Security Target Lite

KCOS e-Passport Version 3.0

S3FT9KS/KT/KF

KOMSCO

Version: 1.0

Date: 2014. 01. 24

Filename: EPS-04-AN-ST(Lite)

KOMSCO

Technology Research Institute

IT Research Center

This page left blank on purpose for double-side printing

[Table of Contents]

Copyright Ⓒ 2014 KOMSCO, All rights reserved

Copyright Ⓒ 2014 KOMSCO, All rights reserved

[List of Tables]

[List of Figures]

Copyright Ⓒ 2014 KOMSCO, All rights reserved

1. Introduction

This document is the Security Target(ST) to describe KCOS e-Passport Version 3.0 S3FT9KS/KT/KF developed by the Korea Minting, Security Printing & ID Card Operating Corporation(KOMSCO).
This chapter identifies the Security Target and the TOE and supports the Security Target overview, Common Criteria conformance and other areas.

1.1 ST Reference

- Title: KCOS e-Passport Version 3.0 S3FT9KS/KT/KF Security Target Lite V1.0(EPS-04-AN-ST(Lite)-1.0, Public version)
- ST Version Number : V1.0
- Author : IT Research Center, Technology Research Institute, KOMSCO
- Applicant : Korea Minting, Security Printing & ID Card Operating Corporation
- Evaluation Criteria : Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning, Notice No.2013-51)
- Common Criteria Version : V3.1r4
- Compliant to : ePassport Protection Profile V2.1(KECS-PP-0163a-2009)
- Evaluation Assurance Level : EAL5+(ALC_DVS.2, ADV_IMP.2, AVA_VAN.5)
- Keywords: ePassport, IDL, COS, MRTD, ICAO, SAC, EAC, BAC, BAP, EAP, AA

1.2 TOE Reference

- TOE name : KCOS e-Passport Version 3.0 S3FT9KS/KT/KF

  - K3.0.04.00.SS.141C.01(S3FT9KS)

  - K3.0.04.00.SS.141D.01(S3FT9KT)

  - K3.0.04.00.SS.140F.01(S3FT9KF)

    · K3.0 : KCOS e-Passport Version 3.0

    · 04 : Download version

    · 00 : Patch version

    · SS.141C.01 : IC chip identifier(Samsung S3FT9KS Revision 1)

Copyright © 2014 KOMSCO, All rights reserved

- · SS.141D.01 : IC chip identifier(Samsung S3FT9KT Revision 1)
- · SS.140F.01 : IC chip identifier(Samsung S3FT9KF Revision 1)

- TOE Version : Version 3.0
- TOE Components
  - IC chip : Samsung S3FT9KF/S3FT9KT/S3FT9KS Revision 1(ANSSI-CC-2013/47)
  - Embedded software : KCOS e-Passport Version 3.0
  - Guidance : EPS-04-QT-OPE-1.3(Operational User Guidance), EPS-04-QT-PRE-1.3 (Preparative Procedures Guidance)

1.3 TOE Overview

The TOE is the native IC Chip Operation System(COS), Machine Readable Travel Document(MRTD or ePassport) application, MRTD(or ePassport) application data, IDL(ISO-compliant Driving License) application and IDL application data implemented on the IC chip and additionally includes S3FT9KF/KT/KS revision 1, which is an IC chip of Samsung Electronics and is certified according to CC EAL 5+(ANSSI-CC-2013/47).

The ePassport application of the TOE follows ICAO document(ICAO MRTD Doc. 9303 Part1 and Part3 Volume 2), SAC specification(ICAO TR Supplemental Access Control for Machine Readable Travel Documents V1.01) and EAC specification(BSI, Advanced Security Mechanisms Machine Readable Travel Documents-Extended Access Control V1.11). Therefore, the TOE carries out the security mechanisms of the ePassport such as AA(Active Authentication), BAC(Basic Access Control), SAC(Supplemental Access Control) and EAC(Extended Access Control).

The IDL application of the TOE follows ISO/IEC specification(ISO/IEC 18013 Part 1, 2, 3). Therefore, the TOE carries out the security mechanisms of the IDL such as AA(Active Authentication), BAP(Basic Access Protection) and EAP(Extended Access Protection).

Additionally, the TOE also carries out the PAC(Personalization Access Control), which is a security mechanism for the secure personalization and management on the personalization phase at the Personalization Agent. It authenticates the Personalization Agent and performs the function that grants the permission to personalize to the Personalization Agent by supporting the multi-authentication mechanism according to departmentalizing the security roles of the Personalization Agent.

The TOE uses generation of random numbers, TDES, AES, Retail MAC, CMAC, SHA, RSA and ECC supported by the ePassport or the IDL chip. And the TOE uses RSA or ECC operations but the Personalization Agent has to select one cryptographic algorithm needed for a security mechanism.

Since The TOE is a composite evaluation product, it includes IC chip, COS, application programs, and etc. There is no non-TOE HW/FW/SW requested to perform TOE security attributes. Note, the RF antenna, the booklet or the card is needed to represent a complete type to the ePassport or the IDL holder, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.3.1 TOE Type

The TOE is the native IC chip operation system that both ePassport and IDL applications are multiply implemented on the IC chip, Samsung Electronics S3FT9KF/KT/KS revision 1. However, the Personalization Agent should select one application and issue the application-compliant data.

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

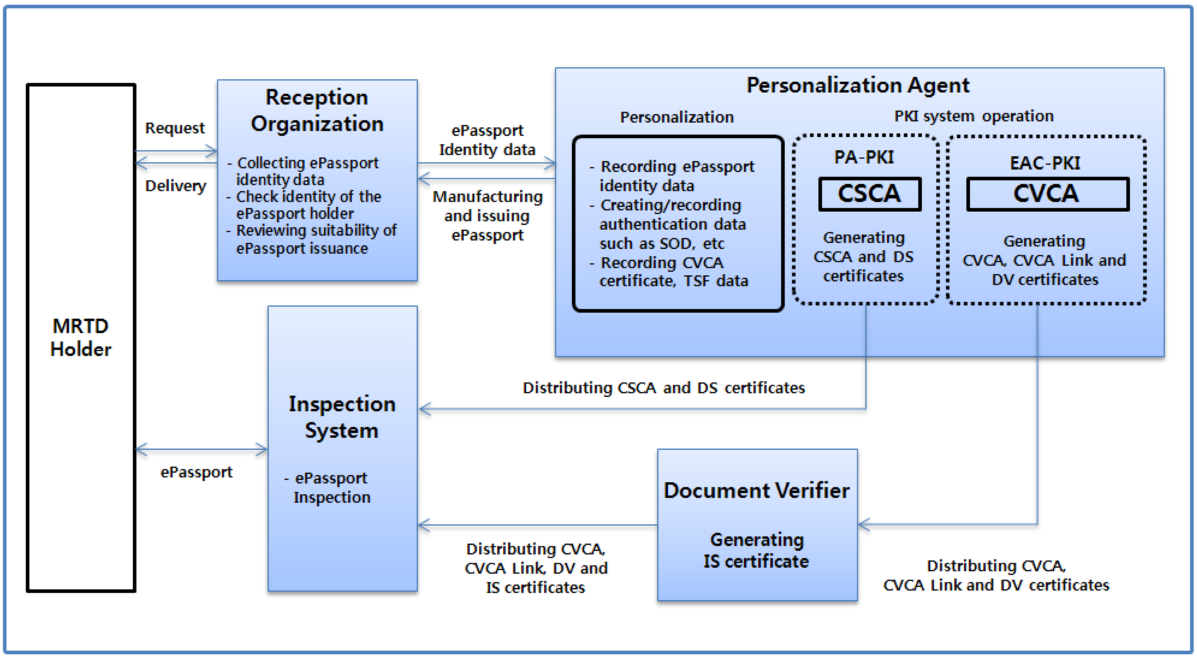
The IDL is an IDL embedding a contactless IC Chip in which the identity and other data of the IDL holder are stored according to the International Standard Organization(ISO). The contactless IC chip used in the IDL is referred to as IDL chip. The IDL chip is loaded with the IDL application and COS to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

1.3.2 ePassport(MRTD) System

[Figure 1] shows the overall configuration of the ePassport system.

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

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


MRTD Holder
Request
Delivery
Reception Organization
- Collecting ePassport identity data
- Check identity of the ePassport holder
- Reviewing suitability of ePassport issuance
ePassport Identity data
Manufacturing and issuing ePassport
Personalization Agent
Personalization
PKI system operation
- Recording ePassport identity data
- Creating/recording authentication data such as SOD, etc
- Recording CVCA certificate, TSF data
PA-PKI
CSCA
Generating CSCA and DS certificates
EAC-PKI
CVCA
Generating CVCA, CVCA Link and DV certificates
Distributing CSCA and DS certificates
Inspection System
- ePassport Inspection
ePassport
Document Verifier
Generating IS certificate
Distributing CVCA, CVCA Link, DV and IS certificates
Distributing CVCA, CVCA Link and DV certificates

[Figure 1] Overall Configuration of ePassport(MRTD) System

The Personalization Agent generates a Document Security Object("SOD" hereinafter) using a digital signature on the user data(identity and authentication data) and records it in the MRTD chip with the ePassport identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the Personalization Agent manufactures and issues the ePassport-embedded MRTD chip to a passport.

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

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

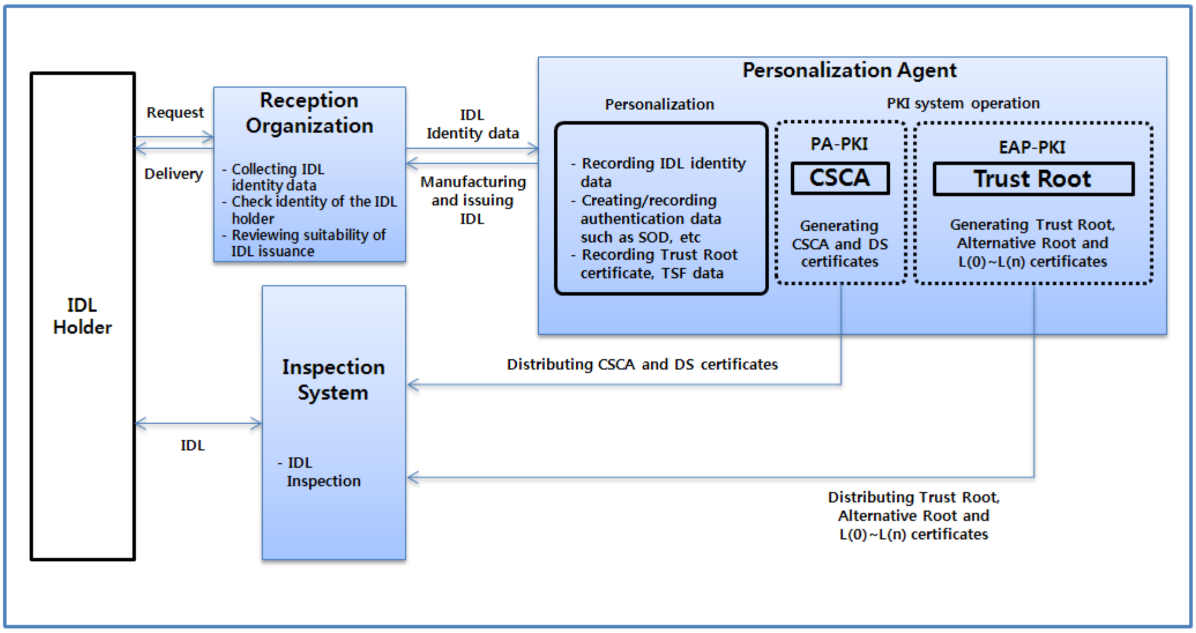
(Table 1) Type of Certificates(ePassport)

Usage	ePassport PKI system	Subjects	Certificates
To verify forgery and corruption of the user data	PA-PKI	CSCA	CSCA certificate
		Personalization Agent	DS certificate
To verify the access-right of the biometric data of the ePassport holder	EAC-PKI	CVCA	CVCA certificate
			CVCA Link certificate
		Document Verifier	DV certificate
		EAC-supporting Inspection System	IS certificate

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

1.3.3 IDL System

[Figure 2] shows the overall configuration of the IDL system.


IDL Holder
Request
Delivery
Reception Organization
- Collecting IDL identity data
- Check identity of the IDL holder
- Reviewing suitability of IDL issuance
IDL Identity data
Manufacturing and issuing IDL
Personalization Agent
Personalization
PKI system operation
- Recording IDL identity data
- Creating/recording authentication data such as SOD, etc
- Recording Trust Root certificate, TSF data
PA-PKI
CSCA
Generating CSCA and DS certificates
EAP-PKI
Trust Root
Generating Trust Root, Alternative Root and L(0)~L(n) certificates
Distributing CSCA and DS certificates
Inspection System
- IDL Inspection
IDL
Distributing Trust Root, Alternative Root and L(0)~L(n) certificates

[Figure 2] Overall Configuration of IDL System

The IDL holder requests an issue of the IDL and receives the IDL issued according to the

Issuing Policy of the IDL. The IDL holder presents the IDL to an IDL officer(or police) so that the IDL can be inspected at a police control. For a police control, the IDL is verified by an IDL officer or by an automatic Inspection System according to the IDL control policy for domestic and foreign countries.

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

The Personalization Agent generates a Document Security Object("SOD" hereinafter) using a digital signature on the user data(identity and authentication data) and records it in the IDL chip with the IDL identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the Personalization Agent manufactures and issues the IDL-embedded chip to the IDL.

The Personalization Agent generates a digital signature key to check against forgery and corruption of the user data stored in the IDL chip. Then, in accordance with the Certification Practice Statement(CPS) of the IDL PKI System, the Personalization Agent generates, issues, and manages the CSCA certificate and DS certificate. According to the Issuing Policy of the IDL, the Personalization Agent generates a digital signature key to verify access-rights to the optional data of the IDL holder to support the EAP security mechanism. The Personalization Agent then generates, issues and manages the Trust Root certificate, Alternative Root certificate and the L(0)~L(n) certificates. Details related to of the IDL PKI System and certification procedure, including the certification server, key generation devices and the physical and procedural security measures depend on the Issuing Policy of the IDL.

The types of certificates used in the IDL system are shown in (Table 2).

(Table 2) Type of Certificates(IDL)

Usage	IDL PKI System	Subjects	Certificates
To verify forgery and corruption of the user data	PA-PKI	CSCA	CSCA certificate
		Personalization Agent	DS certificate
To verify the access-right of the biometric data of the IDL holder	EAP-PKI	Trust Root	Trust Root certificate
			Alternative Root certificate
		EAP-supporting Inspection System	L(0) ~ L(n) certificates

Application Notes: The Personalization Agent generates and issues the certificates for the PA and the EAP and distributes the certificates online and/or offline according to the Issuing Policy of the IDL. Moreover, the Personalization Agent generates the L(n)~L(0) certificates and distributes it to the Inspection System according to the Issuing Policy of the IDL.

Copyright © 2014 KOMSCO, All rights reserved

Application Notes: The certificate verification chaining flexibly composes according to the Issuing Policy of the IDL.

1.4 TOE Description

1.4.1 Life Cycle and Environment of TOE

This section defines the Life Cycle of the TOE, including the Development, Manufacturing, Personalization and Operational Use of the ePassport or the IDL. It also defines the TOE environment and the physical/ logical scope of the TOE.

IC chip and Life Cycle of TOE

The IC chip is S3FT9KS/KT/KF revision 1 which is an IC chip product of Samsung Electronics and is certified according to CC EAL 5+(ANSSI-CC-2013/47). The IC chip consists CPU, memory, peripheral unit, crypto-operation S/W library and etc, as following (Table 3)

(Table 3) Components of IC chip

Component	Details
CPU	· 16 bit microprocessor
Memory	· ROM : 32Kbytes · FLASH : 212Kbytes(KS), 232Kbytes(KT), 264Kbytes(KF) · RAM : 6Kbytes · CRYPTO RAM : 2.5Kbytes
Peripheral unit	· TDES operator, AES operator, · RSA/ECC operator TORNADO 2Mx2 · 16bits random number generator · Abnormal condition detectors · Memory protection unit · 16bits Timer and 20bits watchdog timer · ISO7816 contact interface, ISO14443 contactless interface
S/W library	· ECC library v3.2 : 192bits ~ 512bits · RSA library v3.2 : 1280bits ~ 2048bits · TRNG random number generator v1 · DRNG random number generator v1 · DTRNG random number generator v1

The TOE includes as following cryptographic algorithms.

Copyright Ⓒ 2014 KOMSCO, All rights reserved

(Table 4) Cryptographic Algorithms of TOE

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

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

(Table 5) shows the Life Cycle of the TOE. The transmission process has been omitted. TOE development process corresponds to phase 1(Development) and phase 2(Manufacturing), while the TOE operational environment corresponds to phase 3(Personalization) and phase 4(Operational Use).

(Table 5) Life Cycle of TOE

Phase	Life Cycle of TOE(1) (In case that a subject to download a Flash code is an IC chip manufacturer)
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W.
	② The S/W developer to develop the Embedded S/W(COS, MRTD/IDL application) by using the IC chip and the Dedicated S/W. ③ Delivery to the IC chip manufacturer the Flash code including the initial PAC authentication key.

Copyright Ⓒ 2014 KOMSCO, All rights reserved

Phase	Life Cycle of TOE(1) (In case that a subject to download a Flash code is an IC chip manufacturer)
Phase 2 (Manufacturing)	④ The IC chip manufacturer to download the Flash code in the FLASH area, to record the IC chip identifier, to produce the IC chips and to deliver the TOE to the Personalization Agent. Or the S/W developer to deliver the TOE to the Personalization Agent after getting it from the IC Chip manufacturer.
	⑤ The ePassport/IDL manufacturer to embed the IC chip in the passport book or the card by a request of the Personalization Agent.
Phase 3 (Personalization)	⑥ The Personalization Agent to operate the functions of the PAC authentication key update and patch. ⑦ The Personalization Agent to create a user data storage space according to the LDS format, ICAO document and ISO/IEC specification and to record it in FLASH area. ⑧ The Personalization Agent to create a SOD using a digital signature on the ePassport or the IDL identity data. ⑨-1 The ePassport Personalization Agent to record the ePassport identity data, the authentication data(including SOD) and the TSF data(The TOE itself creates the BAC authentication key using the command of the Personalization Agent) in the TOE. ⑨-2 The IDL Personalization Agent to record the IDL identity data, the authentication data(including SOD) and the TSF data(The TOE itself creates the BAP authentication key using the command of the Personalization Agent) in the TOE. ⑩ The Personalization Agent to check a normal operation. ⑪ Issue, discard or re-personalization according to the checking result.
Phase 4 (Operational Use)	⑫ The Inspection System to verify the ePassport or the IDL and to check identity of the ePassport or the IDL holder by communicating with the TOE.

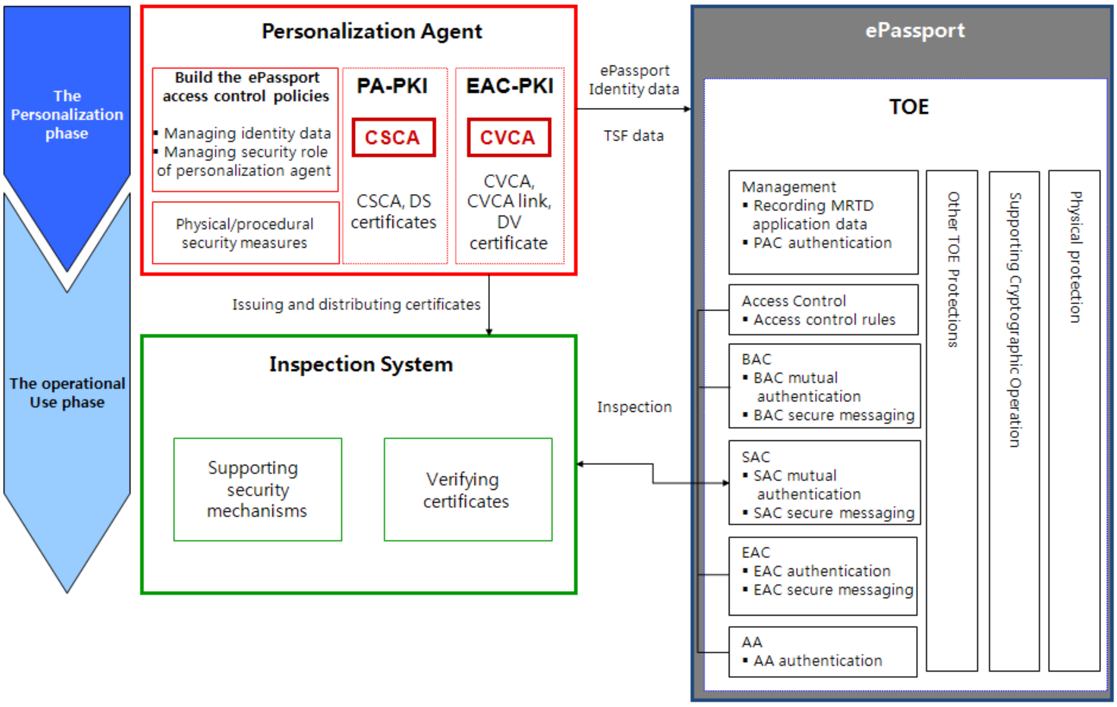
Phase	Life Cycle of TOE(2) (In case that a subject to download a Flash code is a S/W developer)
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W.
	② The S/W developer to develop the Embedded S/W (COS, MRTD/IDL application) by using the IC chip and the Dedicated S/W.
Phase 2 (Manufacturing)	③ The IC chip manufacturer to record the IC chip identifier, to produce the IC chips and to deliver it to the S/W developer.
	④ The S/W developer to download the Flash code including the initial PAC authentication in the FLASH area and to deliver the TOE to the Personalization Agent.
	⑤ The ePassport/IDL manufacturer to embed the IC chip in the passport book or the card by a request of the Personalization Agent.
Phase 3 (Personalization)	⑥ The Personalization Agent to operate the functions of the PAC authentication key update and patch. ⑦ The Personalization Agent to create a user data storage space according to the LDS format, ICAO document and ISO/IEC specification and to record it in FLASH area. ⑧ The Personalization Agent to create a SOD using a digital signature on the

Phase	Life Cycle of TOE(2) (In case that a subject to download a Flash code is a S/W developer)
	ePassport or the IDL identity data. ⑨-1 The ePassport Personalization Agent to record the ePassport identity data, the authentication data(including SOD) and the TSF data(The TOE itself creates the BAC authentication key using the command of the Personalization Agent) in the TOE. ⑨-2 The IDL Personalization Agent to record the IDL identity data, the authentication data(including SOD) and the TSF data(The TOE itself creates the BAP authentication key using the command of the Personalization Agent) in the TOE. ⑩ The Personalization Agent to check a normal operation. ⑪ Issue, discard or re-personalization according to the checking result.
Phase 4 (Operational Use)	⑫ The Inspection System to verify the ePassport or the IDL and to check identity of the ePassport or the IDL holder by communicating with the TOE.

Application Notes: When issuing the TOE, one application should be selected among ePassport and IDL applications by the policy of the Personalization Agent.

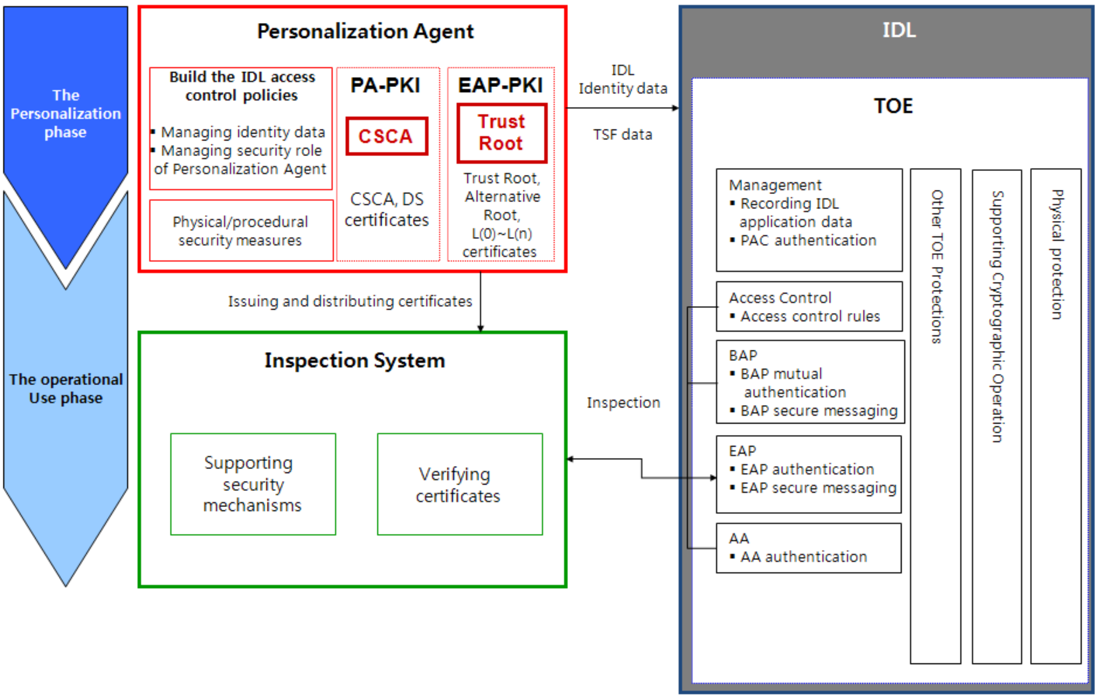
TOE Operational Environments

[Figure 3] shows the operational environment of the TOE in the phases of the ePassport Personalization and Operational Use through the relationship with major security functions of the TOE and external entities(the Personalization Agent and the Inspection System) that interact with the TOE.



[Figure 3] TOE Operational Environment(ePassport)

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


The Personalization phase
The operational Use phase
Personalization Agent
Build the IDL access control policies
▪ Managing identity data
▪ Managing security role of Personalization Agent
Physical/procedural security measures
PA-PKI
CSCA
CSCA, DS certificates
EAP-PKI
Trust Root
Trust Root, Alternative Root, L(0)~L(n) certificates
IDL Identity data
TSF data
Issuing and distributing certificates
Inspection System
Supporting security mechanisms
Verifying certificates
Inspection
IDL
TOE
Management
▪ Recording IDL application data
▪ PAC authentication
Access Control
▪ Access control rules
BAP
▪ BAP mutual authentication
▪ BAP secure messaging
EAP
▪ EAP authentication
▪ EAP secure messaging
AA
▪ AA authentication
Other TOE Protections
Supporting Cryptographic Operation
Physical protection

[Figure 4] TOE Operational Environment(IDL)

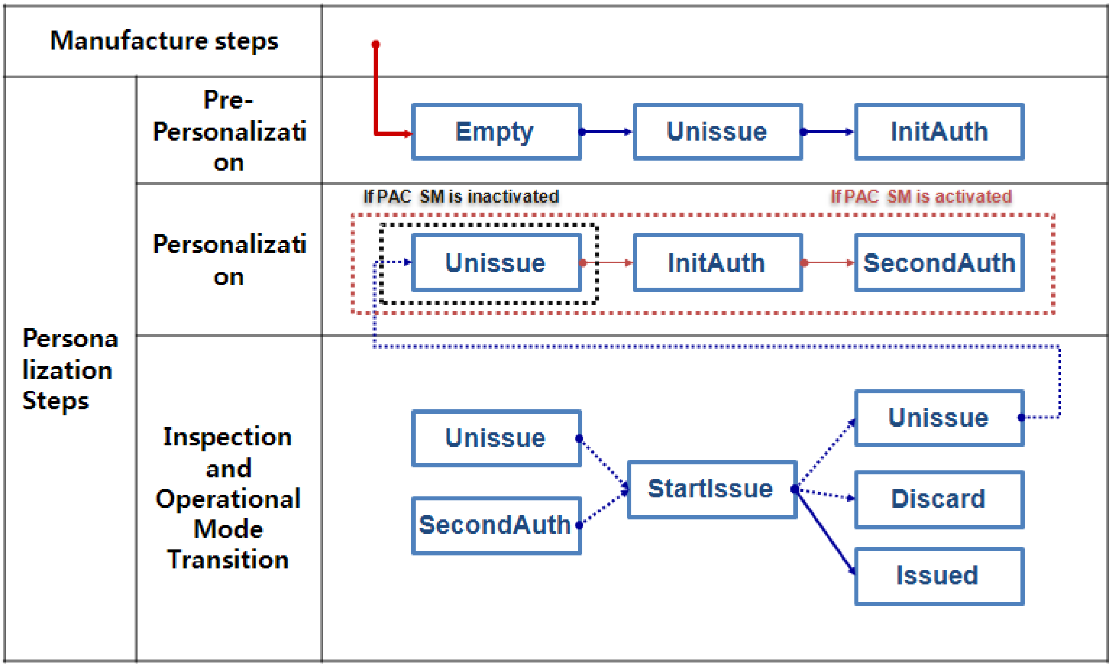
TOE Personalization Phases

The TOE manages 8 operational modes for secure personalization and management.

- ● EMPTY mode : An initialization of the TOE including selecting one application is performed.
- ● UNISSUE mode : PAC mutual authentication is performed to authenticate the Personalization Agent. If PAC SM is inactivated, all functionalities(Personalization, patching, key updating and etc) of the personalization can be performed in this mode instead of both INITAUTH and SECONDAUTH modes.
- ● INITAUTH mode : Creating EFs and updating PAC Key 1 are performed. This mode can be available if PAC SM is activated.
- ● SECONDAUTH mode : Creating EFs and Update PAC Key 2~7 are performed. Plus, patching the TOE, changing the operational mode and re-issuance are performed. This mode can be available if PAC SM is activated.
- ● STARTISSUE mode : Inspection System can check the normal operation of the TOE. If the checking result is not normal, the Personalization Agent can re-issue the data or discard the TOE. And this mode can be skipped.

- ISSUED mode : The Personalization Agent inspects the operational functionalities of the TOE. According to the result, the Personalization Agent delivers it to the holder or discards it.
- BLOCK mode : In case that PAC mutual/management authentications are not successfully performed more than 3 times, the operational mode of the TOE is transited to this mode.
- DISCARD mode : All functionalities of the TOE are not activated and all data should be removed.

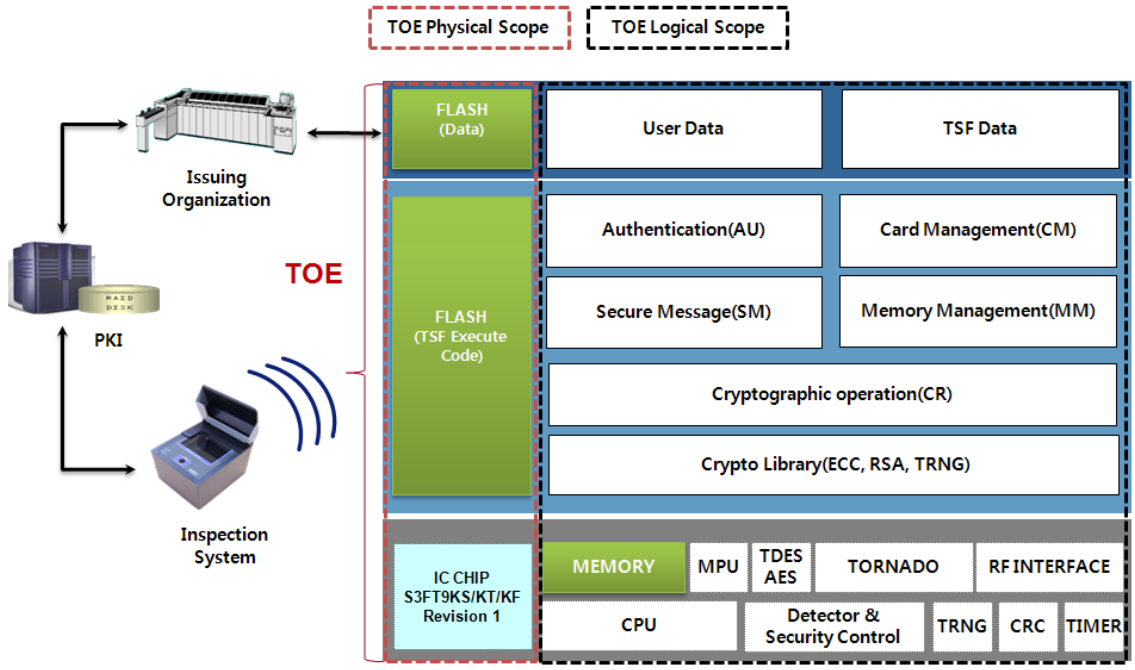
The personalization phase is divided into pre-personalization, personalization, inspection and operational mode transition, as following [Figure 5].



[Figure 5] Internal Operational Mode Transition according to Personalization

1.4.2 TOE Scope

[Figure 6] shows the physical and logical scope of the TOE.



[Figure 6] Scope of TOE

1.4.2.1 Physical Scope of TOE

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

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

The TOE supports 2 applications(ePassport and IDL). However, one application should be selected in the personalization step.

- Scope of the TOE when selecting the ePassport application : IC chip, COS, ePassport application, ePassport application data and guidance
- Scope of the TOE when selecting the IDL application : IC chip, COS, IDL application, IDL application data and guidance

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

Copyright ⓒ 2014 KOMSCO, All rights reserved

and the ICAO document in addition to the security mechanism to protect the data securely. And the ePassport application is added to the EAC security mechanism by the EAC specifications, as the biometric data of the ePassport holder is included in the ePassport identity data.

The IDL application is the IC chip application that implements the function to store and process the IDL identity data according to LDS(Logical Data Structure) format and the IDL ISO/IEC specification in addition to the security mechanism to protect the data securely. And the IDL application is added to the EAP security mechanism by the ISO/IEC specifications, as the optional data of the IDL holder is included in the IDL identity data.

The ePassport and the IDL applications also include the PAC security mechanism, which is the security mechanism for a personalization. The applications are stored in the FLASH area of the IC chip.

The application data consists of the user data, including the identity data and the TSF data required in the security mechanisms. The application data is stored the FLASH area of the MRTD or the IDL IC chip.

The identifier and components of the TOE are identified in (Table 6).

(Table 6) Identifier and Components of TOE

Type		Identifier	Explanation
TOE	HW+SW	KCOS e-Passport Version 3.0 S3FT9KS/KT/KF	IC Chip + COS + Application
TOE Components	HW	Samsung S3FT9KS/S3FT9KT/ S3FT9KF	Revision 1
	SW	KCOS e-Passport Version 3.0 - KOCS_KS_FLASH-1.3 - KCOS_KT_FLASH-1.3 - KCOS_KF_FLASH-1.3	Flash code
	DOC	Operational User Guidance : EPS-04-QT-OPE-1.3	Soft copy or Booklet
		Preparative Procedures Guidance : EPS-04-QT-PRE-1.3	

1.4.2.2 Logical Scope of TOE

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

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

Assets

In order to protect the TOE assets shown in (Table 7), the TOE provides security functions such as the confidentiality, the integrity, the authentication and the access control.

(Table 7) TOE Assets

Category			Descriptions	Storage Space
User Data	Identity Data	Personal Data of the ePassport or the IDL holder	EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16(ePassport) EF.DG1(IDL)	EF File
		Biometric Data of the ePassport holder	EF.DG3, EF.DG4	
		Optional Data of the IDL holder	EF.DG2~EF.DG11	
	Authentication Data	ePassport	EF.CARDACCESS, EF.SOD, EF.DG14(EAC chip authentication public key), EF.DG15(AA public key)	
		IDL	EF.SOD, EF.DG12, EF.DG13(AA public key), EF.DG14(EAP chip authentication key)	
	EF.CVCA		In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System	
	EF.COM		LDS version info., tag list of DGs used, etc. DG info. or EAP, Key info. for EAP-TA(IDL)	
TSF Data	EAC Chip Authentication Private Key		In EAC-CA, Chip Private key used by the TOE to demonstrate a non-forged MRTD chip	Secure memory
	EAP Chip Authentication Private Key		In EAP-CA, Chip Private key used by the TOE to demonstrate a non-forged IDL chip	
	CVCA Certificate		In personalization phase, Root CA Certificate issued in EAC-PKI	
	Trust Root Certificate		In personalization phase, Root CA certificate issued in EAP-PKI	
	CVCA Digital Signature Verification Key		After the personalization phase, CVCA certificate public key is newly created by a certificate update	
	Trust Root Digital Signature Verification Key		After the personalization phase, Trust Root certificate public key is newly created by a certificate update	
	Current Date(ePassport)		In the personalization phase, the date of issue of the ePassport is recorded. However, in the Operational Use	

Category		Descriptions	Storage Space
		phase, the TOE internally updates it as the latest date among the issuing dates of the CVCA Link certificate, the DV certificate or the Issuing State IS certificate.	
	Current Date(IDL)	In the personalization phase, the date of issue of the IDL is recorded. However, in the Operational Use phase, the TOE internally updates it as the latest date among the issuing dates of the Alternative Root certificate.	
	BAC Authentication Key	BAC authentication encryption key BAC authentication MAC key	
	BAP Authentication Key	BAP authentication encryption key BAP authentication MAC key	
	SAC Authentication Key	SAC authentication key, CAN	
	AA Private Key	Private key of the chip used by the TOE to prove that the chip is not substituted	
	PAC Authentication Key	Symmetric key for PAC mutual authentication and PAC personalization management authentication	
	TSF execute Code for patching	Additional Execute code for improving function	
	TSF integrity verification key	MAC key for making integrity value TSF	
	Other TSF Data	TOE Operational Data, etc.	
	BAC Session Key	BAC session encryption key BAC session MAC key	Temporary memory
	BAP Session Key	BAP session encryption key BAP session MAC key	
	SAC Session Key	SAC session encryption key SAC session MAC key	
	EAC Session Key	EAC session encryption key EAC session MAC key	
	EAP Session Key	EAP session encryption key EAP session MAC key	
	PAC Session Key	PAC session encryption key PAC session MAC key	

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

Application Notes: The optional data obtained from an IDL holder include the detailed information of the holder and the Personalization Agent, the face, the signature, the fingerprint and the iris scan. The optional data is included optionally according to the Issuing Policy of the IDL. This Security Target includes security functional requirements for the EAP specifications by assuming the optional data to be contained.

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

The LDS in which the user data are stored defines the MF, DF and EF file structure. (Table 8) shows the content of ePassport EF files, in which parts of the user data is stored.

(Table 8) LDS Contents of User Data(ePassport)

Category	DG	Contents
Detail(s) recorded in MRZ	DG1	Document (Passport) type
		Issuing state
		Name (of holder)
		Document number
		Check digit (of doc. number)
		Nationality
		Date of birth
		Check digit (of DOB)
		Sex
		Data of expiry of valid until date
		Check digit (of DOE/VUD)
		Composite check digit
Biometric data	DG2	Encoded face info.
	DG3	Encoded fingerprint info.
	DG4	Encoded iris info.
The other data and authentication information	DG5	Photo image
	DG6	-
	DG7	Signature image
	DG8	-
	DG9	-
	DG10	-
	DG11	Personalization additional info.
	DG12	Additional info.
	DG13	-
	DG14	EAC chip authentication public key
	DG15	AA digital signature verification key
	DG16	Person(s) to notify
	EF.CARDACCESS	SAC info
	EF.COM	LDS version info., tag list of DG used, etc.
	EF.SOD	Document of security
	EF.CVCA	In EAC-TA, CVCA digital signature verification key identifier list

(Table 9) shows the content of IDL EF files, in which parts of the user data is stored.

(Table 9) LDS Contents of User Data(IDL)

Category	DG	Contents
Detail(s) of Text data (Demographic data and endorsement/restriction information)	DG1	Family name
		Given name
		Date of birth
		Date of issue
		Date of expiry
		Issuing country
		Issuing authority
		License number
		Categories of vehicles/restrictions/conditions
The other optional data and authentication information	DG2	Details of the license holder
	DG3	Details of the issuing authority
	DG4	Portrait image
	DG5	Signature / usual mark image
	DG6	Biometric face info.
	DG7	Biometric fingerprint info.
	DG8	Biometric iris template
	DG9	Other biometric template
	DG10	-
	DG11	Domestic data
	DG12	Non-match alert info.
	DG13	AA Digital Signature Verification Key
	DG14	EAP Chip Authentication Public Key
	DG15	-
	DG16	-
	EF.COM	Common data
	EF.SOD	Document security object

Security Mechanisms

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

(Table 10) shows the security mechanisms of TOE.

(Table 10) TOE Security Mechanisms

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

	EAC Secure Messaging	Secure Messaging	EAC Session Key (Encryption and MAC Keys)
	EAC-TA	RSASSA SHA-256	CVCA, CVCA Link, DV, IS Certificates
		ECDSA SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	CVCA, CVCA Link, DV, IS Certificates
EAP	EAP-CA	ECDH Key Distribution Protocol SHA-1	EAP-CA Public Key EAP-CA Private Key
	EAP Secure Messaging	Secure Messaging	EAP Session Key (Encryption and MAC Keys)
	EAP-TA	ECDSA SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	Trust Root, Alternative Root, L(n)~L(0) Certificates
PAC	PAC Mutual Authentication	TDES-CBC Retail MAC	PAC Authentication Keys (K1, K2, K7)
	PAC Personalization Management Authentication		PAC Authentication Keys (K3, K4, K5, K6)
	PAC Key Distribution		PAC Encryption Session Key PAC MAC Session Key
	PAC Secure Messaging		

< PAC (Personalization Access Control) >

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

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

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

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

< SAC (Supplemental Access Control) >

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

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

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

< BAC (Basic Access Control) >

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

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

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

< BAP (Basic Access Protection) >

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

The TOE uses the BAP authentication key stored in secure memory and the BAP-supporting Inspection System uses the BAP authentication key generated from reading optically the SAI(Scanning Area Identifier). And according to the first byte of the input string obtained from the SAI, the Inspection System determines the BAP configuration. The TOE and the Inspection System then perform encryption by a generated random number and exchange the numbers. The TOE and the BAP-supporting Inspection System execute the BAP mutual authentication by checking the exchanged random number. The session is ended in case of a mutual authentication failure.

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

< AA (Active Authentication) >

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

< EAC (Extended Access Control) >

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

The EAC-CA implements the ephemeral-static DH/ECDH key distribution protocol for the EAC session key distribution and the chip authentication. The TOE transmits the EAC chip authentication public key so that the Inspection System authenticates itself and executes the

Copyright © 2014 KOMSCO, All rights reserved

key distribution protocol by using a temporary public key received from the Inspection System. The session is ended if the EAC-CA fails. When the EAC-CA is successful, the TOE establishes the EAC secure messaging using the EAC session key.

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

< EAP (Extended Access Protection) >

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

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

The EAP-TA is used by the TOE to implement the challenge-response authentication protocol based on the digital signature in order to authenticate the EAP-supporting Inspection System. The TOE authenticates the Inspection System, verifying the value of the digital signature by the Inspection System in the temporary public key used for the EAP-CA using the L(n)~L(0) certificate. The TOE, when receiving the Alternative Root certificate from the EAP-supporting Inspection System, verifies the Alternative Root certificate using the Trust Root digital signature verification key in secure memory. Then, by verifying a valid date of the Alternative Root certificate, the TOE updates the digital signature verification key and the current date of the Trust Root certificate if necessary. After verifying the L(n)~L(0) certificate and checking that it is a suitable certificate, the TOE allows access of the EAP-supporting Inspection System to read the optional data of the IDL holder and transmits the data through EAP secure messaging.

TOE Access Control and Security Management

Copyright Ⓒ 2014 KOMSCO, All rights reserved

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

< Access control of the Personalization Agent>

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

< Access control of the ePassport IS >

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

In addition, in the Operational Use phase, the TOE provides the access control functions for the read right of the user data based on the access right of the Inspection System, which is authenticated through performance of the security mechanisms. Therefore, if the Inspection System succeeds with the SAC authentication, the TOE grants a SAC authorization(the read-rights for the personal data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM). If the Inspection System doesn't perform SAC authentication and succeeds with the BAC authentication, the TOE grants a BAC authorization(the read-rights for the personal data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM). If the Inspection System also succeeds with the EAC authentication and the CVCA certificate, DV certificate and IS certificate that the Inspection System has included with the read-rights for the biometric data, the TOE then grants the EAC authorization(the read-rights for the personal data of ePassport holder, the biometric data of ePassport holder, ePassport authentication data, EF.CVCA and EF.COM).

< Access control of the IDL IS >

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

In addition, in the Operational Use phase, the TOE provides the access control functions for the read right of the user data based on the access right of the Inspection System, which is authenticated through performance of the security mechanisms. Therefore, if the Inspection System succeeds with the BAP authentication, the TOE grants a BAP authorization(the read-rights for the mandatory data of IDL holder, the optional data of the IDL holder permitted by a BAP authorization, IDL authentication data and EF.COM). If the Inspection System also succeeds with the EAP authentication and the Trust Root certificate, the Alternative Root certificate and L(n)~L(0) certificate that the Inspection System has included with the read-rights for the optional data, the TOE then grants the EAP authorization(the read-rights for the mandatory data of the IDL holder, the optional data of the IDL holder permitted by the EAP authorization, IDL authentication data and EF.COM).

An EAP authorization should be needed to access the fingerprint, the iris and the other biometric template information(DG7~9) of the IDL holder among the optional data. And an access to the other optional information of the IDL holder may need an EAP authorization according to the policy of the Personalization Agent.

< Personalization management of the Personalization Agent >

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

< TOE self protection management >

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

Other TOE Protections

The TOE executes the functions to detect modifications of the transmitted TSF data using the MAC function of the IC chip. When detecting a modification, the TOE performs the function of session termination. Loading the TSF data from temporary memory to perform the security mechanism, the TOE provides the integrity measure by checking CRC of the TSF data. And the TOE provides the integrity measure by performing Retail-MAC operation for the execute code.

To improve the TOE functions, the Personalization Agent executes the patch function.

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

1.4.3 Functions of IC Chip

The IC Chip supports all functions concerning the RF communication. And it provides the

TDES/AES cryptographic algorithm, Retail MAC algorithm, CMAC, TRNG, Hash, ECC/RSA cryptographic algorithm. Thus, the TOE is provided CRC function for memory integrity.

The IC Chip provides functions that consider countermeasures to the DPA/SPA, which is an attack technique, by analyzing the physical phenomena(electric current, voltage, an electromagnetism change) during the cryptographic algorithm. Additionally, the IC Chip provides a security detector mechanism as to whether the TOE departs from the normal operational range of the TSF with an Active-Shield and sensor test function for the TOE.

Among the functions supported by the IC chip, (Table 11) shows the functions used in the TOE .

(Table 11) Functions used in TOE

Functions supported by IC Chip		Functions used in TOE
Security functions	TDES Cryptographic function	O
	AES Cryptographic function	O
	RSA Cryptographic function ECC Cryptographic function	O
	HASH function	O
	TRNG, DTRNG, DRNG	TRNG
	Abnormal condition detectors	O
	Memory protection function	O
	Memory encryption function	O
	Random wait generator Random current generator	Random wait generator
	Variable clock function	O
Communication functions	ISO7816 contact interface	X
	ISO14443 contactless interface	O

1.5 Conventions

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

Iteration

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

Selection

This is used to select one or more options provided by the CC in stating a requirement. The

Copyright Ⓒ 2014 KOMSCO, All rights reserved

result of a selection is shown as *underlined and italicized*.

Refinement

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

Assignment

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

Application Notes

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

1.6 Security Target Organization

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

Chapter 2 defines the conformance claim.

Chapter 3 describes the threats, organizational security policies and assumptions for the TOE.

Chapter 4 describes the security objectives of the TOE and environment by supporting the assumptions and organizational security policies to counter the threats.

Chapter 5 describes the extended components that are not based on CC part 2 or part 3.

Chapter 6 describes the security functional requirements and assurance requirements for the security objectives.

Chapter 7 provides the TOE security functionality as the TOE summary.

2. Conformance Claim

2.1 CC Conformance

This Security Target claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 r4, September. 2012, CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1 r4, September. 2012, CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1 r4, September. 2012, CCMB-2012-09-003

as follows:

- Common Criteria for Information Technology Security Evaluation, Part 2 extended
- Common Criteria for Information Technology Security Evaluation, Part 3 conformant

The Common Criteria for Information Technology Security Evaluation, Part 4: Evaluation Methodology, Version 3.1 r4, September. 2012, CCMB-2012-09-004, has to be taken into account.

2.2 PP Conformance

This Security Target claims conformance to:

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

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

2.3 Package Conformance

This Security Target claims conformance to:

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

3. Security Problem Definition

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

3.1 Threats

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

<Threats to the TOE in the Personalization phase>

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

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

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

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

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

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

Copyright Ⓒ 2014 KOMSCO, All rights reserved

Application Notes: The BAC/SAC/BAP authentication key is generated by the Personalization Agent in the Personalization phase and saved in secure memory. A threat can attempt to access the BAC/SAC/BAP authentication key that is saved in secure or in the temporary memory of the MRTD or the IDL Chip.

T. BAC/BAP_ReplayAttack

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

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

<EAC/EAP-related Threats in the Operational Use phase>

T. Damage_to_Biometric/Optional_Data

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

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

T. EAC-CA/EAP-CA_Bypass

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

T. IS_Certificate_Forgery

To obtain access rights to the biometric data of the ePassport holder, a threat agent can attempt to bypass the EAC-TA by forging the CVCA Link certificate, DV certificate and IS certificate and requesting verification of the certificates by the TOE.
To obtain access rights to the optional data of the IDL holder, a threat agent can attempt to bypass the EAP-TA by forging the Alternative Root certificate and L(n)~L(0) certificate and requesting verification of the certificates by the TOE.

<Threats related to IC Chip Support>

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

<Other Threats in the Personalization and the Operational Use phase>

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

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

T. Skimming

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

T. Leakage_CryptographicKey_Info

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

T. ePassport/IDL_Reproduction

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

T. Residual_Info

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

T. ICChip_Replacement

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

3.2 Organizational Security Policies

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

P. International_Compatibility

The Personalization Agent shall ensure compatibility between the security mechanisms of the ePassport or the IDL and the security mechanisms of the Inspection System.

Application Notes: International compatibility shall be ensured according to the ICAO document, EAC, SAC and IDL ISO/IEC specifications concerning the ePassport and the IDL.

P. Security_Mechanism_Application_Procedures

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

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

Application Notes: The basic operation flow of the IDL security mechanisms complies with the basic operation flow of the ePassport security mechanisms.

P. Application_Program_Install

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

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

P. Personalization_Agent

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

P. Access_Control

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

Application Notes: According to the ICAO document, EAC, SAC and IDL ISO/IEC specifications concerning the ePassport and the IDL, the TOE shall build access control policies as of following (Table 12) ~ (Table 17).

(Table 12) ePassport Access Control Policies in Operational Use Phase

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

(Table 13) ePassport Access Control Policies in the Personalization Phase

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

(Table 14) ePassport TSF Data Access Control Policies

		Objects	Objects											
		Objects	EAC Chip Authentication Private key		CVCA Certificate and CVCA Digital Signature Verification Key Current Date		BAC Authentication Key		AA Private key		PAC Authentication Key		SAC Authentication Key, CAN	
Subjects		Security Attributes Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	Personalization Agent	Personalization Agent Issuing Authorization	deny	allow	deny	allow	deny	allow	deny	allow	deny	allow	deny	allow

(Table 15) IDL Access Control Policies in Operational Use Phase

		Objects List	Objects							
		Objects List	Personal data of the IDL holder		Optional data of the IDL holder		IDL authentication data		EF.COM	
Subjects List		Security Attributes Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	BIS	BAP Authorization	allow	deny	allow/deny	deny	allow	deny	allow	deny

Subjects List		Objects List	Objects							
		Objects List	Personal data of the IDL holder		Optional data of the IDL holder		IDL authentication data		EF.COM	
		Security Attributes Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
	EIS	BAP Authorization	allow	deny	allow/deny	deny	allow	deny	allow	deny
		EAP Authorization	allow	deny	allow	deny	allow	deny	allow	deny

Application Notes: An EAP authorization should be needed to access the fingerprint, the iris and the other biometric template information(DG7~9) of the IDL holder among the optional data. And an access to the other optional information of the IDL holder should need a BAP authorization or an EAP authorization according to the policy of the Personalization Agent.(By reading EF.COM, it is possible to check a category of DGs that should request an EAP authorization.)

(Table 16) IDL Access Control Policies in the Personalization Phase

Subjects List		Objects List	Objects							
		Objects List	Personal data of the IDL holder		Optional data of the IDL holder		IDL authentication data		EF.COM	
		Security Attributes Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	Personalization Agent	Personalization Agent Issuing Authorization	allow	allow	allow	allow	allow	allow	allow	allow

(Table 17) IDL TSF Data Access Control Policies

Subjects		Objects	Objects									
		Objects	EAP Chip Authentication private key		Trust Root Certificate and Alternative Root Certificate Digital Signature Verification Key Current Date		BAP Authentication Key		AA private key		PAC Authentication Key	
		Security Attributes Security Attributes	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights	Read Rights	Write Rights
Subjects	Personalization Agent	Personalization Agent Issuing Authorization	deny	allow	deny	allow	deny	allow	deny	allow	deny	allow

P. PKI

The Issuing State of the ePassport shall implement the PA-PKI and EAC-PKI security mechanism according to the ePassport PKI System and execute the practice of certification(creating, issuing, operating and destroying the certificates) by securely generating and managing digital signature keys in accordance with the Certification Practice

Statement(CPS).

The Issuing State of the IDL shall implement the PA-PKI and EAP-PKI security mechanism according to the IDL PKI System and execute the practice of certification(creating, issuing, operating and destroying the certificates) by securely generating and managing digital signature keys in accordance with the Certification Practice Statement.

In addition, the Issuing State of the ePassport or the IDL shall update certificates according to the policies to maintain a valid date of the certificates and securely delivery them to the Verifying State and Inspection System.

When the EAC-TA provides the TOE with the CVCA Link certificate, the DV certificate and the IS certificate after the ePassport Inspection System, obtaining information from EF.CVCA stored in the TOE, the TOE shall internally update certificates by verifying the validity of the certificates.

When the EAP-TA provides the TOE with a Alternative Root certificate and L(n)~L(0) certificate after the IDL Inspection System, obtaining information from EF.COM stored in the TOE, the TOE shall internally update certificates by verifying the validity of the certificates.

P. Range_RF_Communication

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

P. IC_Chip

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

3.3 Assumptions

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

A. Certificate_Verification

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

The EIS shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA Link certificate, the DV certificate and the IS certificate in the EAC-TA, or with the Alternative Root certificate and L(n)~L(0) in the EAP-TA.

A. Inspection_System

The ePassport Inspection System shall implement the security mechanisms of the PA, the AA, the SAC, the BAC and the EAC according to the ICAO document, EAC specification and SAC specification on the basis of the verifying policy of the ePassport for the ePassport holder.
The IDL Inspection System shall implement the security mechanisms of the PA, the AA, the BAP and the EAP according to the IDL ISO/IEC specification on the basis of the verifying policy of the IDL for the IDL holder.
Additionally, after the session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the SAC session key, the BAC/BAP session key, the EAC/EAP session key and the other session information.

A. MRZ_Entropy

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

<IC chip ST Assumption>

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

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

4. Security Objectives

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

4.1 Security Objectives for TOE

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

O. Management
The TOE shall provide the means to manage the ePassport or the IDL application data in the Personalization phase to the authorized Personalization Agent.

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

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

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

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

Application Note: The TOE forms a secure communication channel using the PAC Session key during the Personalization phase. The TOE forms a secure communication channel using the BAC/BAP Session key, the SAC Session key and the EAC/EAP Session key during the Operational Use phase.

O. Certificate_Verification

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

O. Secure_State

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

O. Deleting_Residual_Info

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

O. Replay_Prevention

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

O. Access_Control

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

O. Handling_Info_Leakage

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

O. BAC

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

O. BAP

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

O. EAC

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

O. EAP

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

Application Note: An EAP authorization should be needed to access the fingerprint, the iris and the other biometric template information(DG7~9) of the IDL holder among the optional data. And an access to the other optional information of the IDL holder may need an EAP authorization according to the policy of the Personalization Agent.

O. IC_Chip

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

O. SAC

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

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

O. AA

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

O. PAC

The TOE carries out the PAC mutual authentication and the PAC personalization and management authentication to provide a means of management for the ePassport or the IDL personalization(EF file creation, PAC authentication key update, operational mode change, an execution code and data patch, unblock, and TSF data management) to only an authorized Personalization Agent.

4.2 Security Objectives for Operational Environment

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

OE. PassportBook/Card_Manufacturing_Security

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

OE. Procedures_of_ePassport/IDL_holder_Check

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

The officer(or police) shall prepare for procedures to check the identity of the IDL holder against the printed identity information page of the IDL.

OE. Application_Program_Install

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

OE. Certificate_Verification

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

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

The EIS shall securely hold the digital signature generation key that corresponds to the L(0) certificate and shall provide the TOE with an Alternative Root certificate and L(n)~L(0) certificate in the EAP-TA.

OE. Personalization_Agent

Copyright Ⓒ 2014 KOMSCO, All rights reserved

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

OE. Inspection_System

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

OE. MRZ_Entropy

The Personalization Agent shall ensure the MRZ entropy to ensure the security of the BAC authentication key. And the Personalization Agent shall ensure the entropy for the BAP seed value to ensure the security of the BAP authentication key.

OE. PKI

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

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

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

OE. Range_RF_Communication

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

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

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

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

4.3. Security Objectives Rationale

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

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

The Rationale of the Security Objectives demonstrates the following:

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

(Table 18) shows the mapping between Security Problem Definitions and Security Objectives.

(Table 18) Mapping between Security Problem Definitions and Security Objectives

Security Objectives	TOE Security Objectives																		Security Objectives for Environment								
Security Problem Definition	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Secure_State	O.Certificate_Verification	O.Deleting_residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_ Info_Leakage	O.IC_Chip	O.AA	O.BAC	O.EAC	O.PAC	O.SAC	O.BAP	O.EAP	OE.PassportBook/Card_Manufacturing_Security	OE.Procedures_of_ePassport/IDL_Holder_Check	OE.Application_ Program_Install	OE.Certificate_Verification	OE.Personalization_ Agent	OE.Inspection_System	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Communication
T.TSF_Data_ Modification	X		X	X					X						X								X				
T.Disguise_of_ Personalization_Agent															X												
T.Eavesdropping				X																				X			
T.Forgery_Corruption_ Personal_ Data			X						X				X			X	X							X			

Security Objectives Security Problem Definition	TOE Security Objectives																		Security Objectives for Environment								
	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Secure_State	O.Certificate_Verification	O.Deleting_residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_ Info_Leakage	O.IC_Chip	O.AA	O.BAC	O.EAC	O.PAC	O.SAC	O.BAP	O.EAP	OE.PassportBook/Card_Manufacturing_Security	OE.Procedures_of_ePassport/IDL_Holder_Check	OE.Application_ Program_Install	OE.Certificate_Verification	OE.Personalization_ Agent	OE.Inspection_System	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Communication
T. Authentication _Key_Disclose	X		X				X		X											X							
T.BAC/BAP_ReplayAttack								X																			
T.Damage_to_Biometric/Optional _Data			X	X		X			X					X				X				X		X		X	
T.EAC-CA/EAP-CA_Bypass		X																		X		X		X			
T.IS_Certificate_Forgery	X					X																X					
T.SessionData_Reuse								X																X			
T.Skimming									X				X	X		X	X	X						X			X
T.Malfunction					X						X																
T.Leakage_ CryptographicKey_Info										X	X																
T.ePassport/IDL_Reproduction																			X	X							
T.Replacement_of _ICChip												X															
T.Residual_Info							X																				
P.International_ Compatibility																							X				
P.Security_Mechanism_ Application_Procedures		X																						X			
P.Application_Program _Install																					X						
P.Personalization_Agent	X														X								X				
P. Access _Control	X								X				X	X	X	X	X	X					X	X			
P.PKI						X																				X	
P.Range_RF_ Communication																											X
P.IC_Chip											X																
A.Certificate_Verification																						X	X			X	
A.Inspection System																								X			
A.MRZ_Entropy																									X		

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

5. Definition of Extended Component

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

FCS_RNG Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are 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*].

Copyright © 2014 KOMSCO, All rights reserved

6. Security Requirements

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

6.1 Security Functional Requirements

The security functional requirements for this Security Target consist of the following components from Part 2 of the CC and the added components described in chapter 5, as summarized below (Table 19).

(Table 19) Security Functional Requirements

Security functional class	Security functional components	
Cryptographic Support (FCS)	FCS_CKM.1(1)	Cryptographic key generation(ePassport key derivation mechanism)
	FCS_CKM.1(2)	Cryptographic key generation(PAC session key)
	FCS_CKM.1(3)	Cryptographic key generation(SAC)
	FCS_CKM.1(4)	Cryptographic key generation(IDL key derivation mechanism)
	FCS_CKM.2(1)	Cryptographic key distribution(KDF seed distribution for BAC session key generation)
	FCS_CKM.2(2)	Cryptographic key distribution(KDF seed distribution for EAC session key generation)
	FCS_CKM.2(3)	Cryptographic key distribution(Seed distribution for PAC session key generation)
	FCS_CKM.2(4)	Cryptographic key distribution(KDF seed distribution for SAC session key generation)
	FCS_CKM.2(5)	Cryptographic key distribution(KDF seed distribution for BAP session key generation)
	FCS_CKM.2(6)	Cryptographic key distribution(KDF seed distribution for EAP session key generation)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation(Symmetric key cryptographic operation)
	FCS_COP.1(2)	Cryptographic operation(MAC)
	FCS_COP.1(3)	Cryptographic operation(Hash function)
	FCS_COP.1(4)	Cryptographic operation(Digital signature verification for certificates verification)
	FCS_COP.1(5)	Cryptographic operation(Digital signature generation)
	FCS_RNG.1	Random number generation
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control(ePassport)
	FDP_ACF.1(1)	Security attribute based access control(ePassport)
	FDP_ACC.1(2)	Subset access control(IDL)
	FDP_ACF.1(2)	Security attribute based access control(IDL)
	FDP_DAU.1	Basic data authentication

Security functional class	Security functional components	
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1(1)	Basic data exchange confidentiality(ePassport)
	FDP_UIT.1(1)	Data exchange integrity(ePassport)
	FDP_UCT.1(2)	Basic data exchange confidentiality(IDL)
	FDP_UIT.1(2)	Data exchange integrity(IDL)
Identification and Authentication (FIA)	FIA_AFL.1(1)	Authentication failure handling(ePassport)
	FIA_AFL.1(2)	Authentication failure handling(IDL)
	FIA_UAU.1(1)	Timing of authentication(BAC mutual authentication)
	FIA_UAU.1(2)	Timing of authentication(EAC-TA)
	FIA_UAU.1(3)	Timing of authentication(PAC mutual authentication)
	FIA_UAU.1(4)	Timing of authentication(PAC personalization management authentication)
	FIA_UAU.1(5)	Timing of authentication(SAC mutual authentication)
	FIA_UAU.1(6)	Timing of authentication(BAP mutual authentication)
	FIA_UAU.1(7)	Timing of authentication(EAP-TA)
	FIA_UAU.4(1)	Single-use authentication mechanisms(ePassport)
	FIA_UAU.4(2)	Single-use authentication mechanisms(IDL)
	FIA_UAU.5(1)	Multiple authentication mechanisms(ePassport)
	FIA_UAU.5(2)	Multiple authentication mechanisms(PAC mutual authentication and PAC personalization and management authentication)
	FIA_UAU.5(3)	Multiple authentication mechanisms(IDL)
	FIA_UID.1(1)	Timing of identification(ePassport)
	FIA_UID.1(2)	Timing of identification(IDL)
Security Management (FMT)	FMT_MOF.1(1)	Management of security functions behavior
	FMT_MOF.1(2)	Management of security functions behavior(Initialization)
	FMT_MSA.1(1)	Management of security attributes(ePassport)
	FMT_MSA.1(2)	Management of security attributes(IDL)
	FMT_MSA.3(1)	Static attribute initialization(ePassport)
	FMT_MSA.3(2)	Static attribute initialization(IDL)
	FMT_MTD.1(1)	Management of TSF data(Certificate verification information)
	FMT_MTD.1(2)	Management of TSF data(SSC initialization)
	FMT_MTD.1(3)	Management of TSF data(Key write)
	FMT_MTD.1(4)	Management of TSF data(TOE operational mode and PAC authentication key management)
	FMT_MTD.1(5)	Management of TSF data(Transition of TOE operational mode and changing ticket)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy(FRP)	FPR_UNO.1	Unobservability
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1(1)	Inter-TSF detection of modification(ePassport)
	FPT_ITI.1(2)	Inter-TSF detection of modification(IDL)

Copyright ⓒ 2014 KOMSCO, All rights reserved

Security functional class	Security functional components	
	FPT_PHP.3	Resistance to physical attack
	FPT_TST.1	TSF testing

6.1.1. Cryptographic Support

FCS_CKM.1(1) Cryptographic key generation(ePassport key derivation mechanism)

Hierarchical to: No other components.

Dependencies: [**FCS_CKM.2(1) Cryptographic key distribution(KDF seed distribution for BAC session key generation) and**
FCS_CKM.2(2) Cryptographic key distribution(KDF seed distribution for EAC session key generation) or
FCS_COP.1(3) Cryptographic operation(Hash function)]
FCS_CKM.4 Cryptographic key destruction

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

FCS_CKM.1(2) Cryptographic key generation(PAC session key)

Hierarchical to: No other components.

Dependencies: [**FCS_CKM.2(3) Cryptographic key distribution(Seed distribution for PAC session key generation) or**
FCS_COP.1(1) Cryptographic operation(Symmetric key cryptographic operation)]
FCS_CKM.4 Cryptographic key destruction

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

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

Hierarchical to: No other components.

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

Copyright Ⓒ 2014 KOMSCO, All rights reserved

FCS_CKM.1.1. The TSF shall generate encryption keys in accordance with a specified cryptographic key generation algorithm [key generation method column in (Table 20)] and specified cryptographic key sizes [key length column in below table] that meets the following: [SAC specification, ANS X9.62].

(Table 20) SAC Key Generation

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

FCS_CKM.1(4) Cryptographic key generation(IDL key derivation mechanism)

Hierarchical to: No other components.

Dependencies: [**FCS_CKM.2(5) Cryptographic key distribution(KDF seed distribution for BAP session key generation) and**
FCS_CKM.2(6) Cryptographic key distribution(KDF seed distribution for EAP session key generation) or
FCS_COP.1(3) Cryptographic operation(Hash function)]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1. The TSF shall generate **encryption keys and MAC keys** in accordance with a specified cryptographic key generation algorithm [B.4 Key Derivation Mechanism] and specified cryptographic key sizes [112bit, 128bit, 192bit, 256bit] that meet the following: [IDL ISO/IEC specification].

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

Hierarchical to: No other components

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

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

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

Hierarchical to: No other components.

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

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

FCS_CKM.2(3) Cryptographic key distribution(Seed distribution for PAC session key generation)

Hierarchical to: No other components.

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

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

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

FCS_CKM.2(4) Cryptographic key distribution(KDF seed distribution for SAC session key generation)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(3) Cryptographic key generation(SAC)]
FCS_CKM.4 Cryptographic key destruction

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

FCS_CKM.2(5) Cryptographic key distribution(KDF seed distribution for BAP 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(4) Cryptographic key generation(IDL key derivation mechanism)]
FCS_CKM.4 Cryptographic key destruction

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

FCS_CKM.2(6) Cryptographic key distribution(KDF seed distribution for EAP 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(4) Cryptographic key generation(IDL key derivation mechanism)]
FCS_CKM.4 Cryptographic key destruction

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(ePassport key derivation mechanism)
FCS_CKM.1(2) Cryptographic key generation(PAC session key)
FCS_CKM.1(3) Cryptographic key generation(SAC)
FCS_CKM.1(4) Cryptographic key generation(IDL key derivation mechanism)]

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

FCS_COP.1(1) Cryptographic operation(Symmetric key cryptographic operation)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(ePassport key derivation mechanism)
FCS_CKM.1(2) Cryptographic key generation(PAC session key)
FCS_CKM.1(3) Cryptographic key generation(SAC)
FCS_CKM.1(4) Cryptographic key generation(IDL key derivation mechanism)]
FCS_CKM.4 Cryptographic key destruction

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

FCS_COP.1(2) Cryptographic operation(MAC)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(ePassport key derivation mechanism)
FCS_CKM.1(2) Cryptographic key generation(PAC session key)
FCS_CKM.1(3) Cryptographic key generation(SAC)
FCS_CKM.1(4) Cryptographic key generation(IDL key derivation mechanism)]
FCS_CKM.4 Cryptographic key destruction

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

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

Hierarchical to: No other components.

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

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

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

FCS_COP.1(4) Cryptographic operation(Digital signature verification for certificates verification)

Hierarchical to: No other components.

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

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

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

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No other components.

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

FCS_RNG.1.2 The TSF shall provide random numbers **together with a post processing described in TRNG application note and TRNG library** that meet [the "standard" level of ANSSI requirements (French metric). In addition, 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].

6.1.2. User Data Protection

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

Hierarchical to: No other components.

Dependencies: **FDP_ACF.1(1) Security attribute-based access control(ePassport)**

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

a) Subjects

(1) Personalization Agent

(2) BIS

(3) EIS

(4) [None]

b) Objects

(1) Personal data of the ePassport holder

: EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16

(2) The biometric data of the ePassport holder

: EF.DG3, EF.DG4

(3) ePassport authentication data

: EF.DG14, EF.DG15, EF.SOD

(4) EF.CVCA

(5) EF.COM

(6) [EF.CARDACCESS]

c) Operations

(1) Read

(2) Write

(3) [None]

]

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

Hierarchical to: No other components.

Dependencies: **FDP_ACC.1(1) Subset access control(ePassport)**

FMT_MSA.3(1) Static attribute initialization(ePassport)

FDP_ACF.1.1 The TSF shall enforce [the ePassport access control policy] on objects based on the following: [**(Table 21), (Table 22),** [none]].

(Table 21) Subject-relevant Security Attributes(ePassport)

Subject	Security attributes
BIS	**SAC authorization**, BAC authorization
EIS	**SAC authorization**, BAC authorization, EAC authorization
Personalization Agent	Personalization Agent issuing authorization

(Table 22) Object-relevant Security Attributes(ePassport)

Object	Security attributes	
	Security attributes of object's operation	Security attributes of object's access-rights
Personal data of the ePassport holder	Read-rights	**SAC authorization**, BAC authorization, EAC authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
Biometric data of the ePassport holder	Read-rights	EAC authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
ePassport authentication data	Read-rights	**SAC authorization,** BAC authorization, EAC authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization

Copyright © 2014 KOMSCO, All rights reserved

EF.CVCA	Read-rights	**SAC authorization,** BAC authorization, EAC authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
EF.COM	Read-rights	**SAC authorization,** BAC authorization, EAC authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
EF.CARDACCESS	**Read-rights**	**-**
	Write-rights	**Personalization Agent issuing authorization**

Operation	Security attributes
Read	none
Write	

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

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

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

b) [none]

]

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

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

a) Explicitly deny access of subjects to objects, if the instructions order of the Inspection System is not correct in order to ensure the application order of security mechanisms according to the inspection procedures of the EAC specification and the **inspection procedures of the SAC specification**.

b) Explicitly Deny reading of subjects to biometric data if there are no read-rights of biometric data in the IS certificate of the EIS that has the EAC authorization

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

d) [Access of subjects to objects that are explicitly denied for the commands that cannot be executed in each operational mode(EMPTY, UNISSUE, INITAUTH, SECONDAUTH, STARTISSUE, ISSUED, BLOCK and DISCARD) of the TOE

e) Access of subjects to objects that are explicitly denied for the invalid commands such as not ISO command, not industrial command and invalid P1/P2/Lc command.

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

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

Hierarchical to: No other components.

Dependencies: **FDP_ACF.1(2) Security attribute-based access control(IDL)**

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

a) Subjects
   (1) Personalization Agent
   (2) BIS
   (3) EIS
b) Objects
   (1) Mandatory data of the IDL holder
   : EF.DG1
   (2) Optional data of the IDL holder
   : EF.DG2 ~ EF.DG11
   (3) IDL authentication data
   : EF.DG12, EF.DG13, EF.DG14, EF.SOD
   (4) EF.COM

c) Operations
    (1) Read
    (2) Write
  ]

FDP_ACF.1(2) Security attributes based access control(IDL)

Hierarchical to: No other components.

Dependencies: **FDP_ACC.1(2) Subset access control(IDL)**
FMT_MSA.3(2) Static attribute initialization(IDL)

FDP_ACF.1.1 The TSF shall enforce [the IDL access control policy] on objects based on the following: [**(Table 23), (Table 24),** [none]].

(Table 23) Subject-relevant Security Attributes(IDL)

Subject	Security attributes
BIS	BAP authorization
EIS	BAP authorization, EAP authorization
Personalization Agent	Personalization Agent issuing authorization

(Table 24) Object-relevant Security Attributes(IDL)

Object	Security attributes	
	Security attributes of object's operation	Security attributes of object's access-rights
Mandatory data of the IDL holder	Read-rights	BAP authorization, EAP authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
Optional data of the IDL holder	Read-rights	BAP authorization or EAP authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
IDL authentication data	Read-rights	BAP authorization, EAP authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization
EF.COM	Read-rights	BAP authorization, EAP authorization, Personalization Agent issuing authorization
	Write-rights	Personalization Agent issuing authorization

Operation	Security attributes
Read	none
Write	

Application Notes: The BAP authorization is the right given to the user identified with the Inspection System that supports the IDL application by FIA_UID.1 when the BAP mutual authentication succeeds. The EAP authorization is the right given when the Inspection System with the BAP authorization succeeds in the EAP-CA and the EAP-TA and the read-rights of the optional data is included in the certificates held by that Inspection System. Even when the EAP-CA and the EAP-TA succeed, the Inspection System comprises only the BAP authorization if the certificates do not include the read-rights. Issuing authorization is the right given when PAC mutual authentication and PAC personalization and management authentication succeed due to the Personalization Agent.

Application Notes: An EAP authorization should be needed to access the fingerprint, the iris and the other biometric template information(DG7~9) of the IDL holder among the optional data. And an access to the other optional information of the IDL holder should need a BAP authorization or an EAP authorization according to the policy of the Personalization Agent.(By reading EF.COM, it is possible to check a category of DGs that should request an EAP authorization.)

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

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

]

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

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

a) Explicitly deny access of subjects to objects, if the instructions order of the Inspection System is not correct in order to ensure the application order of security mechanisms

b) Explicitly Deny reading of subjects to the optional data if there are no read-rights of the optional data in the certificate of the EIS that has the EAP authorization

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

d) [Access of subjects to objects that are explicitly denied for the commands that cannot be executed in each operational mode(EMPTY, UNISSUE, INITAUTH, SECONDAUTH, STARTISSUE, ISSUED, BLOCK and DISCARD) of the TOE

e) Access of subjects to objects that are explicitly denied for the invalid commands such as not ISO command, not industrial command and invalid P1/P2/Lc command.

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

Application Notes: The basic operation flow of the IDL security mechanisms complies with the basic operation flow of the ePassport security mechanisms.

FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1. The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [the AA private key].

FDP_DAU.1.2. The TSF shall provide [BIS, EIS] with the ability to verify evidence of the validity of the indicated information.

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

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) BAC session key

b) EAC session key

c) BAC authentication key

d) [PAC session key,

e) PAC authentication key,

f) AA private key,

g) EAC chip authentication private key,

h) CVCA digital signature verification key and domain information,

i) SAC authentication key,
j) SAC session key,
k) BAP session key,
l) EAP session key,
m) BAP authentication key,
n) EAP chip authentication private key,
o) Trust Root certificate digital signature verification key and domain information]

Application Notes: After the termination of the session, the TSF deletes the SAC authentication key, SAC session key, BAC authentication key, BAC session key, EAC session key, PAC authentication key, PAC session key, AA private key, EAC chip authentication key, CVCA digital signature verification key and domain information, BAP authentication key, BAP session key, EAP session key, Trust Root certificate digital signature verification key and domain information and SSC/Ticket and the flag of random number usage in temporary memory by writing '0x00' in the memory. After finished the issuance and the operational mode of the TOE is ISSUED mode, PAC authentication key is physically deleted by writing '0xFF' in the memory. And when the operational mode of the TOE is DISCARD, all key information is physically deleted by writing ‘0xFF’ in the memory.

FDP_UCT.1(1) Basic data exchange confidentiality(ePassport)
Hierarchical to: No other components.
Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1(1) Subset access control(ePassport), or
FDP_IFC.1(1) Subset information flow control(ePassport)]

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

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

FDP_UIT.1(1) Data exchange integrity(ePassport)
Hierarchical to: No other components.

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

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

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

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

FDP_UCT.1(2) Basic data exchange confidentiality(IDL)
Hierarchical to: No other components.
Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1(2) Subset access control(IDL), or
FDP_IFC.1(2) Subset information flow control(IDL)]

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

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

FDP_UIT.1(2) Data exchange integrity(IDL)
Hierarchical to: No other components.
Dependencies: [**FDP_ACC.1(2) Subset access control(IDL)**, or
FDP_IFC.1(2) Subset information flow control(IDL)]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

Copyright © 2014 KOMSCO, All rights reserved

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

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

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

6.1.3. Identification and Authentication

FIA_AFL.1(1) Authentication failure handling(ePassport)

Hierarchical to: No other components.

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

FIA_AFL.1.1. The TSF shall detect when *[a certain number of times (see (Table 25))]* unsuccessful authentication attempts occur related to the following:

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

FIA_AFL.1.2. When *the defined number* of unsuccessful authentication attempts has been *met*, the TSF shall perform [**the actions specified in the following (Table 25)**].

(Table 25) Authentication Failure Handling(ePassport)

Assignment: Number of unsuccessful authentication attempts	Assignment: Specified authentication events	Assignment: Actions
1	BAC mutual authentication	Session termination

Copyright © 2014 KOMSCO, All rights reserved

1	EAC-TA authentication	Subset residual information removal, Maintaining secure communication channel
3	PAC mutual authentication PAC Personalization management authentication	Session termination and operational mode transition
1	SAC mutual authentication	Session termination

Application Notes: The TSF halts all functions for 1 sec after terminating the session when BAC mutual authentication failed. When EAC-TA authentication is failed, EAC secure communication channel is lasted. TSF guarantees accessing for all of DG files except for DG3 and DG4. When PAC authentication is failed, the operational mode is transited to BLOCK mode.

FIA_AFL.1(2) Authentication failure handling(IDL)

Hierarchical to: No other components.

Dependencies: **FIA_UAU.1(3) Authentication(PAC mutual authentication)**
FIA_UAU.1(4) Authentication(PAC personalization management authentication)
FIA_UAU.1(6) Authentication(BAP mutual authentication)
FIA_UAU.1(7) Authentication(EAP-TA)

FIA_AFL.1.1. The TSF shall detect when *[a certain number of times (see (Table 26))]* unsuccessful authentication attempts occur related to the following:

a) [BAP mutual authentication,
b) EAP-TA,
c) PAC mutual authentication,
d) PAC Personalization management authentication]

FIA_AFL.1.2. When *the defined number* of unsuccessful authentication attempts has been *met*, the TSF shall perform [the actions specified in the following (Table 26)].

(Table 26) Authentication Failure Handling(IDL)

Assignment: Number of unsuccessful authentication attempts	**Assignment: Specified authentication events**	**Assignment: Actions**
1	BAP mutual authentication	Session termination
1	EAP-TA authentication	Subset residual information removal, Maintaining secure communication channel
3	PAC mutual authentication PAC personalization management authentication	Session termination and operational mode transition

Application Notes: The TSF halts all functions for 1 sec after terminating the session when BAP mutual authentication failed. When EAP-TA authentication is failed, EAP secure communication channel is lasted. TSF guarantees accessing for all of DG files except for the optional data that requests an EAP authorization according to the policies of the Personalization Agent. When PAC authentication is failed, the operational mode is transited to BLOCK mode.

FIA_UAU.1(1) Timing of authentication(BAC mutual authentication)
Hierarchical to: No other components.
Dependencies: **FIA_UID.1(1) Timing of identification(ePassport)**

FIA_UAU.1.1. The TSF shall allow [

a) to indicate that supports the BAC mechanism
b) [None]

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

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

FIA_UAU.1(2) Timing of authentication(EAC-TA)
Hierarchical to: No other components.
Dependencies: [**FIA_UAU.1(1) Timing of authentication(BAC mutual authentication) or**
FIA_UAU.1(5) Timing of authentication(SAC mutual authentication)]

FIA_UAU.1.1. The TSF shall allow [

a) performance of the EAC-CA
b) reading user data except for the biometric data of the ePassport holder
c) [None]

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

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

FIA_UAU.1(3) Timing of authentication(PAC mutual authentication)
Hierarchical to: No other components.
Dependencies: [**FIA_UID.1(1) Timing of identification(ePassport)** or
FIA_UID.1(2) Timing of identification(IDL)]

FIA_UAU.1.1. The TSF shall allow [

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

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

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

FIA_UAU.1(4) Timing of authentication(PAC personalization management authentication)
Hierarchical to: No other components.
Dependencies: [**FIA_UID.1(1) Timing of identification(ePassport) or**
FIA_UID.1(2) Timing of identification(IDL)]

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

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

FIA_UAU.1(5) Timing of authentication(SAC mutual authentication)
Hierarchical to: No other components.
Dependencies: **FIA_UID.1(1) Timing of identification(ePassport)**

FIA_UAU.1.1. The TSF shall allow [
a) the reading of EF.CARDACCESS
]on behalf of the user to be performed before the user is authenticated.

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

FIA_UAU.1(6) Timing of authentication(BAP mutual authentication)
Hierarchical to: No other components.

Dependencies: **FIA_UID.1(2) Timing of identification(IDL)**

FIA_UAU.1.1. The TSF shall allow [to indicate that supports the BAP mechanism] 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(7) Timing of authentication(EAP-TA)
Hierarchical to: No other components.
Dependencies: **FIA_UAU.1(6) Timing of authentication(BAP mutual authentication)**

FIA_UAU.1.1. The TSF shall allow [

a) performance of the EAP-CA
b) reading user data except for the optional data of the IDL holder

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

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

FIA_UAU.4(1) Single-use authentication mechanisms(ePassport)
Hierarchical to: No other components.
Dependencies: No dependencies.

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

a) BAC mutual authentication
b) EAC-TA
c) [PAC Mutual authentication,
d) PAC personalization management authentication
e) AA authentication
f) SAC mutual authentication]]

FIA_UAU.4(2) Single-use authentication mechanisms(IDL)
Hierarchical to: No other components.
Dependencies: No dependencies.

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

a) BAP mutual authentication
b) EAP-TA

Copyright Ⓒ 2014 KOMSCO, All rights reserved

c) PAC Mutual authentication,

d) PAC personalization management authentication

e) AA authentication]

FIA_UAU.5(1) Multiple authentication mechanisms(ePassport)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1. The TSF shall provide [

a) BAC mutual authentication

b) EAC-TA

c) [SAC mutual authentication]

] to support user authentication.

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

a) BIS or EIS shall succeed with the BAC mutual authentication to allow the BAC authorization.

b) EIS, to succeed with EAC authorization, shall succeed with the SAC mutual authentication or the BAC mutual authentication, EAC-CA, and EAC-TA, and shall include the read-rights of the biometric data in the CVCA certificate, DV certificate and IS certificate. To do this, the TSF shall provide the EAC-CA.

c) [BIS or EIS shall succeed with the SAC mutual authentication to allow the SAC authorization]]

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1. The TSF shall provide [

a) PAC mutual authentication

b) PAC personalization and management authentication(PAC-LifeCycle authentication, PAC-Patch authentication, PAC-KeyUpdate authentication, and PAC-Unblock authentication)] to support user authentication.

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

a) In case the operational mode of the TOE in Personalization phase is in the UNISSUE mode, PAC mutual authentication has to be successfully performed.

b) In case the operational mode of the TOE in the Personalization phase is in the INITAUTH mode, PAC personalization and management authentication(PAC-LifeCycle authentication) has to be successfully performed to transit the operational mode of the TOE.

c) In case the operational mode of TOE in Personalization phase is in the INITAUTH mode and the issuing right for updating the PAC authentication key is not obtained, PAC personalization and management authentication along with PAC-KeyUpdate authentication has to be successfully performed to update the PAC authentication key.

d) In case the operational mode of TOE in Personalization phase is in the SECONDAUTH mode and the issuing right for updating the PAC authentication key is not obtained, PAC personalization and management authentication along with PAC-KeyUpdate authentication has to be successfully performed to update the PAC authentication key.

e) In case the operational mode of the TOE in the Personalization phase is in the SECONDAUTH mode and the issuing right for patching the execution code and data is not obtained, PAC personalization and management authentication along with PAC-Patch authentication has to be successfully performed to patch the execution code and data.

f) In case the operational mode of the TOE in the Personalization phase is in the SECONDAUTH mode and the issuing right for transiting the operational mode of the TOE is not obtained, PAC personalization and management authentication along with PAC-LifeCycle authentication has to be successfully performed to transit the operational mode.

g) In case the operational mode of the TOE in the Personalization phase is in the STARTISSUE mode, PAC personalization and management authentication(PAC-LifeCycle authentication) has to be successfully performed to transit the operational mode of the TOE.

h) In case the operational mode of the TOE in the Personalization phase is in the BLOCK mode, PAC-Unblock authentication has to be successfully performed to unblock it.

]

FIA_UAU.5(3) Multiple authentication mechanisms(IDL)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1. The TSF shall provide [

a) BAP mutual authentication

b) EAP-TA

] to support user authentication.

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

a) BIS or EIS shall succeed with the BAP mutual authentication to allow the BAP authorization.

b) EIS, to succeed with EAP authorization, shall succeed with the BAP mutual authentication, EAP-CA, and EAP-TA, and shall include the read-rights of the optional data in the Trust Root certificate, Alternative Root certificate and L(n)~L(0) certificate. To do this, the TSF shall provide the EAP-CA.]

FIA_UID.1(1) Timing of identification(ePassport)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1. The TSF shall allow [

a) the establishment of a communication channel based on ISO/IEC 14443-4

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

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

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

FIA_UID.1(2) Timing of identification(IDL)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1. The TSF shall allow [

a) the establishment of a communication channel based on ISO/IEC 14443-4

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

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

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

6.1.4 Security Management

FMT_MOF.1(1) Management of security functions behavior

Hierarchical to: No other components.

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

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

FMT_MOF.1(2) Management of security functions behavior(Initialization)

Hierarchical to: No other components.

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

FMT_MOF.1.1. The TSF shall restrict the ability to *enable* [the functions (see (Table 27))] to [roles (see (Table 27))].

(Table 27) Security Attributes for Security Functions Behavior

Assignment: Functions	Assignment: Roles
Initialization of the TOE personalization	Personalization Agent in the personalization phase
Initialization of the TOE re-personalization	
Initialization of LDS file system	

FMT_MSA.1(1) Management of security attributes(ePassport)

Hierarchical to: No other components.

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

Copyright ⓒ 2014 KOMSCO, All rights reserved

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

FMT_MSA.1(2) Management of security attributes(IDL)

Hierarchical to: No other components.

Dependencies: [**FDP_ACC.1(2) Subset access control(IDL) or**
FDP_IFC.1(2) Subset information flow control(IDL)]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

FMT_MSA.3(1) Static attribute initialization(ePassport)

Hierarchical to: No other components.

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

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

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

FMT_MSA.3(2) Static attribute initialization(IDL)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1(2) Management of security attributes(IDL)
FMT_SMR.1. Security roles

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

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

Copyright © 2014 KOMSCO, All rights reserved

FMT_MTD.1(1) Management of TSF data(Certificate verification information)

Hierarchical to: No other components.

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

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

a) EAC or EAP chip authentication private key

b) Initial current date

c) Initial CVCA certificate

d) Initial CVCA digital signature verification key

e) [Initial Trust Root certificate

f) Initial Trust Root certificate digital signature verification key]

] to [the 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 or SAC secure messaging before establishing EAC secure messaging after generating the EAC session key. And The TSF shall initialize SSC as "0" in order to terminate the BAP secure messaging before establishing EAP secure messaging after generating the EAP session key.

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

Hierarchical to: No other components.

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

FMT_MTD.1.1. The TSF shall restrict the ability to [*write in secure memory*] the [TSF data (see (Table 28))] to [**the restrictions (see (Table 28))**].

(Table 28) Security Attributes for TSF data

TSF data	Authorized roles	Operation
AA private key	Personalization Agent in the Personalization phase	Write to protected memory
SAC authentication key, CAN	Personalization Agent in the Personalization phase	
TSF Patch code	Personalization Agent in the Personalization phase	
BAC authentication key	TSF	
BAP authentication key	TSF	
Initialization data	Personalization Agent in the Personalization phase	

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

Hierarchical to: No other components.

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

FMT_MTD.1.1. The TSF shall restrict the ability to *query, modify* the [PAC authentication key, Operational mode of TOE in the Personalization Phase, TOE identification information, IC chip identification information] to [Authorized Personalization Agent and Inspection System]

FMT_MTD.1(5) Management of TSF data(Transition of TOE operational mode and changing Ticket)

Hierarchical to: No other components.

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

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

Application Notes: When the Personalization Agent executes the command for TOE initialization, the operation mode for TOE is changed the EMPTY mode into the UNISSUE mode. In the UNISSUE mode, if the integrity check for executing code failed, the TSF changes the operational mode of the TOE into the DISCARD mode. The TSF must changes the operational mode to the UNISSUE mode when the communication channel is closed in INITAUTH or SECONDAUTH modes. The operational mode of the TOE changes UNISSUE into INITAUTH mode when the PAC mutual authentication is successfully performed. In the

INITAUTH mode, the operational mode of the TOE changes INITAUTH into SECONDAUTH mode when the PAC personalization management authentication(PAC-LifeCycle) is successfully performed. If PAC mutual or personalization management authentication is failed more than 3 times, the operational mode of the TOE changes to the BLOCK mode and the TOE operation mode is then changed the DISCARD mode if PAC-Unblock authentication is failed more than 3 times.

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

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

Application Notes: The TSF shall use only secure values as random numbers to resistant against high attack potential. The TSF shall preserve secure values by verifying the valid data of the CVCA Link certificate, DV certificate and IS certificate/Alternative certificate and L(n)~L(0) certificate provided by the EIS when executing the EAC-TA/EAP-TA and internally updating the certificates and related data 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 management functions: [

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

g) A function to verify and update the Trust Root certificate, Trust Root certificate digital signature verification key and the current data in the IDL Operational Use phase]]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: [FIA_UID.1(1) Timing of identification(ePassport) or
FIA_UID.1(2) Timing of identification(IDL)]

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

a) Personalization Agent(ePassport Personalization Agent, IDL Personalization Agent)

b) [Inspection System(ePassport Inspection System, IDL Inspection System)]]

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

6.1.5 Privacy

FPR_UNO.1 Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) FCS_COP.1(1) A cryptographic operation(Symmetric key cryptographic operation)

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

c) FCS_COP.1(4) A cryptographic operation(Digital signature verification for certificates verification)

d) [FCS_COP.1(5) A cryptographic operation(Digital signature generation)]

] on [

a) BAC authentication key

b) BAC session key

c) EAC session key

d) EAC chip authentication private key

e) [AA Private key,
PAC authentication key,
PAC session key,

SAC authentication key,
SAC session key,
BAP authentication key,
BAP session key,
EAP session key,
EAP chip authentication private key]
] by [TSF].

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

6.1.6 TSF Protection

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

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

a) Failure detected during self-testing by FPT_TST.1
b) Conditions outside the normal operating conditions of the TSF detected by the IC chip
c) [a status that the PAC secure channel is terminated when the Operational mode is in INITAUTH or SECONDAUTH mode]

]

FPT_ITI.1(1) Inter-TSF detection of modification(ePassport)
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 another trusted IT product within the following metric: [strength of the Retail MAC and AES-CMAC].

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

a) Termination of BAC secure messaging or EAC secure messaging
b) Deletion of the BAC session key or the EAC session key

c) Management action specified in FMT_MSA.1(1)

d) [Termination of the PAC secure messaging and deletion of the PAC session key

e) Termination of the SAC secure messaging and deletion of the SAC session key]

] if modifications are detected.

FPT_ITI.1(2) Inter-TSF detection of modification(IDL)

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 another trusted IT product within the following metric: [strength of the Retail MAC and AES-CMAC].

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

a) Termination of BAP secure messaging or EAP secure messaging

b) Deletion of the BAP session key or the EAP session key

c) Termination of the PAC secure messaging and deletion of the PAC session key

d) Management action specified in FMT_MSA.1(2)

] if modifications are detected.

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 probing] to the [TSF] by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

FPT_TST.1.3. The TSF shall provide **an authorized Personalization Agent in the**

Personalization phase with the capability to verify the integrity of [*the stored TSF executable code*].

6.2 Security Assurance Requirements

The security assurance requirements for this Security Target consist of the components from Part 3 of the CC summarized in (Table 29). The evaluation assurance level is EAL5+(ALC_DVS.2, ADV_IMP.2, AVA_VAN.5).

(Table 29) Security Assurance Requirements

Assurance class	Assurance components	
Security Target evaluation	ASE_INT.1	Security Target Introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.5	Complete semi-formal functional specification with additional error information
	ADV_ARC.1	Security architecture description
	ADV_TDS.4	Semi-formal modular Design
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
	ADV_INT.2	Well-structured internals
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.5	Development tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance with Implementation standards
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Testing: Modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

Copyright ⓒ 2014 KOMSCO, All rights reserved

6.3 Security Requirements Rationale

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

6.3.1 Security Functional Requirements Rationale

The rationale of TOE security functional requirements demonstrates the followings :

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

(Table 30) presents the mapping between the security objectives and the security functional requirements.

(Table 30) Mapping between Security Objectives and Security Functional Requirements

Security Objectives Security Functional Requirements	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_esidual_Info	O.Replay_Prevention	O.Access_ Control	O.Handling_Info_Leakage	O.BAC	O.EAC	O.IC Chip	O.PAC	O.AA	O.SAC	O.BAP	O.EAP
FCS_CKM.1(1)											X	X						
FCS_CKM.1(2)														X				
FCS_CKM.1(3)																X		
FCS_CKM.1(4)																	X	X
FCS_CKM.2(1)								X			X							
FCS_CKM.2(2)												X						
FCS_CKM.2(3)								X						X				
FCS_CKM.2(4)																X		
FCS_CKM.2(5)								X									X	
FCS_CKM.2(6)																		X
FCS_CKM.4							X											
FCS_COP.1(1)				X							X		X	X		X	X	
FCS_COP.1(2)				X							X		X	X		X	X	
FCS_COP.1(3)											X	X	X		X	X	X	X
FCS_COP.1(4)					X							X	X					X
FCS_COP.1(5)													X		X			
FCS_RNG.1													X					

Copyright © 2014 KOMSCO, All rights reserved

Security Objectives / Security Functional Requirements	O.Management	O.Security_Mechanism_Application_Procedures	O.Session_Termination	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_esidual_Info	O.Replay_Prevention	O.Access_ Control	O.Handling_Info_Leakage	O.BAC	O.EAC	O.IC Chip	O.PAC	O.AA	O.SAC	O.BAP	O.EAP
FDP_ACC.1(1)									X									
FDP_ACF.1(1)	X	X							X		X	X		X		X		
FDP_ACC.1(2)									X									
FDP_ACF.1(2)	X	X							X					X			X	X
FDP_DAU.1															X			
FDP_RIP.1							X	X										
FDP_UCT.1(1)				X				X										
FDP_UIT.1(1)				X				X										
FDP_UCT.1(2)				X				X										
FDP_UIT.1(2)				X				X										
FIA_AFL.1(1)		X	X						X		X	X		X		X		
FIA_AFL.1(2)		X	X						X					X			X	X
FIA_UAU.1(1)			X						X		X							
FIA_UAU.1(2)		X	X						X			X						
FIA_UAU.1(3)			X						X					X				
FIA_UAU.1(4)			X						X					X				
FIA_UAU.1(5)			X						X							X		
FIA_UAU.1(6)			X						X								X	
FIA_UAU.1(7)		X	X						X									X
FIA_UAU.4(1)								X			X	X		X	X	X		
FIA_UAU.4(2)								X						X	X		X	X
FIA_UAU.5(1)		X							X		X	X				X		
FIA_UAU.5(2)									X					X				
FIA_UAU.5(3)		X							X								X	X
FIA_UID.1(1)											X	X		X		X		
FIA_UID.1(2)														X			X	X
FMT_MOF.1(1)	X								X					X				
FMT_MOF.1(2)	X								X					X				
FMT_MSA.1(1)				X					X									
FMT_MSA.1(2)				X					X									
FMT_MSA.3(1)	X								X					X				
FMT_MSA.3(2)	X								X					X				
FMT_MTD.1(1)	X								X					X				
FMT_MTD.1(2)		X																
FMT_MTD.1(3)	X								X					X				
FMT_MTD.1(4)	X								X					X				
FMT_MTD.1(5)	X								X					X				
FMT_MTD.3					X			X				X	X					X
FMT_SMF.1	X				X													
FMT_SMR.1	X																	
FMT_UNO.1										X			X					
FPT_FLS.1						X							X					
FPT_ITI.1(1)			X	X														
FPT_ITI.1(2)			X	X														
FPT_PHP.3													X					
FPT_TST.1						X							X					

Copyright Ⓒ 2014 KOMSCO, All rights reserved

6.3.2 Security Assurance Requirements Rationale

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

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

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

6.3.3 Rationale of Dependency

(Table 31) shows dependency of TOE functional components.

(Table 31) Dependency of TOE Functional Components

No.	Functional component	Dependency	Ref. No.
1	FCS_CKM.1(1)	[FCS_CKM.2(1) or FCS_CKM.2(2) or FCS_COP.1(3)] FCS.CKM.4	[4, 5, 11] 8
2	FCS_CKM.1(2)	[FCS_CKM.2(3) or FCS_COP.1(1)] FCS.CKM.4	[6, 9] 8
3	FCS_CKM.1(3)	[FCS_CKM.2(4) or FCS_COP.1(3)] FCS.CKM.4	[7, 11] 8
4	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)] FCS_CKM.4	[1] 8
5	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)] FCS_CKM.4	[1] 8
6	FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(2)] FCS_CKM.4	[2] 8

Copyright ⓒ 2014 KOMSCO, All rights reserved

No.	Functional component	Dependency	Ref. No.
7	FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[3] 8
8	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1) or FCS_CKM.1(2) or FCS_CKM.1(3)]	1, 2, 3
9	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1) or FCS_CKM.1(2) or FCS_CKM.1(3)] FCS_CKM.4	[1, 2, 3] 8
10	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1) or FCS_CKM.1(2) or FCS_CKM.1(3)] FCS_CKM.4	[1, 2, 3] 8
11	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[none] 8
12	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1(1)] FCS_CKM.4	1 8
13	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	[none] 8
14	FCS_RNG.1	-	-
15	FDP_ACC.1	FDP_ACF.1	16
16	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	15 34
17	FDP_DAU.1	-	-
18	FDP_RIP.1	-	-
19	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	none 15
20	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	15 none
21	FIA_AFL.1	FIA_UAU.1(1), FIA_UAU.1(2), FIA_UAU.1(3), FIA_UAU.1(4), FIA_UAU.1(5)	22,23,24, 25,26
22	FIA_UAU.1(1)	FIA_UID.1	30
23	FIA_UAU.1(2)	FIA_UAU.1(1) or FIA_UAU.1(5)	22, 26
24	FIA_UAU.1(3)	FIA_UID.1	30
25	FIA_UAU.1(4)	FIA_UID.1	30
26	FIA_UAU.1(5)	FIA_UID.1	30
27	FIA_UAU.4	-	-
28	FIA_UAU.5(1)	-	-
29	FIA_UAU.5(2)	-	-
30	FIA_UID.1	-	-
31	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	41 42
32	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	41 42
33	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	15 41 42
34	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	33 42
35	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	41 42
36	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	41 42
37	FMT_MTD.1(3)	FMT_SMF.1	41

Copyright ⓒ 2014 KOMSCO, All rights reserved

No.	Functional component	Dependency	Ref. No.
		FMT_SMR.1	42
38	FMT_MTD.1(4)	FMT_SMF.1 FMT_SMR.1	41 42
39	FMT_MTD.1(5)	FMT_SMF.1 FMT_SMR.1	41 42
40	FMT_MTD.3	FMT_MTD.1(1)	35
41	FMT_SMF.1	-	-
42	FMT_SMR.1	FIA_UID.1	30
43	FPR_UNO.1	-	-
44	FPT_FLS.1	-	-
45	FPT_ITI.1	-	-
46	FPT_PHP.3	-	-
47	FPT_TST.1	-	-

The dependency of EAL5 provided in CC is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in (Table 32).

(Table 32) Dependency of Added Assurance Components

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

Copyright ⓒ 2014 KOMSCO, All rights reserved

7. TOE Summary Specification

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

7.1 TOE Security Functionality

This chapter gives an overview of the TOE Security Functionality composing the TSF.
In the following (Table 33), all TOE security functionalities are listed.

(Table 33) TOE Security Functionality

TSF	Descriptions
SF.PAC_AUTH	PAC mutual authentication PAC session key generation PAC personalization and management authentication
SF.BAC_AUTH	BAC mutual authentication BAC session key generation
SF.BAP_AUTH	BAP mutual authentication BAP session key generation
SF.SAC_AUTH	SAC mutual authentication SAC session key generation
SF.EACCA_AUTH	EAC-CA authentication
SF.EAPCA_AUTH	EAP-CA authentication
SF.EACTA_AUTH	EAC-TA authentication
SF.EAPTA_AUTH	EAP-TA authentication
SF.SEC_MESSAGE	Secure messaging structure Secure communication channel mechanism
SF.ACTIVE_AUTH	AA authentication
SF.ACC_CONTROL	Personalization Agent access control Personalization Agent personalization and management Inspection System access control
SF.RELIABILITY	Residual Information management Vulnerability countermeasure TSF self test Data integrity
SF.IC	IC chip security function

7.2 SF.PAC_AUTH (PAC security mechanism)

This TSF includes a PAC security mechanism for the Personalization Agent for the Inspection

Copyright Ⓒ 2014 KOMSCO, All rights reserved

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

7.3 SF.BAC_AUTH (BAC security mechanism)

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

7.4 SF.SAC_AUTH (SAC security mechanism)

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

7.5 SF.BAP_AUTH (BAP security mechanism)

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

7.6 SF.EACCA_AUTH (EAC-CA security mechanism)

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

7.7 SF.EACTA_AUTH (EAC-TA security mechanism)

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

7.8 SF.EAPCA_AUTH (EAP-CA security mechanism)

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

7.9 SF.EAPTA_AUTH (EAP-TA security mechanism)

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

7.10 SF.SEC_MESSAGE (Secure Messaging)

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

7.11 SF.ACC_CONTROL (Access Control)

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

7.12 SF.ACTIVE_AUTH (AA security mechanism)

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

7.13 SF.RELIABILITY

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

7.14 SF.IC

This TSF provides the several security functionalities(security detector, MPU, RWG, Data scramble, TRNG, TDES, AES, RSA, ECC, SHA and etc) of the IC Chip.

[Works Cited]

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004 , Version 3.1, Revision 4, September 2012

[5] ICAO Doc 9303 Part 1, 2, 3

[6] ICAO MRTD TR Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, November 2010

[7] Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR-03110, October 2005

[8] BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, March 2012

[9] BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 3 - Common Specifications, Version 2.10, March 2012

[10] BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control, Version 1.11, February 2008

[11] ISO/IEC 18013 Information Technology - Personal identification - ISO-compliant driving Licence, Part 1: Physical characteristics and basic data set, October 2005

[12] ISO/IEC 18013 Information Technology - Personal identification - ISO-compliant driving Licence, Part 2: Machine-readable technologies, May 2008 / Cor.1:2011

[13] ISO/IEC 18013 Information Technology - Personal identification - ISO-compliant driving Licence, Part 3: Access control, authentication and integrity validation, March 2009 / Cor.1:2011, Amd.1:2012, Cor.2:2013

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

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

[16] Security IC Platform Protection Profile; registered and certified by BSI under the reference BSI-PP-0035-2007, Version 1.0, June 2007

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

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

[19] BSI Technical Guideline TR-03111 Elliptic Curve Cryptography Based on ISO 15946, TR-03111, April 2009

[20] Security Target Lite of Samsung S3FT9KF/S3FT9KT/S3FT9KS 16-Bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software Version 2.2, June 2013

[21] ePassport Protection Profile V2.1, KECS-PP-0163a-2009, June 2010

[22] KCOS e-Passport Version 3.0 S3FT9KS/KT/KF Security Target V1.3, January 6, 2014 (Confidential Version)

[Abbreviations]

AA	Active Authentication
AES	Advanced Encryption Standard
BAC	Basic Access Control
BAP	Basic Access Protection
BIS	BAC Inspection System
	BAP Inspection System
CA	Chip Authentication
CAN	Card Access Number
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CMAC	Cipher-based Message Authentication Code
COS	Card Operating System
CSCA	Country Signing Certification Authority
CSN	Chip Serial Number
CVCA	Country Verifying Certification Authority
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie-Hellman
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAP	Extended Access Protection
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FLASH	Flash memory semiconductor
EF	Elementary File
EIS	EAC Inspection System
	EAP Inspection System
IC	Integrated Circuit
ICAO	International Civil Aviation Organization

Copyright ⓒ 2014 KOMSCO, All rights reserved

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