1*].

Application Notes: The TOE utilizes the RSA library if the RSA algorithm is used for the EAC security mechanism and the ECC library if ECC algorithm is used for EAC security mechanism.

FCS_COP.1(5) Cryptographic operation (Digital Signature Generation)
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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

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

FCS_RNG.1 Random number generation
Hierarchical to: No other components.
Dependencies: No other components.

FCS_RNG.1.1 The TSF shall provide a *physical* random number generator that implements [total failure test for the random source]

FCS_RNG.1.2 The TSF shall provide a random numbers that meet ["standard" level of ANSSI requirements (French metric), AIS31 version 1 Functional Classes and Evaluation Methodology for Physical Random Number Generators, 25 September 2001, Class P2]

Application Notes: The SFR is related to [ST of the IC chip]. IC chip provides TRNG Library version 2.0, TRNG Application note rev 1.2.

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

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

a) Subjects
   (1) Personalization agent
   (2) BIS
   (3) EIS
   (4) [None]
b) Objects
   (1) Personal data of the ePassport holder
   : EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16
   (2) The biometric data of the ePassport holder
   : EF.DG3, EF.DG4
   (3) ePassport authentication data
   : EF.DG14, EF.DG15, EF.SOD
   (4) EF.CVCA
   (5) EF.COM
   (6) [EF.CARDACCESS]
c) Operations
   (1) Read
   (2) Write
   (3) [None]

]

FDP_ACF.1 Security attributes based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1. Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce [the ePassport access control policy] on objects based on the following: [**(Table 16), (Table 17),** [none]].

(Table 16) Subject-relevant Security Attributes

Subjects	Security attributes

BIS	**SAC authorization**, BAC authorization
EIS	**SAC authorization**, BAC authorization, EAC authorization
Personalization agent	Personalization agent issuing authorization

(Table 17) Object-relevant Security Attributes

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

Operation	**Security attributes**
Read	none
Write	

Application Notes: The SAC authorization is the right given to the user identified with the Inspection System that supports the ePassport application by FIA_UID.1 when the SAC mutual authentication succeeds. When the Inspection System does not support SAC function, BAC

authorization is tried. The BAC authorization is the right given to the user identified with the Inspection System that supports the ePassport application by FIA_UID.1 when the BAC mutual authentication succeeds. The EAC authorization is the right given when the Inspection System with the BAC or SAC authorization succeeds in the EAC-CA and the EAC-TA and the read-rights of the biometric data is included in the CVCA certificate, the DV certificate and the IS certificate held by that Inspection System. Even when the EAC-CA and the EAC-TA succeed, the Inspection System comprises only the BAC or SAC authorization if the certificates do not include the read-rights. Issuing authorization is the right given when PAC mutual authentication and PAC personalization and management authentication succeed due to the Personalization Agent. The Personalization Agent and the Inspection System can read EF.CARDACCESS without any right

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) The operation is allowed only when the security attributes of the subjects are included in the security attributes of the object's access-rights and if the operations correspond to security attributes of the object's operation.

b) [none]

]

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

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

a) Explicitly deny access of subjects to objects, if the instructions order of the Inspection System is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specification and 2.2 Inspection Procedures of the SAC specification.
b) Explicitly Deny reading of subjects to biometric data if there are no read-rights of biometric data in the IS certificate of the EIS that has the EAC authorization
c) Explicitly Deny access (read, write, etc.) of the unauthorized Inspection System to all objects
d) [Access of subjects to objects that are explicitly denied for the commands that cannot be executed in each life cycle (Empty, Unissue, InitAuth, SecondAuth, StartIssue, Issued, Block and Discard) of the TOE].
e) Access of subjects to objects that are explicitly denied for the invalid commands such as not ISO command, not industrial command and invalid P1/P2/Lc command.

f) Access of subjects to objects that are explicitly denied for the irregular order of personalization]

FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_DAU.1.1. The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [the AA private key].
FDP_DAU.1.2. The TSF shall provide [BIS, EIS] with the ability to verify evidence of the validity of the indicated information.

Application Notes: The TSF shall perform the 2048 bit RSA digital signature algorithm in AA.

FDP_RIP.1 Subset residual information protection
Hierarchical to: No other components.
Dependencies: No dependencies.
FDP_RIP.1.1. The TSF shall ensure that any previous information content of a resource is made unavailable upon *the deallocation of the resource from* the following objects:[

a) BAC session key
b) EAC session key
c) BAC authentication key
d) [PAC session key,
e) PAC authentication key,
f) AA private key,
g) EAC chip authentication private key,
h) CVCA digital signature verification key and domain information,
i) SAC authentication key
j) SAC session key]

Application Notes: After the termination of the session, the TSF deletes the SAC authentication key, SAC session key, BAC authentication key, BAC session key, EAC session key, PAC authentication key, PAC session key, AA private key, EAC chip authentication key, CVCA digital signature verification key and domain information and SSC/Ticket and the flag of random number usage in temporary memory by writing '0x00' in the memory. After finished the issuance and a status of TOE is Issued, PAC authentication key is physically deleted by writing '0xFF' in the memory.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

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

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

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

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

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

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

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

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

6.1.3. Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: **FIA_UAU.1(1) Authentication(BAC mutual authentication)**
FIA_UAU.1(2) Authentication(EAC-TA)
FIA_UAU.1(3) Authentication(PAC mutual authentication)
FIA_UAU.1(4) Authentication(PAC Personalization management authentication)
FIA_UAU.1(5) Authentication(SAC mutual authentication)

FIA_AFL.1.1. The TSF shall detect when *[a certain number of times (see (Table 18))]* unsuccessful authentication attempts occur related to the following:

a) BAC mutual authentication
b) EAC-TA
c) [PAC mutual authentication,
d) PAC Personalization management authentication
e) SAC mutual authentication]

FIA_AFL.1.2. When *the defined number* of unsuccessful authentication attempts has been *met*, the TSF shall perform [**the actions specified in the following (Table 18)**].

(Table 18) Authentication Failure Handling

Assignment: Number of unsuccessful authentication attempts	Assignment: Specified Authentication events	Assignment: Actions
1	BAC mutual authentication	Session Termination
1	EAC-TA authentication	Subset residual information removal, Maintaining secure communication channel
3	PAC mutual authentication PAC Personalization management authentication	Session Termination and operational mode transition
1	SAC mutual authentication	Session Termination

Application Notes: The TSF halts all functions for 1 sec after terminating the session when BAC mutual authentication failed. When EAC-TA authentication is failed, EAC secure communication channel is lasted. TSF guarantees accessing for all of DG files except for DG3/4.

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1. The TSF shall allow [
a) to indicate that supports the BAC mechanism
b) [None]
]on behalf of the user to be performed before the user is authenticated.

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

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) or FIA_UAU.1(5) Timing of authentication (SAC mutual authentication)**

FIA_UAU.1.1. The TSF shall allow [
a) performance of the EAC-CA
b) reading user data except for the biometric data of the ePassport holder
c) [None]
]on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.1(3) Timing of authentication (PAC Mutual Authentication)
Hierarchical to: No other components.
Dependencies: FIA_UID.1 identification

FIA_UAU.1.1. The TSF shall allow [
a) TOE Personalization initialization of the Personalization phase
b) Transmission of a crypto CSN and Ticket and generation of Ticket
c) Transmission and generation of a random number
]on behalf of the user to be performed before the user is authenticated.

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

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

FIA_UAU.1(4) Timing of authentication (PAC personalization management authentication)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 identification

FIA_UAU.1.1. The TSF shall allow [

a) TOE Personalization Initialization in the Personalization phase
b) Transmission of a crypto CSN and Ticket and generation of Ticket
c) Transmission and generation of a random number
d) PAC Mutual authentication

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

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

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

FIA_UAU.1(5) Timing of authentication (SAC mutual authentication)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 identification

FIA_UAU.1.1. The TSF shall allow [

a) the reading of EF.CARDACCESS

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

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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) BAC mutual authentication
b) EAC-TA

c) [PAC Mutual authentication,
d) PAC personalization management authentication
e) AA authentication
f) SAC mutual authentication]]

FIA_UAU.5(1) Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1. The TSF shall provide [
a) BAC mutual authentication
b) EAC-TA
c) [SAC mutual authentication]
] to support user authentication.

FIA_UAU.5.2. The TSF shall authenticate any user's claimed identity according to [
a) BIS or EIS shall succeed with the BAC mutual authentication to allow the BAC authorization.
b) EIS, to succeed with EAC authorization, shall succeed with the SAC mutual authentication or the BAC mutual authentication, EAC-CA, and EAC-TA, and shall include the read-rights of the biometric data in the CVCA Certificate, DV Certificate and IS Certificate. To do this, the TSF shall provide the EAC-CA.
c) [BIS or EIS shall succeed with the SAC mutual authentication to allow the SAC authorization]]

Application Notes: The TSF shall perform 2048 bits RSA digital signature algorithms or, 192, 224, 256, 384, 512 bit ECDSA digital signature algorithm in EAC-TA.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1. The TSF shall provide [
a) PAC mutual authentication
b) PAC personalization and management authentication (PAC-LifeCycle authentication, PAC-Patch authentication, PAC-KeyUpdate authentication, and PAC-Unblock authentication)] to support user authentication.

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

a) In case the life cycle of the TOE in Personalization phase is in the Unissue mode, PAC mutual authentication has to be performed.
b) In case the life cycle of the TOE in the Personalization phase is in the InitAuth mode, one of the PAC personalization and management authentications (PAC-LifeCycle authentication) has to be performed to transmit the life cycle of the TOE.
c) In case the life cycle of TOE in Personalization phase is in the InitAuth mode and the issuing right for updating the PAC authentication key is not obtained, PAC personalization and management authentication along with PAC-KeyUpdate authentication have to be performed successfully to update the PAC authentication key.
d) In case the life cycle of TOE in Personalization phase is in the SecondAuth mode and the issuing right for updating the PAC authentication key is not obtained, PAC personalization and management authentication along with PAC-KeyUpdate authentication have to be performed successfully to update the PAC authentication key.
e) In case the life cycle of the TOE in the Personalization phase is in the SecondAuth mode and the issuing right for patching the execution code and data is not obtained, PAC personalization and management authentication along with PAC-Patch authentication have to be performed successfully to patch the execution code and data.
f) In case the life cycle of the TOE in the Personalization phase is in the SecondAuth mode and the issuing right for transmitting the life cycle of the TOE is not obtained, PAC personalization and management authentication along with PAC-LifeCycle authentication have to be performed successfully to transmit the life cycle.
g) In case the life cycle of the TOE in the Personalization phase is in the StartIssue mode, PAC-LifeCycle authentication has to be performed to change the life cycle of the TOE.
h) In case the life cycle of the TOE in the Personalization phase is in the Block mode, PAC-Unblock authentication has to be performed to unblock it.

]

Application Notes: The life cycle of the TOE is changed to the InitAuth mode and the TOE has the right to create EF if PAC mutual authentication was performed successfully. If PAC personalization and management authentication along with PAC-LifeCycle authentication was performed successfully in the InitAuth mode, the life cycle of the TOE is changed to the SecondAuth mode and the TOE can change the life cycle to the other life cycles. The personalization right of the Personalization Agent includes that the Personalization Agent can assign the rights of reading or writing for user data and the TSF and the life cycle is changed InitAuth to SecondAuth, from SecondAuth to StartIssue or Issued mode.

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

FIA_UID.1.1. The TSF shall allow [
a) the establishment of a communication channel based on ISO/IEC 14443-4
]on behalf of the user to be performed before the user is identified.

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

Application Notes: When the external entities that communicate with the TOE request the use of the ePassport application or the access of EF.CARDACCESS, the TOE identifies it with the Inspection System. In addition, when the external entities that communicate with the TOE request the use of the personalization program, the TOE identifies it with the Personalization Agent.

6.1.4 Security Management

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

FMT_MOF.1.1. The TSF shall restrict the ability to *disable* the functions [writing function, **PAC secure communication channel**] to [the Personalization agent in the Personalization phase].

Application Notes: The writing function of the application data on ePassport executed in the SecondAuth mode. After issuing, the operating mode of TOE is also the SecondAuth mode. The Personalization agent changes into the StartIssue mode by using PAC-LifeCycle authentication for checking the data. After checking, the operating mode of TOE is also changed into the Issued mode by using PAC-LifeCycle authentication. In the Issued mode, the function of writing is disabled. According to the policy of the Personalization Agent, secure messaging may not be applied during personalization phase.

FMT_MOF.1(2) Management of security functions behavior(initialization)
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MOF.1.1. The TSF shall restrict the ability to *enable* [the functions (see (Table 19))] to [roles (see (Table 19))].

(Table 19) Security Attributes for Security Functions Behavior

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

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

FMT_MSA.3 Static attribute Initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1. Security roles

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

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

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

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

Hierarchical to: No other components.

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

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

a) EAC chip authentication private key
b) Initial current date
c) Initial CVCA Certificate
d) Initial CVCA digital signature verification key
e) [none]

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

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

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

Hierarchical to: No other components.

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

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

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

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1. The TSF shall restrict the ability to [*write in secure memory*] the [TSF data (see (Table 20))] to [**the restrictions (see (Table 20))**].

(Table 20) Security Attributes for TSF data

TSF data	Authorized roles	Operation
AA private key	Authorized Personalization agent according to FIA_UAU.5(2) in the Personalization phase	write to protected memory
SAC authentication key, CAN	Authorized Personalization agent according to FIA_UAU.5(2) in the Personalization phase	
TSF Patch code	Authorized Personalization agent according to FIA_UAU.5(2) in the Personalization phase	
BAC authentication key	TSF	
Initialization data	Authorized Personalization agent according to FIA_UAU.5(2) in the Personalization phase	

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

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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1. The TSF shall restrict the ability to *query, modify* the [PAC authentication key, life cycle of TOE in the Personalization Phase, TOE identification information, IC chip identification information] to [Authorized Personalization agent and Inspection system]

Application Notes: The initial PAC authentication key is stored in ROM during the Manufacturing phase. This key can be updated in the Personalization phase. And the Personalization agent can check the current TOE operation mode without any special

authentication. And the Personalization Agent must use the command for the change of operation mode. Especially, in the Block mode, only unblock command is only permitted. And also the checking command for TOE identification information always can be used.

FMT_MTD.1(5) Management of TSF data (change of TOE life cycle and Ticket)
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MTD.1.1. The TSF shall restrict the ability to *modify* the [life cycle of TOE and Ticket in the Personalization Phase] to [TSF].

Application Notes: When the Personalization agent executes the command for TOE initialization, the operation mode for TOE is changed the Empty mode into the Unissue mode. In the the Unissue mode, if the integrity check for executing code failed, the TSF changes the life cycle of the TOE into the Discard mode. The TSF must changes the life cycle to the Unissue mode when the communication channel is closed in InitAuth or SecondAuth modes. The life cycle of the TOE changes Unissue into InitAuth when the PAC mutual authentication is successfully performed. The TOE operation mode is changed the Discard mode if the number of PAC-Unblock authentication failure is more than 3.

FMT_MTD.3 Secure TSF data
Hierarchical to: No other components.
Dependencies: **FMT_MTD.1(1) Management of TSF data(certificate verification information)**

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

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

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

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

a) A function to write the user data and TSF data in the Personalization phase
b) A function to verify and update the CVCA Certificate, CVCA digital signature verification key and the current data in the Operational Use phase
c) [A function to manage the TSF security: a function to verify the security attributes and SSC initialization, a function to check the random number reuse, a function to set IC chip registers,
d) A function of the personalization management in the Personalization phase: initialization of EEPROM area, a function to change and check the life cycle, a function to patch the execution code and data, a function to unblock, a function to update the PAC authentication key, a function to inactivate the writing function and PAC secure channel in the Personalization phase
e) A function to check TOE identification information]]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

a) Authorized Personalization agent

Authorized Personalization agent to update the PAC authentication key in the Personalization phase

Authorized Personalization agent to change the life cycle in the Personalization phase

Authorized Personalization agent for Unblock operations in the Personalization phase

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

b) [Inspection System]]

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

Application Notes: The Personalization agent is defined with the role to execute the a), d), e) security management function of FMT_SMF.1. The TSF executes security management functions for FMT_SMT.1 b) and c) of FMT_SMF.1. However, the TSF is not defined with this, as it is not a user. The IC chip and ePassport manufacturer can perform a role for management of security if delegated as the Personalization agent. And also, the Personalization and Inspection system perform a role for e) of FMT_SMF.1.

6.1.5 Privacy

FPR_UNO.1 Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) FCS_COP.1(1) A cryptographic operation (Symmetric key cryptographic operation)
b) FCS_COP.1(2) A Cryptographic operation (MAC)
c) FCS_COP.1(4) A cryptographic operation (Digital signature verification for certificates verification)
d) [FCS_COP.1(5) A cryptographic operation (Digital signature generation)]

] on the following: [

a) BAC authentication key
b) BAC session key
c) EAC session key
d) EAC chip authentication private key
e) [AA Private key
PAC authentication key
PAC session key
SAC authentication key
SAC session key]]

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

6.1.6 TSF Protection

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) Failure detected during self-testing by FPT_TST.1
b) Conditions outside the normal operating conditions of the TSF detected by the IC

chip

c) [a status that the PAC secure channel is terminated when the Operational mode is in InitAuth or SecondAuth mode]

]

FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

a) Termination of BAC secure messaging or EAC secure messaging
b) Deletion of the BAC session key or the EAC session key
c) Management action specified in FMT_MSA.1
d) [Termination of the PAC secure messaging and deletion of the PAC session key
e) Termination of the SAC secure messaging and deletion of the SAC session key]

] if modifications are detected.

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

FPT_PHP.3 Resistance to the physical attack

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_PHP.3.1. The TSF shall resist [physical manipulation and probing] to the [TSF] by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1. The TSF shall run a suite of self tests [*before executing the TSF*] to demonstrate

the correct operation of *the TSF*.

FPT_TST.1.2. The TSF shall provide authorized users with the capability to verify the integrity of [*TSF data stored to perform the security mechanisms*].

FPT_TST.1.3. The TSF shall provide **an authorized Personalization agent** with the capability to verify the integrity of [*the stored TSF executable code*].

6.2 Security Assurance Requirements

The security assurance requirements for this Security Target consist of the components from Part 3 of the CC summarized in (Table 21). The evaluation assurance level is EAL5+(ALC_DVS.2, ADV_IMP.2, AVA_VAN.5).

The assurance components are augmented follows:

- ALC_DVS.2 Sufficiency of security measures
- ADV_IMP.2 Complete mapping of the implementation representation of the TSF
- AVA_VAN.5 Advanced methodical vulnerability analysis

(Table 21) Security Assurance Requirements

Assurance class	Assurance component	
Security Target evaluation	ASE_INT.1	Security Target 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_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_ARC.1	Security architecture description
	ADV_TDS.4	Semi-formal modular Design
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
	ADV_INT.2	Well-structured internals

Assurance class	Assurance component	
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.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with Implementation standards
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: Modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

6.3 Security Requirements Rationale

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

6.3.1 Security Functional Requirements Rationale

The rationale of TOE security functional requirements demonstrates the followings :

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

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

(Table 22) Mapping between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_esidual_Info	O.Replay_Prevention	O.Access_Control	O.handling_Info_Leakage	O.BAC	O.EAC	O.IC Chip	O.PAC	O.AA	O.SAC
FCS_CKM.1(1)											X	X				
FCS_CKM.1(2)														X		
FCS_CKM.1(3)																X
FCS_CKM.2(1)								X			X					
FCS_CKM.2(2)												X				
FCS_CKM.2(3)														X		
FCS_CKM.2(4)																X
FCS_CKM.4							X									
FCS_COP.1(1)				X							X		X	X		X
FCS_COP.1(2)				X							X		X	X		X
FCS_COP.1(3)											X	X	X		X	X
FCS_COP.1(4)					X							X	X			
FCS_COP.1(5)													X		X	
FCS_RNG.1													X			
FDP_ACC.1									X							
FDP_ACF.1	X	X							X		X	X		X		X
FDP_DAU.1															X	
FDP_RIP.1							X	X								
FDP_UCT.1				X				X								
FDP_UIT.1				X				X								
FIA_AFL.1		X	X						X		X	X		X		X
FIA_UAU.1(1)			X						X		X					
FIA_UAU.1(2)		X	X						X			X				
FIA_UAU.1(3)			X						X					X		
FIA_UAU.1(4)			X						X					X		
FIA_UAU.1(5)			X						X							X
FIA_UAU.4								X			X	X		X	X	X
FIA_UAU.5(1)		X							X		X	X				X
FIA_UAU.5(2)									X					X		
FIA_UID.1											X	X		X		X
FMT_MOF.1(1)	X								X					X		
FMT_MOF.1(2)	X								X					X		
FMT_MSA.1				X					X							
FMT_MSA.3	X								X					X		
FMT_MTD.1(1)	X								X					X		
FMT_MTD.1(2)		X														
FMT_MTD.1(3)	X								X					X		

Security Objectives / Security Functional Requirements	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting _esidual_ Info	O.Replay_ Prevention	O.Access_ Control	O.handling_ Info_ Leakage	O.BAC	O. EAC	O. IC Chip	O. PAC	O. AA	O. SAC
FMT_MTD.1(4)	X								X					X		
FMT_MTD.1(5)	X								X					X		
FMT_MTD.3					X			X				X	X			
FMT_SMF.1	X				X											
FMT_SMR.1	X															
FMT_UNO.1										X			X			
FPT_FLS.1						X							X			
FPT_ITI.1			X	X												
FPT_PHP.3													X			
FPT_TST.1						X							X			

6.3.2 Security Assurance Requirements Rationale

The security assurance level of this Security Target was selected as EAL5+(ADV_IMP.2, ALC_DVS.2, AVA_VAN.5) by considering the value of assets protected by the TOE and level of threats, etc.
EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.
EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

This ST augmented assurance components partially higher than EAL5 as follows.

- ADV_IMP.2 Complete mapping of the implementation representation of the TSF
- ALC_DVS.2 Sufficiency of security measures
- AVA_VAN.5 Advanced methodical vulnerability analysis

6.3.3 Rationale of Dependency

(Table 23) shows dependency of TOE functional components.

(Table 23) Dependency of TOE Functional Components

No.	Functional Component	Dependency	Ref. No.
1	FCS_CKM.1(1)	[FCS_CKM.2(1) or FCS_CKM.2(2) or FCS_COP.1(3)] FCS.CKM.4	[4, 5, 11] 8
2	FCS_CKM.1(2)	[FCS_CKM.2(3) or FCS_COP.1(1)] FCS.CKM.4	[6, 9] 8
3	FCS_CKM.1(3)	[FCS_CKM.2(4) or FCS_COP.1(3)] FCS.CKM.4	[7, 11] 8
4	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)] FCS_CKM.4	[1] 8
5	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)] FCS_CKM.4	[1] 8
6	FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(2)] FCS_CKM.4	[2] 8
7	FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[3] 8
8	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1) or FCS_CKM.1(2) or FCS_CKM.1(3)]	1, 2, 3
9	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1) or FCS_CKM.1(2) or FCS_CKM.1(3)] FCS_CKM.4	[1, 2, 3] 8
10	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1) or FCS_CKM.1(2) or FCS_CKM.1(3)] FCS_CKM.4	[1, 2, 3] 8
11	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[none] 8
12	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)] FCS_CKM.4	1 8
13	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[none] 8
14	FCS_RNG.1	-	-
15	FDP_ACC.1	FDP_ACF.1	16
16	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	15 34
17	FDP_DAU.1	-	-
18	FDP_RIP.1	-	-
19	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	none 15

No.	Functional Component	Dependency	Ref. No.
20	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	15 none
21	FIA_AFL.1	FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.1(3), FIA_UAU.1(4), FIA_UAU.1(5)	22,23,24, 25,26
22	FIA_UAU.1(1)	FIA_UID.1	30
23	FIA_UAU.1(2)	FIA_UAU.1(1) or FIA_UAU.1(5)	22, 26
24	FIA_UAU.1(3)	FIA_UID.1	30
25	FIA_UAU.1(4)	FIA_UID.1	30
26	FIA_UAU.1(5)	FIA_UID.1	30
27	FIA_UAU.4	-	-
28	FIA_UAU.5(1)	-	-
29	FIA_UAU.5(2)	-	-
30	FIA_UID.1	-	-
31	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	41 42
32	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	41 42
33	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	15 41 42
34	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	33 42
35	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	41 42
36	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	41 42
37	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	41 42
38	FMT_MTD.1(4)	FMT_SMF.1 FMT_SMR.1	41 42
39	FMT_MTD.1(5)	FMT_SMF.1 FMT_SMR.1	41 42
40	FMT_MTD.3	FMT_MTD.1(1)	35
41	FMT_SMF.1	-	-
42	FMT_SMR.1	FIA_UID.1	30
43	FPR_UNO.1	-	-
44	FPT_FLS.1	-	-
45	FPT_ITI.1	-	-
46	FPT_PHP.3	-	-
47	FPT_TST.1	-	-

The dependency of EAL5 provided in CC is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in (Table 24).

(Table 24) Dependency of Added Assurance Components

No.	Assurance Component	Dependency	Ref. No.
1	ADV_IMP.2	ADV_TDS.3 ALC_TAT.1 ALC_CMC.5	EAL4 EAL4 None(EAL6)
2	ALC_DVS.2	None	-
3	AVA_VAN.5	ADV_ARC.1 ADV_FSP.4 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1	EAL5 EAL4 EAL4 1 EAL5 EAL5 EAL4

7. TOE Summary Specification

This chapter describes the TOE Security Functionality covering the requirements of the previous chapter.

7.1 TOE Security Functionality

This chapter gives an overview of the TOE Security Functionality composing the TSF.
In the following (Table 25), all TOE Security Functionality are listed and if appropriate, a SOF claim is stated.

(Table 25) TOE Security Functionality

TSF	Description
SF.PAC_AUTH	PAC mutual authentication, PAC session key generation, PAC personalization and management authentication
SF.BAC_AUTH	BAC mutual authentication, BAC session key generation
SF.SAC_AUTH	SAC mutual authentication, SAC session key generation
SF.CHIP_AUTH	EAC-CA authentication
SF.TERMINAL_AUTH	EAC-TA authentication
SF.SEC_MESSAGE	Secure messaging structure, Secure communication channel mechanism.
SF.ACTIVE_AUTH	AA authentication
SF.ACC_CONTROL	Personalization Agent access control, Personalization Agent personalization and management Inspection System access Control
SF.RELIABILITY	Residual Information management, Vulnerability countermeasure, TSF self test, Data integrity
SF.IC	IC chip security function

7.2 SF.PAC_AUTH (PAC security mechanism)

This TSF includes a PAC security mechanism for the Personalization agent for the Inspection System.

The PAC security mechanism provides authority control of the security role to the Personalization agent in the issue stage. This TSF is composed of PAC mutual authentication, PAC session Key generation, and PAC personalization and management authentication.

7.3 SF.BAC_AUTH (BAC security mechanism)

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

7.4 SF.SAC_AUTH (SAC security mechanism)

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

7.5 SF.CHIP_AUTH

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

7.6 SF.TERMINAL_AUTH

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

7.7 SF.SEC_MESSAGE

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

7.8 SF.ACC_CONTROL

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

7.9 SF.ACTIVE_AUTH

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

7.10 SF.RELIABILITY

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

7.11 SF.IC

This TSF provides the several security functionality of IC Chip. (Table 26) shows the TSF in IC chip.

(Table 26) TSF of IC Chip

TSF of IC chip	Description
Security detectors	Voltage detector, Frequency detector, Active Shield Removal detector and Inner Insulation Removal detector, Light and laser detector, Temperature detector, Voltage Glitch detector
MPU	Memory partition and access control service
RWG, RCG, Variable clock	Random Wait Generator(RWG), Random Current Generator(RCG), variable clock services for protecting from power analysis attack
Data Scramble	RAM/EEPROM data bus scramble
TRNG	TRNG Service according to AIS311 Class P2 and French metric
TDES	TDES Encryption/ Decryption, Retail-MAC security cryptographic operation service
AES	AES Encryption/ Decryption, CMAC security cryptographic operation service
RSA	RSA, RSA-CRT, DH security cryptographic operation service
ECC	ECDSA, ECDH security cryptographic operation service

SHA	SHA security cryptographic operation service
etc	CPU register integrity protection service

[Works Cited]

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010

[5] Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents –Extended Access Control (EAC), Version 1.11, TR-03110, 2005.8

[6] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)

[7] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, November 2011

[8] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009

[9] Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007

[10] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004 , Version 3.1, Revision 3, July 2009

[11] ISO/IEC 11770-3: Information technology — Security techniques — Key management -- Part 3: Mechanisms using asymmetric techniques, 2008

[12] PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009

[14] ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008

[15] ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11

[16] Security Target Lite of Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-Bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software Version 2.1(2012. 9)

[17] ePassport Protection Profile V2.1, June 10, 2012, KECS-PP-0163a-2009

[Abbreviations]

AA	Active Authentication
BAC	Basic Access Control
BIS	BAC Inspection System
BSI	Bundesamt für Sicherheit in der Informationstechnik / German Federal Office for Information Security
CA	Chip Authentication
CAN	Card Access Number
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CMAC	Cipher-based Message Authentication Code
COS	Card Operating System
CSCA	Country Signing Certification Authority
CSN	Chip Serial Number
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
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EIS	EAC Inspection System
FIPS	Federal Information Processing Standard
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IS	Inspection System

ISO	International Organization for Standardization
IT	Information Technology
KDF	Key Derivation Function
KDM	Key Derivation Mechanism
KECS	Korea Evaluation and Certification Scheme
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NIST	National Institute of Standards and Technology
PA	Passive Authentication
PAC	Personalization Access Control
PIS	PA Inspection System
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA-CRT	RSA Chinese Remainder Theorem
SAC	Supplemental Access Control
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOD	Security Object of Document
SOF	Strength of Function
SPA	Simple Power Analysis
SSC	Send Sequence Counter
ST	Security Target
TA	Terminal Authentication
TDES	Triple-DES
TOE	Target of Evaluation
TSF	TOE Security Functionality

[Glossary]

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

BIS(BAC/SAC Inspection System)
The IS implemented with the BAC(or SAC) 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

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

Card Access Number(CAN)
Password derived from a shot number printed on the front side of the datapage

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

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, SAC 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

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.

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