LG CNS

XSmart e-Passport V1.3 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target Lite V1.1

Document ID: XSMART_ASE_LITE_ENG

[Modification History]

Version	Modified Item	Modification Detail	Date	Approval
1.0		-Initial Draft	2014.01.20	Han Kwanghee
1.1		-Final release	2014.01.21	Han Kwanghee

[Table of Contents]

[List of Tables]

[List of Figures]

Referenced Documents

[CC]	Common Criteria for Evaluation of IT Security, Version 3.1r4, CCBM-2012-09-001
[CEM]	Common Criteria Methodology for Evaluation of IT Security, Version 3.1r4, CCBM-2012-09-004,
[SCG]	Guide to Preparing Submission Material of SmartCard Evaluation for Developers, Korea Internet & Security Agency, 2005. 4
[OSCPP]	E-Passport Protection Profile, Version 2.1, National Intelligence Service, 2010. 6
[JCSPP]	Java Card System Protection Profile Collection, Version 1.0b, Sun Microsystems, Inc. August 2003
[ICPP]	Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002, Atmel Smart Card IC, Hitachi Europe Ltd., Infineon Technologies AG, and Philips Semiconductors, July 2001.
[MRTDPP]	Machine Readable Travel Document with ,,ICAO Application", Basic Access Control, Version 1.0, BSI-PP-0017, BSI, August 2005
[MRTDEPP]	Machine Readable Travel Document with ,,ICAO Application", Extended Access Control, Version 1.1, BSI-PP-0026, BSI, September 2006
[ICST]	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 2.2, 2012. 09. 26
[GPCS]	GlobalPlatform Card Specification, Version 2.1.1, GlobalPlatform Inc., March 2003.
[VGP]	VISA GlobalPlatform 2.1.1 Card Implementation Requirements, Version 1.0, VISA, May 2003.
[VGPG]	VISA GlobalPlatform 2.1.1 Card Production Guide, Version 1.0, VISA, February 2004.
[JCVM]	Java Card Platform 2.2.1, Virtual Machine Specification, Sun Microsystems, October 2003.
[JCRE]	Java Card Platform 2.2.1, Runtime Environment Specification, Sun Microsystems, October 2003.
[JCAPI]	Java Card Platform 2.2.1, Application Programming Interface, Sun Microsystems, October 2003.
[MRTD]	Machine Readable Travel Document, Part 1 Machine Readable Passport, Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability, Doc 9303, ICAO, Sixth Edition, 2006
[EAC]	Advanced Security Mechanism for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, BSI, 2007

Definition of Terms

Among the terms used in this security target, those that are also used in common criteria follow the common criteria.

DV : Document Verifier

Certification authority that generates and issues IS certificate.

Personalization Agent

Authority which receives ePassport identification information and such from receipt/issuance authority, generates SOD by electronically signing it, record them on IC chip of ePassport, then generate TSF data for ePassport, stores them on protected memory area of IC chip of ePassport, and operates PA-PKI and/or EAC-PKI.

SOD : Document Security Object

Generated digital signature of Personalization agent on the identification/authentication information of ePassport recorded in the ePassport issuance Phase. Object implemented as Signed Data Type of "RFC 3369 Cryptographic Message Syntax, 2002.8" and encoded in DER method.

Executable File

A collection of executable modules stored on EEPROM.

Executable Module

The executable code of a single application program.

Ciphertext Only Attack

An attack attempting deciphering based on the ciphertext collected by threat agents.

Encryption Key

The key used in TDES to encrypt data for data exposure protection.

Passport Digital signature

Unique information signed on ePassport with the digital signature generation key issued by the issuance authority for issuance and confirmation of recorded items of electronically processed passport.

Passport Digital signature System

A system to provide authentication service such as issuance of certificates necessary for passport digital signature and management of authentication-related records.

Reverse Engineering

Analyzing completed products in detail to understand and reproduce the basic design concepts and applied technologies.

Certificate

Electronic information signed electronically on digital signature verification key by issuance authority to confirm and prove that the digital signature generation key uniquely belongs to the owner.

Applet

Application program executed on the Javacard platform written in Javacard language.

ePassport

A passport containing contactless IC chip with identification and other information of the passport applicant according to the international standard prescribed by ICAO and ISO.

ePassport User Data

Includes ePassport identification information and ePassport authentication information.

ePassport Identification Information

Includes ePassport application basic information and bio information.

ePassport Applicant Basic Information

Visually distinguishable information and other identification information printed on the identification information page of ePassport stored on ePassport IC chip in LDS structure.

ePassport Applicant Bio Information (Sensitive Data)

The fingerprint and/or iris information of the ePassport applicant stored on ePassport IC chip in LDS structure.

ePassport Applied Data

Includes ePassport user data and TSF data.

ePassport Application Program (MRTD Application)

A program to load on the ePassport IC chip that is programmed according to LDS of ePassport standard and provides security mechanisms such as BAC and EAC.

ePassport Authentication Information

The information stored on ePassport IC chip in LDS format to support ePassport security mechanism including SOD for PA, chip authentication public key for EAC, AA chip authentication public key, etc.

ePassport IC Chip (MRTD Chip)

A contactless IC chip including ePassport application programs and the IC chip operating system necessary for operating them and supporting communication protocol according to ISO/IE 14443.

ePassport TSF Data

The information stored on the protected memory area of ePassport IC chip to support ePassport security mechanism.

KDM : Key Derivation Mechanism

The mechanism to generate encryption key and MAC key from seed value using hash algorithm.

KDF : Key Derivation Function

A function generating encryption key and MAC key from seed value using hash algorithm.

Inspection

The procedure where the immigration authority inspects the ePassport IC chip presented by the ePassport carrier and confirms the identity of the ePassport carrier through verification of ePassport IC chip.

IS : Inspection System

An information system which implements optical MRZ reading capability and security mechanisms (PA, BAC, EAC, AA, etc.) to support ePassport inspection and consists of the terminal for RF communication with ePassport IC chip and the system sending commands to the ePassport IC chip through this terminal and processing the responses.

AA (Active Authentication)

A security mechanism where ePassport IC chip verifies its authenticity by signing on the random number transferred from the inspection system and the inspection system verifies the authenticity of ePassport IC chip by verifying the signature value.

Application Protocol Data Unit (APDU)

A data format for exchanging packaged data between SmartCard and terminal. APDU is divided into command APDU and response APDU. TPDU of subordinate layer according to the communication protocol between the card and the terminal exists and APDU is converted to appropriate TPDU and then transferred.

BAC (Basic Access Control)

A security mechanism which implements the symmetric-key-based entity authentication protocol for mutual authentication of ePassport IC chip and inspection system and the symmetric-key-based entity authentication protocol for generating session key needed to establish a secure messaging between them.

BAC Mutual Authentication

Mutual authentication of ePassport IC chip and inspection system according to ISO 9798-2 symmetric-key-based entity authentication protocol.

BAC Session Keys

BAC session keys and MAC keys generated using key derivation mechanism from the random value for session key generation shared in the BAC mutual authentication

BAC Secure Messaging (BAC Secure Messaging)

A messaging which encrypts the transfer data with BAC session key, generates message authentication value with BAC session MAC key before transfer to provide confidentiality and integrity of transfer data.

BAC Authentication Key (Document Basic Access Keys)

BAC authentication key and MAC key generated by using key derivation mechanism from MRZ (passport number, passport number check digit, date of birth, date of birth check digit, expiry date, expiry date check digit) for mutual authentication of ePassport IC chip and inspection system.

BAC inspection system (BIS : BAC Inspection System)

An inspection system which implements BAC, PA, and AA security mechanism.

CSCA Certificate

A certificate proving the validity of digital signature verification key against the digital signature generation key of PA-PKI highest authentication authority by self-signing the digital signature verification key with the digital signature generation key of the PA-PKI highest authentication authority.

CVCA Link Certificate

A certificate where the EAC-PKI highest authentication authority generates a new CVCA certificate before the expiration of CVCA certificate and digitally signs with the digital signature generation key corresponding to the previous CVCA certificate.

CVCA Certificate

A certificate which includes the value where EAC-PKI highest authentication authority digitally signs the digital signature verification key with the digital signature generation key of EAC-PKI highest authentication authority to prove the validity of CVCA link certificate and DV certificate.

CVM (Cardholder Verification Method)

A SmartCard user authentication method using a password, which is a personal identification number.

DFA (Differential Fault Analysis)

A method of inferring the encryption key by inducing malfunction through enforced deformation of voltage or clock in the encryption calculation process.

DPA (Differential Power Analysis)

A method of inferring the encryption key by collecting a large amount of power usage consumed in the encryption calculation process and performing a statistical analysis.

DS certificate (Document Signer Certificate)

A certificate of Personalization agent signed with the digital signature generation key of PA-PKI highest authentication authority used by inspection system to verify SOD of PA security mechanism.

DV certificate

A certificate including the value of digitally signing digital signature verification key of inspection system with digital signature generation key of DV to prove the validity of digital signature verification key of inspection system.

EAC (Extended Access Control)

A security mechanism composed of EAC-CA procedure for chip authentication and EAC-TA procedure for inspection system authentication where only EAC-supporting inspection system (EIS) can read the bio information of ePassport applicant to control access to ePassport applicant bio information stored on ePassport IC chip.

EAC Session Key

EAC session encryption key & MAC key used to establish a secure messaging for transfer protection of ePassport applicant bio information and generated using KDF with the key shared with EIS through Ephemeral-Static DH key distribution protocol in the EAC-CA process as seed value.

EAC Chip Authentication Public Key and EAC Chip Authentication Private key

DH key pair used by the ePassport IC chip to authenticate itself to the EAC-supporting inspection system in EAC-CA process and recorded in the ePassport IC chip issuance Phase by the Personalization agent.

EAC inspection system (EIS : EAC Inspection System)

An inspection system which implements BAC, PA and EAC security mechanisms with the option of AA.

EAC-CA (EAC-Chip Authentication)

A security mechanism which implements Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) so that EAC-supporting inspection system can authenticate ePassport IC chip through key confirmation for the EACP chip authentication public key and private key of ePassport IC chip and the temporary public key and private key of EIS.

EAC-TA (EAC-Terminal Authentication)

A security mechanism which implements a digital-signature-based Challenge-Response authentication protocol where ePassport IC chip authenticates EIS with ePassport IC chip using IS certificate where ePassport IC chip uses IS certificate to verify the value where EIS digitally signed the temporary public key with its digital signature generation key in EAC-CA process.

EAC-PKI Highest Authentication Authority (CVCA : Country Verifying Certification Authority)

Highest authentication authority which generates and issues CVCA certificate, CVCA link certificate, and DV certificate by securely generating digital signature key in the EAC-PKI passport digital signature system to support EAC security mechanism.

EEPROM (Electrically Erasable Programmable Read-Only Memory)

A non-volatile memory device which retains data for a long period of time without power; a storage area storing major properties to be protected by the operating system and ePassport application programs such as ePassport user data and portions of TSF data.

EF.COM

Includes LDS version information and tag information for Data Groups.

EF.CVCA

EF-type file specifying the list and reading rights for CVCA digital signature verification key identification information needed for verification of CVCA certificate validity

EMA (Electromagnetic Analysis)

A method inferring the encryption key collecting and analyzing the electromagnetic wave leaked from cryptographic calculation process.

Grandmaster Chess Attack

An attack which uses the IC chip that can perform the relay for messaging between ePassport IC chip and the inspection system to disguise as the ePassport IC chip.

GP Registry

A storage area for information necessary for management of the operating system and installed application programs.

IC Chip (Integrated Circuit Chip)

An important semi-conductor to process the functions of SmartCard and an processor including four function units of mask ROM, EEPROM, RAM, and I/O port.

ICAO-PKD

A storage are for DS certificates operated and managed by ICAO which distributes online

the requested DS certificate of the corresponding country when requested by domestic/foreign inspection systems.

IS certificate

A certificate used to verify the digital signature value transferred to inspection system by ePassport IC chip in EAC-TA process where DV digitally signed digital signature verification key of EIS with digital signature generation key.

LDS (Logical Data Structure)

A logical data structure defined in ePassport specification to store ePassport user data on ePassport IC chip.

MAC Key (Key for Message Authentic Code)

A key used in symmetric key ciphering algorithm according to ISO 9797 in order to generate message authentication code to prevent data counterfeiting/falsification.

PA (Passive Authentication)

A security mechanism which proves that the identification information recorded on the ePassport is not counterfeit or falsified by verifying the has value of the corresponding ePassport user value according to the reading rights of the ePassport access control policy where the inspection system with DS certificate verifies the digital signature signed on SOD.

PA-PKI Highest Authentication Authority (CSCA : Country Signing Certification Authority)

The highest authentication authority which generates and issues CSCA certificate and DS certificate by securely generating digital signature key in the PA-PKI passport digital signature system to support PA security mechanism.

Probing

An attack exploring data by plugging in a probe to the IC chip.

RAM (Random Access Memory)

A volatile memory device that retains recorded information only while power is supplied and a storage area for storing data temporarily used by the operating system or application programs.

ROM (Read-Only Memory)

A type of semiconductor memory device where the contents can be read but not modified.

SCP02 (Secure Channel Protocol 02) mutual authentication

A symmetric-key-based entity authentication protocol defined in GlobalPlatform 2.1.1 Card Specification.

SCP02 Session Key

A session key generated in the SCP02 mutual authentication process.

SPA (Simple Power Analysis)

A method of inferring encryption key by collecting and analyzing the power consumption in the cryptographic /< process.

COB(Chip On Board)

As semiconductor fabrication technology, the way a microchip or a die attach directly to the final circuit board or electrically interconnection

1. Security Target Introduction

This section provides the information necessary for identifying and controlling security target and TOE.

1.1. Security Target Reference

Subject	XSmart e-Passport V1.3 on S3CT9KCW/S3CT9KC/S3CT9K9 Security Target V1.2
ST Identification	XSMART e-Passport V1.3_ASE_V1.2.docx
Version	V1.2
Product Name	XSmart V2.3
Author	LG CNS
Evaluation Criteria	Information Protection System Common Criteria V3.1r4
Evaluation Assurance Level	EAL5+ (ADV_IMP.2)
Protection Profile	ePassport Protection Profile V2.1
IC Chip	S3CT9KW/S3CT9KC/S3CT9K9
Keywords	ePassport, MRTD, ICAO

Table 1 Reference of Security Target

1.2. TOE Reference

TOE	XSmart e-Passport V1.3 on S3CT9KW/S3CT9KC/S3CT9K9
Component of TOE	- XSmart e-Passport V1.3 - User's Guide for Management(XSmart e-Passport V1.3_AGD_V1.1)
TOE code identification	-ROM code identification : XSMART_e-Passport_V1.3_S3CT9KW_01.rom (impelemented on S3CT9KW) XSMART_e-Passport_V1.3_S3CT9KC_01.rom (impelemented on S3CT9KC) XSMART_e-Passport_V1.3_S3CT9K9_01.rom (impelemented on S3CT9K9) -EEPROM code idenfication : XSMART_e-Passport_V1.3_S3CT9KW_01.eep (impelemented on S3CT9KW) XSMART_e-Passport_V1.3_S3CT9KC_01.eep(impelemented on S3CT9KC) XSMART_e-Passport_V1.3_S3CT9K9_01.eep (impelemented on S3CT9K9)
IC Chip	S3CT9KW/S3CT9KC/S3CT9K9

Reference of IC Chip Authentication	ANSSI-CC-2012/70

Table 2 Reference of TOE

1.3. TOE Outline

This document is the security target regarding the XSmart e-Passport V1.3 on S3CT9KW/S3CT9KC/S3CT9K9(referred to as **"XSmart e-Passport V1.3"** hereafter), which is the composite TOE composed of a COS in charge of the chip operating system and an IC chip as a part of hardware.

S3CT9KW/S3CT9KC/S3CT9K9 is a contact/contactless IC chip of Samsung Electronics and it is certified CC authentication separately from BSI.

- The OS is composed of Java layer, GP layer, Native OS (NOS).
  GP Layer performs to manage life cycle of applications such as loading, installing, and deletion of applications according to 'GP Standard'
  In accordance with 'Java Card Standard', Java layer provides functions such as firewall, deletion residual information, memory management, transaction process and so on. NOS actually performs I/O handling according to ISO/IEC 7816 and ISO/IEC 14443 and memory management through the chip interface.
  After ePassport application is installed, the Operating system only performs the functionality of passport, it becomes impossible to install or delete applications anymore.
- EPassport application is an implementation of [MRTD] standards defined by International Civil Aviation Organization (ICAO) and [EAC] standard of BSI. After ePassport program is loaded on ROM for the first time, it is active throughout the processing of installation and issuance.
- S3CT9KW/S3CT9KC/S3CT9K9 are the contact/contactless IC chips from Samsung Electronics Co. that have been certified by the Common Criteria from CEA-LETI.
- PP used: Eurosmart Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035
- TOE: S3CT9KW/ S3CT9KC/ S3CT9K9 revision 2
- Certification Number: ANSSI-CC-2012/72
- Assurance Level: CC EAL 5+ (AVA_VAN.5, ALC_DVS.2)
- Certified cryptography library: TORNADO 2MX2 Secure RSA/ECC library v2.2

1.4. TOE Description

XSmart V2.3, ePassport product of LG CNS, is the type of manufactured COB loading TOE on S3CT9KW/S3CT9KC/S3CT9K9, Samsung Electronics IC chip.
The type of COB, component of the e-passport booklets, is to be made with the inlay, and is used after issuing.

TOE is composed of the software format of the OS, ePassport application programs and IC chip as part of H/W.
TOE manages ePassport application data such as ePassport MRZ area information, ePassport applicant basic information, bio information including ePassport applicant face and fingerprints, encryption key for authentication and secure communication, etc. and performs access control to ePassport user data by authenticating Personalization agent and inspection systems.

The ePassport application programs comprising TOE implement 'ePassport standard' and 'EAC standard' with Javacard technology. ePassport application program, at the issuance Phase, uses SCP02 security mechanism of card manager to authenticate the Personalization agent and grants writing rights for ePassport user data and TSF data, and at the usage Phase, uses BAC and EAC security mechanism to authenticate inspection system and grants reading rights for ePassport user data, performing access control. Also, to allow inspection systems to detect counterfeiting and delicacy of ePassport, AA functions are provided.

The OS, which is the other part of TOE, is composed of Javacard platform and card manager. Javacard platform is a runtime environment which allows multiple application programs including ePassport application program to safely execute on a single IC chip. Javacard platform, according to 'Javacard standard,' provides functions of firewall, memory management such as deletion of residual information, transaction processing and such, and provides the encryption key management and cryptographic calculation functions through API for application programs to perform cryptographic calculations. Card manager performs management function for OS. Card manager, according to 'GP standard' and 'VGP standard,' provides manager rights authentication through SCP02 security mechanism, OS management of loading/installation/deletion of application program, life cycle management of OS and application programs and such.
TOE becomes ePassport-only after installation of ePassport, so it is impossible to

load/install/delete other applications.

The composition elements of the IC chip TOE is based on includes IC chip hardware, dedicated IC chip firmware, and cryptographic calculation software library for RSA/ECC calculation. TOE actives the active shield, temperature sensor, voltage sensor, filter and such of the IC chip hardware, and provides security measures against physical attacks by encrypting ROM, RAM, and EEPROM. When generating random numbers, random number generator (TRNG) is used, and when performing TDES cryptographic calculation, secure DES module is used to countermeasure attacks such as SPA and DPA. Also, ECC cryptographic calculation software library is used to perform ECDH encryption key exchange and ECDSA digital signature generation/verification calculations and countermeasure attacks such as SPA and DPA, and RSA cryptographic calculation software library is used to generate digital signature and countermeasure attacks such as SPA and DPA.

1.4.1. TOE Type

ePassport which uses XSmart e-Passport V1.3 is designated as the standard by ICAO (International Civil Aviation Organization) and ISO (International Standard Organization). This standard is composed of the physical part dealing with the mechanical recognition through bare eye and OCR (Optical Character Recognition) for identification information, picture, passport number, and MRZ(Machine Readable Zone) printed on the passport, and the logical part dealing with the electronic management of traveler information using contactless IC chip of ISO 14443 standard.

The physical part of ePassport is composed of the contactless IC chip and antenna for wireless communication attached to the passport booklet or the cover. The contactless IC chip used in the ePassport is called ePassport IC chip (MRTD Chip), which contains the IC chip OS (COS) which supports resource management for hardware elements of IC chip, IT technology for electronic storage and processing of ePassport identification information, and information protection technology and ePassport application. The hardware of ePassport IC chip is generally composed of CPU, auxiliary arithmetic unit, I/O port, RAM, ROM, EEPROM and such. Figure 1 illustrates the physical composition of ePassport.

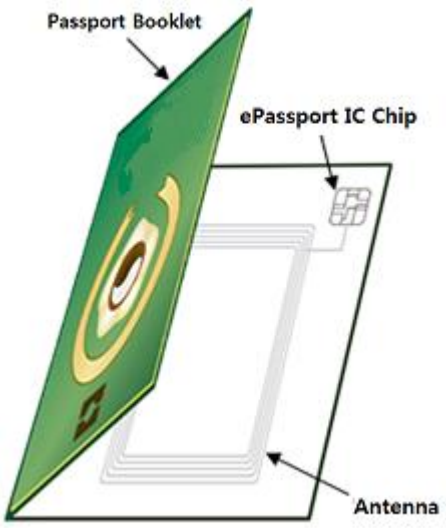


Figure 1 Physical Composition of ePassport

The logical part of ePassport includes not only the picture and personal information of the traveler and MRZ (Machine Readable Zone) information written on the passport, but also bio information data such as face, fingerprint, and iris for bio-recognition and encryption key for authentication between the inspection systems and ePassport and for secure message communication.

1.4.2. ePassport System

Figure 2 illustrates the entire composition diagram of ePassport system.

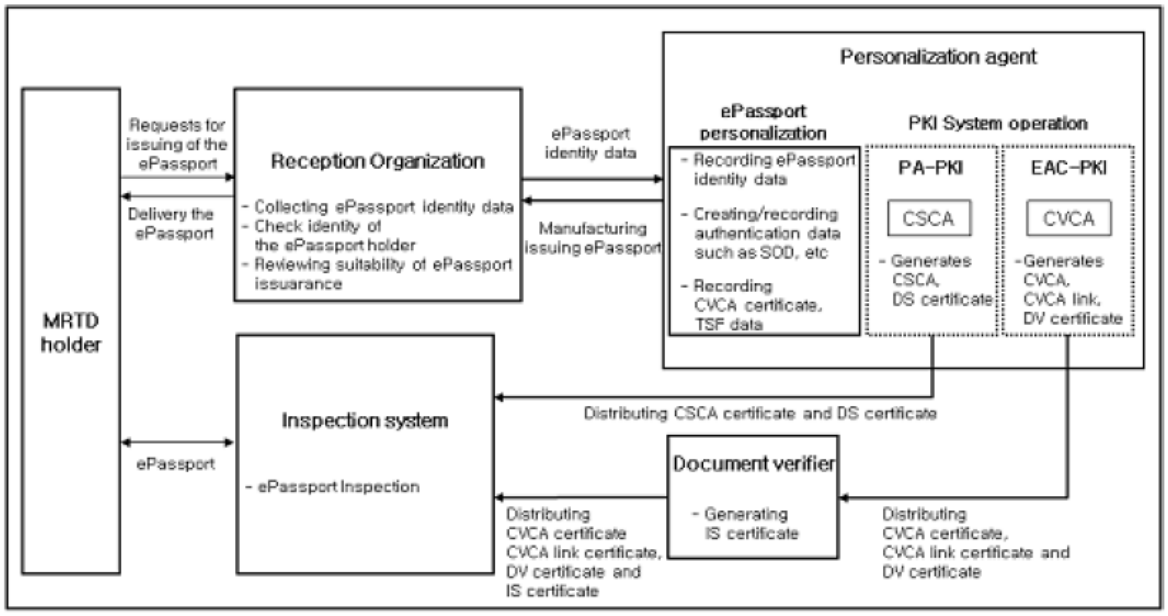


Figure 2 Entire Composition Diagram of ePassport System

ePassport applicant requests the issuance of ePassport and receives the ePassport properly issued according to ePassport issuance policy. ePassport applicant carries the issued ePassport and when going through domestic/foreign immigration, presents the ePassport to the immigration officer for inspection. During immigration, according to the ePassport immigration policy of each country, either the officer verifies the ePassport or unattended inspection system verifies ePassport.

The registration/issuance agency collects the basic/bio information of the ePassport applicant and cooperates with the police and such relevant agencies to confirm the identity and requests the issuance of ePassport with such information.

Personalization agent digitally signs the ePassport user data (ePassport identification information and authentication information) to generate security object (referred to as **"SOD"** hereafter), and records on the ePassport IC chip along with the ePassport identification information received from the registration/issuance agency. Also, the ePassport TSF data is recorded onto the protected memory area, and the ePassport IC chip is embedded to the passport and then the ePassport is produced and issued. The details of the data recorded on the ePassport is explained in Table 4.

The Personalization agent generates the digital signature key necessary for falsification/counterfeiting verification of ePassport user data stored on the ePassport IC chip, and performs the authentication tasks such as generation/issuance/management of CSCA certificate and DS certificate according to the authentication task regulations of passport digital signature system. According to the ePassport issuance policy, if EAC security mechanism is supported, the digital signature key necessary for verification of access rights for ePassport applicant bio information, and the authentication tasks such as generation/issuance/management of CVCA certificate, CVCA link certificate and DV certificate are performed. Items regarding establishment of passport digital signature and authentication tasks such as authentication server, key generation devices, physical/procedural security measures and such follow the ePassport issuance policy.

Authentication authority generates the IS certificate using CVCA certificate and DV certificate and then provides them to the inspection systems.

The types of certificates used in ePassport system is as follows in 오류! 참조 원본을 찾을 수 없습니다..

Use	Passport Digital	Certificate Subject	Certificate

	Signature System,		
Verification of ePassport user data falsification/counterfeiting	PA-PKI	PA-PKI highest authentication authority	CSCA certificate
		Personalization agent	DS certificate
Verification of access rights to ePassport applicant bio information	EAC-PKI	EAC-PKI highest authentication authority	CVCA certificate
			CVCA link certificate
		Authentication authority	DV certificate
		EAC inspection system	IS certificate

Table 3 Types of Certificates

1.4.3. TOE Scope

In this security target, the life cycle of TOE is divided into Phases among the entire life cycle for ePassport of development, production, issuance, usage and such, and TOE operation environment and the scope of physical/logical TOE are defined as follows.

In this security target, TOE is described as including the operating system loaded on ePassport IC chip, the ePassport application, the IC chip hardware which is the component of the IC chip, the firmware, RSA/ECC cryptographic calculation library.

Figure 3 illustrates the scope of TOE.

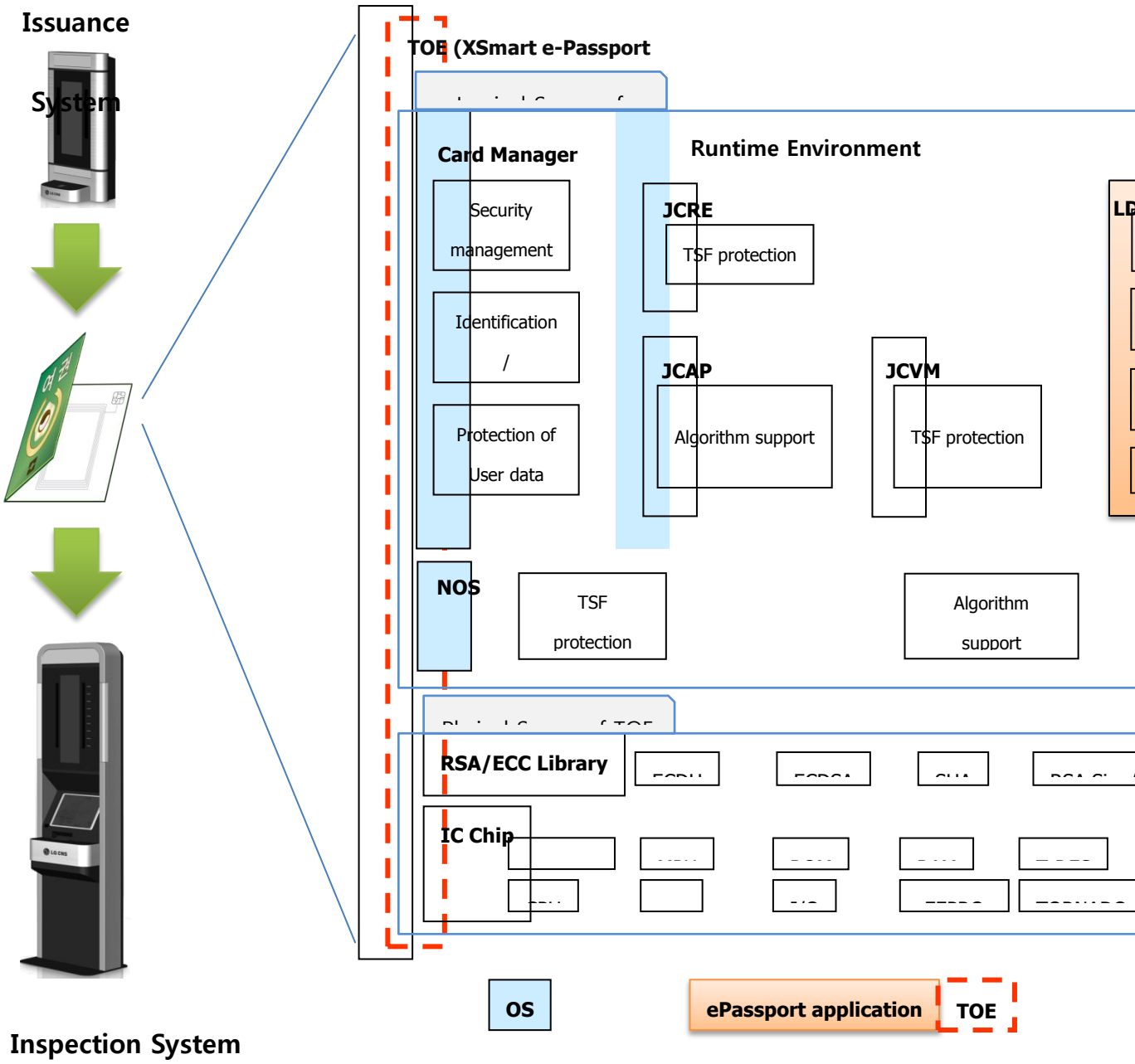


Figure 3 TOE Scope

Application Notes :

SHA-1, a hash function, is provided as software implementation.

1.4.3.1. Life Cycle and Operation Environment of TOE

TOE Life Cycle

Table 4 shows the IC chip life cycle divided into ePassport IC chip life cycle and TOE life cycle Phase by Phase, and the delivery process is omitted. From the life cycle of Table 3 Types of Certificates, TOE development process is Phase 1 (development) and 2 (production), and TOE operation environment corresponds to 3 (issuance), 4 (usage), and 5 (termination).

Phase	ePassport IC Chip Life Cycle	TOE Life Cycle
1 (Development)	① IC chip developer designs the IC chip and develops dedicated IC chip S/W	
		② S/W developer uses IC chip and dedicated IC chip S/W to develop TOE (OS, ePassport application program)
2 (Production)	③ IC chip producer performs the ROM Masking of TOE, chip identifier recording, and production of IC chip.	
		④ ePassport producer performs initialization of COS ⑤ ePassport producer installs ePassport application program to generate user data storage area in EEPROM according to ePassport LDS standard ⑥ ePassport producer embeds IC chip to the passport booklet
3 (Issuance)		⑦ Personalization agent records Personalization agent identification and authentication information on OS ⑧ Personalization agent generates SOD by digitally signing the ePassport identity information ⑨ Personalization agent records the ePassport identity information, authentication information (including SOD) and TSF data onto ePassport application program
4 (Usage)		⑩ Inspection system communicates with TOE to authenticate ePassport and confirm the identity of the carrier
5 (Termination)		⑪ Personalization agent changes the status of ePassport so that it is no longer usable

Table 4 Life Cycle of ePassport IC Chip and TOE

TOE Operation Environment

Figure 4 TOE Operation Environmentillustrates the TOE operation environment at ePassport issuance and usage Phase with the major security functions of TOE and the external entities interacting with TOE (Personalization agent, inspection system).

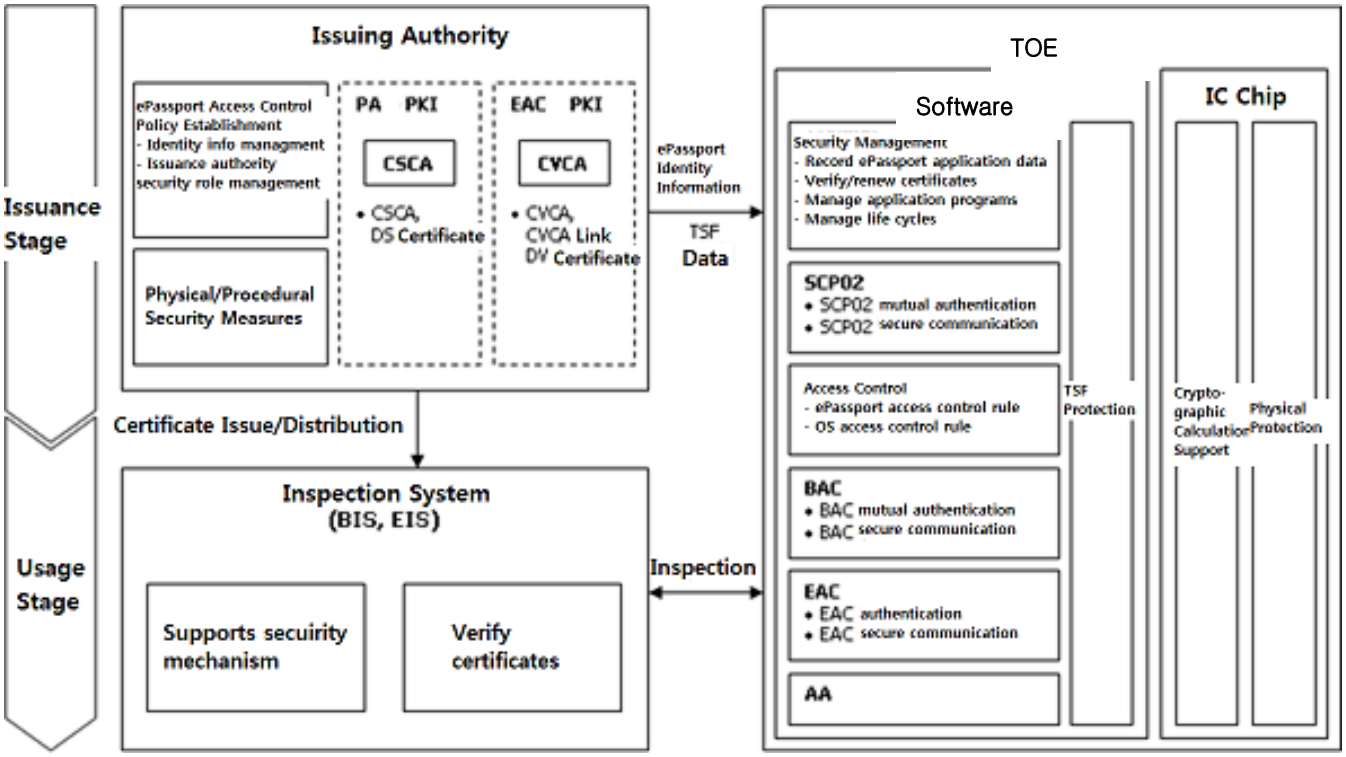


Figure 4 TOE Operation Environment

1.4.3.2. Physical Scope of TOE

Figure 5 illustrates the physical scope of TOE.

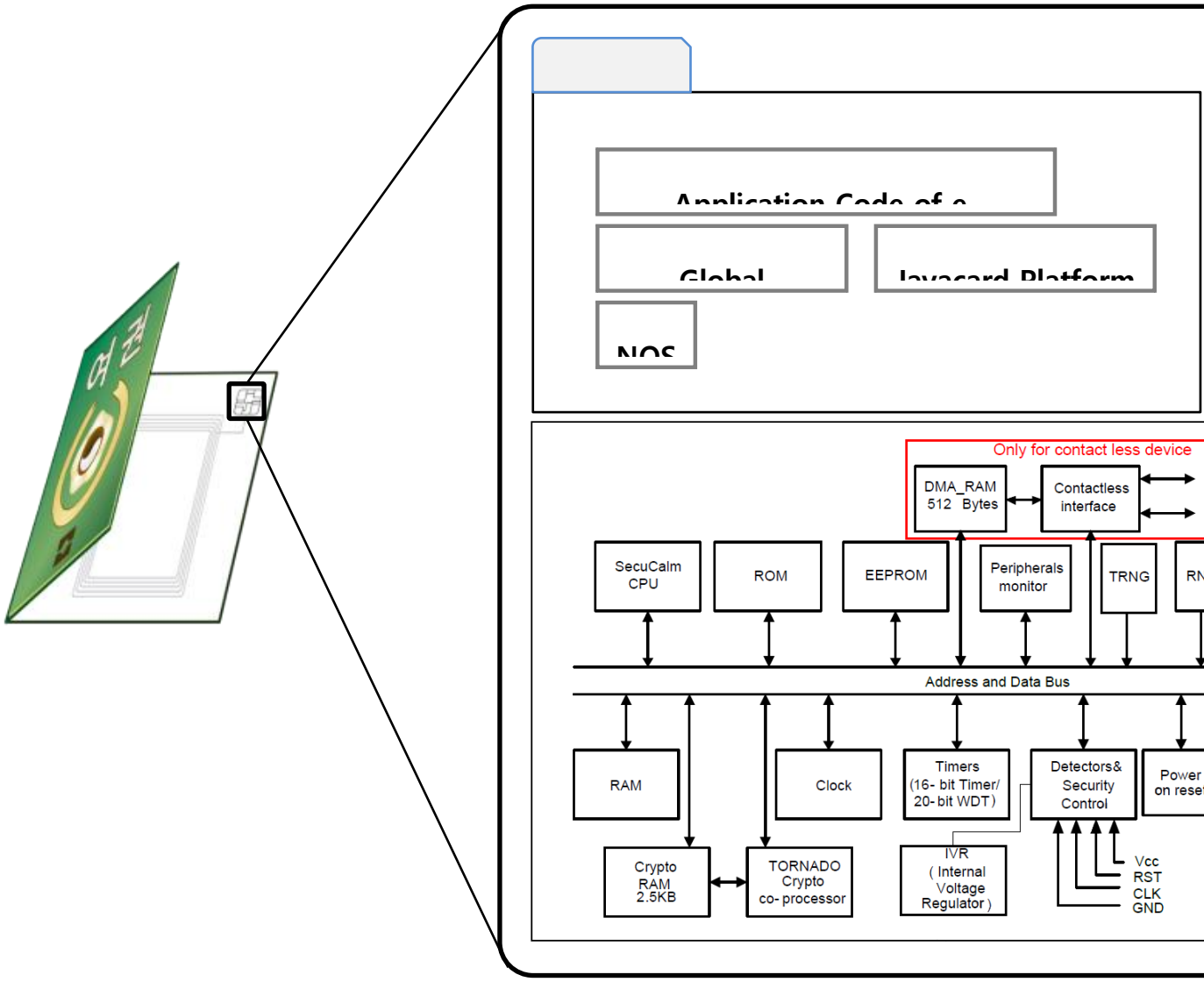


Figure 5 Physical Scope of TOE

The physical scope of TOE includes the IC chips, S3CT9CW/S3CT9KC/S3CT9K9. In addition to that, IC chips includes the OS, e-Passport Application Code, e-Passport User Data and TSF Data. Also, the components of IC chips are SecuCalm CPU, TORN ADO Crypto Co-Processor, I/O, Memory (RAM, ROM, EEPROM) and various H/W functions.

TOE defined in ST is Chip Operation System (COS), e-Passport Application Code, e-Passport User and TSF data, and H/W functions of an IC chip.

In the case of COS, it is loaded onto ROM. Also, NOS which directly controls the IC chip function, Global Platform (GP) and JavaCard Platform which provide the open platform environment and Application Code of e-Passport which is compatible with ICAO Doc 9303, EAC V.11 loaded onto ROM.

However, biometric data (face, fingerprint) and TSF data (Authenticate key, Seed key for BAC, private key for CA) of e-Passport are loaded onto EEPROM.

At last, S3CT9CW/3SCT9KC/S3CT9K9 of Samsung Electronics, which is the composition element of the IC chip, is a product certified with CCRA EAL5+ assurance level, and the composition elements included in the authentication area are IC chip hardware, firmware recorded on ROM, and cryptographic calculation software library as shown in the following.

IC Chip Hardware

- 16 bit microprocessor (CPU)
- 6KB RAM, 2.5KB Crypto RAM, 384KB ROM
- EEPROM : 144KB(S3CT9KW), 80KB(S3CT9KC), 40KB(S3CT9K9)
- Memory protection unit (MPU), random number generator (RNG), timer (TIM), DES calculation engine(DES), big number calculation engine (TORNADO 2Mx2)
- RF interface, address and data bus (ADBUS)

Software Library for Cryptographic Calculation RSA/ECC Library

- **RSAECC Library**
  - ☐ ECDSA key generation
  - ☐ ECDSA sign/verify
  - ☐ ECDH key sharing
  - ☐ RSA key generation
  - ☐ RSA sign/verify
  - ☐ Hash function(SHA-224, SHA-256, SHA-384, SHA-512)
- Non-Determinant Random Number Generator (TRNG)

Figure 6 IC Chip Hardware Composition Diagramillustrates the composition diagram of IC chip hardware.

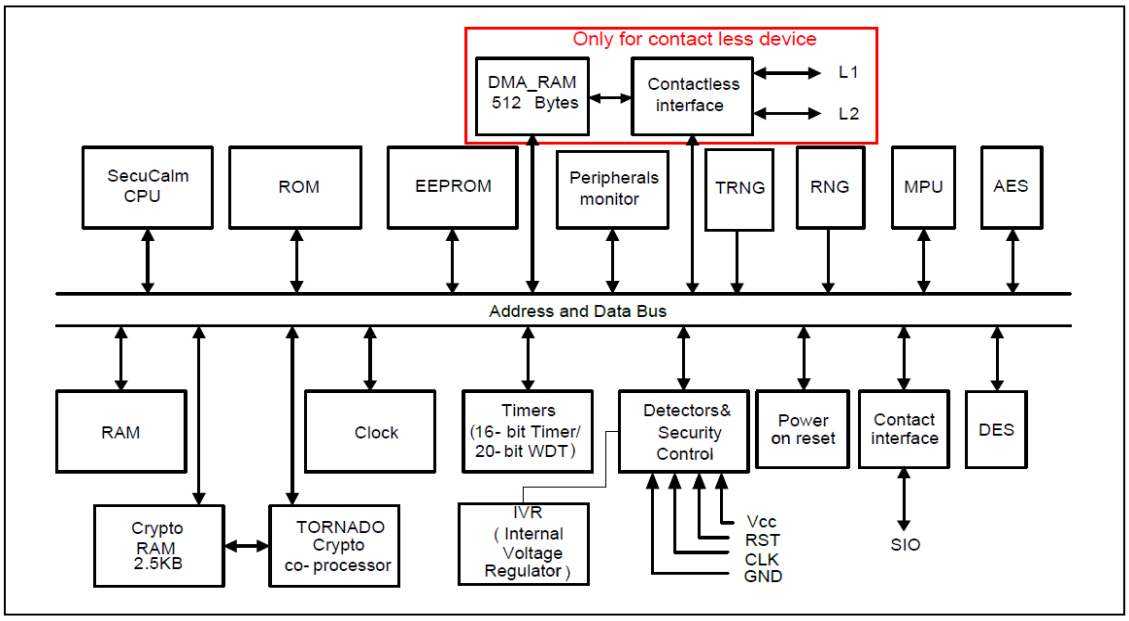


Figure 6 IC Chip Hardware Composition Diagram

The IC chip hardware among the IC chip composition elements provide DES module used in the symmetric key encryption according to DES and TDES standards, Tornado 2MX2 Crypto module used in the asymmetric key encryption, physical security measures such as shield, temperature sensor, voltage sensor, and filter, and non-determinant hardware random number generator. The firmware provides IC chip hardware management function such as EEPROM recording and the function for hardware testing, and the cryptographic calculation software library provides calculations such as digital signature generation/verification for hash value, ECDH key exchange, ECC/RSA key pair generation, and ECC/RSA public key verification.

The cryptographic algorithms provided by the IC chip composition elements are used in the following cryptographic calculations.

DES Module

- TDES data encryption and decryption calculation
- Retail MAC and Full Triple DES MAC generation and verification calculation

TRNG Module

- Calculation of big number necessary for the ECC/RSA cryptographic calculation process

RSA/ECC Cryptographic Library

- Key distribution calculation for EAC session key distribution in EAC process
- Digital signature verification calculation for certificate verification in EAC process
- Hash calculation using SHA algorithm
- Digital signature generation calculation using chip authentication private key in AA process

ECC/RSA Library V2.2

The ECC/RSA library certified with CCRA EAL5+ assurance level is a part of IC chip composition elements and the IT environment of TOE not included in TOE scope.

ECC Library

The ECC library provides functions such as ECDSA digital signature generation and verification, ECDH key exchange, ECC key pair generation, and ECC public key verification. In TOE, however, only the functions of ECDSA digital signature generation and verification and ECDH key exchange are used. The ECC library includes countermeasures against SPA, DPA, EMA, DFA and such.

RSA Library

The RSA library provides functions such as RSA digital signature generation, verification, and key pair generation. The RSA library also includes countermeasures against SPA, DPA, EMA, DFA and so on.
Also, this library includes functions of SHA-224, SHA-256, SHA-384, SHA-512.

1.4.3.3. Logical Scope of TOE

TOE communicates with the inspection system according to the communication protocol defined in ISO/IEC 14443-4. TOE implements the security mechanism defined in 'ePassport Standard' and 'EAC Standard,' and provides access control and security management functions. Also, it provides self-protection functions for TSF such as self-test, secure state preservation, and separation of area.

Figure 7 shows the logical scope of TOE.

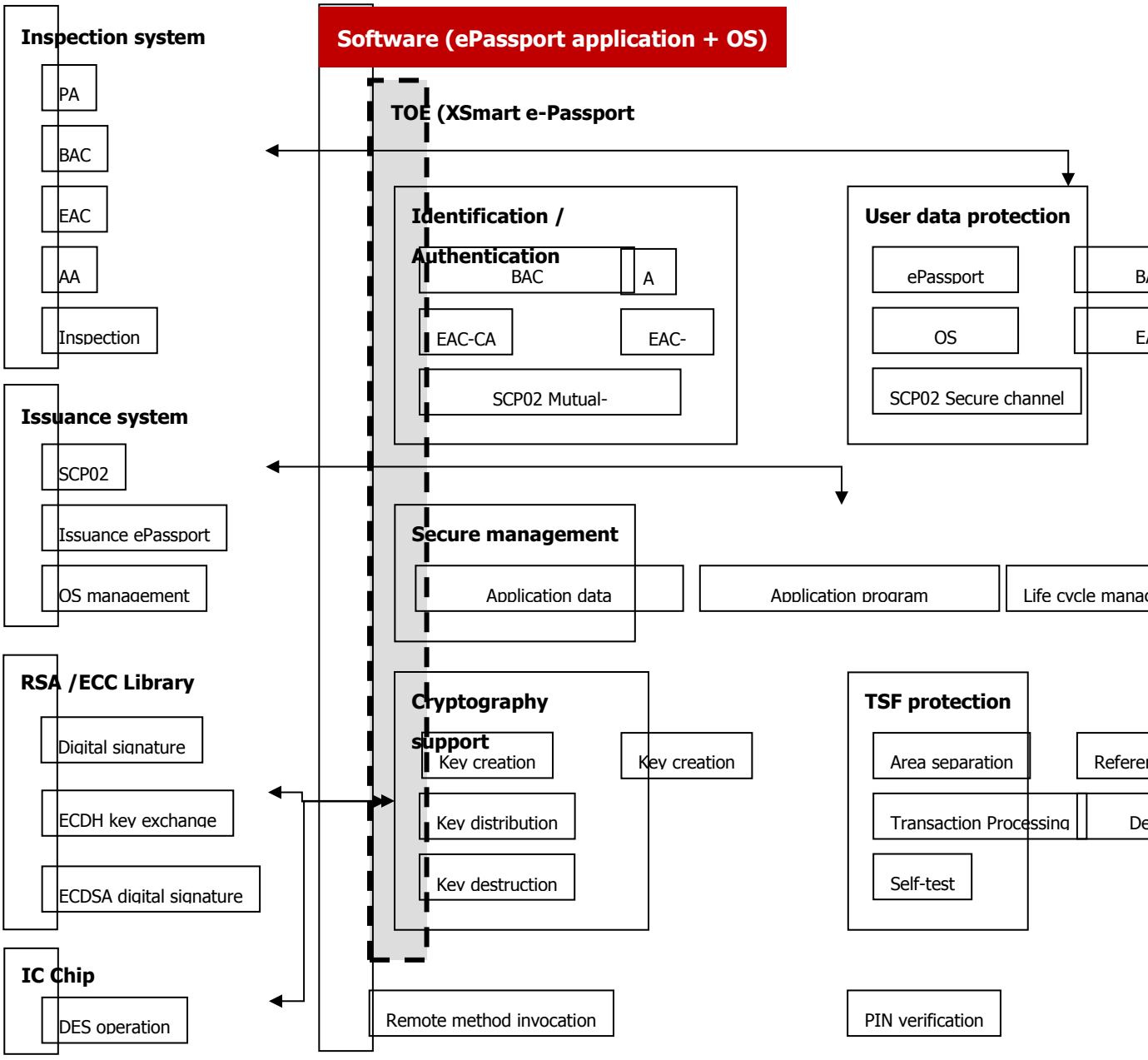


Figure 7 Logical Scope of TOE

ePassport Application Program (LDS Application)

ePassport application program is an IC chip application program which implements the function for storing/processing ePassport identity information and the security mechanism to securely protect it according to the LDS (Logical Data Structure) format defined in 'ePassport standard' and 'EAC standard.' ePassport application program provides security management function for ePassport application program to the authenticated Personalization agent through SCP02 security mechanism provided in the card manager,

and permits access to ePassport user data through BAC and EAC secure messaging only when the access rights were acquired through BAC and EAC secure messaging. Also, AA security mechanisms are provided as methods to judge counterfeiting of ePassport user data.

Card Manager

Card manager provides management function of OS defined in 'GP standard' and 'VGP standard.' Card manager provides functions such as loading/installation/deletion of application programs, management of Personalization agent basic information and authentication information, and management of OS and application program life cycle .
After installation of the LDS, card manager does not work anymore absolutely, so additional installation or deletion of applications is impossible.

Among the functions of card manager implemented in XSmart e-passport V1.3, the Global PIN which can be used commonly by all application programs on the card is a function for verifying user password which is not used in the TOE, and therefore is excluded from TOE scope.

Runtime Environment

The runtime environment provides the functions of JCRE, JCVM, and JCAPI which are the composition elements of Javacard platform defined in 'Javacard standard.' The runtime environment provides TSF protection functions such as firewall, transaction processing, and removal of residual information for secure operation of ePassport application program, and provides cryptographic calculation function to ePassport application program.
The remote invocation (RMI) provided by Javacard virtual machine (JCVM) and the owner PIN verification provided by Javacard API to manage the unique PIN for each application program are not used in TOE and therefore are excluded from TOE scope.

Native OS(NOS)

The Native OS provides functions including hardware-dependent implementation, IC chip start-up, resource management of the hardware, implementation of the algorithm, and chip secure setting. Also, CVM (Cardholder Verification Method) of NOS which is responsible for practical implementation of global PIN in card manager and owner PIN of Javacard API in NOW is also excluded from TOE scope.

Assets

TOE provides information protection functions such as confidentiality, integrity,

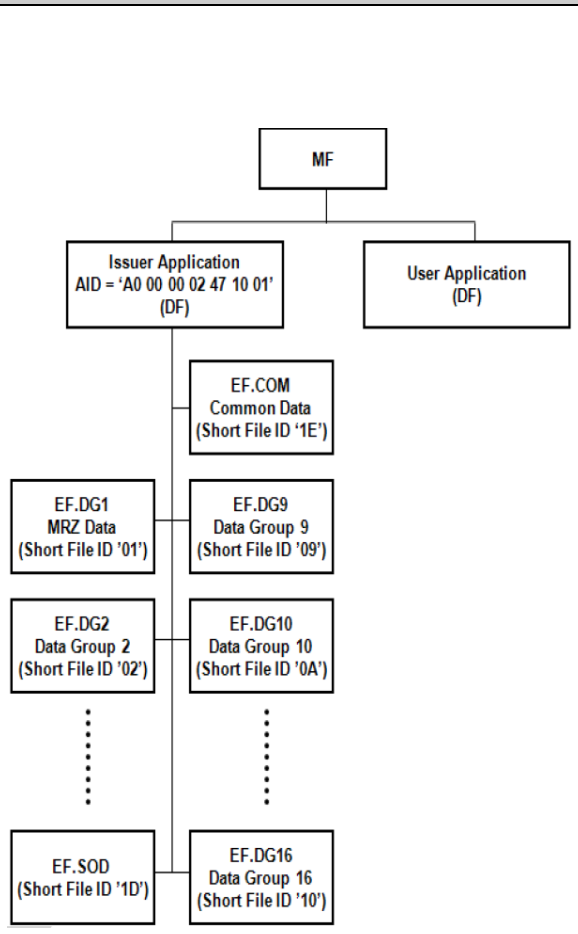
authentication, and access control in order to protect the TOE assists of the following Table 5.

Category			Description	Storage Area
User Data	ePassport Identity Information	Personal Data of the ePassport holder	Data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13, and EF.DG16	EF File
		Biometric Data of the ePassport holder	Data stored on EF.DG3 and EF.DG4	
	ePassport Authentication Data		EF.SOD, EAC chip authentication public key(EF.DG14), AA chip authentication public key(EF.DG15)	
	EF.CVCA		List of CVCA digital signature verification key identification information used by TOE to authenticate IS in EAC-TA process	
	EF.COM		LDS version information, list of used DG tags	
ePassport TSF Data	EAC chip authentication private key		Chip private key used by TOE to prove that ePassport IC chip is not counterfeited in the EAC-CA process	Secure Memory
	CVCA certificate		Certificate of highest authentication authority issued by EAC-PKI at the time of ePassport issuance	
	CVCA digital signature verification key		Public key of CVCA certificate newly generated by certificate renewal after ePassport issuance Phase	
	Current date		At the time of ePassport issuance, ePassport issuance date is recorded, but at the ePassport usage Phase, it is updated internal by TOE to the most recent issue date of CVCA link certificate, DV certificate or IS certificate of issuance country	
	BAC authentication key		BAC authentication encryption key, BAC authentication MAC key	
	BAC session key		BAC session encryption key, BAC session MAC key	Temporary Memory
	EAC session key		EAC session encryption key, EAC session MAC key	
OS User Data	Personalization agent Basic data		Issuing-authority-related basic data such as Personalization agent identification information, serial number, and issuance date	OS Memory
	Personalization agent authentication		Confidential key for SCP02 mutual authentication	

	data		
	Executable file	Application program executable file code loaded on the OS	
	Application program	Application program instance installed on the OS	
OS TSF Data	GP registry	OS management data such as installed application program ID, application program life cycle state, and application program rights	
	OS Life Cycle	OS life cycle state value	
	SCP02 session key	SCP02 session encryption key and MAC key	Temporary Memory

Table 5 TOE Assets

LDS where ePassport User Data of TOE is stored defines the file structures of MF, DF, EF, and Table 6 shows the contents of EF.DG1 ~ EF.DG16 where a portion of TOE user data is stored.

category	DG	Contents	LDS Structure
Detail(s) Recorded in MRZ	DG1	Document type	
		Issuance State	
		Name (of Holder)	
		Document number	
		Check Digit-Doc Number	
		Nationality	
		date of birth	
		Check Digit-DOB	
		Sex	
		Date of expiry or Valid Until date	
		Check Digit DOE/VUD	
		Composite Check Digit	
Encoded Identification Features	DG2	Encoded face	
	DG3	Encoded finger(s)	
	DG4	Encoded Iris(s)	
Miscellaneous	DG5	Displayed Portrait	
	DG6	-	
	DG7	Displayed signature	

	DG8	-	
	DG9	-	
	DG10	-	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	-	
	DG14	EAC chip authentication public key	
	DG15	AA Digital Signature Verification Key	
	DG16	Person(s) to Notify	

Table 6 LDS Contents where TOE User Data is Stored

Security Mechanism

TOE provides information protection functions such as confidentiality, integrity, access control, and authentication for protection of ePassport user data and TSF data such as ePassport identity information and ePassport authentication information. Such information protection functions are implemented with SCP02 security mechanism of 'GP Standard,' BAC security mechanism of 'ePassport Standard,' and EAC security mechanism of 'EAC Standard'. Table 7 summarizes ePassport security mechanisms.

ePassport security mechanism				IT Security characteristic of the TOE
Security Mechanism	Security characteristic	Cryptography	Cryptographic Key/Certificate Type	
PA	ePassport User Data Authentication	A function performed by the inspection system; no cryptographic calculation on TOE's part	N/a: a function performed by the inspection system	Access control for SOD • Read rights: BIS, EIS • Write rights: Personalization agent
BAC	BAC mutual authentication	Symmetric Key-Based Entity Authentication Protocol TDES-CBC SHA-1 Retail MAC	BAC authentication key (Encryption Key, MAC key)	TOE decrypts IS transfer value, performs MAC calculation, and verifies to confirm if inspection system has access rights TOE encrypts, performs MAC calculation, and sends to inspection system to verify itself

	BAC Key Distribution	Symmetric Key-Based Key Distribution Protocol TDES-CBC SHA-1 Retail MAC	BAC session key (Encryption Key, MAC key)	Generate BAC session key by using KDF from the exchanged key-sharing random number based on TDES-based key distribution protocol
	BAC secure messaging	ISO Secure Messaging	BAC session key (Encryption Key, MAC key)	Encrypt with BAC session key, generate MAC and send message Verify MAC with BAC session key, decrypt, and receive message
EAC	EAC-CA	ECDH Key Distribution Protocol	EAC chip authentication public key EAC chip authentication private key	TOE performs Ephemeral-static D-H Key Distribution Protocol
	EAC secure messaging	ISO Secure Messaging	EAC session key (Encryption Key, MAC key)	Encrypted communication using the EAC session key shared in the EAC-CA process
	EAC-TA	ECDSA-SHA-1 ECDSA-SHA-224 ECDSA-SHA-256	CVCA certificate CVCA link certificate DV certificate IS certificate	IS certificate verification using certificate chain and link certificate Digital signature verification regarding EIS transfer message for EIS authentication
AA	ePassport Piracy Verification	RSA-SHA-1	AA authentication public key AA authentication private key	TOE generates and sends digital signature to inspection system to authenticate itself
SCP02	SCP02 mutual authentication	Secure Channel Protocol 02 Full Triple DES MAC TDES-CBC Retail MAC	Personalization agent authentication information SCP02 session key	TOE performs MAC calculation on the TOE random number and Personalization agent's random number and sends TOE random number and MAC value to Personalization agent to authenticate itself TOE performs MAC calculation on the TOE random number and Personalization agent's random

				number and verifies the MAC value of the Personalization agent.
	SCP02 secure messaging	SCP02 Secure Messaging TDES-CBC Retail MAC	SCP02 session key	Encrypted communication using SCP02 session key used in SCP02 mutual authentication

Table 7 ePassport Security Mechanisms

Security Function

TOE provides security functions such as identification and authentication, user data protection, security management, TSF protection, and cryptography support.

Identification and Authentication

TOE provides SCP02 mutual authentication, BAC mutual authentication, EAC-CA, EAC-TA, AA as the methods for identification and authentication.

<SCP02 Mutual Authentication>

SCP02 (Secure Channel Protocol 02) is the security mechanism for authenticating Personalization agent with write, add, and renew rights for ePassport applicant identity information and TSF data in TOE, and includes SCP02 mutual authentication and secure messaging. TOE and Personalization agent use Personalization agent authentication information and SC (Sequence Counter) to generate SCP02 session key, and then mutually verify the MAC value for the exchanged random numbers to perform mutual authentication. If the SCP02 mutual authentication fails, the session is terminated, and if it succeeds, TOE forms a secure messaging using SCP02 session key.

<BAC Mutual Authentication>

The inspection system supporting BAC uses BAC authentication key generated from the optically read MRZ and TOE either generates BAC authentication key from MRZ information of DG1 or uses stored BAC authentication key to each encrypt the generated random number values and exchange. The inspection system supporting BAC and the TOE perform mutual authentication by confirming the exchanged random number value. If the BAC mutual authentication fails, the session is terminated.

<EAC-CA>

EAC-CA implements the Ephemeral-static DH key distribution protocol to provide EAC session key distribution and chip authentication. TOE sends EAC chip authentication public key so that it can be authenticated by the inspection system, and uses the temporary

public key received from the inspection system to perform key distribution protocol. If the EAC-CA succeeds, TOE forms EAC secure messaging using EAC session key. Even if EAC-CA fails, BAC secure messaging is maintained, and the inspection system can confirm that TOE has been pirated.

<EAC-TA>
EAC-TA implements the digital-signature-based Challenge-Response authentication protocol so that TOE can authenticate the inspection systems supporting EAC. The value which the inspection system digitally signed on the temporary public key used in EAC-CA process is verified by TOE with IS certificate to authenticate the inspection system. When TOE receives CVCA link certificate, DV certificate, and IS certificate from the inspection system supporting EAC, it uses the CVCA digital signature verification key in protected memory area to verify CVCA link certificate, and checks the expiry date of CVCA link certificate and renews the CVCA digital signature verification key and the current date within TOE when necessary. Once TOE confirms that the certificate is appropriate by verifying IS certificate, it permits read access by the inspection system to the ePassport applicant bio information and sends through EAC secure messaging.

<AA>
AA (Active Authentication) implements the digital-signature-based Challenge-Response authentication protocol so that the inspection system can authenticate TOE. Once TOE generate the digital signature with AA chip authentication private key in protected memory area on top of the received value provided by the inspection system, the inspection system verifies with the EF.DG15 AA chip authentication public key acquired through BAC secure messaging or EAC secure messaging to authenticate TOE. AA is a security mechanism providing a method to verify the authenticity of TOE.

User Data Protection
TOE provides access control and secure messaging for user data protection.

<SCP02 Secure Messaging >
TOE establishes SCP02 secure messaging using the SCP02 session key generated in the SCP02 mutual authentication process to perform secure communication with the Personalization agent which performed the SCP02 mutual authentication successfully. When sending data through this channel, data is encrypted using TDES encryption algorithm to provide confidentiality and MAC Verification using Retail MAC algorithm provides integrity.

<BAC Secure Messaging >
TOE confirms the reading rights of inspection system for ePassport applicant Basic Information through BAC mutual authentication, and then generates BAC secure messaging using the BAC session key shared through BAC key distribution to transfer ePassport applicant basic information securely. When sending data through this channel, data is encrypted using TDES encryption algorithm to provide confidentiality and MAC Verification using Retail MAC algorithm provides integrity.

<EAC Secure Messaging >
TOE generates EAC secure messaging using EAC session key shared through EAC key distribution of EAC-CA process to perform secure communication with the inspection system. When sending data through this channel, data is encrypted using TDES encryption algorithm to provide confidentiality and MAC Verification using Retail MAC algorithm provides integrity.

<OS Access Control>
TOE provides access control function which permits only the Personalization agent that acquired management rights by succeeding in SCP02 mutual authentication to have the application program management function to load/install/delete executable code and application program to the OS at the ePassport issuance Phase and usage Phase and the write rights to the basic information of the Personalization agent. Also, the access control function which prohibits performance of all operations except reading the Personalization agent basic information at the termination Phase of TOE life cycle is provided.

<ePassport Access Control>
TOE provides access control function which permits only the Personalization agent that acquired management rights by succeeding in SCP02 mutual authentication to perform the write functions for ePassport user data and TSF data. Also, access control function provided for ePassport user data reading rights based on the access rights of inspection system granted through performance of security mechanisms at the ePassport usage Phase.

Security Management
TOE limits the method of managing the security properties of user and user data of the ePassport application program and OS and the TSF data such as session key, authentication key and GP registry to the authorized Personalization agent and defines

this as the security role. Also, several security management functions such as CVCA certificate and current date renewal and secure messaging identification information initialization are performed by TSF itself.

TSF Protection

TOE provides functions such as reference monitor, domain separation, deletion of residual information, transaction processing, and self-test for TSF protection.

<Reference Monitor>

TOE guarantees that for all APDU commands which are the external interface of TOE, the access control will not be bypassed but invoked every time to protect TSF from interference and invasion by an unauthorized subject.

<Domain Separation>

TOE provides Javacard Firewall within Javacard virtual machine to separate the area use such as other application programs and the area where ePassport application program executes.

After LDS application is installed in TOE, all functions such as additional installation, deletion, and retrieval of other applet are prohibited. Therefore, the area is separated from other unauthorized subjects because only ePassport area exists in TOE.

<Deletion of Residual Information >

TOE provides the function to delete residual information when allocating resources to the object or retrieving resources back from the object so that previous information is not employed for not only temporarily generated information in the temporary memory area such as BAC session key, EAC session key, SCP02 session key, and random number, but also the information generated in the protected memory are such as BAC authentication key.

<Transaction Processing>

TOE provides transaction function to detect TSF malfunctioning when a power-supply shut-off or enforced termination of TSF service during operation occurs, and resume TSF service from the state before the malfunctioning.

<Self-Test>

TOE performs TSF data change detection and measure functions, and performs self-test to

verify the integrity of stored TSF data and executable code. Also, when a failure from self-test or an abnormal operation status from the IC chip is detected, it maintains secure state so that malfunctioning of TSF does not occur.

Cryptography Support

TOE provides hash calculation, and provides random number generation, key exchange calculation operation mode, encryption/decryption calculation operation mode, and MAC and digital signature calculation operation mode using the IC chip and cryptographic calculation library.

TOE guarantees that encryption-related information cannot be found by abusing physical phenomenon (current, voltage, electromagnetic change, etc.) occurring during performance of cryptographic calculation, and provides a method to verify integrity for the encryption key. The cryptographic algorithms included in TOE are as shown in Table 8.

Classification	Algorithm	Use
Hash	SHA-1, SHA-224, SHA-256	• BAC session key and EAC session key generation
Key Exchange	ECDH operation mode	• Generation of shared confidential information in EAC-CA
Encryption/ Decryption	TDES operation mode	• confidentiality of SCP02 secure messaging • confidentiality of BAC secure messaging • confidentiality of EAC secure messaging • SCP02 session key generation
MAC	Retail MAC operation mode	• Integrity of SCP02 secure messaging • Integrity of BAC secure messaging • Integrity of EAC secure messaging
	Full Triple DES MAC operation mode	• Generation of authentication information of SCP02 mutual authentication
Digital Signature	ECDSA-SHA-1 operation mode	• Verification of digital signature in EAC-TA
	ECDSA-SHA-224 operation mode ECDSA-SHA-256 operation mode	• Verification of digital signature in EAC-TA
	RSA-SHA-1 operation mode	• Creation of digital signature in AA

Table 8 Cryptographic Algorithms used by TOE

Functions Excluded from TOE

The functions provided in XSmart e-Passport V1.3 but excluded from TOE are function for integrity and verification of global PIN and PIN of application program, remote method invocation (RMI).

The function for integrity and verification of global PIN and application program PIN is not used in the TOE of ePassport and thus excluded from the TOE scope.

The RMI (Remote Method Invocation) function which supports execution of application programs within TOE from outside of TOE is not used in ePassport application program and thus excluded from the TOE scope.

1.5. Preparation Rules

This security target uses English terms to clearly convey several meanings and acronyms. The used notation, shape, and preparation rules follow the common criteria of information protection system (referred to as **"common criteria"** hereafter).

Common criteria allows repetition, allocation, selection, and elaboration that can be performed in a security function requirement. Each operation is used in this security target.

Repetition
Used when a component is repeated multiple times with various application of an operation. The result of a repetition operation is denoted with the repetition number in parentheses, as in (repetition number).

Selection
Used to select one or more selection items provided by the common criteria for information protection system. The result of selection operation is denoted *underlined and italicized*.

Elaboration
Used to limit the requirement further by adding details to the requirement. The result of an elaboration operation is denoted in **bold**..

Allocation
Used to allocate a certain value to a non-specified parameter (e.g. password length). The result of an allocation operation is denoted in brackets, as in [allocated value].

1.6. Composition of Security Target

The referenced documents are described for cases where the user needs background or related information beyond what is mentioned in this security target, and the definition of terms are provided to aid in understanding of the terms or acronyms used in this security target.

Section 1 of Security Target Introduction provides TOE outline information necessary for identification of security target.

Section 2 of Conformance Claim claims conformance to Common Criteria, Protection Profile, and Package, and describes the rationale of conformance claims and the method of conformance by the security target.

Section 3 of Security Problem Definitions describe the security problems of TOE and TOE operation environment from the perspectives of threats, organizational security policies, and assumptions.

Section 4 of Security Objectives describe the security objectives for TOE and the operation environment to countermeasure the threats identified in the security problem definitions, perform organizational security policies, and support assumptions.

Section 5 of Extended Component Definition identifies the extended security requirement of this security target and provides due explanation.

Section 6 of Security Requirements describe the function and assurance requirements the TOE of this security target must satisfy.

Section 7 of TOE Summary Specification describes the TOE security function and assurance method satisfying TOE security requirements.

2. Conformance Claim

This section describes the explanation of TOE and the product type, operation environment, and evaluation scope of TOE.

2.1. Common Criteria Conformance Claim

This Security Target claims conformance to

· Common Criteria for Information Technology Security Evaluation, part 1: Introduction and general model, Version 3.1r4, September. 2012, CCMB-2012-09-001

· Common Criteria for Information Technology Security Evaluation, part 2: Security functional requirements, Version 3.1r4, September. 2012, CCMB-2012-09-002

· Common Criteria for Information Technology Security Evaluation, part 3: Security assurance requirements, Version 3.1r4, September. 2012, CCMB-2012-09-003

as follows

· Part 2 Extension

· Part 3 Conformant

2.2. Protection Profile Claim

2.2.1. Protection Profile Re-establishment

The following are the items of security target which re-established the protection profile.

Security Environment

- A.inspection system
- T.RESIDUAL_INFO
- P.PERSONALIZATION_AGENT
- P.EPASSPORT_ACCESS_CONTROL

Security Objective

- O.Session Termination
- O.Access Control

Security Function Requirement

- FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FPR_UNO.1.

- FCS_CKM.2(1), FCS_CKM.4
- FDP_ACC.1(1), FDP_ACF.1(1), FDP_RIP.1, FDP_UIT.1
- FIA_AFL.1(1), FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.4, FIA_UAU.5
- FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(1), FMT_SMF.1, FMT_SMR.1
- FPT_FLS.1, FPT_ITI.1, FPT_TST.1

2.2.2. Protection Profile Additions

The items described below are additional to the protection profile for this security target.

Security Environment

- T.Personalization agent authentication reuse

Security Objective

- O.SCP02
- O.AA
- O.IC_Chip

security function requirement

- FCS_CKM.1(2), FCS_CKM.3, FCS_RNG.1
- FDP_ACC.1(2), FDP_ACF.1(2), FDP_DAU.1
- FIA_AFL.1(2), FIA_UAU.1(3)
- FMT_MOF.1(2), FMT_MTD.1(3), FPT_PHP.3

2.3. Package Claim

This Security Target is conforming to assurance package as follows

・Assurance Package : EAL5 augmented with (ADV_IMP.2)

2.4. Conformance Rationale

- Compliance protection profile : ePassport Protection Protection Profile V2.1
- Compliance type : demonstrable conformance

2.4.1. Rationale for Conformance of Security Problem Definitions

Re-established for this security target of 'ePassport Protection Profile' are T.RESIDUAL_INFO among the threats, A.inspection system among the assumptions, and P.PERSONALIZATION_AGENT, P.EPASSPORT_ACCESS_CONTROL among the organizational

security policies, and it conforms to the all the rest of security environment, and the additionally defined security environment is the threat of T.Personalization agent authentication reuse and the security policy of P.IC_Chip of the organization.

Re-established Security Environment

- A.inspection system: re-established so that BIS and EIS support AA.
- T.RESIDUAL_INFO: the residual information remaining from the process of recording and using the SCP02 session key on temporary memory is added as a threat and re-established.
- P.PERSONALIZATION_AGENT: re-established so that ePassport Personalization agent establishes the OS access control policy.
- P.EPASSPORT_ACCESS_CONTROL: the subjects of BIS and EIS cannot be distinguished at the identification Phase, and the performance of access control rule is possible with just the rights attributed to inspection systems, the subject divided into BIS and EIS is unified to inspection system and re-established.

Added Security Environment

T.Personalization agent authentication reuse: this threat is added where the threat agent reuses the random number delivered to the Personalization agent by TOE in the Personalization agent authentication process and attempts bypassing the Personalization agent authentication.

P.IC_Chip : The IC chip, a component of the TOE, provides the functions to protect the TOE from the IC chip cryptographic calculation and physical attacks.

A.Process_Sec_IC : The process between the delivery of the TOE by the manufacturer and the delivery to the end-consumer is secure by maintaining confidentiality and integrity of the TOE.

A.Plat_Appl : The Security IC Embedded Software which is loaded onto a low platform of the IC chip is designed by the authenticated procedure.

The following tables show that the threat, the security policy of the organization and the assumption defined on the security problem definitions are suggested based on that there is no contradiction between the composite-ST and the platform-ST.

Separation	Threat	Basis
PP scope	T.Eavesdropping	
	T.Fogery_Corruption_Personal_Data	
	T.BAC_ReplayAttck	
	T.Damage_to_Biometric_Data	
	T.EAC_CA_Bypass	
	T.IS_Certificate_Forgery	
	T.SessionData_Reuse	

	T.Skimming	
	T.Malfunction	
	T.Leakage_CryptographicKey_Info	
	T.MRTD_Reproduction	
	T.Residual_Info	The threat on the SCP02 session key, which is recorded in the temporary memory and remained after using it, is added.
	T.TSF_Data_Modification	The threat on the TSF data being accessed, while recording through the Inspection System, is added.
Addition	T.IC_Chio_Forgery	The treat agent may reuse the random number, which is sent from the TOE to Personalization agent, and bypass the authentication process of Personalization agent.

Table 9 Relation of threat between the composite-ST and the platform-ST

Separation	Security policy of Organization	Basis
PP Scope	P.International_Compatibility	The applied security policy of the organization based on the PP scope
	P.Security_Mechanism_Application_Procedures	
	P.PKI	
	P.Range_RF_Comnunication	
	P.Personalization_Agent	The reestablishment that to make only the Personalization Agent to establish the policy of the accessing the operation system.
	P.MRTD_Access_Control	The reestablishment that the main agent of BIS and EIS cannot be distinguish during the identification process and only by the authority gained from the system, it is possible to process the access control rule.
	P.Application_Program_Install	The application note is added that the e-Passport application cannot be deleted when it is in use.
Addtion	P.IC_Chip	The IC chip, a component of the TOE, provides the functions to protect the TOE from the IC chip cryptographic calculation and physical attacks.

Table 10 Relation of the security policy of the organization between the composite-ST and the platform-ST

Separation	Assumption	Basis
PP scope	A.Certificate_Verification	
	A.Inspection_System	

	A.MRZ_Entrophy	The applied assumption based on the PP scope.
	A.IC_Chip	The TOE should apply all assumptions of a low platform of the IC chip and follow the A.IC_Chip assumption.
Addition	A.Process_Sec_IC	The assumption, that the security delivery process from the IC chip manufacturing to the Personalization agent and the integrity of TOE should be guaranteed, is added.
	A.Plat_Appl	The assumption, that the Security IC Embedded Software should be designed and loaded by the authenticated procedure, is added.

Table 11 Relation of the assumption between the composite-ST and the platform-ST

The following table shows the security problem mapping between the composite-ST and the platform-ST aginst the threat, the security policy of the organization and the assumption defined on the security problem definitions.

Separation	Platform TOE	Composite TOE	Mapping
Threat	T.leak-Inherent	T.Malfunction T.Leakage_CryptographicKey_Info	Mapped
	T.Phys-Probing	T.Malfunction T.Leakage_CryptographicKey_Info	Mapped
	T.Malfunction	T.Malfunction	Mapped
	T.Phys-Manipulation	T. Malfunction T. Leakage_CryptographicKey_Info	Mapped
	T.leak-Forecd	T. Malfunction T. Leakage_CryptographicKey_Info	Mapped
	T.Abuse-Func	T. Leakage_CryptographicKey_Info	Mapped
	T.RND	T. Malfunction T. Leakage_CryptographicKey_Info	Mapped
	T.Mem_Access	-	-
Security Policy of Organization	P.Process-TOE	-	-
	P.Add-Functions	T.Forgery_Corruption_Personal_Data T.Damage_to_Biometric_Data T.Skimming T.MRTD_Reproduction	Mapped

		T.Leakage_CryptographicKey_Info T.Malfunction P.MRTD_Access_Control P.IC_Chip	
Assumption	A.Process-Sec-IC	A.Process-Sec-IC T.Leakage_CryptographicKey_Info	Mapped
	A.Plat-Appl	A.Plat-Appl	Mapped
	A.Resp-Appl	O.Secure_State	Mapped
	A.Key-Function	O.Deleting_Residual_Info	Mapped

Table 12 Treat/Organization of the Security policy/Assumption mapping between the composite-ST and the platform-ST

2.4.2. Rationale for Conformance of Security Objectives

This security target re-established O.Session Termination, O.Access Control among the security objectives of 'ePassport Protection Profile,' conforms to all the other security objectives, and additionally defined security objectives are O.AA, O.SCP02 and O.IC_Chip.

Re-established Security Objective

- O.Session Termination: the failure of SCP02 mutual authentication for Personalization agent authentication is added to session termination situations, and the case of EAC-TA failure which does not terminate the session is deleted and re-established.
- O.Access Control: re-established for TOE to provide access control for OS.
- O.Secure_State: re-established by adding the application notes that the ePassport application loaded onto the TOE should not be deleted at the issuance and the personalization procedure.

Added Security Objective

- O.AA: added as a security objective to provide a method for inspection system to determine the authenticity of TOE.
- O.SCP02: added to support SCP02 security mechanism for Personalization agent authentication.
- O.IC_Chip: added to support the IC chip security that protects against the composite nature of the TOE.
- OE.Process_Sec_IC: added to support the secure delivery procedure from the manufacturing of the IC Chip to the end customer and the integrity of the TOE.
- OE.Plat_Appl: added to support that the Security IC Embedded Software should be designed and loaded by the authenticated procedure.

•

The following tables show that there is no contradiction between the security objective of the platform-ST and the one of the composite-ST

Separator	Security Objective	Basis
PP scope	O.Management	The applied security objective based on the PP scope
	O.Security_Mechanism_Application_Procedures	
	O.Session_Management	
	O.Personalization_Agent_Authentication	
	O.Certificate_Verification	
	O.Deleting_Residual_Info	
	O.Replay_Prevention	
	O.Access_Control	
	O.Handling_Info_Leakage	
	O.BAC	
	O.EAC	
	O.Secure_State	The reestablishment for not to make the ePassport application to be deleted while in issuance and personalization phases by adding the application notes.
Addition	O.SCP02	Added to support the SCP02 security mechanism for the issuance authentication.
	O.AA	Added to support the way for the inspection system to distinguish whether the TOE is reproduced.
	O.IC_Chip	Added to support the IC chip security that protects against the composite nature of the TOE.

Table 13 Relation of the security objectives between the composite TOE and the platform TOE

Separator	Security Objective	Basis
PP scope	OE.MPTD_Manufaacturing_Security	The applied security objective for running environment based on the PP scope
	OE.Procedures_of_MRTD_Holder_Check	
	OE.Application_Program_Install	
	OE.Certificate_Verification	
	OE.Personalization_Agent	
	OE.Inspection_System	
	OE.MRZ_Entropy	
	OE.PKI	
	OE.Range_RF_Communication	
	OE.IC_Chip	The TOE should apply all the running environmental security objectives and follows the OE.IC_Chip.
Addition	OE.Process_Sec_IC	By applying the security objective that the

		security delivery process from the IC chip manufacturing to the Personalization agent and the integrity of TOE, OE,Process_Sec_IC is added.
	OE.Plat_Appl	By applying the security objective that the Security IC Embedded Software which is designed and loaded by the authenticated procedure, OE.Plat_Appl is added.

Table 14 Relation of the security objectives for the running environment between the composite TOE and the platform TOE.

The following table defines the mapping between the platform-ST and the composite-ST against the security objectives for the running environment of the TOE security objectives.

Separator	Platform TOE	Composite TOE	Mapping
Security objectives of the TOE	O.leak-Inherent	O.Handling_Info_Leakage O.IC_Chip	Mapped
	O.Phys-Probing	O.IC_Chip	Mapped
	O.Malfunction	O.Secure_State	Mapped
	O.Phys-Manipulation	O.IC_Chip	Mapped
	O.leak-Forecd	O.Handling_Info_Leakage O.IC_Chip O.Secure_State	Mapped
	O.Abuse-Func	-	-
	O.Identification	-	-
	O.RND	O.IC_Chip	Mapped
	O.Add-Functions	O.IC칩 O.BAC O.AA O.Certificate_Verification O.EAC O.SCP02	
	O.Mem_Access	-	-
security objectives for the running environment	OE.Process-Sec-IC	OE.Process-Sec-IC	Mapped
	OE.Plat-Appl	OE.Plat-Appl	Mapped

Table 15 Mapping of the security objectives for the running environment between the composite-ST and the platform-ST

2.4.3. Rational for Conformance of Security Function Requirements

This security target conforms to the security function requirement of 'ePassport Protection Profile,' and the operations are completed and re-established according to the preparation rules allowed in the security function requirement of Table 9, and the security function requirements of Table 10 **Relation of the security policy of the organization between the composite-ST and the platform-ST**were additionally defined.

Re-established Security Function Requirements

Protection Profile	Security Target	Rationale
FCS_CKM.2(1)	FCS_CKM.2(1)	Selected
FCS_CKM.2(2)	FCS_CKM.2(2)	Selected
FCS_CKM.4	FCS_CKM.4	Allocated
FCS_COP.1(1)	FCS_COP.1(1)	Selected
FCS_COP.1(2)	FCS_COP.1(2)	Selected
FCS_COP.1(3)	FCS_COP.1(3)	Allocated, Selected
FCS_COP.1(4)	FCS_COP.1(4)	Allocated, Selected
-	FCS_RNG.1	Allocated, Selected
FDP_ACC.1	FDP_ACC.1(1)	Allocated, Elaboration
FDP_ACF.1	FDP_ACF.1(1)	Allocated, Elaboration
FDP_RIP.1	FDP_RIP.1	Allocated, Selected
FDP_UIT.1	FDP_UIT.1	Selected
FIA_AFL.1	FIA_AFL.1(1)	Allocated, Selected
FIA_UAU.1(1)	FIA_UAU.1(1)	Allocated
FIA_UAU.1(2)	FIA_UAU.1(2)	Allocated
FIA_UAU.4	FIA_UAU.4	Allocated
FIA_UAU.5	FIA_UAU.5	Allocated
FMT_MSA.1	FMT_MSA.1	Elaboration
FMT_MSA.3	FMT_MSA.3	Elaboration
FMT_MTD.1(1)	FMT_MTD.1(1)	Allocated
FMT_MTD.3	FMT_MTD.3	Allocated
FMT_SMF.1	FMT_SMF.1	Allocated
FMT_SMR.1	FMT_SMR.1	Allocated
FPT_FLS.1	FPT_FLS.1	Allocated

FPT_ITI.1	FPT_ITI.1	Allocated
FPT_TST.1	FPT_TST.1	Allocated, Selected

Table 16 Rationale for Re-established Security Function Requirements

Additional rationale for security function requirement re-established through elaboration is described.

- FDP_ACC.1(1): according to Organizational Security Policies P.EPASSPORT_ACCESS_CONTROL, subjects of BIS and EIS are combined and elaborated to inspection systems to perform access control based on the security properties of the subject.
- FDP_ACF.1(1): according to Organizational Security Policies P.EPASSPORT_ACCESS_CONTROL, subjects of BIS and EIS are combined and elaborated to inspection systems to perform access control based on the security properties of the subject.
- FIA_AFL.1(1): elaborate by removing EAC-TA which does not terminate user session.
- FMT_MSA.1: elaborate so that the added access control policy of OS access control is enforced
- FMT_MSA.3: enforce the added access control policy of OS access control policy, and as the security properties may not have other initial values due to performing the access control policy with implementation logic of TOE, elaborate the role of specifying the selective initial values of security properties as none.

Added Security Function Requirements

Security Function Requirements	Rationale
FCS_CKM.1(2)	Defines security function requirement regarding SCP02 session key generation to perform SCP02 mutual authentication.
FCS_CKM.3	Defines security function requirement regarding encryption key access performed by application programs other than ePassport functions.
FCS_COP.1(5)	Defines the security function requirement for the creation of the digital signature value.
FCS_RNG.1	Defines the SFR to use the function of the platform TOE for creating of the random value.
FDP_ACC.1(2)	Defines security function requirement for OS access control.
FDP_ACF.1(2):	Defines security function requirement for OS access control rules.
FDP_DAU.1	Defines security function requirement for data authentication to confirm the authenticity of ePassport.
FIA_AFL.1(2):	Defines security function requirement for Personalization agent authentication failure.

FIA_UAU.1(3):	Defines security function requirement for performing SCP02 mutual authentication to authenticate Personalization agent.
FMT_MOF.1(2):	Adds security function requirement that only Personalization agent may grant the function to change the OS life cycle status to application programs.
FMT_MTD.1(3):	Defines security function requirement for GP registry management of OS
FPT_PHP.3	Defines the SFR to satisfy the O.IC_Chip due to the evaluation of the TOE as composite.

Table 17 Added Security Function Requirements

2.4.4. Rationale for Conformance of Assurance Requirements

This security target confroms to all assurance requirements of EAL4+ (ADV_IMP.2, AVA_VAN.4) assurance level required by 'ePassport Protection Profile,' and the additionally defined assurance requirements are of EAL5+, and are as follows.

Added Assurance Requirements

- ADV_FSP.5 : Semi-standardized and complete function specification providing additional error information
- ADV_INT.2 : Well-structured inside of TSF
- ADV_TDS.4 : Semi-standardized modularization design
- ALC_CMS.5 : Scope of configuration management of development tools
- ALC_TAT.2 : Applied implementation standard
- ATE_DPT.3 : Modularization design test

Next, it shows that there is no contradiction between the guaranteed requirement of the composite TOE and the one the IC chip used as the platform against the security objectives, the security requirement and the security environment.

The guaranteed requirement of the composite TOE is that among the security requirement of the IC chip which got the EAL 5+ guaranteed rank is in the range of the security requirement of the EAL 5+ guaranteed rank. Also, based on the ePassport profile, ADV_IMP.2, which is at the EAL 5+ guaranteed rank, is chosen to develop the EAL 5+ guaranteed rank.

Guaranteed Class	Composite TOE	Platform TOE	Conformity of the composite TOE
Security objective specification	ASE_INT.1	ASE_INT.1	accordance
	ASE_CCL.1	ASE_CCL.1	Accordance

	ASE_SPD.1	ASE_SPD.1	Accordance
	ASE_OBJ.2	ASE_OBJ.2	Accordance
	ASE_ECD.1	ASE_ECD.1	Accordance
	ASE_REQ.2	ASE_REQ.2	Accordance
	ASE_TSS.1	ASE_TSS.1	Accordance
Development	ADV_ARC.1	ADV_ARC.1	Accordance
	ADV_FSP.5	ADV_FSP.5	Accordance
	ADV_IMP.2	ADV_IMP.1	ADV_IMP.2 observance according to the requirement of PP
	ADV_INT.2	ADV_INT.2	Accordance
	ADV_TDS.4	ADV_TDS.4	Accordance
Instructions	AGD_OPE.1	AGD_OPE.1	Accordance
	AGD_PRE.1	AGD_PRE.1	Accordance
Supporting life cycle	ALC_CMC.4	ALC_CMC.4	Accordance
	ALC_CMS.5	ALC_CMS.5	Accordance
	ALC_DEL.1	ALC_DEL.1	Accordance
	ALC_DVS.1	ALC_DVS.2	Subset observance of the platform TOE ST
	ALC_LCD.1	ALC_LCD.1	accordance
	ALC_TAT.2	ALC_TAT.2	accordance
Test	ATE_COV.2	ATE_COV.2	accordance
	ATE_DPT.3	ATE_DPT.3	accordance
	ATE_FUN.1	ATE_FUN.1	accordance
	ATE_IND.2	ATE_IND.2	accordance
Evaluation of the weakness	AVA_VAN.4	AVA_VAN.5	Subset observance of the platform TOE ST

Table 18 The guaranteed requirement relation between the composite TOE and the platform TOE

3. Security Problem Definition

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

3.1. Threats

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

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

< Threats to the TOE in the Personalization phase>

T.Personalization _Agent_Authentication_Replay
After intercepting the transmitted information from TOE and personalization agent in the initial process of the personalization agent authentication mechanism, SCP02, the threat agent may bypass the SCP02 mutual authentication as replaying.

Application Notes: When the TOE uses the same values for the authentication information and SCP02 session key, they are vulnerable to ciphertext only attack.

T.TSF_DATA_MODIFICATION
When the ePassport personalization agent records the TSF data, the threat agent can modify the data, and attempt to access in the stored TSF data using outer interfaces through the inspection system.

< BAC-related Threats in the TOE Use phase>

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

T.FORGERY_CORRUPTION_ PERSONAL_ DATA

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

T.BAC_AUTHENTICATION_KEY_DISCLOSE

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

Application Notes: BAC authentication key is generated by the personalization agent in the ePassport personalization phase or by the TOE in the ePassport using phase after the ePassport personalization phase. At the first case of the writer of the security objective specification should consider about the threat of leakage of the BAC authentication key stored in the protect and temporary memory region of the ePassport IC chip according to the way of the creating BAC authentication key while the other case of the writer should consider about the threat of leakage of the BAC authentication key remained in the temporary memory region with residual information.

T.BAC_REPLAYATTACK

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

Application Notes: The TOE delivers the random number of plaintext to Inspection System according to „get_challenge‟ instruction of the Inspection System in the BAC. Therefore, the threat agent can bypass the BAC mutual authentication by intercepting the random number and response value of the Inspection System and re-transmitting the response value of the Inspection System to the next session. Also, the threat agent may find the transmission data as threat agent can generate the BAC session key after obtaining the BAC authentication key by T.BAC_Authentication_Key_Disclose.

< EAC-related Threats in the Operational Use phase>

T. DAMAGE_TO_BIOMETRIC_DATA

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

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

T.EAC-CA_BYPASS

The threat agent may bypass the authentication of the Inspection System so that to go through EAC-CA by using the threat agent generated EAC chip authentication public key.

T.IS_CERTIFICATE_FORGERY

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

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

T.SESSIONDATA_REUSE

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

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

T.SKIMMING

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

< Threats related to IC Chip Support>

T.MALFUNCTION

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

< Other Threats in the Operational Use phase>

T.LEAKAGE_CRYPTOGRAPHICKEY_INFO

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

T.EPASSPORT_REPRODUCTION

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

T.RESIDUAL_INFO

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

3.2. Organizational Security Policies

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

P.INTERNATIONAL_COMPATIBILITY

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

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

P.SECURITY_MECHANISM_APPLICATION_PROCEDURES

The TOE shall ensure the order of security mechanism application according to the type of

the Inspection System so that not to violate the ePassport access control policies of the Personalization agent.

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

P.APPLICATION_PROGRAM_INSTALL

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

Application notes: The application program installing can only be done by organizations holding the same authority as the Personalization agent. Also, ePassport application program installed in the IC chips cannot be deleted in the utilized procedure.

P.PERSONALIZATION_AGENT

The personalization agent shall issue the ePassport in the secure manner so that to confirm that the issuing subject has not been changed and shall deliver the TOE to the Operational Use phase after verifying that the data inside MRTD chip are operating normally after issuing. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase. Also, the personalization agent should establish the access control policy about the operation system management.

Application Notes: SCP02 security mechanism of 'GP standard' as the security mechanism is used for the personalization agent authentication

P.EPASSPORT_ACCESS_CONTROL

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

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

List of Objects	Objects				
	Personal data of the ePassport holder	Biometric data of the ePassport holder	ePassport authentication data	EF.CVCA	EF.COM

List of Subjects		Security Attribute / Security Attribute	Read-Right	Write-Right	Read-Right	Write-Right	Read-Right	Write-Right	Read-Right	Write-Right	Read-Right	Write-Right
Subjects	BIS	BAC Authorization	Allow	Deny	Deny	Deny	Allow	Deny	Allow	Deny	Allow	Deny
	EIS	BAC Authorization	Allow	Deny	Deny	Deny	Allow	Deny	Allow	Deny	Allow	Deny
		EAC Authorization	Allow	Deny	Allow	Deny	Allow	Deny	Allow	Deny	Allow	Deny
	Personalization Agent	Personalization Authorization	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow

Table 19 ePassport Access Control Policies

P. PKI

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

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

P.RANGE_RF_COMMUNICATION

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

P.IC_Chip

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

Application Notes :

To ensure the secure TOE environment, the IC chip shall be a certified product, S3CT9KW/S3CT9KC/S3CT9K9, of CCRA EAL4+(SOF-high) or higher level. The cryptographic operation supported by the IC chip may be provided in the co-processor of

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

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 in order to limit the scope of security consideration.

A.Certificate_Verification

The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically.
The EIS shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA link certificate, the DV certificate and the IS certificate in the EAC-TA.

Application Notes: The Inspection System should connect to ICAO-PKD periodically, and download CSCA certificates to verify the certificate for PA of the inspection system.

A.Inspection_System

The Inspection System shall implement security mechanisms of the PA, the BAC and the EAC according to the ICAO document and EAC specifications on the basis of the verifying policy of the ePassport for the ePassport holder.
Also, after session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the BAC session key, the EAC session key and session information, etc.

Application Notes: The TOE denies the request to access EF.SOD by the Inspection System that failed the BAC mutual authentication.
As the BIS supports the BAC and PA security mechanisms, it obtains the read-rights for the personal and authentication data of the ePassport holder if the BAC mutual authentication using the BAC authentication key succeeds. Then, by establishing the BAC secure messaging with the BAC session key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the BAC. Then, by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder. As the EIS supports the BAC, EAC and PA security mechanisms, it obtains the read-rights for the personal, authentication and biometric data

of the ePassport holder. The EIS, when the BAC mutual authentication and secure messaging succeed, executes the EAC-CA by using the EAC chip authentication public key read in the BAC to verify the genuine TOE. Then, it executes the PA in order to verify the EAC chip authentication public key. When the EAC-CA is succeeded, the BAC secure messaging is ended and the EAC secure messaging with the EAC session key is started, and the EAC-TA that the TOE authenticates inspection system.
The Inspection System is executed. When the EAC-TA is succeeded, the EIS obtains the read-rights for the biometric data of the ePassport holder. Therefore, the EIS is provided the biometric data of the ePassport holder from the TOE. BIS or EIS could implement AA security mechanism additionally, verify the digital signature provided by TOE using the AA digital signature verification key of EF.DG15, and verify the probability of TOE.

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

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

<The Assumption of the IC chip>

The followings are quoted from "3.4 Assumptions" of [ICST].

A.Process-Sec-IC (Protection during Packaging, Finishing and Personalisation)
It is assumed that security procedures are used after delivery of the composite TOE(H/W and Embedded Software) by the Manufacturer up to delivery to the consumer to maintain confidentiality and integrity of the composite TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
This means that the Phases after composite TOE Delivery are assumed to be protected appropriately.

A.Plat-Appl (Usage of Hardware Platform)
The Security IC Embedded Software is designed so that the requirements from the

following documents are met: H/W TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and findings of the H/W TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

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

4.1. Security Objectives for the TOE

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

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

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

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

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

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

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

O. Certificate_Verification

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

O. Secure_State

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

Application Notes: The ePassport application program should not be deleted in the personalization and operational use phase

O. Deleting_Residua_Info

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

O. Replay_Prevention

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

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

O. Access_Control

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

Application Notes: Only the authorized Personalization agent in the Personalization phase can record the MRTD application data or TSF data and access control policies for the read-rights according to the type of the Inspection System shall be built in the Operational Use phase. Also, the access control policy is established about operation system user data including execute file, application program and fundamental information for personalization agent or authority in the personalization or 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 Notes :

As the co-processor of the IC chip or cryptographic libraries loaded in the IC chip provide countermeasures to satisfy this security objective, the ST specifies it as a security objective for the TOE.

O.BAC

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

O.EAC

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

O.SCP02

TOE implements the security mechanism SCP02 to provide means managing ePassport application data by only the authorized personalization agent, and performs SCP02 mutual authentication between TOE and inspection system.

O.AA

TOE implements AA security mechanism to recognize the illegal reproduction of TOE by the inspection system.

O.IC_Chip

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

Application Notes:
In case performing TDES operation, RSA operation or ECDSA operation, the co-processor of the IC chip or cryptographic libraries loaded in the IC chip shall implement countermeasures to prevent exploiting of leakage information

4.2. Security Objectives for the Environment

The following are security objectives handled by IT fields or nontechnical/procedure-related means.

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

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

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

OE. Certificate_Verification
The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically. The EIS shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA link certificate, the DV certificate and the IS certificate in the EAC-TA.

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

delivery to the Operational Use phase.

OE. .Inspection_System

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

OE.MRZ_Entropy

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

OE.PKI

The Issuing State of the ePassport shall execute certification practice to securely generate · manage a digital signature key and to generate · issue · operate · destroy certificates according to the CPS by implementing the PA-PKI and EAC-PKI according to the ePassport PKI System. Also, The Issuing State of the ePassport shall update certificates according to the policies to manage valid date of certificates, therefore securely deliver them to the Verifying State and Inspection System.

OE.Range_RF_Communication

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

<The running environment of the IC chip>

The followings are quoted from "4.2 Security Objectives for the Security IC Embedded software development Environment" of [ICST].

OE.Process-Sec-IC (Protection during composite product manufacturing)
Security procedures shall be used after composite TOE(H/W and Embedded Software) Delivery up to delivery to the "consumer" to maintain confidentiality and integrity of the composilte TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after composilte TOE Delivery up to the end of Phase 6 must be protected appropriately.

OE.Plat-Appl (Usage of Hardware Platform)

To ensure that the composite TOE(H/W and Embedded Software) is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: hardware data sheet for the H/W TOE, data sheet of the IC Dedicated Software of the H/W TOE , application notes, other guidance documents, and (iv) findings of the H/W TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.

4.3. Security Objectives Rationale

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

The rationale of security objectives demonstrates the following:

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

Table 20 shows the mapping between Security Problem Definition and Security Objectives.

Security Objectives / Security Environment	TOE Security Objective															Security Objective for environment											
	O.Management	O.Security_Mechanism_Application_Procedure	O.Session_Termination	O.Secure_Messaging	O.Certificate_Verifi.	O.Secure_State	O.Deleting_Residu_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakag	O.AA	O.BAC	O.EAC	O.IC_Chip	O.SCP02	OE.ePassport_Manufacturing_Security	OE.Procedures_ePassport_holder_check	OE.Application_Program Install	OE.Certificate_Verifi.	OE.Personalization_Age.	OE.Inspection_system	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Comm.	OE.Process-Sec-IC	OE.Plat-appl
T.Personalization_Agent_Authen._Rreplay								x																			
T.TSF_DATA_MODIFICATION	x		x						x											x							
T.Eavesdropping				x																	x						
T.FORGERY_CORRUPTION_ PERSONAL_ DATA			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	
T.MALFUNCTION						X								X										
T.LEAKAGE_CRYPTOGRAPHICKEY_INFO										X				X										
T.EPASSPORT_REPRODUCTION											X		X			X	X			X				
T.RESIDUAL_INFO							X																	
P.INTERNATIONAL_COMPATIBILITY																			X					
P.SECURITY_MECHANISM_APPLICATION_PROCEDURES		X																		X				
P.APPLICATION_PROGRAM_INSTALL						X											X							
P.PERSONALIZATION_AGENT	X								X					X					X					
P.EPASSPORT_ACCESS_CONTROL	X								X			X	X						X	X				
P.PKI					X																	X		
P.Range_RF_Comm.																							X	
P.IC_Chip														X									X	
A.Certificate_Vefification																			X	X		X		
A.Inspection_System																				X				
A.MRZ_Entropy																					X			
A.Process-Sec-IC																							X	
A.Plat-Appl																								X

Table 20 The mapping between Security Environment and Security Objectives

4.3.1. Security Objective Rationale for the TOE

O. Management

This security objective ensures that the TOE provides the means to write user data in EF domain and the means to write TSF data in secure memory only to the authorized Personalization agent in the Personalization phase and prevents unauthorized access using external interface by deactivating the MRTD application data writing function of the Personalization agent in the Operational Use phase. Therefore, this security objective is required to counter the threats of T.TSF_Data_Modification and T.BAC_Authentication_Key_Disclose and to enforce the organizational security policies of P.ePassport_Access_Control and P.Personalization_Agent. Also, this security objective provides the Personalization agent with the means to record CVCA certificate in secure

memory in the Personalization phase, therefore is required to counter the threat of T.IS_Certificate_Forgery.

O. Security_Mechanism_Application_Procedures

This security objective is required to enforce the organizational security policies of P.Security_Mechanism_Application_Procedures since the TOE ensures that the application order of the PA, BAC and EAC security mechanisms according to 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specifications and by not allowing requests from the Inspection System that do not correspond to the security mechanism application order. Also, this security objective is required to counter the threat of T.EAC-CA Bypass by eliminating the cases of demonstrating the genuine TOE to the unauthorized Inspection System as it ensures the application order of security mechanisms so that to enable the EAC-CA execution by only the Inspection System with access-rights for the EAC chip authentication public key through the BAC execution.

O. Session_Termination.

This security objective ensures that the TOE prevents continuous authentication attempts of authentication in order for access to forge and corrupt the personal or biometric data of the ePassport holder and terminates session in case modification for the transmitted TSF data is detected. Therefore, this security objective is required to counter the threats of T.Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data, T.BAC_Authentication_Key_Disclose and T.TSF_Data_Modification.

O. Secure_Messaging

This security objective ensures that the TOE establishes the BAC or EAC secure messaging for secure transmission of the personal and biometric data of the ePassport holder to the Inspection System, and provides the confidentiality and integrity for the transmitted personal and biometric data of the ePassport holder. Therefore, this security objective is required to counter the threats of T.Damage_to_Biometric_Data and T.Eavesdropping.

O. Certificate_Verification

This security objective is required to enforce the organizational security policies of P. PKI as it ensures for the TOE to check the valid date on the basis of the CVCA link certificate provided by the Inspection System, therefore to automatically update the certificate and the current date. This security objective is required to counter the threats of T.Damage_to_Biometric_Data and T.IS_Certificate_Forgery by determining the status of forgery as the TOE verifies validity of the CVCA link certificate, DV certificate and IS

certificate in the EAC-TA.

O. Secure_State

This security objective is required to counter the threat of T.Malfunction as the TOE detects modification of the TSF and data through self-testing, and protects the TOE itself by preserving a secure state so that malfunction of TSF do not occur. Also, this security objective should not delete the application program, and operate Organizational Security Policies P.APPLICATION_PROGRAM_INSTALL.

O. Deleting_Residua_Info

This security objective is required to counter the threat of T.Residual_Info by deleting all of the previous security-related information (BAC session key and EAC session key, etc.) so that it is not included when the TOE allocates or deallocates memory resources, therefore ensuring that information is not available. This security objective is required to counter the threat of T.BAC_Authentication_Key_Disclose by providing the means to ensure that residual information remaining in temporary memory is not available.

O. Replay_Prevention

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

O. Access_Control

This security objective is required to counter the threats of T. Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data and T.Skimming and enforce the organizational security policies of P.ePassport_Access_Control by implementing the rules of allowing or denying of Inspection System to read user data in accordance with the ePassport access control policies by the Personalization agent. Also, this security objective shall implement access control function according to application management authority, access authority for fundamental information and authorized information of personalization agent and perform Organizational Security Policies

P.PERSONALIZATION_AGENT.

O.Handling_Info_Leakage

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

O.AA

This security objective is mapping Threats T.EPASSPORT_REPRODUCTION because TOE shall implement AA security mechanism that the inspection system is utilizing for recognizing the illegal reproduction of TOE.

O.BAC

This security objective is required to enforce the organizational security policies of P.ePassport_Access_Control as the TOE implements the BAC security mechanism to control access to the personal data of the ePassport holder, therefore gives the read-rights for the personal data of the ePassport holder only to the authorized Inspection System of which the BAC mutual authentication is successfully completed. This security objective is required to counter the threats of T. Forgery_Corruption_Personal Data and T.Skimming as the TOE allows the read-rights for the personal data of the ePassport holder only to the authorized Inspection System by generating the BAC session key during the BAC mutual authentication and denies access by the Inspection System that does not have the read-rights.

O.EAC

This security objective is required to enforce the organizational security policies of P.ePassport_Access_Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the ePassport holder, therefore gives the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System of which the EAC-TA is successfully completed. This security objective is required to counter the threats of T.Damage_to_Biometric_Data and T.Skimming as the TOE allows the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System through the EAC-TA by generating the EAC session key during the EAC-CA and denies access by the Inspection System that does not have the read-rights. Also, it is mapping Threats T.EPASSPORT_REPRODUCTION because of providing means to recognize the illegal reproduction of TOE through EAC_CA.

O.IC_Chip

This security objective is required to support the assumption of A.IC_Chip as it uses EAL4+(SOF-high) IC chip as a TOE component that generates random number and provides cryptographic op-eration in order to support security functions of the TOE and provides the malfunction detection and physical protection, etc. Therefore, it is required to counter OSP P.IC_Chip.

Also, this security objective is required to counter the threat of T.Malfunction as the IC chip detects malfunction outside the normal operating conditions, and this security objective is required to counter the threat of T.Leakage_CryptographicKey_Info as it uses EAL5+ IC Chip that is assured.

O.SCP02

This security objective shall perform Organizational Security Policies P.EPASSPORT_ACCESS_CONTROL, P.PERSONALIZATION_AGENT as TOE shall authorize ePassport personalization agent, implement SCP02 mutual authentication for personalizing securely, and provide management means about ePassport applicant information and TSF data to only personalization agent succeeding SCP02 mutual authentication.

4.3.2. Security Objective Rationale for Operating Environment

OE. ePassport_Manufacturing_Security

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

OE. Procedures_of_ePassport_Holder_Check

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

OE. Application_Program_Install

This security objective for environment is required to enforce the organizational security

policies of P.Application_Program_Install by ensuring that only the application programs are loaded to the MRTD chip in a secure manner by the Personalization agent.

OE. Certificate_Verification

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

OE. Personalization_Agent

This security objective for environment is required to enforce the organizational security policies of P.International_Compatibility and P.Personalization_Agent by ensuring that the TOE is delivered to the Operational Use phase after securely issuing the ePassport so that the Personalization agent can check that the issuing subject has not been changed, verifying normal operation and compatibility of the ePassport in the Personalization phase and deactivating writing function. This security objective for environment also is required to enforce the organizational security policies of P.ePassport_Access_Control as it defines the role of the Personalization agent. Also, this security objective for environment is required to support the assumption of A.Certificate_Verification because the Personalization agent makes certificates necessary in the PA and EAC support available to the Inspection System. This security objective for environment is required to counter the threat of T.TSF_Data_Modification because the Personalization agent deactivates writing function in the Operational Use phase, therefore disables the writing function for modification of the TSF data.

Application Notes :

Basically, the TOE supports the BAC mechanism and it supports also the AA or the EAC mechanism as optional. This option can be decided according to the personalization policy of the Personalization agent and it is set by the install option of the TOE.

OE. Inspection_System

This security objective for environment is required to support the assumption of

A.Inspection System and enforce the organizational security policies of P.Security_Mechanism_Application_Procedures and P.ePassport_Access_Control as the Inspection System implements and ensures application order of security mechanisms in accordance with the type of the Inspection System so that not to violate the ePassport access control policies of the Personalization agent and by ensuring that information used in communication with the TOE is securely destroyed after session termination.
This security objective for environment is required to counter the threat of T.Eavesdropping as the confidentiality and integrity of the transmitted data are ensured by establishing the BAC secure messaging after generating the BAC session key through the BAC key distribution when the Inspection System communicates with the TOE.
This security objective for environment is required to counter the threats of T. Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data, T.Skimming and T.EAC-CA_Bypass as the Inspection System supports the BAC mutual authentication, EAC and PA.
This security objective for environment is required to counter the threat of T.SessionData_Reuse as the Inspection System generate different temporary public key per session to be transmitted to the TOE in the EAC-CA.

OE. MRZ_Entropy

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

OE.PKI

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

OE. Range_RF_Communication

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

ePassport attached with the IC chip is not opened.

<The rationale of the security objective against the environment of the IC chip>

OE.Process-Sec-IC (Protection during composite product manufacturing)
This security objective for environment is required to counter the assumption of A.Process-Sec-IC by requiring Composite Product Manufacturer to apply security procedure to maintain confidentiality and integrity of the TOE through delivery to the end customer.

OE.Plat-Appl (Usage of Hardware Platform)
This security objective for environment supports the assumption of A.Plat-Appl and A.Key-Function by requiring Embedded S/W developer to implement while satisfying TOE guidance documents and findings of IC chip evaluation report.

5. Definition of Extended Component

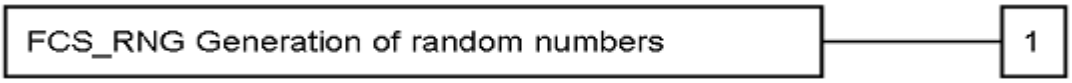
This chapter identifies the extended security requirement of this Security Target and provides the explanation about them.

The component belongs to the cryptographic calculation providing the function to generate the random number so it is included in the FCS class. There was no family supporting the function to generate the random number so it is included in the FCS class. It supports only the function to generate the random number therefore only one component is required to be exist.

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 intended 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, hybrid] 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 quality metric].

6. Security Requirements

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

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

This Security Target defines all subjects, objects, operation, security attributes employed in security requirements as Table 21. Also, it defines SSC (Send Sequence Counter) with session security attributes related to establishing secure messaging.

Subject	Subject Security Properties	Object	Object Security Properties		Operation
			Operation Security Properties	Access Rights Security Properties	
BIS	BAC Rights	ePassport Applicant Basic Info	Read Rights	BAC Rights EAC Rights	· Read · Write
			Write Rights	Issuing Authority Issuance Rights	
EIS	BAC Rights EAC Rights	ePassport Applicant Bio Information	Read Rights	EAC Rights	
			Write Rights	Issuing Authority Issuance Rights	
Issuing Authority	Issuing Authority Issuance Rights	ePassport Authentication Info	Read Rights	BAC Rights EAC Rights	
			Write Rights	Issuing Authority Issuance Rights	
		EF.CVCA	Read Rights	BAC Rights EAC Rights	
			Write Rights	Issuing Authority Issuance Rights	
		EF.COM	Read Rights	BAC Rights EAC Rights	
			Write Rights	Issuing Authority Issuance Rights	

Subject	Subject Security Properties	Object	Object Security Properties		Operation
			Operation Security Properties	Access Rights Security Properties	
Issuing Authority	Management/ Usage Rights	Executable File	Load Rights	Management Rights	· Install · Delete · Select · Read · Write · Change
			Delete Rights	Management Rights	
		Application Program	Install Rights	Management Rights	
			Deletion Rights	Management Rights	
			Selection Rights	Usage Rights	
		Issuing Authority Basic Information	Read Rights	Usage/Management Rights	
			Write Rights	Management Rights	
			Change Rights	Management Rights	
		Issuing Authority Authentication Info	Write Rights	Management Rights	
			Change Rights	Management Rights	

Table 21 Definition of Subject, Object, related Security Attributes and Operation

6.1. TOE Security Function Requirements

The security requirement of this Security Target consists of the components from Part 2 of the common criteria. The following Table 22 shows the security requirement using in this Security Target in order to satisfy TOE security objective identified in the previous chapter.

Security Functional Class	Security Functional Components	
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.1(2)	Cryptographic key generation (Generation of SCP02 Session Key)
	FCS_CKM.2(1)	Cryptographic key distribution (KDF Seed Distribution for BAC session key generation)
	FCS_CKM.3	Cryptographic key access
	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 Verifica-tion)
	FCS_COP.1(5)	Cryptographic operation (Digital Signature Generation for AA)
	FCS_RNG.1	Random Number Generation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (ePassport access control)
	FDP_ACC.1(2)	Subset access control (operation system access control)
	FDP_ACF.1(1)	Security attribute based access control (ePassport access control)
	FDP_ACF.1(2)	Security attribute based access control (OS access control)
	FDP_DAU.1	Basic data authentication
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
identification and Authentication (FIA)	FIA_AFL.1(1)	Authentication failure handling (user session termination)
	FIA_AFL.1(2)	Authentication failure handling (retry prohibited)
	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 (SCP02 mutual authentication)
	FIA_UAU.4	Single-use authentication mechanism
	FIA_UAU.5	Multiple authentication mechanism
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1(1)	Management of security functions behavior (ePassport writing)
	FMT_MOF.1(2)	Management of security functions behavior (OS life cycle

		change)
	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 (SCC initialization)
	FMT_MTD.1(3)	Management of TSF data (OS management)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Privacy (FPR)	FPR_UNO.1	Unobservability
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_PHP.3	Resistance to physical attack
	FPT_TST.1	TSF TESTING

Table 22 TOE Security Functional Requirements

6.1.1. Cryptographic Support

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

Hierarchical to: No other components.

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

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

Application Notes: The TOE generates the BAC authentication key, BAC session key and EAC session key by using key derivation mechanism. BAC authentication key is generated and provided by the Personalization agent, or in the case the Personalization agent does not provide it, it is generated directly by TOE and recorded on the protected memory area of TOE.

FCS_CKM.1(2) Cryptographic key generation

Hierarchical to: No other components

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

FCS_CKM.1.1 The TSF shall generate the encryption key of the specified encryption key length of [112 bit] with the specified encryption key generation algorithm [Appendix E.4.1 DES Session Keys, Part 3 : Block ciphers] compliant with the following standard of [GP standard, ISO/IEC 18033-3].

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

Hierarchical to: No other components.

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

FCS_CKM.2.1 The TSF shall distribute KDF Seed for the BAC session key generation in accordance with a specified cryptographic key distribution *KeyEstablishmentMechanism 6* that meets the *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 SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target Copyright ⓒ Samsung SDS Co., Ltd. All rights reserved Page 55 of 94

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

Application Notes:

To create the session key for EAC-CA, the TOE use ECC cryptographic library and supports key length at ECC 224 and 256 bits.

FCS_CKM.3 Cryptographic key access

Hierarchical to: No other components

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

FCS_CKM.3.1 The TSF shall perform [encryption key storage/inspection] using the specified cryptographic key access method of [access using memory address] compliant with the following [‘no standard’].

Caution when Applying:

The application programs loaded on TOE may call the command to access the key according to the standards below.

Standard List	Encryption Key Access Method	Encryption Key Access Type
GPCS VGP	PUT Key command STORE DATA command	Encryption key storage
LDS	PUT Key command STORE DATA command	Encryption key storage
JCAPI	getKey	DES key inspection
	setKey	DES key storage
	getS	ECPrivateKey inspection
	setS	ECPrivateKey storage
	getW	ECPublicKey inspection
	setW	ECPublicKey storage
	getExponent getModulus	RSAPrivateKey inspection RSAPublicKey inspection
	setExponent setModulus	RSAPrivateKey storage RSAPublicKey storage

Table 23 List of Key access command

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies to: No other components.

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy the **cryptographic key and MAC key** according to the specified encryption key destruction method ['deleting memory data physically by overwriting'] compliant with the following ['no standard'].

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

Hierarchical to: No other components

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

FCS_COP.1.1 The TSF shall perform [message encryption, decryption operation] in accordance with *TDES* and cryptographic key sizes, *112 bits,* that meet the *ISO/IEC 18033-3.*

Application Notes :

The TOE uses the TDES cryptographic algorithm for the confidentiality protection of the transmitted data of the BAC or EAC secure messaging, for the BAC mutual authentication and for the BAC key distribution. The cryptographic algorithm operation mode when it is in use is the CBC mode which is defined in ISO/IEC 10116 with the IV value equals to 0.

FCS_COP.1(2) Cryptographic operation (MAC)

Hierarchical to: No other components

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

FCS_COP.1.1 The TSF shall perform [MAC operation] in accordance with *Retail MAC* and cryptographic key sizes, *122 bits,* that meet the *ISO/IEC 9797-1*.

Application Notes :

The TOE uses the Retail MAC algorithm for the integrity protection of the trans-mitted data of the BAC or EAC secure messaging and for the BAC mutual authentication. The

Retail MAC uses the MAC algorithm 3, the block cipher DES, the sequence message counter and the pad-ding mode 2 defined in ISO/IEC 9797-1.

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 [Hash operation] in accordance with *SHA-1, SHA-224, SHA-256* and cryptographic key sizes [None] that meet the *ISO/IEC 10118-3* .

Application Notes :

In the key derivation mechanism of the ICAO document, the SHA-1 implemented in the COS is used as a hash function in order to generate the session key used in the BAC or EAC secure messaging. The TOE used the SHA-224 and SHA-256 from the library provided by the IC chip and the SHA-1 from the software loaded onto it.

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]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [digital signature verification] in accordance with *ECDSA-SHA-1, ECDSA-SHA-224, ECDSA-SHA-256* and cryptographic key sizes [224 bits, 256 bits, 320 bits] that meet the *ISO/IEC 15946-2*.

Application Notes :

In Appendix A.3 Terminal Authentication of the EAC specifications, the digital signature algorithm, hash algorithm and digital signature key sizes are defined as of the following. The TOE specifies the cryptographic key sizes specified in the [] so that counter attackers possessing high attack potential required by AVA_VAN.4.

Digital Signature Algorithm	Hash Algorithm	Digital Signature Key Length
ECDSA	SHA-1, SHA-224 / SHA-256	224, 256, 320

Table 24 Digital signature related EAC specification

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 [RSASSA-PKCS1-v1.5-SHA-1] and cryptographic key sizes [2048 bits] that meet the [PKCS#1].

Application Notes :

The TOE creates the digital signature value by using the RSA library provided by the IC chip.

Digital Signature Algorithm	Hash Algorithm	Digital Signature Key Length
RSA	SHA-1	2048

Table 25 Digital signature related AA specification

FCS_RNG.1 Random number generation

Hierarchical to : No other components

Dependencies : No dependencies

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

FCS_RNG.1.2 The TSF shall provide random numbers that meet [AIS 31 version 1 Functional Classes and Evaluation Methodology for Physical Random Number Generators, 25 September 2001 , Class P2]

Application Notes : The SFR provided by IC chip is applied as it is.

6.1.2. User Data Protection

FDP_ACC.1(1) Subset access control (ePassport 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) Biometric data of the ePassport holder
      : EF.DG3, EF.DG4
   (3) ePassport authentication data
      : EF.DG14, EF.DG15, EF.SOD
   (4) EF.CVCA
   (5) EF.COM
   (6) [None]
c) Operations
   (1) Read
   (2) Write
   (3) [None]

].

FDP_ACC.1(2) Subset access control (OS access control)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

a) Subject

(1) Personalization agent

b) Object
(1) Executable File
(2) Application program
(3) Personalization agent basic information
(4) Personalization agent authentication information

c) Operation
(1) Load
(2) Install
(3) Delete
(4) Read
(5) Write
(6) Change
(7) Select

].

Caution when Applying:
Personalization agent basic information includes Issuer Identification Number, Card Image Number, Card Recognition Data defined in 'GP Standard' and Card Production Life Cycle, Key Derivation Data defined in 'VGP Standard,' and may additionally include the information defined by the Personalization agent.

Personalization agent authentication information refers to the Personalization agent authentication key used in the SCP02 mutual authentication and SCP02 session key generation, and includes 3 DES keys of 112-bit used for cryptographic calculation SCP02 session key, MAC SCP02 session key, and generation of SCP02 session key for cryptographic calculation regarding confidential information.

FDP_ACF.1(1) Security attribute based access control(ePassport 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] to objects based on the following: [Table 26, Table 27, [None]].

Subject	Security Properties

BIS	BAC rights
EIS	BAC rights, EAC rights
Personalization Agent	Personalization agent issuance rights

Table 26 Security Properties per Subject

Object	Security Properties	
	Operation Security Properties of Object	Access Rights Security Properties of Object
ePassport applicant basic information	Read rights	BAC rights, EAC rights
	Write rights	Personalization agent issuance rights
ePassport applicant bio information	Read rights	EAC rights
	Write rights	Personalization agent issuance rights
ePassport authentication information	Read rights	BAC rights, EAC rights
	Write rights	Personalization agent issuance rights
EF.CVCA	Read rights	BAC rights, EAC rights
	Write rights	Personalization agent issuance rights
EF.COM	Read rights	BAC rights, EAC rights
	Write rights	Personalization agent issuance rights

Table 27 Security Properties per Object

Application Notes :

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

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

The issuance rights of Personalization agent is acquired when the use of ePassport application program is requested at the ePassport issuance Phase according to FIA_UID.1, and the user recognized as the Personalization agent has succeeded in the Personalization agent authentication.

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

a) Execution of the operation is allowed only when security attributes of subjects are included in security attributes of the object's access-rights and operations corresponds to security attributes of the object's operation.
b) [None]

]

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

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

a) Explicitly deny access of subjects to objects if instructions order of the inspection system is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specifications
b) Explicitly deny read of subjects to biometric data if there is no the read-rights of biometric data in IS certificate of the EIS that has the EAC authorization
c) Explicitly deny access(read, write, etc.) of the unauthorized Inspection System to all objects
d) [None]

FDP_ACF.1(2) Security attribute based access control (OS 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 [OS access control policy] to objects based on [the following Table 28 and Table 29].

Subject	Security Properties
Personalization agent	Usage rights, management rights

Table 28 Security Properties per Subject

Object	Security Properties	
	Operation Security Properties	Access Rights Security Properties
Executable File	Loading rights	Management rights
	Deletion rights	Management rights
Application Program	Loading rights	Management rights
	Deletion rights	Management rights
	Selection rights	Usage rights
Personalization agent Basic Information	Reading rights	Usage rights, management rights
	Selection rights	Management rights
	Change rights	Management rights
Personalization agent Authentication Information	Selection rights	Management rights
	Change rights	Management rights

Table 29 Security Properties per Object

Caution when Applying:
Usage rights are acquired by the user recognized as the Personalization agent when the use of card manager is requested at the ePassport issuance Phase and usage Phase according to FIA_UID.1.

Management rights are acquired when the Personalization agent succeeds in Personalization agent authentication.

FDP_ACF.1.2 The TSF shall enforce the following in order to determine whether to allow the operation between a controlled subject and a controlled object: [

a) The mapped operation is permitted only if the security properties of the subject are included in the access rights security properties of the object, and the operation matches the operation security properties of the object.
b) [none]

]

FDP_ACF.1.3 The TSF shall specifically permit the access of the subject to the object based on the following additional rules: [none]

FDP_ACF.1.4 The TSF shall specifically deny the access of the subject to the object based on the following rules.

a) At the termination Phase, all operations except read operation for Personalization agent basic information are denied.
b) The deletion operation for ePassport application programs is denied.
c) The selection operation for an application program not installed is denied.
d) [Additional application installation will be rejected.]

FDP_DAU.1 Basic Data Authentication

Hierarchical to: No other components

Dependencies: No dependencies.

FDP_DAU.1.1 The TSF shall provide the ability to generate the evidence to be used for guaranteeing the validity of [ePassport user data].

FDP_DAU.1.2 The TSF shall provide an [inspection system] with the ability to verify the evidence regarding the validity of designated information.

Application Notes:

In order to guarantee the validity of ePassport user data, when AA request is received from inspection system (BIS or EIS), TOE generates digital signature from the random number value received in the AA request process with the AA chip authentication private key stored on the protected memory area which is provided to the inspection system. Inspection system verifies the digital signature with AA chip authentication public key acquired from EF.DG15 to verify the authenticity of TOE. Also, in the case of EAC-CA request from EIS, ECDH calculation is performed using the temporary public key generated using EAC-CA chip authentication public key information of EF.DG14 and the EAC-CA chip authentication private key stored on the protected memory of TOE, thus EIS verifies the authenticity of TOE depending on the success of EAC-CA.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) BAC session key
b) EAC session key
c) BAC authentication key
d) [SCP02 session key, random number value]

].

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

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

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

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

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]

The TSF shall enforce the [ePassport access control policy] to *transmit, receive* user data in a manner protected from *modification, deletion, insertion, and reuse*.

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

Application Notes : The TSF protects integrity of the transmitted data by using the MAC key for BAC session or EAC session. This provides the method of protection against modification, deletion and insertion of user data. Also, a method to protect from reuse using SSC is provided.

6.1.3. Identification and Authentication

FIA_AFL.1(1) Authentication failure handling (user session temination)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when the number of failed attempts related to [
a) BAC mutual authentication
b) EAC-TA
c) [SCP02 mutual authentication]
] reaches *1.*

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

FIA_AFL.1(2) Authentication failure handling (Retry Prohibited)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of identification

FIA_AFL.1.1 The TSF shall detect when the number of failed attempts related to [EAC-TA] reaches *1* .

When the defined number of unsuccessful authentication attempts has been met the TSF shall [prohibit retry of EAC-TA].

Application Notes:

When EAC-TA fails, the mechanism, to reject the additional EAC-TA by changing the life cycle of the application, is provided.

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) indication that support the BAC mechanism
b) [None]

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

FIA_UAU.1.2 The TSF shall authenticate the user successfully before allowing any other actions mediated by TSF on behalf of the user except the action specified in FIA_UAU.1.1.

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

Hierarchical to: No other components.

Dependencies: FIA_UAU.1(1) Timing of authentication(BAC mutual authentication)

FIA_UAU.1.1

The TSF shall allow [

a) to perform the EAC-CA
b) to read user data except the biometric data of the ePassport holder
c) [AA Performance]

] 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 (SCP02 mutual authentication)

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [reading Personalization agent basic information] which will be performed on behalf of the user before the user is authenticated.

FIA_UAU.1.2 The TSF shall authenticate the user successfully before allowing any other actions mediated by TSF on behalf of the user except the action specified in FIA_UAU.1.1.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to [

a) BAC mutual authentication
b) EAC-TA
c) [SCP02 mutual authentication]

].

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1

The TSF shall provide [

a) BAC mutual authentication
b) EAC-TA
c) [SCP02 mutual authentication]

] to support user authentication.

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

a) The BIS or EIS shall succeed the BAC mutual authentication in order to have the BAC authorization.
b) The EIS, in order to have the EAC authorization, shall succeed the BAC mutual authentication, EAC-CA and EAC-TA and include the read-rights of biometric data in all of the CVCA certificate, DV certificate and IS certificate. For this, the TSF shall provide the EAC-CA.
c) [For Personalization agent to have issuance rights or management rights, it must succeed in SCP02 mutual authentication.]

].

FIA_UID.1 Timing of identification

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

FIA_UID.1.1 The TSF shall allow [
a) to establish the messaging 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:
TOE recognizes the external entity requesting the use of ePassport application programs at the ePassport issuance Phase as the Personalization agent, and as the inspection system if at the ePassport usage Phase. Also, if the use of card manager is requested at the ePassport issuance or usage Phase, it is recognized as Personalization agent.

6.1.4. Security Management

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

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

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

FMT_MOF.1(2) Management of security functions behavior (OS security function)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to disable the functions [the following security functions] to *stop, resume, load, delete and change*.

Security Function	Role
Change of life cycle of application programs	Personalization agent
Installation of application programs	Personalization agent
Deletion of application programs	Personalization agent
Change of Personalization agent key	Personalization agent

Application Notes:
This determines whether to grant the application programs installed by the Personalization agent the rights to change OS life cycle. The application program may change the OS life cycle to the states of CARD_LOCKED and TERMINATED only.

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [ePassport access control policy, OS access control policy] to restrict the ability to *[initialization]* the security attributes [security attributes of subjects defined in FDP_ACF.1(1) and FDP_ACF.1(2)] to [TSF].

Application Notes : As an action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1, the TSF shall reset security attributes of subjects defined in FDP_ACF.1(1) and FDP_ACF.1(2).

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, OS access control policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [None] to specify alternative initial values to override the default values when an object or information is created.

Application Notes:
The operation security properties and access rights security properties of objects of ePassport access control policy and OS access control policy are determined according to Table 26 Security Properties per Subjectof FDP_ACF.1(1) and Table 27 Security Properties per Object오류! 참조 원본을 찾을 수 없습니다.of FDP_ACF.1(2) by the implemented logic of TOE at the development Phase and the change of default value is not allowed.

FMT_MTD.1(1) Management of TSF data (Certificate Verification Info.)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1
The TSF shall restrict the ability to *[write in secure memory]* the [
a) EAC chip authentication private key
b) initial current date
c) initial CVCA certificate
d) initial CVCA digital signature verification key
e) [AA chip authentication private key]
] to [Personalization agent in the Personalization phase].

FMT_MTD.1(2) Management of TSF data (SSC Initialization
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

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

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

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *modify* the [GP registry] to [Personalization agent].

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

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

a) Function to write user data and TSF data in the Personalization phase
b) Function to verify and update the CVCA certificate, CVCA digital signature verification key and current data in the Operational Use phase
c) [
   A. Function to load, install, and delete executable files and application programs at the issuance Phase and usage Phase of ePassport
   B. Function to write/change Personalization agent basic information, Personalization agent authentication information, and GP registry at the issuance Phase and usage Phase of ePassport

C. Granting application programs the rights to change the OS life cycle at the issuance Phase and usage Phase of ePassport
D. Function to inquire about Chip Serial Number of ePassport
]
]

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

FMT_SMR.1.1
The TSF shall maintain the roles [
a) Personalization agent
b) [None]
].

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

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

6.1.5. Privacy

FPR_UNO.1 Unobservability
Hierarchical to: No other components.
Dependencies: No dependencies.

FPR_UNO.1.1 The [TSF] shall ensure that [external entity] are unable to observe the operation [
a) FCS_COP.1(1) Cryptographic operation (Symmetric Key Cryptographic Operation)
b) FCS_COP.1(2) Cryptographic operation (MAC)
c) FCS_COP.1(4) Cryptographic operation (Digital Signature Verification for Certificates Verification)
d) FCS_CKM.1(1)(2) Cryptographic key generation(SCP02 session key)
e) FCS_COP.1(5) Cryptographic operation (Digital Signature Generation)

] on [

a) BAC authentication key
b) BAC session key
c) EAC session key
d) EAC chip authentication private key
e) [SCP02 session key]

]

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

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 in self-testing by FPT_TST.1
b) Conditions outside the normal operating of the TSF detected by the IC chip
c) [State with power supply shut off during TSF operation]

]

FPT_ITI.1 Inter-TSF detection of modification
Hierarchical to: No other components.
Dependencies: No dependencies.

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

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data

transmitted between the TSF and a remote trusted IT product and perform [

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

] if modifications are detected.

Application Notes : The Strength of Retail MAC is equivalent to the secure Retail MAC. Also, Personalization agent messaging uses SCP02 secure messaging, which detects change through Retail MAC.

FPT_PHP.3 Resistance to physical attack
Hierarchical to: No other components.
Dependencies: No dependencies

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

Application Notes :
The SFR provided by the IC chip is applied as it is.

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 *during initial start-up* to demonstrate the correct operation of *TSF*.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *parts of TSF*.

6.2. TOE Security Assurance Requirements

The security assurance requirements for this Security Target consist of the following

components from Part 3 of the CC, summarized in the following [Table 30 Assurance Requirements] and evaluation assurance level is EAL5+(ADV_IMP.2).

In this Security Target, the assurance components are augmented follows:

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

Assurance Class	Component	
Security Target	ASE_INT.1	Security Target Introduction
	ASE_CCL.1	Conformance Claims
	ASE_SPD.1	Definition of Security Problems
	ASE_OBJ.2	Security Objective
	ASE_ECD.1	Extended Component Definitions
	ASE_REQ.2	Derived Security Requirements
	ASE_TSS.1	TOE Summary Specification
Development	ADV_ARC.1	Security Structure Specification
	ADV_FSP.5	Semi-Standardized and Complete Function Specification Providing Additional Error Information
	ADV_IMP.2	Complete mapping of the implementation representation of TSF
	ADV_INT.2	Well-structured inside of TSF
	ADV_TDS.4	Semi-standardized modularization design
Manual	AGD_OPE.1	User operation manual
	AGD_PRE.1	Preparation procedure
Life Cycle Support	ALC_CMC.4	Production support, reception procedure, and automation
	ALC_CMS.5	Scope of configuration management of development tools
	ALC_DEL.1	Distribution procedure
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Life cycle model defined by developer
	ALC_TAT.2	Applied implementation standard
Test	ATE_COV.2	Analysis of test range
	ATE_DPT.3	Modularization design test
	ATE_FUN.1	Function test
	ATE_IND.2	Independent test: specimen test
Vulnerability Test	AVA_VAN.4	Systematic vulnerability analysis

Table 30 Assurance Requirements

6.2.1. Security Target

ASE_INT.1 ST Introduction

Dependencies: No dependencies.

Developer action elements :

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

Content and presentation elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

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

ASE_CCL.1 Conformance Claim

Dependencies:

ASE_INT.1 ST Introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements :

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

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

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

Evaluator action elements:

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

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

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

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

Evaluator action elements:

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

ASE_OBJ.2 Security objectives

Dependencies:

ASE_SPD.1 Security problem definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

Evaluator action elements:

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

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

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

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.
ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:
ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C All operations shall be performed correctly.
ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

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

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:
ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

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

Evaluator action elements:

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

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

6.2.2. Development

ADV_ARC.1 Security architecture description

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

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

ADV_FSP.5 Semi-standardized and complete function specification providing additional error information

Dependencies:

ADV_TDS.1 Basic Design

ADV_IMP.1 Expression of Implementation regarding TSF

Developer action elements:

ADV_FSP.5.1D The developer must provide function specification.

ADV_FSP.5.2D The developer must provide traceability from function specification to SFR.

Content and presentation elements:

ADV_FSP.5.1C Function specification must express TSF completely.

ADV_FSP.5.2C **Function specification must describe TSFI in a semi-standardized method.**

ADV_FSP.5.3C Function specification must describe the objective and usage method for all TSFI.

ADV_FSP.5.4C Function specification must identify and describe all parameters related to each TSFI.

ADV_FSP.5.5C Function specification must describe all actions related to each TSFI.

ADV_FSP.5.6C Function specification must describe all direct error messages occurring as a result of each TSFI call.

ADV_FSP.5.7C **Function specification must describe all error messages occurring from causes other than TSFI calls.**

ADV_FSP.5.8C **Traceability must provide the rationale for each error message whose function specification is included in TSF implementation but occurring from causes other than TSFI call.**

ADV_FSP.5.9C Traceability must prove that SFR is traced to TSFI in function specification.

Evaluator action elements:

ADV_FSP.5.1E The evaluator must confirm that provided information satisfies all evidence requirements.

ADV_FSP.5.2E The evaluator must determine if the function specification substantializes

SFR precisely and completely.

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

Dependencies: ADV_TDS.3 Basic modular design
ALC_TAT.1 Well-defined development tools
ALC_CMC.5 Advanced support

Developer action elements:

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

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

Content and presentation elements:

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

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

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

Evaluator action elements:

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

ADV_INT.2 Well-Structured Inside of TSF

Dependencies:
ADV_IMP.1 Expression of Implementation regarding TSF
ADV_TDS.3 Basic Modularization Design
ALC_TAT.1 Well-Defined Development Tool

Developer action elements:

ADV_INT.2.1D The developer must design and implement so that the entire TSF is well-structured inside.

ADV_INT.2.2D The developer must provide explanation and justification for the inside of TSF.

Content and presentation elements:

ADV_INT.2.1C Justification must describe the characteristics used to judge the meaning of "well-structured."

ADV_INT.2.2C The explanation of inside the TSF shall prove that the entire TSF is well-structured.

Evaluator action elements:

ADV_INT.2.1E The evaluator must confirm that the provided information satisfies all evidence requirements.

ADV_INT.2.2E The evaluator must perform internal analysis regarding TSF.

ADV_TDS.4 Basic modular design

Dependencies:

ADV_FSP.5 Semi-standardized and complete function specification providing additional error information

Developer action elements:

ADV_TDS.4.1D The developer shall provide the design of the TOE.

ADV_TDS.4.2D

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

Content and presentation elements:

ADV_TDS.4.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.4.2C The design must **designate each module as SFR-Execution, SFR-Support or SFR-No_interference** and describe TSF from the perspectives of modules.

ADV_TDS.4.3C The design shall identify all subsystems of the TSF.

ADV_TDS.4.4C The design must provide **semi-standardized** explanation on each subsystem of TSF and, when necessary, must **support non-standardized explanation text**.

ADV_TDS.4.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.4.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.4.7C The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

ADV_TDS.4.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

ADV_TDS.4.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.4.10C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke it.

Evaluator action elements:

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

ADV_TDS.4.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3. Guidance Documents

AGD_OPE.1 Operational user guidance

Dependencies:

ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

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

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

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

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of

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

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

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

Evaluator action elements:

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

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

6.2.4. Life-cycle support

ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage

ALC_DVS.1 Identification of security measures
ALC_LCD.1 Developer defined life-cycle model Objectives

Developer action elements:
ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.4.2D The developer shall provide the CM documentation.
ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:
ALC_CMC.4.1C The TOE shall be labeled with its unique reference.
ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.
ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6C The CM documentation shall include a CM plan.
ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:
ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.5 Development tools CM coverage
Dependencies: No dependencies.

Developer action elements:
ALC_CMS.5.1D
The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.5.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

Evaluator action elements:

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

ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation elements:

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

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

Evaluator action elements:

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

ALC_TAT.2 Applied Implementation Standard

Dependencies:

ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.2.1D The developer shall provide the documentation identifying each development tool being used for the TOE.

ALC_TAT.2.2D The developer shall document and provide the selected implementation-dependent options of each development tool.

ALC_TAT.2.3D **The developer must describe the implementation standard he/she is applying.**

Content and presentation elements:

ALC_TAT.2.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.2.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.2.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

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

ALC_TAT.2.2E **The evaluator must confirm that the implementation standard is applied**.

6.2.5. Testing

ATE_COV.2 Analysis of coverage

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

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

ATE_DPT.3 Modularization Design Test

Dependencies:

ADV_ARC.1 Security architecture description

ADV_TDS.4 Semi-standardized modular design

ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.3.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and SFR-enforcing modules in the TOE design.

ATE_DPT.3.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.3.3C The analysis of the depth of testing shall demonstrate that the SFR-enforcing modules in the TOE design have been tested.

Evaluator action elements:

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

ATE_FUN.1 Functional testing

Dependencies:

ATE_COV.1 Evidence of coverage

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

ATE_IND.2 Independent testing - sample

Dependencies:

ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

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

6.2.6. Vulnerability analysis

AVA_VAN.4 Methodical vulnerability analysis

Dependencies:

ADV_ARC.1 Security architecture description

ADV_FSP.2 Complete functional specification
ADV_TDS.3 Basic modular design
ADV_IMP.1 Implementation representation of the TSF
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:
AVA_VAN.4.1D The developer shall provide the TOE for testing.

Content and presentation elements:
AVA_VAN.4.1C The TOE shall be suitable for testing.

Evaluator action elements:
AVA_VAN.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.4.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.4.3E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.4.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing Moderate attack potential.

6.3. Security Requirements Rationale

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

6.3.1. TOE Security Functional Requirements Rationale

The rationale of TOE security functional requirements demonstrates the followings :

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

Security Objects			Security Object of TOE

Security Functional Requirements	O.Management	O. Security_Mechanism_Application_Procedures	O.Session_Termination	O. Secure_Messaging	O. Certificate_Verification	O. Secure_State	O. Deleting_Residua_Info	O. Replay_Prevention	O. Access_Control	O. Handling_Info_Leakage	O.AA	O.BAC	O.EAC	O.IC칩	O.SCP02
FCS_CKM.1(1)												X	X		
FCS_CKM.1(2)															X
FCS_CKM.2(1)								X				X			
FCS_CKM.2(2)													X	X	
FCS_CKM.3				X											
FCS_CKM.4							X								
FCS_COP.1(1)				X								X		X	
FCS_COP.1(2)				X								X		X	
FCS_COP.1(3)												X	X	X	
FCS_COP.1(4)					X								X	X	
FCS_COP.1(5)											X			X	
FCS_RNG.1														X	
FDP_ACC.1(1)									X						
FDP_ACC.1(2)									X						
FDP_ACF.1(1)	X	X							X			X	X		X
FDP_ACF.1(2)	X								X						X
FDP_DAU.1											X		X		
FDP_RIP.1							X	X							
FDP_UCT.1				X				X							
FDP_UIT.1				X				X							
FIA_AFL.1(1)		X	X						X			X			X
FIA_AFL.1(2)		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.4								X				X	X		X
FIA_UAU.5		X							X			X	X		X
FIA_UID.1												X	X		X
FMT_MOF.1(1)	X								X						
FMT_MOF.1(2)	X								X						
FMT_MSA.1				X					X						
FMT_MSA.3	X								X						
FMT_MTD.1(1)	X								X						
FMT_MTD.1(2)		X													
FMT_MTD.1(3)	X								X						
FMT_MTD.3					X			X					X		
FMT_SMF.1	X				X										
FMT_SMR.1	X														
FPR_UNO.1										X				X	
FPT_FLS.1						X									
FPT_ITI.1			X	X											
FPT_PHP.3														X	

FPT_TST.1						X									

Table 31 presents the mapping between the security objectives and the security functional requirements.

Security Objects / Security Functional Requirements			Security Object of TOE												
	O.Management	O. Security_Mechanism_Application_Procedures	O.Session_Termination	O. Secure_Messaging	O. Certificate_Verification	O. Secure_State	O. Deleting_Residua_Info	O. Replay_Prevention	O. Access_Control	O. Handling_Info_Leakage	O.AA	O.BAC	O.EAC	O.IC칩	O.SCP02
FCS_CKM.1(1)												X	X		
FCS_CKM.1(2)															X
FCS_CKM.2(1)								X				X			
FCS_CKM.2(2)													X	X	
FCS_CKM.3				X											
FCS_CKM.4							X								
FCS_COP.1(1)				X								X		X	
FCS_COP.1(2)				X								X		X	
FCS_COP.1(3)												X	X	X	
FCS_COP.1(4)					X								X	X	
FCS_COP.1(5)											X			X	
FCS_RNG.1														X	
FDP_ACC.1(1)									X						
FDP_ACC.1(2)									X						
FDP_ACF.1(1)	X	X							X			X	X		X
FDP_ACF.1(2)	X								X						X
FDP_DAU.1											X		X		
FDP_RIP.1							X	X							
FDP_UCT.1				X				X							
FDP_UIT.1				X				X							
FIA_AFL.1(1)		X	X						X			X			X
FIA_AFL.1(2)		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.4								X				X	X		X
FIA_UAU.5		X							X			X	X		X
FIA_UID.1												X	X		X
FMT_MOF.1(1)	X								X						
FMT_MOF.1(2)	X								X						
FMT_MSA.1				X					X						
FMT_MSA.3	X								X						
FMT_MTD.1(1)	X								X						
FMT_MTD.1(2)		X													
FMT_MTD.1(3)	X								X						
FMT_MTD.3					X			X					X		
FMT_SMF.1	X				X										

FMT_SMR.1	X														
FPR_UNO.1										X				X	
FPT_FLS.1						X									
FPT_ITI.1			X	X											
FPT_PHP.3														X	
FPT_TST.1						X									

Table 31 Correspondence of Security Objectives and Security Function Requirements

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

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

FCS_CKM.1(2) Cryptographic Key Generation (SCP02 session key)

This component demands generation of SCP02 session key of 112 bit according to the session key generation algorithm specified in 'GP Standard.' Through this, the SCP02 session key to be used in SCP02 mutual authentication and SCP02 secure messaging is generated. Therefore, this component satisfies security objective O.SCP02.

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

This component defines the method to distribute seed of key derivation mechanism necessary in generating the BAC session key to the Inspection System (ISO/IEC 11770-2 Key Establishment Mechanism 6). The distribution method defined in this component satisfies the security objective of O.Replay_Prevention as it uses random numbers and O.BAC as it enables to generate the BAC session key of FCS_CKM.1(1) by generating KDF seed.

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

This component defines the method(Elliptic Curve Diffie-Hellmankey-agreement protocol) to distribute seed of key derivation mechanism necessary in generating the EAC-CA session key to the Inspection System. The distribution method defined in this component satisfies the security objective of O.EAC as it generates KDF seed by using the public key from the Inspection System and the private key stored while the ePassport personalization phase.

FCS_CKM.3 Cryptographic key access

This component provides the key access method according to 'GP Standard' and 'Javacard platform' standard API, thus satisfying security objective O.Secure Messaging.

FCS_CKM.4 Cryptographic key destruction

This component defines the method of securely destroying the key generated by key derivation mechanism of FCS_CKM.1(1) and SCP02 session key generation of FCS_CKM.1(2). This component suggests the method of destroying the key generated by TSF and remaining in temporary memory area by filling with '0,' thus satisfying the security objective O.Deletion of Residual Information.

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

This component defines the TDES cryptographic calculation which is used to protect from the leakage of the ePassport User Data when it is used to be authenticated by the Inspection System supporting the BAC or transferred. The cryptographic calculation defined in this component encrypts the ePassport User Data transferred between the TOE and the Inspection System so it guarantees the secrecy and satisfies the security objective of O.Secure_Messaging. The cryptographic calculation defined in this component is required for the BAC mutual authentication so it satisfies the security objective, O.BAC. This component satisfies the O.IC_Chip by using the TDES cryptographic function of the IC chip.

FCS_COP.1(2) Cryptographic operation (MAC)

This component defines the Retail MAC for the authentication of the Inspection System supporting the BAC or for the detecting the change of the transmitting ePassport User Data. The MAC calculation defined in this component guarantees the integrity and satisfies the security objective, O.Secure_Messaging, by detecting the change of the ePassport User Data transmitted between the TOE and the Inspection System. The MAC calculation defined in this component is required for the BAC mutual authentication so it satisfies the security objective, O.BAC. This component satisfies the O.IC_Chip by using the TDES cryptographic function of the IC chip.

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

This component defines the hash function, SHA-1, required for the KDF implementation according to GCS_CKM.1. The hash function defined in this component satisfies the

security objectives, O.BAC and O.EAC, by making the KDF to create the BAC session key and the EAC session key. This component satisfies the O.IC_Chip by using the SHA function.

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

This component defines the method of the digital signature authentication required for the EAC-TA procedure. The method of the digital signature authentication defined in this component satisfies the O.Certificate_Verification by authenticating the CVCS link, DV, IS certifications which is provided by the Inspection System to the TOE. Also it satisfies the security objective, O.EAC, by providing the method of the digital signature authentication, EAC-TA while accessing to the biometric data of the ePassport applicant, the access authority is checked. This component satisfies the O.IC_Chip by using the ECC library of the IC chip.

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

This component defines the way of creating the digital signature value required for the AA procedure. The way of creating the digital signature value in this component satisfies the O.AA by providing the function to verify the illegal copy of the ePassport by checking the digital signature value, which is created by the TOE, by the Inspection System.

FCS_RNG.1 Random number generation

This component satisfies the O.IC_Chip by generating the random number using the TRGN of the IC chip.

FDP_ACC.1(1) Subset access control (ePassport access control)

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

FDP_ACC.1(2) Subset access control (OS Access Control)

This component defines the list of subjects, objects, and operations in order to determine the control scope of OS access control policy. The OS access control policy defined in this component defines the Personalization agent as the subject, executable file, application

programs, Personalization agent basic information, Personalization agent authentication information as objects, and their relationship as operations, thus satisfying security objective O.Access Control.

FDP_ACF.1(1) Security attribute based access control (ePassport access control)

In order to enforce the ePassport access control policies, this component defines security attributes of subjects and objects defined in FDP_ACC.1(1) and specifies the ePassport access control rules. Security attributes and the ePassport access control rules defined in this component satisfy the security objectives of O.Management and O.Access_Control as only the authorized Personalization agent with the Personalization agent issuing authorization can perform management functions. Also, this component satisfies the security objectives of O.BAC, O.EAC and O.Access_Control because the read-rights for the personal data of the ePassport holder and ePassport authentication data, etc. is allowed only to the subjects holding the BAC authorization and the read-rights for the biometric data of the ePassport holder is allowed only to the subjects holding the EAC authorization. The explicitly deny rules of FDP_ACF.1.4 defined in this component satisfy the security objective of O.Security_Mechanism_Application_Procedures because the application order of security mechanisms is ensured as access by the Inspection System is denied when the order of transmitted instructions specified in 2.1 Inspection Procedures of the EAC specifications is violated.

FDP_ACF.1(2) Security attribute based access control (OS Access Control)

This component defines the security properties of subjects and objects defined in FDP_ACC.1(2) and specifies OS access control rules in order to perform OS access control policy. The security properties and OS access control rules defined in this component grants management rights to the Personalization agent so that only authorized Personalization agent may perform OS management functions, thus satisfying security objectives O.Management and O.Access Control. Also, it provides OS management method only to the subject with Personalization agent management rights, thus satisfying security objective O.SCP02.

FDP_DAU.1 Basic Data Authentication

This component, in order to verify the validity of ePassport user data, uses the AA chip authentication private key stored on protected memory to generate digital signature when requested by the inspection system and provides it to the inspection system, and the inspection system verifies the digital signature with AA chip authentication public key

acquired in EF.DG15 to confirm if the AA chip authentication private key of protected memory and the AA chip authentication public key of EF.DG15 are a valid key pair so that whether EF file has been modified or not can be checked, thus satisfying security objective O.AA. Also, this component performs ECDH calculation using the temporary public key generated by EIS with EAC chip authentication public key information of EF.DG14 and the EAC chip authentication private key stored on the protected memory of TOE. Depending on the success of EAC-CA, and depending on whether the EAC chip authentication private key of protected memory and EAC chip authentication public key of EF.DG14 are a valid key pair or not, the modification of EF can be confirmed, thus satisfying security objective O.EAC.

FDP_RIP.1 Subset residual information protection

This component ensures that previous information is not included when the TSF allocates or deallocates memory resources for the SCP02 session key, BAC authentication key, BAC session key, EAC session key and random numbers. This component satisfies the security objective of O.Deleting_Residua_Info as it ensures that previous information of the SCP02 session key, BAC authentication key, BAC session key and EAC session key is not available when destroying these keys according to the method of destruction defined in FCS_CKM.4. Also, this component satisfies the security objective of O.Replay_Prevention by ensuring that previous information of random numbers used for the SCP02 mutual authentication, BAC mutual authentication, TAC-TA and generation of session key is not available.

FDP_UCT.1 Basic data exchange confidentiality

This component defines the method to protect from disclosure when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies. This component establishes the BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session encryption key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session encryption key. Therefore, this component satisfies the security objective of O.Secure_Messaging as the confidentiality of user data is ensured. This component satisfies the security objective of O.Replay_Prevention by ensuring that the BAC session encryption key is not used the same as the BAC authentication key when establishing the BAC secure messaging.

FDP_UIT.1 Data exchange integrity

This component defines the method to protect from modification, deletion, insertion,

replay when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies. This component establishes the BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session MAC key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session MAC key. Therefore, this component satisfies the security objective of O.Secure_Messaging as the integrity of user data is ensured. This component satisfies the security objective of O.Replay_Prevention by ensuring that the BAC session MAC key is not used the same as the BAC authentication key when establishing the BAC secure messaging.

FIA_AFL.1(1) Authentication failure handling (User Session Termination)

This component detects if the number of authentication attempts for SCP02 mutual authentication and BAC mutual authentication is greater than 1, and requires termination of user session. This component satisfies the security objective of O.Session_Termination as the session is terminated if the authentication attempt failure number of the SCP02 mutual authentication and BAC mutual authentication is surpassed. Also, this component satisfies the security objective of O.Security_Mechanism_Application_Procedures by disabling the unauthorized external entity to move on to the next phase of inspection procedures by terminating session if the BAC mutual authentication fails. In addition, this component satisfies the security objectives of O.BAC, O.EAC and O.Access_Control because access to user data is denied by terminating session as the SCP02 mutual authentication or BAC mutual authentication failure is considered that there is no the access-rights for user data.

FIA_AFL.1(2) Authentication failure handling (Retry Prohibition)

This component detects if the number of authentication attempts for EAC-TA is greater than 1, and requires prohibiting retry of EAC-TA in the same user session. This component regards the failure in EAC-TA as having no access rights to ePassport applicant bio information and thus denies access to ePassport applicant bio information, thus satisfying security objectives of O.Security Mechanism Application Procedure, O.EAC, and O.Access Control.

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

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

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

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

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

In this component, only the Inspection System of which the BAC mutual authentication succeeded in FIA_UAU.1(1) can execute EAC-CA and reading of user data(exception of the biometric data of the ePassport holder). To read the biometric data of the ePassport holder, the EAC-TA shall be executed. This component satisfies the security objectives of O.Security_Mechanism_Application_Procedures, O.Session_Termination, O.EAC and O.Access_Control as it enables detection by FIA_AFL.1(1) ,if authentication fails and allows the read-rights for the biometric data of the ePassport holder if authentication succeeds.

FIA_UAU.1(3) Timing of authentication (SCP02 mutual authentication)

This component defines the functions the user can perform before SCP02 mutual authentication and performs SCP02 mutual authentication on the user. This component performs SCP02 mutual authentication before the Personalization agent identified in FIA_UID.1 uses management function on ePassport applicant identification information and TSF data. If the authentication fails, detection by FIA_AFL.1(2) is allowed, and if the authentication succeeds, the management functions on ePassport applicant basic information and TSF data are allowed, thus satisfying security objectives of O.Session Termination, O.SCP02, O.Access Control.

FIA_UAU.4 Single-use authentication mechanisms

This component requires that authentication-related information sent by the TSF to the Inspection System in the SCP02 mutual authentication, BAC mutual authentication and the EAC-TA, is not replay. This component satisfies the security objectives of O.Replay_Prevention, O.BAC, O.EAC and O.SCO02 as the TSF executes the SCP02 mutual authentication, BAC mutual authentication and EAC-TA by generating different random numbers used in the SCP02 mutual authentication, BAC mutual authentication and EAC-TA

per session and transmitting them to the Inspection System.

FIA_UAU.5 Multiple authentication mechanisms

This component defines various authentication mechanisms and defines the rules for applying authentication mechanisms according to the type of user data the inspection system wishes to access. For this component, the Personalization agent is given the issuing rights/management rights if it succeeds in SCP02 mutual authentication according to the rules for authentication mechanism application, and the inspection system is given the BAC rights if it succeeds in BAC mutual authentication, and succeeding in EAC-CA, EAC-TA and certificate verification after BAC mutual authentication, it acquires EAC rights, thus satisfying security objectives of O.Security Mechanism Application Procedure, O.Access Control, O.BAC, O.EAC, and O.SCP02.

FIA_UID.1 Timing of identification

This component requires to establish the messaging based on contactless IC card transmission protocol (ISO/ IEC 14443-4) as the functions the user to be performed before the identification and to identify the user. This component satisfies the security objectives of O.BAC, O.EAC and O.SCP02 as the external entity is identified with the Inspection System, if an external entity to establish the messaging request to use the MRTD application.

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

This component defines that the ability to disable writing function is given only to the Personalization agent in the Personalization phase. This component satisfies the security objectives of O.Management and O.Access_Control by deactivating the writing function of the Personalization agent in the Personalization phase so that the TOE in the Operational Use phase cannot record any data.

FMT_MOF.1(2) Management of security functions behavior (OS Life Cycle Change)

This component defines that the application program gives the ability to determine the action regarding the change of OS life cycle only to Personalization agent. This component allows the application program to determine whether the change of OS life cycle state when the Personalization agent installs the application program, thus satisfying security objective of O.Management.

FMT_MSA.1 Management of security attributes

This component requires to restrict the ability of initializing user security attributes only to the TSF as an action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1. This component satisfies the security objectives of O.Secure_Messaging and O.Access_Control as the integrity is ensured and access to the MRTD application data is blocked by resetting the previously given security attributes of the Personalization agent or the Inspection System as an action to be taken if the TSF detects modification of the transmitted TSF data.

FMT_MSA.3 Static attribute Initialization

This component requires that when generating objects, the security properties have a limited value as the default value, and that specifying initial values are denied. In this component, in order to perform ePassport access control policy and OS access control policy, the security properties for ePassport user data and OS user data is specified by TOE implementation logic and does not allow specifying initial values, thus satisfying security objectives of O.Management, O.Access Control.

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

This component restricts that only the Personalization agent in the Personalization phase writes certificate verification information necessary for the EAC-TA in secure memory. This component satisfies the security objectives of O.Management and O.Access_Control by enabling only the authorized Personalization agent to have the ability to write TSF data, such as the EAC chip authentication private key, current data, CVCA certificate and CVCA digital signature verification key, etc., in secure memory in the Personalization phase

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

This component requires to terminate BAC secure messaging before the EAC secure messaging is established. This component satisfies the security objective of O.Security_Mechanism_Application_Procedures by initializing SSC (send sequence counter) to „0" in order to terminate the BAC secure messaging after generating the EAC session key and newly establishing the EAC secure messaging.

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

This component controls that only the Personalization agent successful with SCP02 authentication may change GP registry. This component limits the rights for GP registry change to Personalization agent, thus satisfying security objective of O.Managemen.t

FMT_MTD.3 Secure TSF Data

This component requires to allow only secure values as the TSF data in order to ensure the secure random numbers and to ensure that valid date of certificates used in EAC-TA has not expired. This component satisfies the security objective of O.Replay_Prevention because only the secure random numbers are used in order to prevent a replay attack when the TSF generates session key. Also, the TSF compares the CVCA link certificate provided by the Inspection System with the CVCA certificate stored in the TOE in order for verification of the IS certificate used in the EAC-TA. If the CVCA certificate update is necessary, the TSF internally updates the CVCA certificate, CVCA digital signature verification key, current dates and EF.CVCA, therefore maintains the TSF data as secure values. This component satisfies the security objectives of O.Certificate_Verification and O.EAC because the EAC-TA can be successfully executed by verifying the DV certificate and IS certificate with the secure CVCA certificate.

FMT_SMF.1 Specification of management functions

This component provides the means to manage the MRTD application data in the Personalization phase. This component satisfies the security objective of O.Management as it defines the writing function of user data and TSF data in the Personalization phase. Also, this component satisfies the security objective of O.Certificate_Verification as it provides the function for the TSF to update the CVCA certificate, the CVCA digital signature verification key and current dates, etc. by itself in the Operational Use phase.

Also, this component provides application program management function, Personalization agent basic information, Personalization agent authentication information, functions for reading/changing GP registry, and granting OS life cycle change rights to application program as methods to manage OS application data, thus satisfying security objective O.Management.

FMT_SMR.1 Security roles

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

FPR_UNO.1 Unobservability

This component guarantees that the external entity cannot observe the information related with the cryptographic such as the BAC authentication key, the BAC session key, the EAC session key and the private key for the EAC chip authentication when the TSF processes the cryptographic calculation. This component satisfies the

O.Handling_Info_Leakage by guaranteeing that the external entity cannot find out and exploit the cryptography-related data from physical phenomena(change of current, voltage and electromagnetic, etc.) occurred when the TSF performs cryptographic operations such as the TDES, the MAC and the digital signature authentication. This component satisfies the O.IC_Chip by using the functions such as the TDES and the ECC.

FPT_FLS.1 Failure with preservation of secure state

This component requires that when malfunctioning such as failure detected in self-test and abnormal operation status detected by IC chip, a secure state is maintained. This component stops the operation of TOE when it detects change in integrity of TSF data or executable code in the self-test of FPT_TST.1 or the IC chip detects and notifies of abnormal operation status so as to prevent TSF malfunction, and in the case power supply is shut off during TSF operation, the operations stopped by power supply shut-off are restored to the state before the operation began to maintain secure state when the TOE reoperates, thus satisfying the security objective of O.Secure State.

FPT_ITI.1 Inter-TSF detection of modification

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

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

FPT_PHP.3 Resistance to physical attack

This component is required to resist physical manipulation and physical probing against TSF automatically. This component satisfies the O.IC_Chip by providing the detection of the abnormal action and the physical protection.

FPT_TST.1 TSF testing

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

For this component, self-tests are performed on TSF when initiating TOE to prove precise operative of O.Secure State. Also, the integrity of TSF and TSF data stored on TOE is verified to detect their loss and detecting the loss, thus satisfying security objective of

O.Secure State.

6.3.2. Security Assurance Requirements Rationale

The EAL(Evaluation Assurance Level) of this Security Target was selected as EAL5+ (ADV_IMP.2) by considering the value of assets protected by the TOE and level of threats, etc.

EAL5 allows the developer to acquire the maximum assurance from security engineering based on strict commercial development methodology, which refers to applying an eased version of expert security engineering techniques. Such TOE must be designed and developed with the intention of achieving EAL5 assurance. The additional cost from strict development is not very great. EAL5 demands high-level of security with independent assurance from the development planned by the developer or the user, and is applicable to a case which requires using a strict development methodology without the burden of inappropriate cost due to expert security engineering techniques.

Security Target partially selected assurance components that are higher than EAL4. The rationale of the augmented with assurance components are as follows.

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

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

After ePassport is issued with IC chip inside, it is difficult to make a correction even if a fault occurs, and accordingly the attacker may abuse this. Therefore, ADV_IMP.2 was added to implement TSF precisely and analyze the expression of the entire implementation for existence of faulty code.

6.3.3. Rationale of Dependency

6.3.3.1. Dependency of TOE Security Functional Requirements

Table 32 shows dependency of TOE functional components.

Number	Security Function Component	Dependency	Reference
1	FCS_CKM.1(1)	[FCS_CKM.2 OR FCS_COP.1]	3
		FCS_CKM.4	5
2	FCS_CKM.1(2)	[FCS_CKM.2 OR FCS_COP.1]	3
		FCS_CKM.4	5
3	FCS_CKM.2(1)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
		FCS_CKM.4	5
4	FCS_CKM.3	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	
		FCS_CKM.4	5
5	FCS_CKM.4	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
7	FCS_COP.1(1)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
		FCS_CKM.4	5
8	FCS_COP.1(2)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
		FCS_CKM.4	5
9	FCS_COP.1(3)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
		FCS_CKM.4	5
10	FCS_COP.1(4)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
		FCS_CKM.4	5
11	FCS_COP.1(5)	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1]	1
		FCS_CKM.4	5
12	FCS_RNG.1	-	-
13	FDP_ACC.1(1)	FDP_ACF.1	8
14	FDP_ACC.1(2)	FDP_ACF.1	9
15	FDP_ACF.1(1)	FDP_ACC.1	7
		FMT_MSA.3	25
16	FDP_ACF.1(2)	FDP_ACC.1	7
		FMT_MSA.3	25
17	FDP_DAU.1	–	–
18	FDP_RIP.1	–	–
19	FDP_UCT.1	[FTP_ICT.1 OR FTP_TRP.1]	N/A (NO.1)
		[FDP_ACC.1 OR FDP_IFC.1]	6
20	FDP_UIT.1	[FDP_ACC.1 OR FDP_IFC.1]	6
		[FTP_ITC.1 OR FTP_TRP.1]	N/A (NO.1)
21	FIA_AFL.1(1)	FIA_UAU.1	16,18
22	FIA_AFL.1(2)	FIA_UAU.1	17
23	FIA_UAU.1(1)	FIA_UID.1	21
24	FIA_UAU.1(2)	FIA_UAU.1(1)	16(NO.2)
25	FIA_UAU.1(3)	FIA_UID.1	21

Number	Security Function Component	Dependency	Reference
26	FIA_UAU.4	–	–
27	FIA_UAU.5	–	–
28	FIA_UID.1	–	–
29	FMT_MOF.1(1)	FMT_SMF.1	30
		FMT_SMR.1	31
30	FMT_MOF.1(2)	FMT_SMF.1	30
		FMT_SMR.1	31
31	FMT_MSA.1	[FDP_ACC.1 OR FDP_ICF.1]	6
		FMT_SMF.1	30
		FMT_SMR.1	31
32	FMT_MSA.3	FMT_MSA.1	24
		FMT_SMR.1	31
33	FMT_MTD.1(1)	FMT_SMF.1	30
		FMT_SMR.1	31
34	FMT_MTD.1(2)	FMT_SMF.1	30
		FMT_SMR.1	31
35	FMT_MTD.1(3)	FMT_SMF.1	30
		FMT_SMR.1	31
36	FMT_MTD.3	FMT_MTD.1	26
37	FMT_SMF.1	–	–
38	FMT_SMR.1	FIA_UID.1	21
39	FPR_UNO.1	–	–
40	FPT_FLS.1	-	-
41	FPT_ITI.1		
42	FPT_PHP.3	–	–
43	FPT_TST.1	-	-

Table 32 Security Function Component Dependency

NO.1

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

NO.2

FIA_UAU.1(2) shall have dependency with FIA_UID.1, but the dependency changed to FIA_UAU.1(1) by refinement operation. Since the EAC-TA is executed after the BAC

mutual authentication, FIA_UAU.1(2) depends on FIA_UAU.1(1) and FIA_UAU.1(1) depends on FIA_UID.1. Therefore, indirectly, the dependency is satisfied.

6.3.3.2. Dependency of TOE Security Assurance Requirements

The dependency of EAL5 provided in Common Criteria is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in [Table 33 Dependency of Added Assurance Components]

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

Number	Assurance Component	Dependency	Reference Number
1	ADV_IMP.2	ADV_TDS.3	EAL4
		ALC_TAT.1	EAL4
		ALC_CMC.5	N/A

Table 33 Dependency of Added Assurance Components

6.4. Rationale of Mutual Support and Internal Consistency

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

In „6.3.3.1 Dependency of TOE security functional requirements‟ and „6.3.3.2 Dependency of TOE security assurance requirements‟, the dependency is analyzed as a supportive relationship among security requirements of which it is necessary to depend on other security requirements in order to achieve a security objective because a security requirement is insufficient. In case the dependency was not satisfied, additional rationale is provided. Also, security functional requirements, although there is no dependency among security functional requirements, are mutually supportive and internally consistency in relation to the TSF operations as of the following.

In the Personalization phase, the Personalization agent records the MRTD application data (FMT_MTD.1(1), FMT_MSA.3) and deactivates writing function so that the TOE is not modified by external entities when delivering the TOE to the Operational Use phase(FMT_MOF.1(1), FMT_SMF.1). The role of the Personalization agent as such is defined as the security role (FMT_SMR.1) and is controlled by the ePassport access

control policies (FDP_ACC.1(1), FDP_ACF.1(1)). Therefore, these security requirements are mutually supportive and internally consistent.

The TSF, after identifying the Inspection System (FIA_UID.1), executes the BAC mutual authentication (FIA_UAU.1(1)), the EAC-TA (FIA_UAU.1(2)) and SCP02 mutual authentication(FIA_UAU.1(3)) according to authentication mechanism application rules (FIA_UAU.5). If the Personalization agent or inspection system fails SCP02 mutual authentication or BAC mutual authentication, the session is closed (FIA_AFL.1(1)), and if the inspection system fails EAC-TA, retry of EAC-TA in the same user session is prohibited (FIA_AFL.1(2)). The random numbers must be used so that to prevent reuse of authentication-related data used in authentication (FIA_UAU.4). In order to ensure the secure random numbers used and the secure certificates used in the EAC-TA, the certificates must be verified and updated (FMT_MTD.3). Therefore, these security requirements are mutually supportive and internally consistent.

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

After cryptographic calculation, the TSF shall destroy the cryptography-related data generated in the temporary memory area to prevent reuse (FCS_CKM.4, FDP_RIP.1). Therefore, these security requirements are mutually supportive and internally consistent.

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

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

7. TOE Summary Specification

7.1. TOE security function

This clause explains TOE security function (TSF) satisfying the security requirements described in the last section. Each security function is described with its name and a simple explanation. Detailed information is given in the function specification document.

Security Function	Explanation
SF_CARD_MANAGEMENT	Management of card data
SF_AUTHENTICATION	Identification and authentication
SF_COUNTER_MEASURE	Security measures
SF_OBJECT_ACCESS	Access control for Java Objects
SF_RESOURCE_MANAGEMENT	Resource management
SF_CRYPTOGRAPHY	Support Cryptography
SF_PERSO_CONTROL	Support ePassport issuance
SF_BASIC_ACCESS_CONTROL	Support Basic Access Control
SF_EXTENDED_ACCESS_CONTROL	Support Extended Access Control
SF_ACTIVE_AUTHENTICATION	Support Active Authentication
SF_IC	Security Function supported by IC chip

Table 34 TOE security function

7.1.1. SF_CARD_MANAGEMENT

This is the card management function which includes the functions such as command processing, application program identification/management, life cycle management, and internal structure management of card management service.

7.1.2. SF_AUTHENTICATION

This function manages the security channel for administrator authentication and provides functions such as maintaining message integrity/confidentiality and terminating security channel, and for user authentication, also provides the function of Global PIN commonly used in the card and Owner PIN independently used by the application programs through API.

7.1.3. SF_COUNTER_MEASURE

This provides security measures when security violation occurs, and also provides defensive measures against security attacks.

7.1.4. SF_RESOURCE_MANAGEMENT

This is responsible for resource management and provides the removal function for residual information when allocating/returning.

7.1.5. SF_OBJECT_ACCESS

This controls the access and remote access of application programs to Java objects generated by application programs.

7.1.6. SF_CRYPTOGRAPHY

This security function provides cryptographic functions such as generation/verification of digital signature, encryption/decryption, hash value generation, and random number generation.

7.1.7. SF_PERSO_CONTROL

This security function allows only successfully authenticated Personalization agent to write ePassport user data & TSF data through secure messaging.

7.1.8. SF_BASIC_ACCESS_CONTROL

This security function allows only successfully authenticated inspection system through BAC mutual authentication to read ePassport user data excluding ePassport applicant bio information through BAC-secure messaging which guarantees confidentiality and integrity.

7.1.9. SF_EXTENDED_ACCESS_CONTROL

This security function allows only the inspection system which succeeded EAC-TA on EAC-secure messaging through ECA-CA to read the ePassport user data through EAC-secure messaging which guarantees confidentiality and integrity.

7.1.10. SF_ACTIVE_AUTHENTICATION

This security function implements AA security mechanism which allows the inspection system to judge the illegal piracy state of TOE.

This security function can be selectively used according to the issuance policy of the Personalization agent.

7.1.11. SF_IC

This security function uses the functions provided by the IC chip.

7.2. TSF of the IC chip used by the TOE

When the TOE performs TDES, RSA, ECDSA and ECDH in the IC chip, various security functions described below is used.

Security Function	Mapped SFR	Description
TOE's Detectors	FPT_FLS.1 FPT_PHP.3	Voltage detector, Frequency detector, Active shield removal detector, Inner insulation removal detector, Light and laser detector, Temperature detector, Voltage glitch detector
Memory Encryption	FDP_IFC.1	Memory Encryption when sensitive data into the memory. data will be encrypted before stored in memory so this will enhance the difficultly for an attacker to get useful information on data bytes hamming weight.
TRNG	FCS_RNG.1	TRNG is a hardware true random number generator compliant with AIS31 standard class P2 high.
TDES	FCS_COP.1	Hardware DES has several security countermeasures to prevent side channel attacks. - Secure Key & Data loading - DPA prevent : random mask - Variable clock - RWG automatic enable - High Order DPA prevent : Virtual DES
RSA	FCS_COP.1	The acceleration of modulo exponentiations required in the RSA encryption/decryption algorithm.
ECDSA	FCS_COP.1	ECDSA_sigh_digest, ECDSA_verify_digest
ECDH	FCS_COP.1	ECDH_generate
SHA	FCS_COP.1	SHA224, SHA256

Table 35 Security function of the IC chip

The relation between the SFR provided by the TOE and the SFR provided by the IC chip is described as below.

SFR of the IC Chip	SFR of the TOE	Description
FRU_FLT.2	FPT_FLS.1	Provides the mechanism to protect from the abnormal physical attack.
FPT_FLS.1	FPT_FLS.1	
FMT_LIM.1	[none]	
FMT_LIM.2	[none]	
FAU_SAS.1	[none]	
FPT_PHP.3	FDP_PHP.3	Resistance against the physical attack.
FDP_ITT.1	FPR_UNO.1	Memory data is encrypted to be stored
FDP_IFC.1	FPR_UNO.1	
FPT_ITT.1	FPR_UNO.1	
FCS_RNG.1	FCS_RNG.1	Random number generation
FCS_COP.1/3DES	FCS_COP.1(1)	Symmetric Key Cryptographic Operation
FCS_COP.1/AES	[none]	
FCS_COP.1/RSA	FCS_COP.1(5)	Digital signature generation
FCS_COP.1/ECDSA	FCS_COP.1(4)	Digital signature verification for the certification verification
FCS_COP.1/ECDH	FCS_CKM.2(2)	Distribution of the KDF Seed value for creation of the EAC session key
FDP_ACC.1	[none]	
FDP_ACF.1	[none]	
FMT_MSA.1	[none]	
FMT_MSA.3	[none]	
FMT_SMF.1	[none]	
FCS_CKM.1(ECDSA)	[none]	
FCS_CKM.1(RSA)	[none]	
FCS_COP.1/SHA	FCS_COP.1(3)	Hash calculation

Table 36 SFR Map

7.2.1. TOE's Detectors

The Toe turns its state to the Mute when the following abnormal actions are detected.

List of Detectors :

- Abnormal frequency Detector
- Abnormal voltage Detector
- Abnormal temperature Detector
- Light Detector
- Inner insulation removal Detector

- Active shield removal Detector
- Glitch Detector

7.2.2. Memory Encryption

The TOE performs the memory encryption and decryption against all data stored in the ROM, the RAM and the EEPROM by using this function. In the case of the ROM and the RAM, automatically enabled by the IC chip but in the case of the EEPROM, the TOE enables it for the enhancement of the security against the attack of TSF Data.

7.2.3. TRNG

The TRNG is the method for the identification and the authentication and it is provided for the SCP02 mutual authentication, the BAC mutual authentication, the EAC-CA, the EAC-TA and the AA.

7.2.4. TDES

The TDES is used for the SCP02 mutual authentication, the BAC mutual authentication and the secure channel for the creation of the session key.

7.2.5. RSA

The RSA is the cryptographic algorithm for the AA(Active Authentication) and the verification of the signature value.

7.2.6. ECDSA

The ECDSA is the cryptographic algorithm for the verification of a signature value for the DV(Document Verifier) / IS(Inspection System) of the EAC security mechanism.

7.2.7. ECDH

The ECDH is the security mechanism, in which the ECC encryption algorithm is used, to be used at the creation of the session key. By changing the BAC Key which is used with the encrypted communication, it increases the level of the security of the communication.

7.2.8. SHA

The SHA is the hash algorithm for the creation of the encrypted message and it is used at the creation of the session key, at the verification of the ECDSA signature value and at the creation of the AA signature value.

7.3. Assurance Method

This clause defines the assurance method required by TOE assurance requirements according to EAL5+. Added assurance requirement is ADV_IMP.2

Assurance Requirements	Assurance Method (Document ID)
ASE_INT.1	XSmart e-Passport Security Target
ASE_CCL.1	XSmart e-Passport Security Target
ASE_SPD.1	XSmart e-Passport Security Target
ASE_OBJ.2	XSmart e-Passport Security Target
ASE_ECD.1	XSmart e-Passport Security Target
ASE_REQ.2	XSmart e-Passport Security Target
ASE_TSS.1	XSmart e-Passport Security Target
ADV_ARC.1	XSmart e-Passport Structure Analysis Document
ADV_FSP.5	XSmart e-Passport Function Specification
ADV_INT.2	XSmart e-Passport Interface Specification
ADV_IMP.2	XSmart e-Passport Implementation Verification Document
ADV_TDS.4	XSmart e-Passport Design Document
AGD_OPE.1	XSmart e-Passport Manual
AGD_PRE.1	XSmart e-Passport Manual
ALC_CMC.4	XSmart e-Passport Configuration Management Document
ALC_CMS.5	XSmart e-Passport Configuration Management Document
ALC_DEL.1	XSmart e-Passport Distribution Guide
ALC_DVS.1	XSmart e-Passport Life Cycle Support Document
ALC_LCD.1	XSmart e-Passport Life Cycle Support Document
ALC_TAT.2	XSmart e-Passport Life Cycle Support Document
ATE_COV.2	XSmart e-Passport Test Analysis Document
ATE_DPT.3	XSmart e-Passport Test Analysis Document
ATE_FUN.1	XSmart e-Passport Test Document
ATE_IND.2	-
AVA_VAN.4	-

Table 37 TOE Assurance Method