

---

# **Samsung SDS SPass V2.0**

## **Security Target**

### **Public version**

---

Samsung SDS

---



**SAMSUNG SDS**

## REVISION STATUS

Revision	Date	Author	Description of Change
1.00	2010.07.02	JH Lee	ST final release
1.01	2010.12.10	JH Lee	S3CT9KC maintenance included

# Contents

<b>CONTENTS .....</b>	<b>3</b>
<b>LIST OF FIGURES .....</b>	<b>5</b>
<b>LIST OF TABLES .....</b>	<b>6</b>
<b>1 ST INTRODUCTION.....</b>	<b>8</b>
1.1 ST IDENTIFICATION.....	8
1.2 TOE IDENTIFICATION.....	8
1.3 TOE OVERVIEW .....	9
1.4 TOE DESCRIPTION.....	11
1.4.1 <i>Product Configuration</i> .....	11
1.4.2 <i>TOE Operational Environment</i> .....	11
1.4.3 <i>Security Functionality of the TOE Underlying Platform</i> .....	13
1.4.4 <i>Physical Scope of the TOE</i> .....	14
1.4.5 <i>Logical Scope of the TOE</i> .....	16
1.4.7 <i>TOE Lifecycle</i> .....	23
1.4.8 <i>TOE Operational Mode</i> .....	25
1.5 ST ORGANIZATION.....	26
<b>2 CONFORMANCE CLAIM.....</b>	<b>27</b>
2.1 COMMON CRITERIA CONFORMANCE.....	27
2.2 PROTECTION PROFILE CONFORMANCE.....	27
2.3 PACKAGE CONFORMANCE.....	27
2.4 CONFORMANCE CLAIM RATIONALE.....	27
2.4.1 <i>The Consistency of the TOE Type</i> .....	27
2.4.2 <i>The Consistency of the Security Problem Definition</i> .....	28
2.4.3 <i>Security Objectives Rationale</i> .....	29
2.4.4 <i>The Rationale for the Consistency of Security Function Requirements</i> .....	30
2.4.5 <i>The Consistency of the Security Assurance Requirements</i> .....	35
2.5 CONVENTIONS.....	36
<b>3 SECURITY PROBLEM DEFINITION.....</b>	<b>37</b>
3.1 THREATS .....	37
3.2 ORGANISATIONAL SECURITY POLICIES .....	40
3.3 ASSUMPTION .....	42
<b>4 SECURITY OBJECTIVES.....</b>	<b>44</b>
4.1 SECURITY OBJECTIVES FOR THE TOE .....	44
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT .....	46
4.3 SECURITY OBJECTIVES RATIONALE .....	48
4.3.1 <i>Security Objective Rationale for the TOE</i> .....	50
4.3.2 <i>Security Objective Rationale for Operating Environment</i> .....	54

<b>5</b>	<b>DEFINITION OF EXTENDED COMPONENT</b> .....	<b>58</b>
<b>6</b>	<b>SECURITY REQUIREMENTS</b> .....	<b>59</b>
6.1	TERMS AND DEFINITIONS .....	59
6.2	TOE SECURITY FUNCTIONAL REQUIREMENTS .....	60
6.2.1	<i>ePassport Security Functional Requirements</i> .....	60
6.2.2	<i>MULTOS Security Functional Requirements</i> .....	73
6.2.3	<i>TSF Common Security Functional Requirements</i> .....	78
6.3	TOE SECURITY ASSURANCE REQUIREMENTS .....	79
6.3.1	<i>Security Target</i> .....	80
6.3.2	<i>Development</i> .....	84
6.3.3	<i>Guidance Documents</i> .....	88
6.3.4	<i>Lifecycle Support</i> .....	89
6.3.5	<i>Testing</i> .....	92
6.3.6	<i>Vulnerability Analysis</i> .....	94
6.4	SECURITY REQUIREMENTS RATIONALE .....	95
6.4.1	<i>Security Functional Requirements Rationale</i> .....	95
6.4.2	<i>Security Assurance Rationale</i> .....	108
6.4.3	<i>Rationale of Dependency</i> .....	110
6.4.4	<i>Rationale of Mutual Support and Internal Consistency</i> .....	113
<b>7</b>	<b>TOE SUMMARY SPECIFICATION</b> .....	<b>115</b>
7.1	TOE SECURITY FUNCTION .....	115
7.2	ASSURANCE MEASURES .....	120
<b>8</b>	<b>REFERENCES</b> .....	<b>122</b>
<b>9</b>	<b>TERMS AND ABBREVIATION</b> .....	<b>123</b>
9.1	TERMS.....	123
9.2	ABBREVIATIONS.....	130

## List of Figures

Figure 1. TOE Overview .....	11
Figure 2. ePassport Appearance.....	11
Figure 3. TOE Operational Environment – MULTOS.....	12
Figure 4. TOE Operational Environment – ePassport.....	13
Figure 5. Physical Scope of the TOE .....	15
Figure 6. ePassport Lifecycle .....	24
Figure 7. TOE Operational Mode Relationship .....	25

## List of Tables

Table 1. TOE and TOE Component Identification.....	16
Table 2. The ePassport Security Mechanisms.....	17
Table 3. TOE Assets (MRTD) .....	19
Table 4. Contents of the LDS in which the User Data are Stored.....	22
Table 5. Types of ePassport Certificate .....	23
Table 6 Types of MULTOS Certificates.....	23
Table 7. Lifecycle of the MRTD Chip and the TOE .....	24
Table 8. TOE Operational Mode .....	25
Table 9. List of the Re-establishment of the Security Problem Definition .....	28
Table 10. List of Augmentation to the Security Problem Definition .....	29
Table 11. List of Re-establishment of the Security Objectives.....	29
Table 12. List of the Augmentation to the Security Objectives.....	30
Table 13. List of Re-establishment of the SFR .....	30
Table 14. List of the Additional SFR.....	33
Table 15. ePassport Access Control Policy .....	41
Table 16. The mapping between Security Problem Definition and Security Objectives .....	49
Table 17 Cryptographic Key Distribution Standard and Method .....	62
Table 18 Cryptographic Key Distribution Standard and Method .....	62
Table 19. Subject-relevant Security Attributes .....	63
Table 20. Object-relavant Security Attributes.....	63
Table 21. Authentication Failure Handling for Authentication Mechanism.....	67
Table 22. Open Platform OS Subject-relevant Security Attributes .....	74
Table 23. Open Platform OS Object-relevant Security Attributes .....	74
Table 24. Security Assurance Requirements .....	79
Table 25. Mappings between Security Objectives and Security Functional Requirements.....	96
Table 26. Dependency of TOE Functional Components.....	110
Table 27. Dependency of the Augmented Assurance Component .....	112
Table 28 Countermeasure against TOE Subsystem & SFRs .....	117
Table 29. TOE Assurance Measures .....	120
Table 1. TOE and TOE Component Identification.....	16
Table 2. The ePassport Security Mechanisms.....	17
Table 3. TOE Assets (MRTD) .....	19
Table 4. Contents of the LDS in which the User Data are Stored.....	22
Table 5. Types of ePassport Certificate .....	23

Table 6 Types of MULTOS Certificates.....	23
Table 7. Lifecycle of the MRTD Chip and the TOE .....	24
Table 8. TOE Operational Mode .....	25
Table 9. List of the Re-establishment of the Security Problem Definition .....	28
Table 10. List of Augmentation to the Security Problem Definition .....	29
Table 11. List of Re-establishment of the Security Objectives.....	29
Table 12. List of the Augmentation to the Security Objectives.....	30
Table 13. List of Re-establishment of the SFR .....	30
Table 14. List of the Additional SFR.....	33
Table 15. ePassport Access Control Policy .....	41
Table 16. The mapping between Security Problem Definition and Security Objectives .....	49
Table 17 Cryptographic Key Distribution Standard and Method .....	62
Table 18 Cryptographic Key Distribution Standard and Method .....	62
Table 19. Subject-relevant Security Attributes .....	63
Table 20. Object-relevant Security Attributes.....	63
Table 21. Authentication Failure Handling for Authentication Mechanism.....	67
Table 22. Open Platform OS Subject-relevant Security Attributes .....	74
Table 23. Open Platform OS Object-relevant Security Attributes .....	74
Table 24. Security Assurance Requirements.....	79
Table 25. Mappings between Security Objectives and Security Functional Requirements .....	96
Table 26. Dependency of TOE Functional Components.....	110
Table 27. Dependency of the Augmented Assurance Component.....	112
Table 28 Countermeasure against TOE Subsystem & SFRs .....	117
Table 29. TOE Assurance Measures .....	120

## 1 ST Introduction

This document is the Security Target (hereafter, 'ST') of SAMSUNG SDS SPass V2.0 which shall be embedded in SPass20 product and developed by SAMSUNG SDS.

This section identifies the ST and the TOE and provides summary of ST and the evaluation criteria that TOE conforms to.

### 1.1 ST Identification

- Title : SAMSUNG SDS SPass V2.0 Security Target (Public Version)
- Version : V1.01
- Release date : 10<sup>th</sup> of December, 2010
- Author : SAMSUNG SDS Co., Ltd.
- Evaluation criteria : Common Criteria for Information Technology Security Evaluation V3.1r3
- Evaluation assurance level : EAL5+ (ADV\_IMP.2, ALC\_DVS.2, AVA\_VAN.5)
- PP compliance : ePassport Protection Profile V2.1[1]
- PP certification number : KECS-PP-0163a-2009

### 1.2 TOE Identification

- Developer : SAMSUNG SDS Co., Ltd
- TOE name : SAMSUNG SDS SPass V2.0 (Revision 1)
- TOE element
  - SAMSUNG SDS SM30X and SPass LDS application
  - User guidance and preparative procedure (SP20-AGD-001\_v100, SP20-AGD-002\_v100)
  - Personalization guidance (SP20-AGD-004\_v100) and MULTOS public manual released by MAOSCO
- TOE version : 2.0
  - MULTOS product identification : SM30X R1 Revision 1
    - ROM code identification : T9KW\_SM30xR1\_r01.rom (SM30X R1 ROM Code Revision 1 implemented on S3CT9KW), T9KC\_SM30xR1\_r01.rom (SM30X R1 ROM Code Revision 1 implemented on S3CT9KC)
    - EEPROM code identification : T9KW\_SM30XR1\_r01.eep (SM30X R1 EEPROM Code Revision 1 implemented on S3CT9KW), T9KC\_SM30XR1\_r01.eep (SM30X R1 EEPROM Code Revision 1 implemented on S3CT9KC)
  - LDS application identification : SM30XR1\_LDSV20\_15.alu (LDS application V2.0 Revision 1.5 loaded onto SM30X R1)



### 1.3 TOE Overview

SAMSUNG SDS SPass20 product (hereafter, 'SP20') is an IC chip package for ePassport assuring high security and optimized performance, and is implemented by embedding TOE in SAMSUNG Electronics S3CT9KW<sup>1</sup> IC chip. S3CT9KW has separately achieved Common Criteria certification from BSI as follows.

- PP compliance : BSI-PP-0035-2007
- Certified TOE name : S3CT9KW 16-bit RISC Microcontroller for Smart Card, Revision 0, S3CT9KC 16-bit RISC Microcontroller for Smart Card, Revision 0
- Certification number : BSI-DSZ-CC-0639-2010, BSI-DSZ-CC-0639-2010-MA-01
- Certified cryptographic library version : Secure RSA/ECC Library v1.0, TRNG Library v1.0, DRNG Library v1.0
- Evaluation Assurance Level : EAL5+ (ALC\_DVS.2, AVA\_VAN.5)

SP20 consists of the TOE and its underlying hardware. The underlying hardware shall be located on the thin plastic film (Inlay) which is connected with the antenna for contactless communication after being packaged into COB (Chip On Board) module. The ePassport is composed of passport booklets including inlay and e-Cover and used for international travel after personalization of chip module as well as visual information page of legacy passport.

This ST is for "SAMSUNG SDS SPass V2.0 (hereafter, 'SPass') which is the TOE contained in SP20. The TOE is a combination of the open platform operating system which includes ePassport primitives, SAMSUNG SDS MULTOS SM30X R1 (hereafter, 'SM30X') which is implemented upon IC chip and the SPass LDS application V2.0 (hereafter, 'LDS Application') which is designed to be loaded on MULTOS.

- SM30X is composed of an IC chip operating system 'SM30X Core' which is implemented according to MULTOS V4.2.1[12] specification (hereafter, 'MULTOS specification') and 'ePassport primitives' which provides the security mechanisms of Machine Readable Travel Document. SM30X processes communication protocols using underlying hardware functionality according to ISO/IEC 7816 and ISO/IEC 14443 standard. SM30X provides multiple MULTOS application loading, executing and deleting functionality as it has an open platform structure. SM30X secures separate execution area for each MULTOS application and handles command and respond APDU (Application Protocol Data Unit) first and then forward it through MULTOS Application Abstract Machine (AAM) to relevant MULTOS application. ePassport primitives implements the security mechanisms of BAC and AA with BAC secure channel according to the specifications[7][8][9] of International Civil Aviation Organization (hereafter, 'ICAO specification') and EAC security mechanism with EAC secure channel specified in BSI TR-03110(hereafter, 'EAC specification').
- After being loaded onto EEPROM, LDS application provides basic information which is required to secure ePassport execution code and data area as well as functionality to call ePassport primitives of SM30X to activate ePassport functionality.

---

<sup>1</sup> Throughout this document, the underlying IC chip name 'S3CT9KW' is used on behalf of its family chip product such as S3CT9KW and S3CT9KC.

- SPass ePassport application (hereafter 'ePassport application') means the combination of ePassport primitives of SM30X masked in ROM and LDS application loaded onto EEPROM.

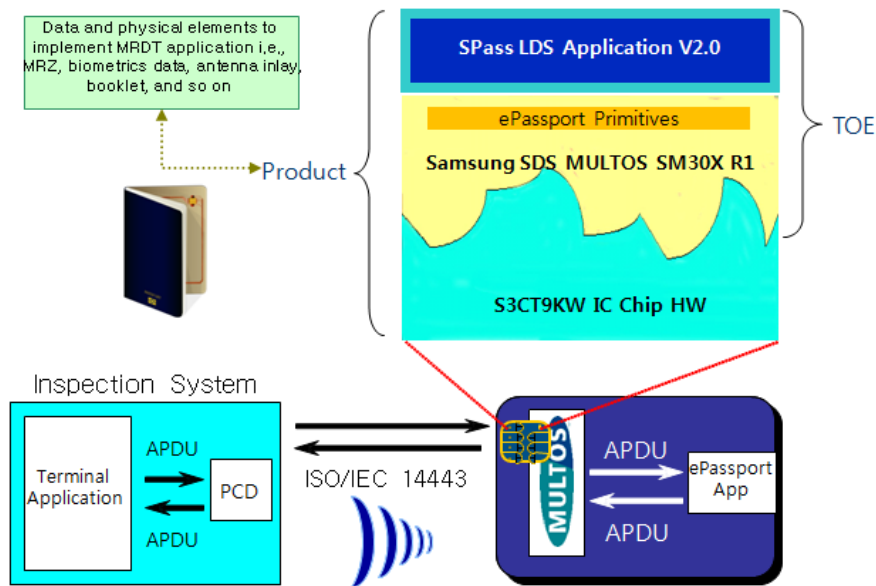


Figure 1. TOE Overview

## 1.4 TOE description

This section describes TOE operational environment, TOE physical scope, TOE logical scope and TOE assets to be protected. Also, TOE lifecycle and operational mode are identified.

### 1.4.1 Product Configuration

The TOE (SPass) includes SM30X, an IC chip operating software where ePassport primitives are included, and the LDS application on SM30X. TOE and the underlying hardware are packaged to compose SP20 product and applied to use as ePassport. As shown in Figure 2, SP20 chip package and associated antenna are embedded on the plastic film which is placed within a data page or the cover of the booklet. ePassport booklet presents identification data such as printed portrait of the MRTD holder and printed MRZ that is same as stored in the chip to the Inspection System so that the Inspection System can recognize. Fingerprints or iris biometric information can be stored in the chip as well depending on personalization agent's policy.



Figure 2. ePassport Appearance

### 1.4.2 TOE Operational Environment

Figure 3 shows TOE operational environment in the relationship with external entity (MCD Issuer) in terms of manufacturing, personalization, operational use including the security functionality of MCD enablement and LDS application loading/deleting.

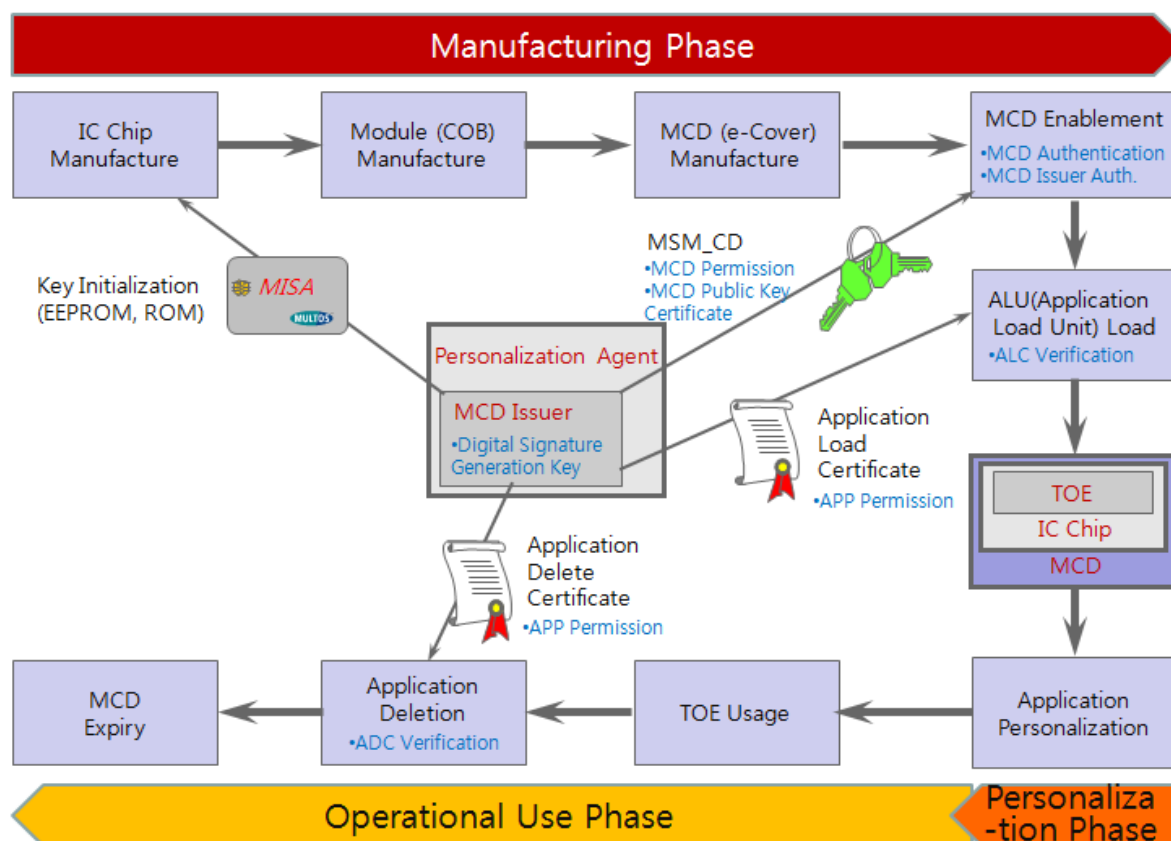


Figure 3. TOE Operational Environment – MULTOS

The MCD Issuer performs MISA operation with MULTOS KMA and IC chip manufacturer, where MISA operation is a step to inject credentials such as key information to be used in MCD authentication and the MCD Issuer authentication. Manufacturers mask TOE image to manufacture up to COB or e-Cover form factor and deliver to the MCD Issuer. TOE performs MCD authentication and the MCD Issuer authentication as per MCD Issuer's request to enable MCD and then performs MULTOS application loading or deleting later. The MCD Issuer loads LDS application in the Personalization phase.

Figure 4 shows the operational environment of the TOE in the phases of the ePassport Personalization and Operational Use through the relationship with major security functions of the TOE and external entities (the Personalization Agent, the Inspection System) that interact with TOE. Inspection System performs BAC mutual authentication, EAC-TA and so on according to the security mechanism procedure enforced by the TOE.

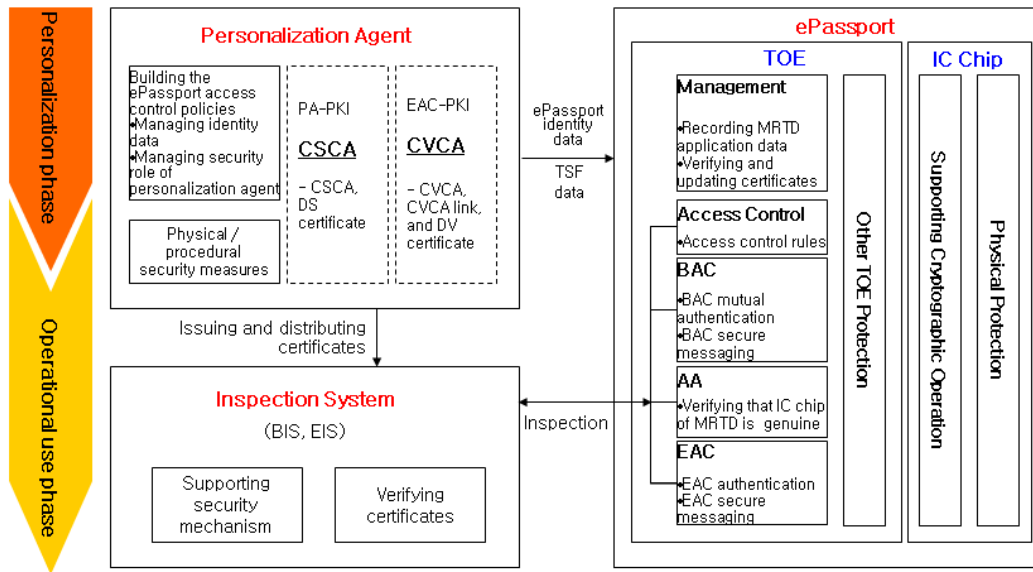


Figure 4. TOE Operational Environment – ePassport

### 1.4.3 Security Functionality of the TOE Underlying Platform

The underlying IC chip and its cryptographic library of the TOE provides security functions as follows.

- Symmetric key cryptographic operation  
The IC chip provides DES and TDES accelerator and relevant control register in order that the TOE can perform operations such as (1)112 bit TDES message encryption and decryption for BAC, (2)Retail MAC calculation based on 112 bit TDES for BAC and EAC, (3) MULTOS DES/TDES decryption of SM30X enablement data, and (4)MULTOS DES/TDES decryption of application load unit when being loaded onto SM30X in confidential mode.
- Asymmetric key cryptographic operation  
The IC chip provides crypto-processor (Tornado<sup>TM</sup>)<sup>2</sup> and relevant cryptographic library capable of 2048-bit modulus RSA and 512-bit ECC operations in order that the TOE can perform operations such as (1)key exchange and agreement based on DH or ECDH, (2)digital signature verification based on RSA or ECDSA for EAC-TA, (3)digital signature generation based on RSA for AA, (4)digital signature verification based on RSA for application load certificate during loading application onto SM30X, (5)digital signature verification based on RSA for application delete certificate during deleting application from SM30X, and (5)Asymmetric Hash operation based on RSA for verifying integrity of SP20 carrying SM30X and its loaded applications.
- One-way hash functions  
The IC chip's cryptographic library provides on-way hash functions of SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 in order that the TOE can perform operations such as (1)KDF

<sup>2</sup> Considering RAM space availability, TOE supports up to 1024-bit modulus in case of RSA.

calculation which derives symmetric key used to perform Secure Messaging of BAC/EAC, (2)digital signature generation and verification based on RSA/ECDSA.

- Random number generation

TRNG (TRNG Library v1.0) evaluated under AIS31 standard class P2 level and DRNG (DRNG Library v1.0) evaluated under AIS20 enables TOE to create unpredictable and irreproducible random number to be used in preventing replay attacks.

- Countermeasures against side channel attacks

The IC chip provides hardware-based countermeasures such as Random Current Generator, Random Wait-state Generator, Virtual DES/TDE against disclosing information from the changes of current, voltage, electro-magnetic or such kind of physical phenomenon during symmetric or asymmetric key cryptographic operations and also provides cryptographic library where countermeasures against DPA or SPA are implemented. Meanwhile, the IC chip provides Abnormal Condition Detector that shall reset the IC chip itself when detecting abnormal frequency, voltage, temperature, light, removal of insulating shield, and power glitch, as well as Data Bus Scrambling function that enables EEPROM and RAM data bus to be scrambled. The relevant control register for each function is provided in order for TOE to use with ease.

#### 1.4.4 Physical Scope of the TOE

ePassport consists of a booklet and an IC chip and antenna embedded in the coversheet. The IC chip comprises of IC chip component, IC chip operating system, MRTD Application and MRTD Application data. The IC chip contains CPU, crypto processor, I/O port, memory (RAM, ROM, EEPROM), random number generator, timer and contactless interface.

This ST defines the TOE as the chip operating system, SM30X, which shall be masked on the ROM and the LDS application which shall be loaded onto the EEPROM, where underlying IC chip is excluded.

The TOE is implemented in the IC chip which is Samsung Electronics' S3CT9KW that is CC EAL5+ certified. The IC chip contains CPU that performs commands including executable code. It also contains hardware like TDES accelerator and Tornado Coprocessor, etc., for implementing cryptographic functions. The IC chip provide Tornado cryptographic library to support RSA, DH, ECDSA and ECDH, that is in the scope of the CC evaluation of the IC chip.

IC chip operating system (COS), SM30X, includes SM30X Core which processes commands and file management according to ISO/IEC 7816-4, 8, 9, executes ePassport application and provides functions for management of ePassport application data. MULTOS, open platform operating system is applied in the ST. Run-time firmware libraries which are supplied by IC chip vendor like Samsung Electronics provide low-level routines to write data on EEPROM when loading and personalizing the LDS application. SM30X Core provides cryptographic functions controlling 2048-bit segments using run-time firmware library provided by the underlying IC chip.

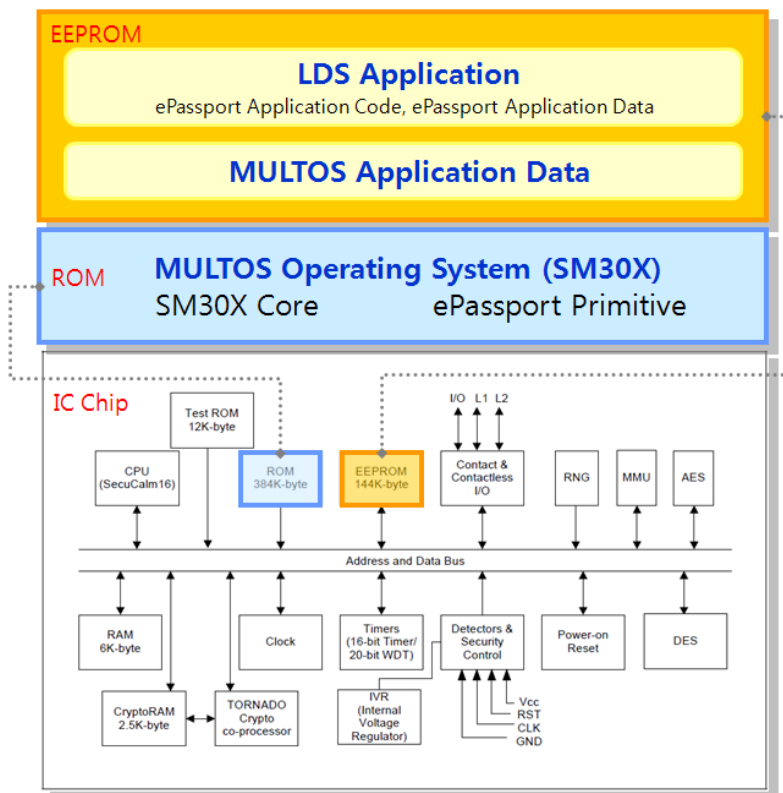


Figure 5. Physical Scope of the TOE

The ePassport primitives implement the functions in connection with the LDS application to store and to process MRTD identification data according to the ICAO LDS format and security mechanisms to protect those data in a secure manner. EAC security mechanism is also added according to EAC specification because the LDS application shall contain MRTD holder's sensitive biometric data. The LDS Application shall be loaded onto the EEPROM using secure mechanism provided by MULTOS. It contains data group and security object specified by ICAO and EAC specification and calls ePassport primitives' code implementing security protocols such as BAC, AA, EAC-CA and EAC-TA.

The ePassport application data, which consists of MRTD user data like MRTD identification information and MRTD TSF data required for security mechanism, and the MULTOS application data, which are required to operate SM30X Core, shall be stored into the EEPROM through secure method provided by MULTOS.

The TOE and TOE component are identified in the following Table 1.

Table 1. TOE and TOE Component Identification

Category (Form)	Name	Configuration Identification (including version/build number)	Explanation
TOE (Software)	Samsung SDS SPass V2.0	Samsung SDS SPass V2.0, Revision 1	Combination of SM30X and LDS application
TOE Component (Software)	SM30X	T9KW_SM30xR1_r01.rom T9KW_SM30xR1_r01.eep	MULTOS V4.21 compliant open platform IC chip operating system which provides ePassport primitives
	LDS Application	SM30xR1_LDS_v20_15.alu	MULTOS application which enables ePassport primitives
TOE Component (Document)	User Guidance	SP20-AGD-001_User Guidance V1.00	Operational guidance
	Preparative Procedures Guidance	SP20-AGD-002_Preparative Procedures V1.00	Preparative procedure guidance
	Personalization Guidance	SP20-AGD-003_Personalization Manual V1.00	Guidance to personalize including installation and start-up

#### 1.4.5 Logical Scope of the TOE

TOE consists of Hardware Abstraction Layer, Extended MULTOS Layer and Application Layer. TOE provides MULTOS relevant security features, ePassport relevant security features, and common security features.

Application Layer calls ePassport primitives and interpret ePassport commands received from the inspection system or personalization agent.

Extended MULTOS Layer implements MULTOS relevant security functionality such as MCD authentication and MCD Issuer authentication as well as provides the MULTOS access control functionality that the authorized MULTOS application can be loaded onto, executed in, or deleted later from the TOE with the MCD management functionality to manage the security attributes regarding these operations. This layer also provides ePassport relevant security functionality such as BAC, AA, EAC, secure messaging, residual information protection, and ePassport access control as well as the management functionality to manage these and the authentication mechanism for personalization agent. Common security features are provided by this layer such as providing integrity verification of execution code and data and supporting relevant security features for both MULTOS and ePassport using IC chip cryptographic functionality.

Hardware Abstraction Layer guarantees secure operation of the TOE using IC chip functionality and verifies randomness of the RNG at start-up. This layer implements contact and contactless communication protocol to receive APDUs from external entity and to respond after processing each APDU



by categorizing and assigning commands to the relevant subsystem for MULTOS access control, ePassport application, and other MULTOS applications.

The ePassport Security mechanisms of the TOE are summarized in Table 2.

Table 2. The ePassport Security Mechanisms

The ePassport Security Mechanisms				IT Security characteristic of the TOE
Security Mechanism	Security characteristic	Cryptography	Cryptographic Key/Certificate Type	
PA	User Data	N/A	N/A	Access control to the SOD - Read-rights: BIS, EIS -Write-rights: Personalization Agent
AA	IC chip genuineness Verification	Asymmetric Key Digital Signature RSASSA SHA	AA Private Key (used to generate digital signature) AA Public Key (used by BIS, EIS)	TOE generates a digital signature to card nonce and terminal nonce and Inspection System verifies it to ensure that the IC chip is genuine
BAC	BAC Mutual authentication	Symmetric key-based entity authentication protocol TDES-CBC SHA MAC	BAC Authentication Key (encryption key, MAC key)	The TOE verifies if the Inspection System has access-rights, by decryption and MAC operation for the transmitted value of the Inspection System. The TOE transmits the value to the Inspection System after encryption and MAC operation for authentication.
	BAC Key Distribution	Symmetric key-based key distribution protocol TDES-CBC SHA MAC	BAC Session Key (encryption key, MAC key)	Generating BAC session key by using KDF from the exchanged key-sharing random number on the basis of the TDES-based key distribution protocol
	BAC Secure messaging	Secure Messaging	BAC Session Key (encryption key, MAC key)	Transmitting messages by creating the MAC after encryption with the BAC session key Receiving messages by decryption it after verifying the MAC with the BAC session

The ePassport Security Mechanisms				IT Security characteristic of the TOE
Security Mechanism	Security characteristic	Cryptography	Cryptographic Key/Certificate Type	
				key
EAC	EAC-CA	DH key distribution protocol ECDH key distribution protocol	EAC Chip Authentication Public Key EAC Chip Authentication Private Key	The TOE executes the ephemeral- static DH key distribution protocol
	EAC Secure messaging	Secure messaging	EAC Session Key (cryptographic key, MAC key)	Secure messaging by using the EAC session key shared in the EAC-CA
	EAC-TA	RSASSA-PSS RSASSA-PKCS1-v1.5 ECDSA	CVCA certificate CVCA link certificate DV certificate IS certificate	Verifying the IS certificate by using the certificate chain and the link certificate Verifying the digital signature for transmitted messages of the EIS for the EIS authentication

#### 1.4.6 TOE Assets

The TOE provides information security functions such as confidentiality, integrity, authentication and access controls in order to protect TOE assets as follows:

##### 1. ePassport User Data

The following user data are stored in the EF of the IC chip where the TOE is implemented.

- Applicant's personal information : data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16
- Applicant's biometric information : data stored in EF.DG3 and EF.DG4
- ePassport authentication information : SOD, EAC-CA public key, and AA public key
- EF.CVCA : the identifier list of the CVCA digital signature verification key used to verify CVCA certificate for the TOE to authenticate the Inspection System during the EAC-TA
- EF.COM : version information of the LDS, tag list of DGs in use, etc.

##### 2. ePassport TSF Data

The following TSF data are stored in the secure memory of the IC chip where the TOE is implemented.

- EAC-CA private key : the chip private key used to prove that the IC chip of the ePassport is not forged during EAC-CA

- AA private key : the chip key used when the TOE generates a digital signature during AA
- CVCA certificate : the root CA certificate of EAC-PKI created during ePassport issuance
- CVCA digital signature verification key : the public key of CVCA certificate newly generated by certificate update after the ePassport issuance
- Current date : the current date is written as the issuance date of the ePassport at first but shall be internally updated in the latest issuance date among CVCA link certificate, DV certificate and IS certificate by the TOE at the Operational Use phase
- Personalization key : the authentication key in order for personalization agent to get authorization and the SM key to perform secure messaging during personalization.
- MRTD access condition: attributes assigned by personalization agent to allow up to BAC (AC\_BAC) or up to EAC (AC\_EAC) after ePassport personalization phase.

The following TSF data are stored in the volatile memory of the IC chip where the TOE is implemented.

- BAC session key : the encryption key and MAC key of the session for BAC mechanism
- EAC session key : the encryption key and MAC key of the session for EAC mechanism
- Personalization session key : the encryption key and MAC key of the session for personalization

Table 3. TOE Assets (MRTD)

Category		Description	Storage Space	
MRTD User Data	ePassport Identity Data	Personal Data of the ePassport holder	Data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13 and EF.DG16	
		Biometric Data of the ePassport holder	Data stored in EF.DG3 and EF.DG4	
	ePassport Authentication Data		SOD, EAC chip authentication public key, etc.	
	EF.CVCA		In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System	
	EF.COM		LDS version info., tag list of DG used, etc.	
MRTD	EAC Chip Authentication Private		In EAC-CA, Chip Private key used by the TOE to demonstrate Not forged	Secure

TSF Data	Key	MRTD chip	memory
	AA Private Key	In AA, AA Private Key used by the TOE to generate digital signature to show it's genuine	memory
	CVCA Certificate	In personalization phase, Root CA Certificate issued in EAC-PKI	
	CVCA Digital Signature Verification Key	After personalization phase, CVCA certificate Public key newly created by certificate update	
	Current Date	In personalization phase, Date of issuing the ePassport is recorded. However, In operational use phase, the TOE internally updates it as the latest date among issuing dates of CVCA link certificate, DV certificate or Issuing State IS certificate.	
	BAC Authentication Key	BAC authentication encryption key, BAC authentication MAC key	
	Personalization Key	Personalization authentication key, Personalization SM key	
	MRTD Access Condition	Attributes assigned by personalization agent to allow up to BAC or up to EAC after ePassport personalization phase	
	BAC Session Key	BAC session encryption key, BAC session MAC key	
	EAC Session Key	EAC session encryption key, EAC session MAC key	
	Personalization Session Key	Personalization session encryption key, Personalization session MAC key	

### 3. MULTOS User Data

Application Load Unit (ALU) is used to load MULTOS application after completing SPass initialization, which consists of code, data, and additional information of the application.

ALU is generated by the Application Provider and provided to the Application Loader. ALU is classified into Unprotected (Plaintext) ALU that has no additional security measure except ALC, Protected ALU that has additional digital signature by Application Provider to Unprotected ALU to prove integrity, and Confidential ALU that encrypts whole or partial area of the Protected ALU using temporary symmetric keys (DES/TDES) and encrypts those symmetric keys using MCD's unique asymmetric transport key (mkd\_pk) to attach as KTU (Key Transformation Unit) according to the transportation type. These 3 types of ALU can be selectively used according to the policy of the personalization agent.

#### 4. MULTOS TSF Data

MULTOS initialization data and the relevant certificates that is required to enable MCD and load/delete the LDS application and MULTOS applications to MCD are MULTOS TSF data.

- Even though kck\_pk and hm that are injected during manufacturing phase are not private keys, It is desirable to prevent kck\_pk and hm from disclosure outside for keeping security level high. They are injected into ROM by MULTOS KMA at the manufacturing place (ROM key integration procedure).
- There are Application Load Certificate (ALC) and Application Delete Certificate (ADC) to load/delete the LDS application ALU or MULTOS application ALU into/from MCD. ALC and ADC are generated by signing information including application ID and permission using kck\_sk, and MULTOS KMA generates them to provide to Application Loader.
- Security data injected to secure memory area through MISA (MULTOS Injection Security Application) operation<sup>3</sup> are as follows :
  - MCD\_ID : A unique identification number of each MCD
  - Enablement Data Transport Key (tkf, tkv) : The unique symmetric transport key per each MCD used at the time of enabling MCD
- Security data injected to secure memory area through MCD enablement procedure are as follows :
  - MSM Security Attributes(MCD permission) : The enablement date, The Personalization Agent ID, and the Personalization Agent's product ID used to check permissions at the time of loading or deleting an application.
  - MCD Private Key (mkd\_sk) : The unique asymmetric transport key per each MCD used to decrypt the KTU that contains encryption keys to decrypt Confidential ALU.

Because TOE is a product that a holder possesses and uses, it may be a target for attackers to steal. Thus, IC chip itself is an asset to be protected from physical threats.

Some information are not such asset that TOE protect directly, but are produced or used during the process of TOE manufacturing thus have a considerable relations toward the integrity and confidentiality of the TOE. This information is called additional assets and the security of additional assets shall be met by the assurance requirements of EAL5+.

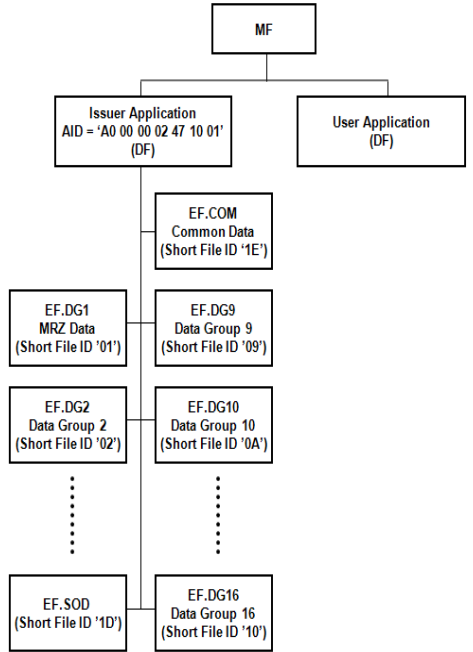
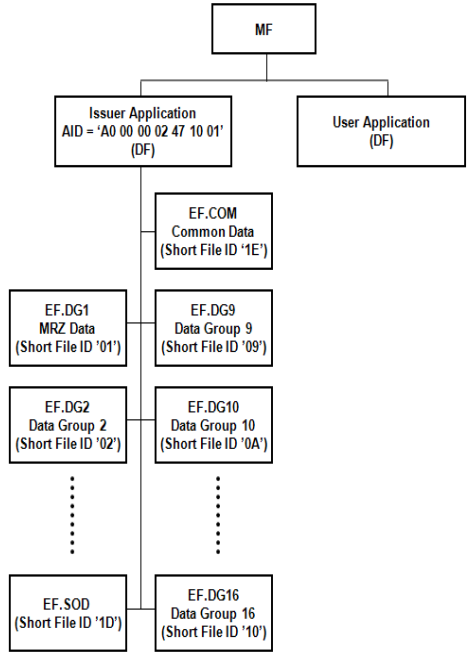
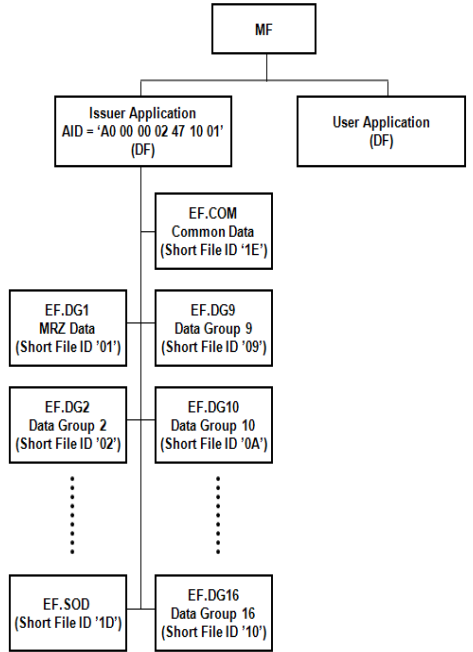
---

<sup>3</sup> MULTOS KMA stores seed value for keys and attributes in a smart card named MISA to pass to the manufacturer in order to assign unique key and attribute to each MCD. This is called MISA Operation.

<Contents of ePassport User Data >

There are MF, DF, and EF structure to be stored ePassport User Data of the TOE in LDS as Table 4.

Table 4. Contents of the LDS in which the User Data are Stored

Category	DG	Content	LDS Structure	
Detail(s) Recorded in MRZ	DG1	Document Type		
		Issuing State		
		Name (of Holder)		
		Document Number		
		Check Digit – Doc Number		
		Nationality		
		Date of Birth		
		Check Digit - DOB		
		Sex		
		Data of Expiry or Valid Until Date		
		Check Digit DOE/VUD		
		Composite Check Digit		
Encoded Identification Features	DG2	Encoded face		
	DG3	Encoded finger(s)		
	DG4	Encoded Eye(s)		
Others	DG5	Displayed Portrait		
	DG6	-		
	DG7	Displayed Signature		
	DG8	-		
	DG9	-		
	DG10	-		
	DG11	Additional Personal Detail(s)		
	DG12	Additional Document Detail(s)		
	DG13	-		
DG14	EAC Chip Authentication Public Key			

	DG15	AA Digital Signature Verification Key (optional)	
	DG16	Person(s) to Notify	

<Types of Certificates in ePassport System >

Types of certificates used in the ePassport system are as shown in Table 5.

Table 5. Types of ePassport Certificate

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

Additional certificates for MULTOS feature are as shown in Table 6.

Table 6 Types of MULTOS Certificates

Usage	Subject	Certificate
To verify load right of application	KMA	Application Load Certificate
To verify delete right of application	KMA	Application Delete Certificate

1.4.7 TOE Lifecycle

SPass ePassport lifecycle and related subjects are as shown in Figure 6.

The time of MCD enablement, application loading, pre-personalization can be conducted immediately after manufacturing inlay or cover sheet according to the policy of personalization agent during manufacturing phase.

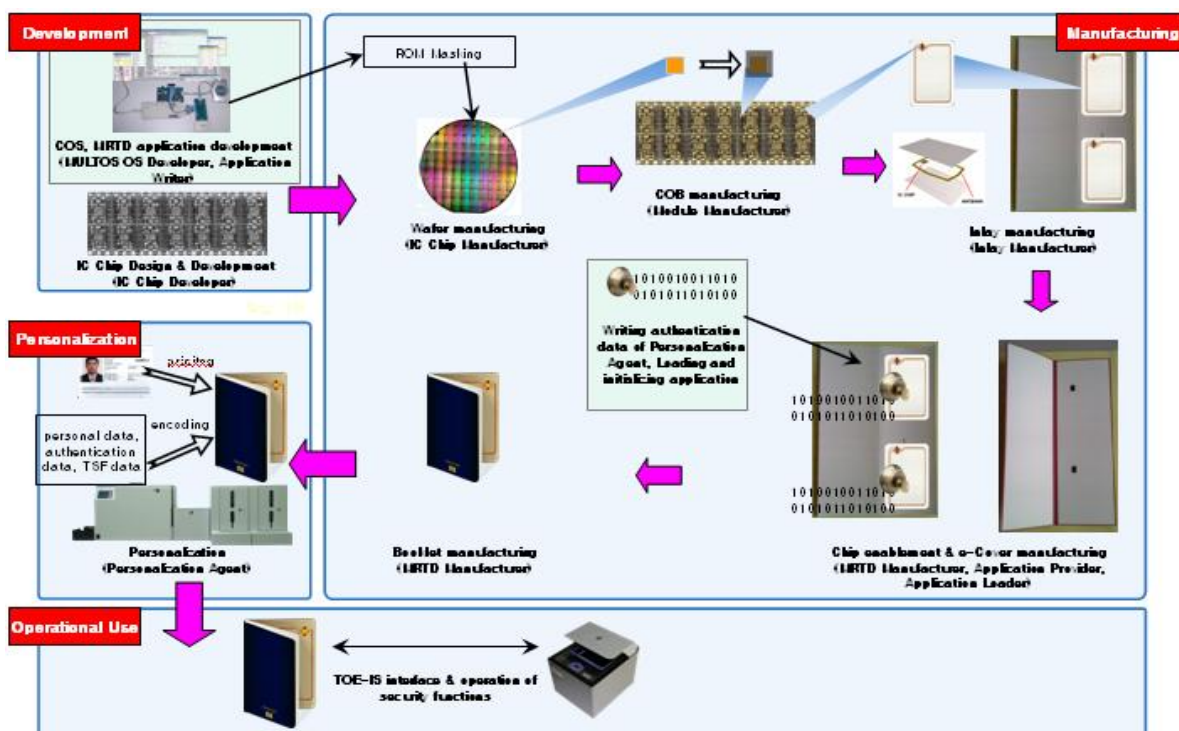


Figure 6. ePassport Lifecycle

Details of lifecycle for MRTD IC chip and the TOE are as shown Table 7. Lifecycle of the MRTD Chip and the TOE

Table 7. Lifecycle of the MRTD Chip and the TOE

Phase	Lifecycle of the MRTD Chip	Lifecycle of the TOE
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W	
Phase 2 (Manufacturing)		② COS developer to develop TOE (SM30X, LDS application) using IC chip and the dedicated software
	③-2. The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier, to produce the IC chip wafer and COB module, and to perform MISA operation after receiving MISA from KMA	③-1. COS developer and KMA to merge KMA public key and relevant information into ROM and to distribute TOE to IC chip manufacturer
		④-1. The e-Cover manufacturer to combine each module to antenna inlay and to make e-Cover



		<p>④-2. The ePassport manufacturer to enable MCD according to MULTOS security mechanism, and (as the role of the application loader) to load the LDS application supplied by the application provider onto EEPROM of MCD</p> <p>⑤ The ePassport manufacturer delegated from The Personalization Agent to write the authentication information of The Personalization Agent into EEPROM</p> <p>⑥ The ePassport manufacturer to embed the IC chip in the passport book</p>
Phase 3 (Personalization)		<p>⑦ The Personalization Agent to make room for personalization data in EEPROM and to create SOD by digital signature on ePassport identity data</p> <p>⑧ The Personalization Agent to record the ePassport identity data, the authentication data (including SOD) and the TSF data in the TOE</p>
Phase 4 (Operational Use)		<p>⑨ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE</p>

### 1.4.8 TOE Operational Mode

TOE can have the following operational mode with regard to the TOE lifecycle.

Table 8. TOE Operational Mode

Operational Mode Code	Operational Mode	Relevant TOE Lifecycle
0x00	PROTECTED	development, manufacturing
0x01	INITIALIZED	personalization
0x03	PERSONALIZED	operational use
0xFF	TERMINATED	disuse

TOE operational mode can be changed toward only one-way as shown in the following figure.

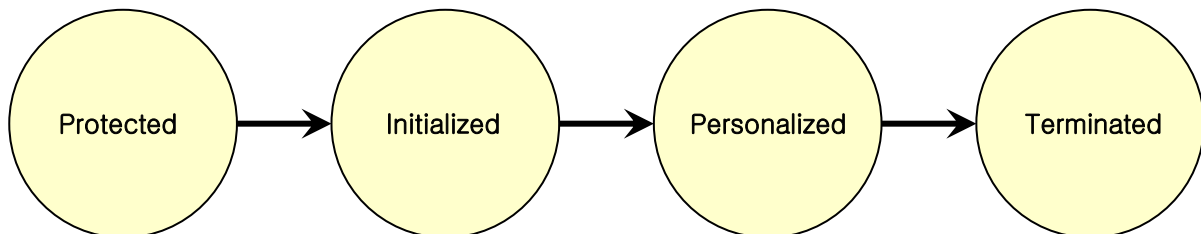


Figure 7. TOE Operational Mode Relationship

## 1.5 ST Organization

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

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

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

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

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

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

**Section 7** shows TOE summary specification explaining TOE security functionality and assurance measures.

**Section 8** defines the terms which is used in this ST.

**Section 9** contains the materials referenced in this ST.

**Terms and Abbreviations** provides terms and abbreviations frequently used.

## 2 Conformance Claim

Conformance claim describes how this ST conforms to the common criteria, the protection profile and the package.

### 2.1 Common Criteria Conformance

The common criteria which this ST conforms to is identified as follows.

- Common Criteria for Information Technology, Part 1: Introduction and general model, version 3.1r3, 2009.7, CCMB-2009-07-001
- Common Criteria for Information Technology, Part 2: Security functional components version 3.1r3, 2009.7, CCMB-2009-07-002
- Common Criteria for Information Technology, Part 3: Security assurance components, version 3.1r3, 2009.7, CCMB-2009-07-003

This ST conforms to the following parts of the CC.

- Common Criteria for Information Technology, Part 2
- Common Criteria for Information Technology, Part 3

### 2.2 Protection Profile Conformance

This ST conforms to the following PP.

- Title : ePassport Protection Profile
- Protection Profile Version : V2.1
- Certification Number : KECS-PP-0163a-2009
- Assurance Package : EAL4 augmented with(ADV\_IMP.2, ATE\_DPT.2, AVA\_VAN.4)
- Type of conformance : demonstrable conformance

### 2.3 Package Conformance

This ST conforms to the following package.

- Assurance package : EAL5 augmented with ADV\_IMP.2, ALC\_DVS.2, AVA\_VAN.5

### 2.4 Conformance Claim Rationale

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type, the security problem definition and the statement of security objectives and the statement of security requirement in the ePassport Protection Profile V2.1.

#### 2.4.1 The Consistency of the TOE Type

The type of TOE in the PP is the software including IC chip operating system (COS) and the application of machine readable travel documents (ePassport application) with the exception of hardware

elements of the chip of machine readable travel documents (MRTD chip). The ePassport application includes the ePassport security mechanisms such as BAC, EAC and the ePassport access controls.

The type of TOE in this ST is the software including an LDS application which executes the ePassport primitives and SM30X which implements open platform IC chip operating system and ePassport primitives. The combination of the ePassport primitive and the LDS application is the ePassport application that implements the ePassport security mechanisms such as BAC, EAC and ePassport access control as well as AA and The personalization agent authentication.

Therefore the type of TOE in this ST includes that in the PP and thus has consistency.

## 2.4.2 The Consistency of the Security Problem Definition

### < The Re-establishment of the Security Problem Definition >

The following table shows that the security problem definition of this ST is equivalent to that of the PP and maintains the consistency.

Table 9. List of the Re-establishment of the Security Problem Definition

PP	ST	Description of reestablishment	Rationale
Moderate-level threat agent	High-level threat agent	Higher level threat agent	Raise the level of the threat agent to make the TOE resistant to high-level attack potential uses logical method.
T.BAC_Authentication_Key_Disclose	T.BAC_Authentication_Key_Disclose	The BAC authentication key is generated by the personalization agent and is stored in the secure memory in the Personalization phase.	Selected the method that The Personalization Agent generates and stores the BAC authentication key out of the 2 methods proposed in the PP. Revised the application note according to this change.
T.Residual_Info	T.Residual_Info	"BAC_Authentication_Key" Removed	BAC Authentication Key is stored in the secure memory and is not stored in the temporary memory. Thus it is not a residual information.
P.Application_Install	P.Application_Install	Changed from personalization agent to the MCD Issuer. Augmented a policy that issuing a certificate to an application program provider.	Modified to add ePassport application install/remove functions according to the MCD issuing policy while conforming the MULTOS specification.
A.Inspection_System	A.Inspection_System	Added AA support	Modified to make the inspection system support AA because the TOE provides AA security mechanism. This is more restrictive thus it satisfies "demonstrable conformance".
A.IC_Chip	A.IC_Chip	Raise the level of the	The TOE is executed on the CC EAL5+

		IC chip from EAL4+ to EAL5+	certified IC chip. This is higher level and is more restrictive than the application note in the PP thus satisfies "demonstrable conformance".
A.MRZ_Entropy	A.MRZ_entropy	Raised from 56-bit to 80-bit.	Raised the MRZ entropy because the level of threat agent is changed to "high".

### < The Augmentation to the Security Problem Definition >

The following table proves that the security problem definition in this ST is more restrictive than that of the PP which is claimed to be conformed and thus it is consistent.

Table 10. List of Augmentation to the Security Problem Definition

Augmentation	Rationale
T.IC_Chip_Forgery	Adding a threat of IC chip forgery attack augments security object thus enhances the security attributes and restricts the security problem definition in the PP.
T.MCD_Forgery	Augmenting threat to MULTOS augments security object thus enhances the security attributes and restricts the security problem definition in the PP.
T.Malware	Augmenting threat to MULTOS augments security object thus enhances the security attributes and restricts the security problem definition in the PP.
T.Application_Compromise	Augmenting threat to MULTOS augments security object thus enhances the security attributes and restricts the security problem definition in the PP.
P.The_Issuing_Policy_of_the_ePassport	Additional OSPs for applying the ePassport personalization policy such as disabling EAC and secure communication channel do not weaken the security attributes in the PP thus the security problem is equivalent.

## 2.4.3 Security Objectives Rationale

### < The Re-establishment of the Security Objectives >

The following table shows the security objectives in this ST is equivalent to those in the PP thus is consistent.

Table 11. List of Re-establishment of the Security Objectives

PP security objectives	ST security objectives	Reestablishment	Rationale
O.Session_Termination	O.Session_Management	Maintain EAC communication channel instead of session termination even if the EAC-TA fails Change the name.	EAC specification mandates maintaining the EAC secure messaging channel generated by successful EAC-CA to protect the transmission data even if the EAC-TA fails.
O.Secure_Messaging	O.Secure_Messaging	Added secure messaging in the personalization phase.	Adding a purpose in order to add a function for the policy to protect the transmission data to enhance security in the

PP security objectives	ST security objectives	Reestablishment	Rationale
			personalization phase.
O.Replay_Prevention	O.Replay_Prevention	Modified the application note, additional authentication data which requires a random number.	The coverage of authentication data which requires replay prevention is widened for AA and personalization authentication are added.
O.Handling_Info_Leakage	OE.Handling_Info_Leakage	Change to security objectives for the environment	Change the TOE security attribute to be a security attribute of the operational environment because IC chip provides this attributes. General rules do not admit but ePassport PP admits by application notes.
OE.Application_Install	OE.Application_Install	Changed to issuing a PKI-based certificate to a MULTOS application provider.	According to the MCD issuing policy, the certificate is issued in secure manner and conforming the MULTOS specification.

#### < The Augmentation to the Security Objectives >

The following table proves that the security objectives in this ST are more restrictive than those in the PP and are consistent.

Table 12. List of the Augmentation to the Security Objectives

Augmentation	Rationale
O.MCD_Issuer_authentication O.MCD_management O.MCD_access_control	The TOE includes an open platform IC chip OS(SM30X Core) which implements the MULTOS specification, thus conforms the security attributes of the PP more restrictively by augmenting the security objectives with the objectives corresponding to the security functions such as MCD enablement, Access control of installing/removing/executing MULTOS applications, and Authentication of MCD issuing management which the SM30X Core shall provide
O.Personalization_agent_authentication	It conforms the security objectives of the PP more restrictively by additional security objective corresponding to the providing a method for authenticating ePassport personalization agent.
O.AA	Augmenting the security attribute of the TOE for verification of genuineness enhances the security properties of the PP and thus conforms more restrictively.

## 2.4.4 The Rationale for the Consistency of Security Function Requirements

#### < The Re-establishment of the SFR >

The following table shows that the SFR in this ST is equivalent to the SFR in the PP and thus maintains its consistency.

Table 13. List of Re-establishment of the SFR

SFR	Operation performed in this ST	Description on re-establishment

SFR		Operation performed in this ST	Description on re-establishment
FCS_CKM.1	-	Iteration	Change to FCS_CKM.1(1)
	FCS_CKM.1.1	Refinement	The TSF generates the key in place of the personalization agent.
FCS_CKM.2(1)	FCS_CKM.2.1	Selection, selection	Applied operations to meet the security objectives.
FCS_CKM.2(2)	FCS_CKM.2.1	Selection, selection, refinement	Refinement on the application notes.
FCS_CKM.4	FCS_CKM.4.1	Assignment, assignment	Applied operations to meet the security objectives.
FCS_COP.1(1)	FCS_COP.1.1	-	Deleted
FCS_COP.1(2)	FCS_COP.1.1	-	Deleted
FCS_COP.1(3)	FCS_COP.1.1	-	Deleted
FCS_COP.1(4)	FCS_COP.1.1	-	Deleted
FDP_ACC.1	-	Iteration	Change the name to FDP_ACC.1(1)
	FDP_ACC.1.1	Refinement, assignment, assignment, assignment	Refined to ePassport personalization agent
FDP_ACF.1	-	Iteration	Change the name to FDP_ACF.1(1)
	FDP_ACF.1.1	Assignment, refinement	Refined to ePassport personalization agent
	FDP_ACF.1.2	Assignment	Applied operations to meet the security objectives.
	FDP_ACF.1.3	Assignment	Applied operations to meet the security objectives.
	FDP_ACF.1.4	Assignment	Applied operations to meet the security objectives.
FDP_RIP.1	FDP_RIP.1.1	Deletion, assignment, selection	Deleted the BAC authentication key from the list of objects
FDP_UCT.1	FDP_UCT.1.1	Refinement	Refinement on the application notes.
FDP_UIT.1	FDP_UIT.1.1	Selection	Applied operations to meet the security objectives.
	FDP_UIT.1.2	Selection, refinement	Refinement on the application notes.
FIA_AFL.1		Iteration	Change the name to FIA_AFL.1(1)
	FIA_AFL.1.1	Assignment, selection, Assignment	Applied operations to meet the security objectives.
	FIA_AFL.1.2	Selection, refinement	Refinement on the method of handling the failure of authentication
FIA_UAU.1(1)	FIA_UAU.1.1	Refinement, iteration	Refined the point of time and the object of the security function execution
	FIA_UAU.1.2	Refinement	Refined the user
FIA_UAU.1(2)	FIA_UAU.1.1	Refinement, assignment	Refined the point of time and the object of the security function execution

SFR		Operation performed in this ST	Description on re-establishment
	FIA_UAU.1.2	Refinement	Refined the user
<b>FIA_UAU.4</b>	FIA_UAU.4.1	Assignment	Applied operations to meet the security objectives.
<b>FIA_UAU.5</b>	FIA_UAU.5.1	Assignment	Applied operations to meet the security objectives.
	FIA_UAU.5.2	Refinement, assignment	Refined including AA security mechanism
<b>FIA_UID.1</b>	-	Iteration	Changed the name to FIA_UID.1(1)
	FIA_UID.1.2	Refinement	Refined application notes.
<b>FMT_MOF.1</b>	-	Iteration	Changed the name to FMT_MOF.1(1)
	FMT_MOF.1.1	Refinement	Refined to ePassport personalization agent
<b>FMT_MSA.1</b>	-	Iteration	Changed the name to FMT_MSA.1(1)
<b>FMT_MSA.3</b>	-	Iteration	Changed the name to FMT_MSA.3(1)
	FMT_MSA.3.2	Refinement	Refined so that the TSF be in place of the personalization agent. Refined application note.
<b>FMT_MTD.1(1)</b>	FMT_MTD.1.1	Assignment, refinement	Change the identification information of the iteration component to "the certificate verification information and the authentication key" Refined The Personalization Agent to ePassport personalization agent. Added an application note.
<b>FMT_MTD.3</b>	FMT-MTD.3.1	Assignment, refinement	Refined to high-level attack potential
<b>FMT_SMF.1</b>	-	Iteration	Change the name to FMT_SMF.1(1)
	FMT_SMF.1.1	Refinement, assignment	Refined security management function in the ePassport operation phase.
<b>FMT_SMR.1</b>	-	Iteration	Changed the name to FMT_SMR.1(1)
	FMT_SMR.1.1	Refinement, assignment	Refined The Personalization Agent to the ePassport personalization agent
<b>FPR_UNO.1</b>	FPR_UNO.1.1	-	Deleted
<b>FPT_FLS.1</b>	FPT_FLS.1.1	Assignment	Applied operations to meet the security objectives.
<b>FPT_ITI.1</b>	FPT_ITI.1.2	Assignment, refinement	Refined application note.
<b>FPT_TST.1</b>	FPT_TST.1.1	Selection, selection	Applied operations to meet the security objectives.
	FPT_TST.1.2	Refinement, selection, assignment	Refined the user to the personalization agent
	FPT_TST.1.3	Refinement, selection	Refined the user to the personalization agent



The PP allows the operational environment(crypto. co-processor or library on the certified IC chip) to support security functions because it enhances the security if the TOE utilize the security function provided by the underlying IC chip instead of the function which the TOE provides by itself. FCS\_COP.1(1), FCS\_COP.1(2), FCS\_COP.1(3), FCS\_COP.1(4) are removed according to this. Besides, because providing the method that handling the leakage of information by IC chip in place of the TOE itself is more secure, the TOE is implemented in that manner and FPR\_UNO.1 is deleted.

The Personalization Agent is refined into the MCD Issuer and the ePassport personalization agent to distinguish the subject issues the MCD and the subject installs the LCD application program and issues ePassport because the TOE includes a open platform OS complying the MULTOS specification and the two personalization agents shall be distinguishable. So FDP\_ACC.1(1), FDP\_ACF.1(1),FMT\_MOF.1(1), FMT\_MTD.1(1), FMT\_SMR.1(1) are refined.

FCS\_CKM.1(1), FDP\_RIP.1, FMT\_MSA.3(1) are restrictively refined since the TOE does not store the BAC authentication key during the BAC mutual authentication procedure but the key is generated by TSF in place of the ePassport personalization agent after storing DG1 file in personalization phase and is stored in the secure memory placed in the EEPROM.

The application notes on FDP\_UCT.1 and FDP\_UIT.1 are refined to reflect the function that enables the selection of the Secure Messaging while the ePassport personalization agent transmits/receives the ePassport user data.

FIA\_AFL.1(1) is changed because the EAC specification mandates maintaining the secure messaging channel instead of terminating the session to protect the transmitted data when the EAC-TA fails. At this point, the equivalent level of security to that of terminating the session is assured since the security of transmitted data is maintained and the access to DG3/DG4 is denied.

FDP\_ACF.1(1), FIA\_UAU.1(1), FIA\_UAU.1(2) are refined to reflect the distinguishable characteristics of the implementation of the TOE according to the modes of operation. FIA\_UAU.5 is restrictively refined to reflect the characteristic of the TOE that supports AA security mechanism to enhance security.

The security management functions of the ePassport's operational use phase in FMT\_SMF.1(1) and the application notes on FCS\_CKM.2(2), FIA\_UID.1, FPT\_ITI.1 are refined to reflect the implementational characteristic of the TOE.

< **The Augmentation to the Security Functional Requirement** >

The following table shows that the SFR in this ST is more restrictive and is consistent with the SFR in the PP by accepting them with additional SFR.

Table 14. List of the Additional SFR

Additional SFR	Rationale
FCS_CKM.1(2)	Added to generate the key used for the authentication mechanism because the ePassport personalization agent authentication mechanism is added.
FDP_ACC.1(2)	This SFR is added to satisfy the MULTOS specification that requires establishing the MULTOS application access control policy.

Additional SFR	Rationale
FDP_ACF.1(2)	This SFR is added to satisfy the MULTOS specification that requires establishing the MULTOS application access control policy.
FDP_DAU.1(1)	This SFR is added since the AA security mechanism is added to the security objective. The ePassport personalization agent provides the function to detect the forged IC chip thus the SFR in this ST accepts the PP restrictively
FDP_DAU.1(2)	This SFR is added to satisfy the MULTOS specification that requires the MCD to demonstrate the validity of the MCD.
FDP_ETC.2	This SFR is added because the TOE shall provide the security attributes so that it can verify whether the MCD is able to install the application program according to the MULTOS specification
FIA_AFL.1(2)	This SFR is for providing an action which shall be performed when the additional ePassport personalization agent authentication failure. This change makes this ST to accept the PP restrictively because the action for the failure of ePassport personalization authentication is enhanced.
FIA_AFL.1(3)	The MCD shall be permanently disabled when the MCD personalization management authentication fails according to the MULTOS specification.
FIA_UAU.1(3)	This SFR is added for the requirement of the measure to authenticate a user as the ePassport personalization agent to connect and maintain the security role of the ePassport personalization agent to user and grant the subject right to the user. This adds a ePassport personalization agent authentication function and accepts the PP restrictively.
FIA_UAU.1(4)	The MULTOS specification requires the MCD to authenticate the MCD personalization management agent when the MCD authentication succeeds.
FIA_UID.1(2)	This is added in order to support multiple communication protocol because the communication protocol is not restricted when indentifying the MCD issuer.
FMT_MOF.1(2)	EAC is unnecessary and disabled when DG3/DG4 are not available according to the policy of the personalization agent. The level of security is equivalent to that of the PP since disabling the EAC is only applicable when DG3/DG4 are not available and the access to DG3/DG4 are explicitly denied when the EAC is disabled so the ePassport access control policy is conformed. The PP does not require the secure messaging in personalization phase, but this ST added this SFR in order to provide the secure messaging and disable it if the personalization environment is secure and does not require the secure messaging.
FMT_MSA.1(2)	This SFR is added because the MULTOS specification requires a function that sets the subject security attributes of the MULTOS access control policy.
FMT_MSA.1(3)	This SFR is added in order to provide the functions that verify the authorised application certificates according to the MULTOS specification.
FMT_MSA.2	To comply the MULTOS specification, the security attributes of the object can be set if and only if the verification of ALC, ADC is successful and the values of the security attributes in the ALC, ADC. This SFR is added to meet this requirement.
FMT_MSA.3(2)	To comply the MULTOS specification, only restricted values of the security attributes are applicable to the security attributes of the object. This SFR is added to meet this requirement.

Additional SFR	Rationale
FMT_MTD.1(3)	<p>This SFR is added since the TOE distinguishes the personalization phase and the operational use phase to manage the ePassport more securely and defines modes of operation and provides management functions in order to implement the command access control according to the phases.</p> <p>This enhances the security and thus accepts the PP restrictively.</p>
FMT_MTD.1(4)	<p>This SFR is added since the TOE is selected as a subject generates the BAC authentication key among the two options in the PP and the TSF generates and stores the BAC authentication key automatically after the DG1 is written successfully.</p>
FMT_SMF.1(2)	<p>This SFR is added for the security attribute management functions manages the MULTOS access control functions added.</p>
FMT_SMR.1(2)	<p>This SFR is added for the requirement of the user whose role is the MULTOS access control security attributes management.</p>
FPT_ITC.1	<p>This SFR is added to provide optional function that enhances the security of transmitted data in the personalization phase to reflect the policy of the personalization agent.</p>

### 2.4.5 The Consistency of the Security Assurance Requirements

This ST specifies CC EAL5 augmented with (ADV-IMP.2, ALC\_DVS.2, AVA\_VAN.5) to assure the secure operation of the TOE that implements the security management system of the MULTOS and counter the high-level threat agent. This assurance package maintains “demonstrable conformance” of the security assurance requirements of the PP since this is a superset includes the assurance package of the PP - EAL 4 augmented with(ADV\_IMP.2, AVA\_VAN.4) – and ALC\_DVS.2 and AVA\_VAN.5 in this assurance package provides higher level of assurance than ALC\_DVS.1 and AVA\_VAN.4 in the EAL5 assurance package.

#### < Additional Security Assurance Requirements >

The PP augments the following security assurance requirements (SAR) to the EAL4 assurance package.

- ADV\_IMP.2 : Complete mapping of the implementation representation of the TSF
- AVA\_VAN.4 : Methodical vulnerability analysis

This ST augments to EAL5 augmented with ALC\_DVS.2, AVA\_VAN.5 SARs to that of the PP. This augmentation is in accordance with the CC. The following is the list of augmented SARs.

- ADV\_FSP.5 : Complete semi-formal functional specification with additional error information
- ADV\_INT.2 : Well-structured internals
- ADV\_TDS.4 : Semiformal modular design
- ALC\_CMS.5 : Development tools CM coverage
- ALC\_DVS.2 : Sufficiency of security measures
- ALC\_TAT.2 : Compliance with implementation standards
- ATE\_DPT.3 : Testing: modular design
- AVA\_VAN.5 : Advanced methodical vulnerability analysis

## 2.5 Conventions

The notation, formatting and conventions used in this ST 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 ST.

### Iteration

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

### Selection

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

### Refinement

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

### Assignment

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

“Application Notes” are provided to help to clarify the intent of a requirement, identify implementation choices or to define "Pass/Fail" criteria for a requirement. Application Notes will follow relevant requirements where appropriate.

### 3 Security Problem Definition

The security problem definition shall describe the threats, OSPs and the assumptions about the operational environment of the TOE.

#### 3.1 Threats

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

In this ST, the IC chip provides functions of physical protection in order to protect the TOE according to the A.IC\_Chip. Therefore, the physical threat of the IC chip itself by the high-level threat agent is not considered. But the high possibility of the high-level attacks using logical methods cannot be ignored. Therefore it has the high possibility that the threat agent has high-level expertise, resources, motivation and the possibility of exploiting the vulnerability which the attackers can use.

#### < MULTOS related Threats >

##### T. MCD Forgery

A threat agent may intercept the TSF data which is required to issue an MCD by providing the MCD issuing agent with the forged MCD.

##### T. Malware

A threat agent may load or remove malicious application on an MCD to disclose or destruct the information stored in the TOE.

##### T. Application\_Compromise

A threat agent may load or execute an disguised application which of the code and data were modified from the intercepted normal application that is supposed to be load into an MCD through internet.

#### < Threats to the TOE in the Personalization Phase >

##### T. TSF\_Data\_Modification

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

#### < Threats to the TOE in the Personalization Phase >

##### T. TSF\_Data\_Modification

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

### < BAC-relevant Threats to the TOE in the Operational Use Phase >

#### **T. Eavesdropping**

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

#### **T. Forgery\_Corruption\_Personal\_Data**

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

#### **T. BAC\_Authentication\_Key\_Disclose**

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

Application Notes : The BAC authentication key may be generated by Personalization Agent in the Personalization phase or by the TOE in the Operational Use phase. The TOE uses the former method. Therefore the TOE considers the threat of disclose of the BAC authentication key stored in secure memory of the MRTD chip. The BAC authentication key is removed from the T.Residual\_Info because it shall never be stored in the temporary memory.

#### **T. BAC\_ReplayAttack**

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

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

### < EAC-related Threats in the Operational Use Phase >

#### **T. Damage\_to\_Biometric\_Data**

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

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

### **T. EAC-CA\_Bypass**

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

### **T. IS\_Certificate\_Forgery**

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

## **< BAC and EAC-related Threats in the Operational Use Phase >**

### **T. SessionData\_Reuse**

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

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

### **T. Skimming**

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

## **< Threats related to IC Chip Support >**

### **T. Malfunction**

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

## **< Other Threats in the Operational Use Phase >**

### **T. Leakage\_CryptographicKey\_Info**

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

#### **T. ePassport\_Reproduction**

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

#### **T. Residual\_Info**

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

#### **T. IC\_Chip\_Forgery**

The threat agent may make an forged MRTD by obtaining the MRTD's personal information including the SOD and loading them on a new IC chip.

### **3.2 Organisational Security Policies**

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

#### **P. International\_Compatibility**

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

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

#### **P. Security\_Mechanism\_Application\_Procedures**

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

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

#### **P. Personalization\_Agent**

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



**P. The Issuing Policy of the ePassport**

The TOE shall deactivate the EAC if the Personalization\_agent does not store the biometric data into the ePassport.

The TOE shall provide the way to deactivate the secure communication channel if it is not required because the issuing environment is insulated from the outside so that the security of transmission data is assured.

**P. ePassport\_Access\_Control**

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

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

Table 15. ePassport Access Control Policy

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

**P. PKI**

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

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

#### **P. Range\_RF\_Communication**

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

#### **P. Application\_Install**

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

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

#### **P. Application Authentication**

The TOE shall install/execute/remove an applications if and only if the application satisfies the security properties those set by the MCD Issuer and is provided by the application provider who have the certificate issued by the MCD Issuer .

### **3.3 Assumption**

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

#### **A. Certificate\_Verification**

The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically.

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

#### **A. Inspection\_System**

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

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

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

As the BIS supports the BAC and PA security mechanisms, it obtains the read-rights for the personal and authentication data of the ePassport holder if the BAC mutual authentication using the BAC au-

thentication key succeeds. Then, by establishing the BAC secure messaging with the BAC session key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the BAC. Then, by calculating and comparing a hash value for the personal and authentication data of the ePassport holder, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder. If the BIS supports the AA security mechanism as an option, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder explicitly by performing the AA and verifying the digital signature which is generated by the TOE.

As the EIS supports the BAC, EAC and PA security mechanisms, it obtains the read-rights for the personal, authentication and biometric data of the ePassport holder. The EIS, when the BAC mutual authentication and secure messaging succeed, executes the EAC-CA by using the EAC chip authentication public key read in the BAC to verify the genuine TOE. Then, it executes the PA in order to verify the EAC chip authentication public key. When the EAC-CA is succeeded, the BAC secure messaging is ended and the EAC secure messaging with the EAC session key is started, and the EAC-TA that the TOE authenticates the Inspection System is executed. When the EAC-TA is succeeded, the EIS obtains the read-rights for the biometric data of the ePassport holder. Therefore, the EIS is provided the biometric data of the ePassport holder from the TOE. If the EIS supports the AA security mechanism as an option, it verifies the forgery and corruption for the personal and authentication data of the ePassport holder explicitly by performing the AA and verifying the digital signature which is generated by the TOE after performing the EAC-CA and the PA.

#### **A. 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 the TOE's malfunction outside the normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using the probing and reverse engineering analysis.

Application Notes : To ensure the secure TOE environment, the IC chip shall be a certified product of CCRA EAL5+(SOF-high) or higher level. The cryptographic operation supported by the IC chip may be provided in the co-processor of the IC chip or cryptographic libraries loaded in the IC chip.

#### **A. MRZ\_Entropy**

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

Application Notes : In order to be resistant to the high-level threat agent, the entropy for the passport number, date of birth, data of expiry or valid until date and check digit used as BAC authentication key seed among the MRZ in the current technological level shall be at least 80bit.

## 4 Security Objectives

This Security Target defines security objectives by categorizing them into the TOE and the environment. The security objectives for the TOE are directly handled by the TOE. The security objectives for the environment are handled by technical/process-relevant means supported from IT environment in order to provide TOE security functionality accurately.

### 4.1 Security Objectives for the TOE

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

#### < ePassport-relevant Security Objectives >

##### **O. Management**

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

Application Notes : In the Personalization phase, the Personalization Agent deactivates the writing function after recording the MRTD application data.

##### **O. Personalization\_Agent\_Authentication**

The TOE shall provide the authentication means, which have the equivalent level to BAC, to connect only the authorized Personalization Agent to issuing management role and subject security attributes. However, it shall provide stronger level of countermeasure than BAC's.

##### **O. Security\_Mechanism\_Application\_Procedures**

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

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

##### **O. Session\_Management**

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

##### **O. Secure\_Messaging**

The TOE shall ensure confidentiality and integrity to protect the transmitted user and TSF data. Also, the TOE shall be able to handle that The Personalization Agent requests the secure messaging in Personalization phase.

### **O.Certificate\_Verification**

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

### **O.Deleting\_Residual\_Info**

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

### **O.Replay\_Prevention**

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

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

### **O.Access\_Control**

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

Application Notes : Only the authorized Personalization Agent in Personalization phase can update the Personalization key and can record the ePassport application data. Also, access control policies for the read-rights according to the type of the Inspection System shall be built in Operational Use phase.

### **O.BAC**

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

### **O.EAC**

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

#### **O.AA**

The TOE shall be able to verify its own genuineness for the Inspection System to detect the forgery of MRTD chip.

#### **<MULTOS-relevant Security Objectives >**

##### **O.MCD\_Authentication**

The TOE shall prove to the MCD Issuer that it has the TSF data injected by the MCD Issuer in Manufacturing phase.

##### **O.MCD\_Issuer\_Authentication**

The TOE shall authenticate the MCD Issuer to allow to set TSF data for MCD issuance and to allow subject's authority of MCD access control. If authentication fails up to the specified times, all actions arbitrated by TSF shall be deactivated permanently.

##### **O.MCD\_Management**

The TOE shall provide the authenticated MCD Issuer with the management measure which is required for MCD access controls such as loading, executing And deleting of MULTOS applications in the personalization phase and the operational use phase.

##### **O.MCD\_Access\_Control**

The TOE shall provide access control functionality to install, execute, and delete only the MULTOS applications allowed by the MCD Issuer.

#### **<TSF Common Security Objectives >**

##### **O.Secure\_State**

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

## **4.2 Security Objectives for the Environment**

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

#### **< ePassport-relevant Security Objectives >**

##### **OE.ePassport\_Manufacturing\_Security**

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

#### **OE. Procedures\_of\_ePassport\_Holder\_Check**

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

#### **OE.Certificate\_Verification**

The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the ePassport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically.

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

#### **OE.Personalization\_Agent**

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

#### **OE.Inspection\_System**

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

#### **OE.MRZ\_Entropy**

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

#### **OE.PKI**

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

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

### **OE.Range\_RF\_Communication**

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

### **< MULTOS-relevant Security Objectives >**

### **OE.Application\_Install**

The MCD Issuer shall securely issue PKI certificates only to the Application provider loaded to MCD

### **< IC-Chip-relevant Security Objectives >**

### **OE.Handling\_Info\_Leakage**

The crypto co-processor of the IC chip or cryptographic library loaded in the IC chip used by the TOE provides the means to prevent analyzing the leakage information (electric power or wave, etc.) during cryptographic operation, and obtaining key information.

### **OE.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 the TOE's malfunction outside the normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using the probing and reverse engineering analysis.

## **4.3 Security Objectives Rationale**

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

The rationale of security objectives demonstrates the following:

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

Table 16 shows the mapping between Security Problem Definition and Security Objectives.



Table 16. The mapping between Security Problem Definition and Security Objectives

Security Problem Definition	TOE Security Objectives													Security Objectives for the Environment																	
	O.Management	O.Personalization_Agent_Authentication	O.Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.EAC	O.BAC	O.AA	O.MCD_Authentication	O.MCD_Issuer_Authentication	O.MCD_Management	O.MCD_Access_Control	O.Secure_State	OE.ePassport_Manufacturing_Security	OE.Procedures_of_ePassport_Holder_Check	OE.Certificate_Verification	OE.Personalization_Agent	OE.Inspection_System	OE.MRZ_Entropy	OE.PKI	OE.Range_RF_Communication	OE.Application_Install	OE.Handling_Info_Leakage	OE.IC_Chip			
T.MCD_Forgery													X																		
T.Malware													X																		
T.Application_Compromise															X																
T.TSF_Data_Modification	X	X		X	X			X													X										
T.Evesdropping					X																	X									
T.Fogery_Corruption_Personal Data				X				X	X												X										
T.BAC_Authentication_Key_Dis close	X			X				X											X												
T.BAC_ReplayAttack							X																								
T.Damage_to_Biometric_Data				X	X	X		X		X										X	X		X								
T.EAC-CA_Bypass			X																X	X	X										
T.IS_Certificate_Forgery	X	X			X															X											
T.SessionData_Reuse							X															X									
T.Skimming								X	X	X												X				X					
T.Malfunction																X															X
T.Leakage_CryptographicKey_I nfo																											X	X			
T.ePassport_Reproduction																		X	X												



### **O.Personalization\_Agent\_Authentication**

This security objective ensure that the TOE provides the means to authorize user as personalization agent for granting write-rights of TSF data in the Personalization phase, therefore is required to counter the threat of T.TSF\_Data\_Modification.

Since personalization agent authentication is conducted before performing the security role to write information relevant to CVCA certificate, a user without the security role shall not be able to write forged CVCA certificate. Therefore, forged IS certificate transmitted from outside shall be detected and this is required to counter the threat of T.I\_Certificate\_Forgery.

This security objective ensures that the TOE provides the means to authorize personalization agent to confirm that personalization subject is not changed, therefore contributes to enforce the organizational security policy of P.Personalization\_Agent.

### **O.Security\_Mechanism\_Application\_Procedures**

This security objective is required to enforce the organizational security policy of P.Security\_Mechanism\_Application\_Procedures since the TOE ensures that the application order of the PA, BAC and EAC security mechanisms according to 2.1.1 Standard ePassport Inspection Procedure and 2.1.2 Advanced ePassport Procedure of the EAC specifications and by not allowing requests from the Inspection System that do not correspond to the security mechanism application order.

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

### **O.Session\_Management**

This security objective ensures that the TOE prevents authentication attempts of authentication in order for access to forge and corrupt the personal data of the ePassport holder and terminates session in case modification for the transmitted TSF data is detected. Therefore, this security objective is required to counter the threat of T.Forgery\_Corruption\_Personal\_Data.

Also, this security objective ensures that the TOE detects the EAC-TA failure of whom attempts access to read, maintains the EAC secure channel, and reduces attack chances, therefore is required to counter the threat of T.Damage\_to\_Biometric\_Data.

### **O.Secure\_Messaging**

This security objective ensures that the TOE establishes the BAC or EAC secure messaging for secure transmission of the personal and biometric data of the ePassport holder to the Inspection System, and provides the confidentiality and integrity for the transmitted personal and biometric data of the ePassport holder. Therefore, this security objective is required to counter the threats of T.Damage\_to\_Biometric\_Data and T.Eavesdropping. Also, this security objective ensures that the TOE establishes the secure messaging when the authorized Personalization Agent writes TSF data, and provides integrity of TSF data. Therefore, this security objective is required to counter the threat of T.TSF\_Data\_Modification.

Also, this security objective ensures that if The Personalization Agent requests the secure messaging the TOE handles it, and that if The Personalization Agent does not request it, the TOE deactivates the secure messaging. Therefore, this security objective contributes to enforce the organizational security policy of P.ePassport\_Personalization\_Policy.

#### **O.Certificate\_Verification**

This security objective is required to enforce the organizational security policy of P. PKI as it ensures for the TOE to check the valid date on the basis of the CVCA link certificate provided by the Inspection System, therefore to automatically update the certificate and the current date.

This security objective is required to counter the threats of T.Damage\_to\_Biometric\_Data and T.IS\_Certificate\_Forgery by determining the status of forgery as the TOE verifies validity of the CVCA link certificate, DV certificate and IS certificate in the EAC-TA.

#### **O.Deleting\_Residual\_Info**

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

#### **O.Replay\_Prevention**

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

#### **O.Access\_Control**

This security objective is required to counter the threats of T. Forgery\_Corruption\_Personal Data, T.Damage\_to\_Biometric\_Data and T.Skimming and enforce the organizational security policy of P.ePassport\_Access\_Control by implementing the rules of allowing or denying of Inspection System to read user data in accordance with the ePassport access control policies by the personalization agent.

This security objective is required to counter the threats of T.TSF\_Data\_Modification and T.BAC\_Authentication\_Key\_Disclose as it allows the authorized personalization agent has the write-rights of the MRTD application data in the Personalization phase and denies the access by personalization agent in the Operational Use phase.

#### **O.BAC**

This security objective is required to enforce the organizational security policy of P.ePassport\_Access\_Control as the TOE implements the BAC security mechanism to control access

to the personal data of the ePassport holder, therefore grants the read-rights for the personal data of the ePassport holder only to the authorized Inspection System of which the BAC mutual authentication is successfully completed.

This security objective is required to counter the threats of T. Forgery\_Corruption\_Personal Data and T.Skimming as the TOE allows the read-rights for the personal data of the ePassport holder only to the authorized Inspection System by generating the BAC session key during the BAC mutual authentication and denies access by the Inspection System that does not have the read-rights.

### **O.EAC**

This security objective is required to enforce the organizational security policy of P.ePassport\_Access\_Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the ePassport holder, therefore grants the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System of which the EAC-TA is successfully completed.

This security objective is required to counter the threats of T.Damage\_to\_Biometric\_Data and T.Skimming as the TOE allows the read-rights for the biometric data of the ePassport holder only to the authorized Inspection System through the EAC-TA by generating the EAC session key during the EAC-CA and denies access by the Inspection System that does not have the read-rights.

### **O.AA**

This security objective is required to counter the threat of T.IC\_Chip\_Forgery as the personalization agent provides the Inspection System with the verification data for genuineness to detect the forged MRTD chip .

## **< MULTOS-relevant Security Objectives >**

### **O.MCD\_Authentication**

This security objective is required to counter the threat of T.MCD\_Forgery as the TOE provides the means to demonstrate ownership of the injected TSF data by the MCD Issuer in the Manufacturing phase and the MCD Issuer is able to detect the MCD forgery.

### **O.MCD\_Issuer\_Authentication**

This security objective is required to counter the threat of T.Malware as the TOE allows only the certified user to have the security role of the MCD personalization management and subject's authority, therefore if the attacker is not certified he /she is not able to have subject's authority and is denied to access the Application stored in MCD.

### **O.MCD\_Management**

This security objective contributes to enforce the organizational security policy of P.Application\_Authorization as the TOE provides the means to manage the set of security attributes

for the MCD access controls(MULTOS application loading, executing, deleting, etc) in the Personalization and Operational Use phase.

#### **O.MCD\_Access\_Control**

This security objective is required to counter the threat of T.Application\_Compromise as the TOE controls the access by allowing to load the application in only case of having the allowed security attributes by the certified MCD Issuer and succeeding to verify certificates and code signature, therefore the attacker is not able to load arbitrary programs.

Also, this security objective contributes to enforce the organizational security policy of P.Application\_Authentication as the TOE provides the access control functionality based on security attributes included in the application certificate to load, execute, and delete only ePassport application certified by the MCD Issuer.

### **< TSF Common Security Objectives >**

#### **O.Secure\_State**

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

## **4.3.2 Security Objective Rationale for Operating Environment**

### **< ePassport-relevant Security Objectives >**

#### **OE.ePassport\_Manufacturing\_Security**

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

#### **OE.Procedures\_of\_ePassport\_Holder\_Check**

This security objective for environment is required to counter the threats of T.ePassport\_Reproduction, T.BAC\_Authentication\_Key\_Disclose and T.EAC-CA\_Bypass by implementing procedural security measures in immigration process, such as procedures to check the printed identify information page of the ePassport and to determine the forgery status of the ePassport book, etc.

#### **OE.Certificate\_Verification**

This security objective for environment verifies the SOD after verifying regularly the DS certificate and CRL in order for the Inspection System, such as the BIS and EIS, to verify for forgery and cor-

ruption of the ePassport identity data recorded in the TOE. Also, this security objective for environment ensures for the EIS to securely maintain digital signature generation key that corresponds to the IS certificate and to provide the TOE with the CVCA link certificate, DV certificate and IS certificate in the EAC-TA. Therefore, this security objective for environment is required to counter the threats of T.Damage\_to\_Biometric\_Data, T. EAC-CA Bypass and T.IS\_Certificate\_Forgery and support the assumption of A.Certificate\_Verification.

### **OE.Personalization\_Agent**

This security objective for environment is required to enforce the organizational security policies of P.International\_Compatibility and P.Personalization\_Agent by ensuring that the TOE is delivered to the Operational Use phase after securely issuing the ePassport so that the personalization agent can check that the issuing subject has not been changed, verifying normal operation and compatibility of the ePassport in the Personalization phase and deactivating writing function. This security objective for environment also is required to enforce the organizational security policy of P.ePassport\_Access\_Control as it defines the role of the personalization agent. Also, this security objective for environment is required to support the assumption of A.Certificate\_Verification because the personalization agent makes certificates necessary in the PA and EAC support available to the Inspection System.

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

### **OE.Inspection\_System**

This security objective for environment is required to support the assumption of A.Inspection\_System and enforce the organizational security policies of P.Security\_Mechanism\_Application\_Procedures and P.ePassport\_Access\_Control as the Inspection System implements and ensures application order of security mechanisms in accordance with the type of the Inspection System so that not to violate the ePassport access control policies of the personalization agent and by ensuring that information used in communication with the TOE is securely destroyed after session termination.

This security objective for environment is required to counter the threat of T.Eavesdropping as the confidentiality and integrity of the transmitted data are ensured by establishing the BAC secure messaging after generating the BAC session key through the BAC key distribution when the Inspection System communicates with the TOE.

This security objective for environment is required to counter the threats of T. Forgery\_Corruption\_Personal Data, T.Damage\_to\_Biometric\_Data, T.Skimming and T.EAC-CA\_Bypass as the Inspection System supports the BAC mutual authentication, EAC and PA.

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

### **OE.MRZ\_Entropy**

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

#### **OE.PKI**

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

#### **OE.Range\_RF\_Communication**

This security objective for environment is required to counter the threat of T.Skimming and enforce the organizational security policy of P.Range\_RF\_Communication by ensuring that RF communication distance between the MRTD chip and the Inspection System is less than 5cm and that RF communication channel is not established if the page of the ePassport attached with the IC chip is not opened.

#### **< MULTOS-relevant Security Objectives >**

#### **OE.Application\_Install**

This security objective for environment contributes to enforce the Organizational Security Policies of P.Application\_Install and P.Application\_Authentication as the MCD Issuer securely issues the certificate based on PKI only to the Application Provider to be loaded MCD.

#### **< IC-Chip-relevant Security Objectives >**

#### **OE.Handling\_Info\_Leakage**

This security objective for environment is required to counter the threat of T.Leakage\_CryptographicKey\_Info as the IC chip, the sub hardware of TOE, provides the means to prevent analyzing the leakage information (electric power and wave, etc.) during cryptographic operation, and obtaining of key information.

#### **OE.IC\_Chip**

This security objective for environment is required to support the assumption of A.IC\_Chip as it uses EAL5+(SOF-high) IC chip that generates random number and provides cryptographic operation in order to support security functions of the TOE and provides the malfunction detection and physical protection, etc.



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

## 5 Definition of Extended Component

This ST does not define extended component.

## 6 Security Requirements

Security requirements specify security functional requirements that must be satisfied by the TOE that is specified in this ST and security functional and assurance requirements that must be satisfied under the operational environment.

ST follows external entities such as the Personalization agent, BIS, EIS, ePassport IC Chip are specified in PP. However, the Personalization agent can perform personalizations of ePassport application data and functions relevant to KMA such as MCD enablement and application management as well. In the latter case, the term 'MCD Issuer' is used for clear specification.

### 6.1 Terms and Definitions

In the security requirements, terms which are not defined clearly in chapter 9 Annexes are defined like below.

Terms	Definition
MCD Issuer	While the personalization agent generates SOD and TSF data and manages PA-PKI, EAC-PKI, the MCD Issuer has the role of Certificate Authority in the MULTOS security scheme.  In the ST, personalization agent without further clarification may include 'MCD Issuer' as well as ePassport personalization agent.
MCD	The device where MULTOS is embedded. In this ST, it means SP20, that is packaged module of wafer where SM30X is masked. If LDS application is loaded, it will be the final TOE configuration.
MSM_CD	MSM controls data which is encrypted with the unique key by the MCD Issuer. Only when SM30X decrypts it successfully, application can be loaded.
ALU	ALU(Application Load Unit) is a unit in which applications are loaded to MULTOS cards and it consists of Code, Data, DIR File Record, FCI Record and Dedicated file data  In case of protected ALU, Application Signature shall be added that has created by conducting digital signature using Application Provider's private key.  In case of confidential ALU, KTU Ciphertext shall be added to the protected ALU where KTU shall be the encryption keys encrypted using mkd_pk in order to protect code and data to be transported
ADC	The certificate includes App Permission related deletion and it is application provider's public key which is signed with MCD Issuer's digital signature generation key (kck_sk)
ALC	The certificate which includes App Permission related load and it is application provider's public key which is signed with MCD Issuer's digital signature generation key (kck_sk)
Active Authentication Private key	Active Authentication private key which generates digital signature based on RSA to detect fabrication of MRTD IC chip

MCD Permission	The attribute value that is written by the MCD Issuer with MSM_CD. It shall be composed of mcd_issuer_product_id, mcd_issuer_id and set_msm_controls_data_date, etc.
MCD Issuer Certificate	MCD Issuer's certificate for kck_pk which is used to verify MULTOS application provider's certificate(ALC/ADC). When MCD Issuer issues ALC/ADC, MULTOS application provider's public key is signed with kck_sk based on RSA.
AID	Uniquely assigned ID for each Application
APP Permission	The attribute value which is composed of mcd_issuer_product_id, mcd_issuer_id and set_msm_controls_data_date, etc. It shall be included in the ALC/ADC created per each application by MCD Issuer before a MULTOS application is loaded to or deleted from MCD.
MCD Public Key Certificate	Signed mcd_pk transferred from MCD Issuer through MSM_CD to MCD using MCD issuer's digital signature generation key.
Personalization Key	The personalization authentication key and personalization SM key which is a symmetric key for the personalization agent to be able to acquire personalization right and to write ePassport TSF data securely.
Personalization Authentication Key	A symmetric key which is used by the personalization agent for acquiring personalization right through External Authentication.
Personalization SM Key	The encryption key and MAC key that are used by the personalization agent for writing securely ePassport TSF data through Secure Messaging
Personalization Session Key	The symmetric key for a single session to establish secure channel in the Personalization Phase. It is composed of encryption key and MAC key generated by key derivation mechanism using random numbers transferred by personalization agent.

## 6.2 TOE Security Functional Requirements

The security functional requirements specified in this ST select and use the relevant functional components from Part2 of the CC to satisfy Security Objectives for the TOE in chapter 4.

### 6.2.1 ePassport Security Functional Requirements

[< Cryptographic Support >](#)

#### FCS\_CKM.1 (1) Cryptographic Key Generation (Key Derivation Mechanism)

Hierarchical to: No other components.

Dependencies: [FCS\_CKM.2(1) Cryptographic key distribution (KDF Seed Distribution for BAC session key generation) and  
FCS\_CKM.2(2) Cryptographic key distribution (KDF Seed Distribution for BAC session key generation) or  
FCS\_COP.1 Cryptographic operation]

#### FCS\_CKM.4 Cryptographic key destruction

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

Application Notes : The personalization agent writes DG1 file and generate BAC authentication key into the TOE , which generates the BAC session key and EAC session key by using key derivation mechanism.

#### **FCS\_CKM.1 (2) Cryptographic Key Generation (Personalization agent Key Generation)**

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 BAC session key generation) or

FCS\_COP.1 Cryptographic operation]

FCS\_CKM.4 Cryptographic key destruction

FCS\_CKM.1.1 The TSF shall generate **personalization authentication key, personalization SM key and session key of Personalization agent** in accordance with a specified cryptographic key generation algorithm [TDES] and specified cryptographic key sizes [ 112 bit ] that meet the following: [No other components].

Application Notes : The TOE uses TDES accelerator ,is supported by IC chip, for personalization agent generation based

#### **FCS\_CKM.2(1) Cryptographic Key Distribution(KDF Seed Distribution for BAC Session Key Generation)**

Hierarchical to: No other components

Dependencies : [FDP\_ITC.1 Import of user data without security attributes, or

FDP\_ITC.2 Import of user data with security attributes, or

FCS\_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism)]

FCS\_CKM.4 Cryptographic key destruction

FCS\_CKM.2.1 The TSF shall distribute **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

Application Notes : The TOE uses TDES accelerator and SHA-1 cryptographic library are supported by IC chip, for KDF Seed for the BAC session key

#### **FCS\_CKM.2(2) Cryptographic Key Distribution(KDF Seed Distribution for EAC Session Key Generation)**

Hierarchical to: No other components

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or

FDP\_ITC.2 Import of user data with security attributes, or  
 FCS\_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism)]  
 FCS\_CKM.4 Cryptographic key destruction

FCS\_CKM.2.1 The TSF shall distribute **KDF Seed for the EAC session key** generation in accordance with a specified cryptographic key distribution method specified cryptographic key distribution method in Table 17 that meets the following: specified standard in Table 17

Table 17 Cryptographic Key Distribution Standard and Method

Standard	Cryptographic Key Distribution Method
PKCS#3	Diffie-Hellman key-agreement protocol
ISO/IEC 15946-3	Elliptic curve Diffie-Hellman key-agreement protocol

Application Notes: The TOE uses DH, ECDH or SHA cryptographic library, supported by IC chip, for KDF Seed for the EAC session key and supports key length.

Table 18 Cryptographic Key Distribution Standard and Method

Standard	Key Length
DH	1024, 1280, 1536, 2048 bits
ECDH	160, 192, 224, 256, 384, 512 bits

**FCS\_CKM.4 Cryptographic Key Destruction**

Hierarchical to: No other components

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or  
 FDP\_ITC.2 Import of user data with security attributes, or  
 FCS\_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism)) and  
 FCS\_CKM.1(2) Cryptographic key generation (personalization agent Key Generation)]

FCS\_CKM.4.1 The TSF shall destroy **encryption keys and MAC keys** in accordance with a specified cryptographic key destruction method [ filling memory data as '0' or deleting physically by overwriting a new key ] that meets the following: [none].

**<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 (MRTD)

FDP\_ACC.1.1 The TSF shall enforce the [ MRTD access control policy ] on [

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

**FDP\_ACF.1(1) Security Attribute Based Access Control (ePassport)**

Hierarchical to: No other components.

Dependencies: FDP\_ACC.1(2) Subset access control (MRTD)

FMT\_MSA.3 Static attribute initialization(MRTD Object Security Attributes)

FDP\_ACF.1.1 The TSF shall enforce the [ MRTD access control policy ] to objects based on the following: [ [Table 19], [Table 20], and [None] ].

Table 19. Subject-relevant Security Attributes

Subjects	Security Attributes
BIS	BAC authorization
EIS	BAC authorization, EAC authorization
<b>ePassport Personalization Agent</b>	Personalization Agent Issuing authorization

Table 20. Object-relevant Security Attributes

Objects	Security attributes	
	Security attributes of object's operation	Security attributes of object's access-rights

Personal data of the ePassport holder	Read-rights	BAC authorization, EAC authorization
	Write-rights	Personalization Agent issuing authorization
Biometric data of the ePassport holder	Read-rights	EAC authorization
	Write-rights	Personalization Agent issuing authorization
ePassport authentication data	Read-rights	BAC authorization, EAC authorization
	Write-rights	Personalization Agent issuing authorization
EF.CVCA	Read-rights	BAC authorization, EAC authorization
	Write-rights	Personalization Agent issuing authorization
EF.COM	Read-rights	BAC authorization, EAC authorization
	Write-rights	Personalization Agent issuing authorization

**Application Notes:** The BAC authorization is the right given to the user identified with the Inspection System that supports the LDS Application by FIA\_UID.1 when the BAC mutual authentication succeeds.

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

The personalization agent issuing authorization is the right given when **the personalization agent** to be successfully authenticated in the Personalization phase.

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

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

- b) [None]

].

FDP\_ACF.1.3. The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [When the operational mode is initialized, personalization agent has permission for delete of entity in the Personalization phase].



FDP\_ACF.1.4. The TSF shall explicitly deny access of subjects to objects based on the [the following rules].

- a) Explicitly deny access of subjects to objects if instructions order of the Inspection System is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specifications
- b) Explicitly deny read of subjects to biometric data if there is no the read-rights of biometric data in IS certificate of the EIS that has the EAC authorization
- c) Explicitly deny access(read, write, etc.) of the unauthorized Inspection System to all objects
- d) Explicitly deny access of the different operational mode to all objects

### **FDP\_DAU.1 Basic Data Authentication (Active 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 [Active authentication 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: TSF provides AA security mechanism up to maximum 2048 bits.

### **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 made unavailable upon the *retrieval of the resource from* the following objects: [

- a) BAC session key
- b) EAC session key
- c) [Random number, Active authentication private key]

Application Notes: After a session termination, the TSF shall not remain the BAC session key, the EAC session key random numbers and active authentication private key in temporary memory. The BAC session key, the EAC session key, random numbers and active authentication private key, etc. can be ensured unavailable by destroying them with the method defined in FCS\_CKM.4. The BAC authentication key is stored into secure memory so it is exclusive in the residual information protection entity.

### **FDP\_UCT.1 Basic Data Exchange Confidentiality**

Hierarchical to: No other components.

Dependencies: [FTP\_ITC.1 Inter-TSF trusted channel, or  
FTP\_TRP.1 Trusted path]

[FDP\_ACC.1(1) Subset access control(MRTD), or

FDP\_IFC.1 Subset information flow control]

FDP\_UCT.1.1 The TSF shall enforce the [ MRTD access control policy ] to be able to transmit, receive objects in a manner protected from unauthorized disclosure.

Application Notes: When the Inspection System successfully completes the BAC mutual authentication, the TSF protects from disclosure by using the BAC session encryption key. When the EAC-CA is successfully executed, data transmitted thereafter are protected from disclosure by using the EAC session encryption key. **When the personalization agent is successfully authenticated, MRTD user data is protected with personalization agent session key in accordance with Secure Messaging option.**

### **FDP\_UIT.1 Data Exchange Integrity**

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1(1) Subset access control, or  
FDP\_IFC.1 Subset information flow control]  
[FTP\_ITC.1 Inter-TSF trusted channel, or  
FTP\_TRP.1 Trusted path]

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

FDP\_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

Application Notes: The TSF protects integrity of the transmitted data by using the MAC key for BAC session or EAC session. This provides the method of protection against modification, deletion and insertion of user data. **When the personalization agent chooses Secure Messaging after successful personalization agent authentication, ePassport user data can be protected from disclosure using personalization agent session key.**

## **<Identification and Authentication>**

### **FIA\_AFL.1(1) Authentication Failure Handling(Inspection System Authentication Failure)**

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1(1) Authentication(BAC mutual Authentication), FIA\_UAU.1(2) Authentication(EAC-TA)

FIA\_AFL.1.1 The TSF shall detect when “[one at a single session given same random number]” unsuccessful authentication attempts occur related to [

- a) BAC mutual authentication
- b) EAC-TA
- c) [None]

].

FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been

met or surpassed, the TSF shall perform [the following [table 21]].

Table 21. Authentication Failure Handling for Authentication Mechanism

Authentication Mechanism	Authentication Failure Handling
BAC mutual Authentication	User Sessin Termination
EAC-TA	Maintaining EAC Secure Messaging

Application Notes: When there is no separate request from The personalization agent at the EAC-TA failure, EAC secure channel created from the EAC-CA should be maintained according to EAC specification.

### **FIA\_AFL.1 (2) Authentication Failure Handling(Personalization Agent Authentication Failure)**

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1(3)(Personalization Agent Authentication)

FIA\_AFL.1.1 The TSF shall detect when “[regardless of sessions 10 cumulative]” unsuccessful authentication attempts occur related to [

- a) Personalization Authentcation

]

FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall change [Operational mode to Terminated mode]

### **FIA\_UAU.1(1) Timing of Authentication (BAC Mutual Authentication)**

Hierarchical to: No other components.

Dependencies to: FIA\_UAU.1 Timing of identification(Contactless communication identification)

FIA\_UAU.1.1 **When operational mode is Personalized**, the TSF shall allow [

- a) indication of the BAC mechanism support
- b) [ none ]

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

FIA\_UAU.1.2 The TSF shall require the **BIS** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions stipulated in FIA\_UAU. 1.1.

Application Notes: BAC mechanism support mark means success of ePassport application selection and execution.

### **FIA\_UAU.1(2) Timing of Authentication (EAC-TA)**

Hierarchical to: No other components.

Dependencies to: FIA\_UAU.1(1) Timing of identification(BAC Mutual Authentication)

FIA\_UAU.1.1 **When operational mode is Personalized**, the TSF shall allow [

- a) to perform EAC-CA

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

c) [ to perform AA ]

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

FIA\_UAU.1.2 The TSF shall require the **EIS** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions stipulated in FIA\_UAU. 1.1.

### **FIA\_UAU.1(3) Timing of Authentication (Personalization Agent Authentication )**

Hierarchical to: No other components.

Dependencies to: FIA\_UAU.1 Timing of identification (communication identification)

FIA\_UAU.1.1 **When operational mode is Initialized**, the TSF shall allow [to select and to execute ePassport application ] on behalf of the user to be performed before the **ePassport personalization agent** is authenticated.

FIA\_UAU.1.2 The TSF shall require the **ePassport personalization agent** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions specified in FIA\_UAU. 1.1.

### **FIA\_UAU.4 Single-Use Authentication Mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies

FIA\_UAU.4.1 The TSF shall prevent reuse of authentication data related to [

a) BAC mutual authentication

b) EAC-TA

c) [ Personalization Agent authentication ]

### **FIA\_UAU.5 Multiple Authentication Mechanisms**

Hierarchical to: No other components.

Dependencies: No dependencies

FIA\_UAU.5.1 The TSF shall provide [

a) BAC mutual authentication

b) EAC-TA

c) [ Personalization Agent authentication ]

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

a) The BIS or EIS shall succeed the BAC mutual authentication in order to have the BAC authorization and **active authentication in case that Inspection System supports**.

b) The EIS, in order to have the EAC authorization, shall succeed the BAC mutual authentication, EAC-CA and EAC-TA and **active authentication in case that Inspection System supports and** include the read-rights of biometric data in all of the CVCA certificate, DV certificate and IS certificate. For this, the TSF shall provide the EAC-CA.

c)[To get personalization permission, The personalization agent should authenticate successfully]  
].

Application Notes: AA authentication is performed according to personalization policy when right TSF data and user data are personalized in the personalization phrase.

#### **FIA\_UID.1(1) Timing of Identification(ePassport User Identification)**

Hierarchical to: No other components.

Dependencies: No dependencies

FIA\_UID.1.1 The TSF shall allow [

a) to establish the communication channel based on ISO/IEC 14443-4

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

FIA\_UID.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions stipulated in FIA\_UID. 1.1.

Application Notes: When external entities communicated with the TOE request the use of the LDS Application, the TOE identifies it with or **the ePassport personalization agent** or the Inspection System.

#### **<Security Management>**

#### **FMT\_MOF.1(1) Management of Security Functions Behavior(Suspending write function)**

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

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

#### **FMT\_MOF.1(2) Management of Security Functions Behavior(Suspending EAC and Secure Messaging)**

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of Management Functions (MRTD)

FMT\_SMR.1 Security roles (Personalization Agent)

FMT\_MOF.1.1 The TSF shall restrict the ability to disable the functions [

a) EAC

b) Secure Messaging in the personalization phase

] to [ the personalization agent in the personalization phase ].

Application Notes: The personalization agent can make EAC function to be disable according to ePassport personalization policy. At this point, DG3 and DG4 are not available in the operational use phase. When The personalization agent makes and operates physical, human and procedural security measures similar level to Secure Messaging in the Personalization phase, it can not use Secure Messaging.

### **FMT\_MSA.1(1) Management of Security Attributes(ePassport)**

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1(1) Subset access control(MRTD) or  
FDP\_IFC.1 Subset information flow control]

FMT\_SMF.1 Specification of Management Functions(MRTD)

FMT\_SMR.1 Security roles(Personalization Agent)

FMT\_MSA.1.1 The TSF shall enforce the [ MRTD access control policy ] to restrict the ability to [ initialization ] the security attributes [ security attributes of subjects defined in FDP\_ACF.1(1) ] to [ TSF ].

Application Notes : As an action to be taken if the TSF detects modification of the transmitted inter-TSF data in FPT\_ITI.1, the TSF shall reset security attributes of subjects defined in FDP\_ACF.1(2).

### **FMT\_MSA.3(1) Static Attribute Initialization (MRTD Object Security Attributes)**

Hierarchical to: No other components.

Dependencies: FMT\_MSA.1(1) Management of security attributes(MRTD)

FMT\_SMR.1(1) Security roles(Personalization Agent)

FMT\_MSA.3.1 The TSF shall enforce the [ MRTD access control policy ] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT\_MSA.3.2 The TSF shall allow the [ **TSF** ] to specify alternative initial values to override the default values when an object or information is created.

Application Notes : When the **TSF** generates ePassport user data (EF.DG1~16, EF.SOD, EF.COM, EF.CVCA) **on behalf of The personalization agent in the Personalization phase**, it **initializes** operation security attributes and access control security attributes **as** specified in FDP\_ACF.1.1(2).

### **FMT\_MTD.1(1) Management of TSF Data (Certificate Verification Information and Authentication Key)**

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of Management Functions(ePassport Issuing Management)

FMT\_SMR.1 Security roles(Personalization Agent)

FMT\_MTD.1.1 The TSF shall restrict the ability to [write in secure memory] the [

- a) EAC chip authentication private key
- b) initial current date
- c) initial CVCA certificate

d) initial CVCA digital signature verification key

e) [ Active authentication private key<sup>4</sup> ]

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

Application Notes: The issuing key defined in FIA\_UAU.1.(3) for The personalization agent to get issuing right can be a generated key at the manufacturing phase or updated key in the Personalization phase..

### **FMT\_MTD.1(2) Management of TSF Data (SSC initialization)**

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of Management Functions(ePassport Issuing Management)

FMT\_SMR.1 Security roles(Personalization Agent)

FMT\_MTD.1.1 The TSF shall restrict the ability to modify the [ SSC(Send Sequence Counter) ] to [TSF].

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

### **FMT\_MTD.1(3) Management of TSF Data(Operational Mode 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 inquiry and alter the [Operational mode ] to [ personalization agent].

### **FMT\_MTD.1(4) Management of TSF Data (Generating and Storing BAC Authentication Key)**

Hierarchical to: No other components.

Dependencies: FMT\_SMF.1 Specification of Management Functions(ePassport Issuing Management)

FMT\_SMR.1 Security roles(Personalization Agent)

FMT\_MTD.1.1 The TSF shall restrict the ability to generate and store the [ BAC Authentication Key ] to [TSF].

Application Notes : The TSF automatically makes BAC authentication key and store it after writing DG1 file.

### **FMT\_MTD.3 Secure TSF Data**

Hierarchical to: No Other Components.

Dependencies: FMT\_MTD.1(1) Management of TSF data

---

<sup>4</sup> Added to deal with AA

FMT\_MTD.3.1 The TSF shall ensure that only secure values are accepted for [ *ePassport TSF data*].

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

### **FMT\_SMF.1(1) Specification of Management Functions(ePassport Security Management)**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- a) Function to write user data and TSF data in the Personalization phase
- b) Function to verify and update the CVCA certificate, CVCA digital signature verification key and current data in the Operational Use phase and **TSF data management such as MRTD subject and object security attribute and SSC initialization**
- c) [Function to decide to enable EAC in the Personalization phase]
- [
- d) Halt security function such as writing, EAC and Secure Messaging in the Personalization phase
- e) Managing mode
- f) BAC authentication key generation and storage in the Personalization

].

### **FMT\_SMR.1 Security Roles(Personalization Agent)**

Hierarchical to: No other components.

Dependencies: None

FMT\_SMR.1.1 The TSF shall maintain the roles [

- a) **ePassport Personalization Agent**
- b) [ None ]

].

FMT\_SMR.1.2 The TSF shall be able to associate users with roles.

Application Notes: In the function to security management defined by FMT\_SMF.1(1), the personalization performs a),c),d) and the TSF performs b),e). However the TSF is not a user thus is not defined as security roles.

### **<TSF Protection>**



### **FPT\_ITC.1 Inter-TSF Confidentiality during Transmission**

Hierarchical to: No other components.

Dependencies: None

FPT\_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

Application Notes: Secure Messaging can be provided optionally according to the personalization's personalization policy.

### **FPT\_ITI.1 Inter-TSF Detection of Modification**

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

- a) Termination of BAC secure messaging or EAC secure messaging
- b) Deletion of BAC session key or EAC session key
- c) Management action specified in FMT\_MSA.1
- d) Termination of personalization agent communication channel
- e) [ personalization agent session key deletion]

] if modifications are detected.

Application Notes: The Strength of Retail MAC is equivalent to the secure Retail MAC specified in FCS\_COP.1(2). **Secure Messaging shall be always conducted in Operational Use phase but it is optional according to personalization policy in the Personalization phase.**

## **6.2.2 MULTOS Security Functional Requirements**

### **<User Data Protection>**

#### **FDP\_ACC.1(2) Subset Access Control (MULTOS)**

Hierarchical to: No other components.

Dependencies: FDP\_ACF.1(1) Security attribute based access control(Open platform OS)

FDP\_ACC.1.1 The TSF shall enforce the [ MULTOS access control policies ] on [

- a) Subject: MCD Issuer
- b) Object: ALU(MULTOS Application Unit)
- c) Operation

- (1) Loading<sup>5</sup>
- (2) Deleting
- (3) Execution

]

**FDP\_ACF.1(2) Security Attribute based Access Control(MULTOS)**

Hierarchical to: No Other Components.

Dependencies: FDP\_ACC.1(2) Subset access control (Open platform OS)

FMT\_MSA.3(2) Static attribute initialization

FDP\_ACF.1.1 The TSF shall enforce the [ MULTOS access control policies ] to objects based on the following: [ Table 22, Table23 ].

Table 22. Open Platform OS Subject-relevant Security Attributes

Subjects	Security Attributes
MCD Issuer Role Process	MCD Permission
	Digital Signature Verification Key(kck_pk) for MCD Certificate
	KTU Encyption Key Transfomission Public Key Pair (mkd_sk, mkd_pk)

Table 23. Open Platform OS Object-relevant Security Attributes

Objects	Security Attributes
ALU	APP Permission of ALC
	APP Permission of ADC
	Application Code Hash of ALC
	Application Signature
	KTU(Key Transformation Unit)

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) Loading allowance rules for subject's ALU
  - a-1. The mcd\_issuer\_product\_ids in the ALC's APP Permission includes the mcd\_issuer\_product\_id in the MCD Permission
  - a-2. The mcd\_issuer\_id in the ALC's APP Permission should be identical to the mcd\_issuer\_id in the MCD Permission

<sup>5</sup> Open MEL Application, Load <컴포넌트>, Create MEL Application 등 일련의 오퍼레이션 전체를 의미함

- a-3. The set\_msm\_controls\_data\_dates in the ALC's APP Permission includes the set\_msm\_controls\_data\_dates in the MCD Permission
- a-4. The mcd\_number in the ALC's APP Permission is 0 or identical to the mcd\_number in the MCD Permission

b) Deleting allowance rules for subject's ALU

- b-1. To delete application's "AID + random\_seed" should be identical to "AID + random\_seed" in the application loading list
- b-2. The mcd\_issuer\_product\_ids in the ADC's APP Permission includes the mcd\_issuer\_product\_id in the MCD Permission
- b-3. The mcd\_issuer\_id in the ADC's APP Permission should be identical to the mcd\_issuer\_id in the MCD Permission
- b-4. The set\_msm\_controls\_data\_dates in the ADC's APP Permission includes the set\_msm\_controls\_data\_dates in the MCD Permission
- b-5. The mcd\_number in the ADC's APP Permission is 0 or identical to the mcd\_number in the MCD Permission

c) Executing allowance rules for subject's ALU

- c-1. There should be enough memory for selected and enabled session data and static data of MULTOS applications loaded to MCD according to Loading allowance rules.

]

FDP\_ACF.1.3. The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

a) Loading allowance additional rules for subject's ALU

- a-1. ALC Certificate validation should be succeeded with MCD Certificate's digital signature validation key(kck\_pk) and Application Signature validation should be succeeded with ALC public key
- a-2. ALC's application code hash validation should be succeeded
- a-3. KTU decryption should be succeeded with KTU encryption transmission private key(mkd\_sk)

b) Deleting allowance additional rules for subject's ALU

- b-1. ADC Certificate validation should be succeeded with MCD Certificate's digital signature validation key(kck\_pk)]

FDP\_ACF.1.4. The TSF shall explicitly deny access of subjects to objects based on the following

a) Prohibiting loading rules for subject's ALU

- a-1. To load Application's AID is not different from AIDs were loaded previously
- a-2. To load application's "AID + random\_seed" should be identical to "AID + random\_seed" in the application loading list

b) Prohibiting executing rules for subject's ALU

- b-1. Different MULOTS application is executing

### **FDP\_DAU.1(2) Basic Data Authentication (MCD 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 [Key information for TSF execution code integrity validation].

FDP\_DAU.1.2 The TSF shall provide [ MCD Issuer] with the ability to verify evidence of the validity of the indicated information.

Application Notes: The TSF provides Check Data mechanism base on Asymmetric Hash

### **FDP\_ETC.2 Export of User Data with Security Attributes**

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]

FDP\_ETC.2.1 The TSF shall enforce the [MULTOS access control policy]) when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP\_ETC.2.2 The TSF shall disclose user data with **security attributes such as MCD Permission, KTU Encryption Public Key, MCD Public Key Certificate** relevant to them.

FDP\_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP\_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [None].

## **<Identification and Authentication>**

### **FIA\_AFL.1 (3) Authentication Failure Handling(MCD Issuer Authentication Failure)**

Hierarchical to: No other components.

Dependencies: FIA\_UAU.1(4)(MCD Issuer Authentication)

FIA\_AFL.1.1 The TSF shall detect when “irregardless of sessions 10 cumulative” unsuccessful authentication attempts occur related to [MCD Issuer Authentication]

FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall perform [MCD disabled permanently]

### **FIA\_UAU.1(4) Timing of Authentication (MCD Issuer Authentication )**

Hierarchical to: No other components.

Dependencies to: FIA\_UID.1(2) Timing of identification(MCD issuer Identification)

FIA\_UAU.1.1 The TSF shall allow [MCD authentication defined in FDP\_DAU.1(2)] on behalf of the user to be performed before the user is authenticated.

FIA\_UAU.1.2 The TSF shall require user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions stipulated in FIA\_UAU. 1.1.

### **FIA\_UID.1(2) Timing of Identification(MCD Issuer Identification)**

Hierarchical to: No other components.

Dependencies: No dependencies

FIA\_UID.1.1 The TSF shall allow [

to establish the communication channel according to user's communication method] 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 authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions stipulated in FIA\_UID. 1.1.

Application Notes: When external entities communicated with the TOE transmits commands related MCD issuing, the TOE identifies it as the MCD Issuer.

## <Security Management>

### **FMT\_MSA.1 (2) Management of Security Attributes (MSM\_CD)**

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1(2) Subset access control(MULTOS) or

FDP\_IFC.1 Subset information flow control]

FMT\_SMF.1(2) Specification of Management Functions(Function to MCD management)

FMT\_SMR.1(2) Security roles(MCD Issuer)

FMT\_MSA.1.1 The TSF shall enforce the [MULTOS access control policy] to restrict the ability to [ set up ] the security attributes [ security attributes of subjects defined in FDP\_ACF.1(2) ] to [ MCD Issuer ].

### **FMT\_MSA.1 (3) Management of Security Attributes (ALC, ADC Certificate Validation)**

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1(2) Subset access control(MULTOS) or

FDP\_IFC.1 Subset information flow control]

FMT\_SMF.1(2) Specification of Management Functions(Function to MCD management)

FMT\_SMR.1(2) Security roles(MCD Issuer)

FMT\_MSA.1.1 The TSF shall enforce the [MULTOS access control policy] to restrict the ability to [ validate ] the security attributes [ ALC, ADC ] to [ MCD Issuer ].

### **FMT\_MSA.2 Secure Security Attributes**

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1(2) Subset access control(MULTOS) or  
FDP\_IFC.1 Subset information flow control]  
FMT\_MSA.1 Management of security attributes(ALC,ADC Certificate Validation)  
FMT\_SMR.1(2) Security roles(MCD Issuer)  
FMT\_MSA.2.1 The TSF shall ensure that only secure values are accepted for [ALC, ADC].

### **FMT\_MSA.3(2) Static Attribute Initialization (MULTOS Security Attributes)**

Hierarchical to: No other components.

Dependencies: FMT\_MSA.1 Management of security attributes(ALC,ADC Certificate Validation)  
FMT\_SMR.1(2) Security roles(MCD Issuer)

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

FMT\_MSA.3.2 The TSF shall allow the [ MCD Issuer ] to specify alternative initial values to override the default values when an object or information is created.

### **FMT\_SMF.1(2) Specification of Management Functions(MCD Management)**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- a) Subject-relevant security attributes defined in FDP\_ACF.1(2)
- b) ALC, ADC Validation

].

### **FMT\_SMR.1(2) Security Roles (MCD Issuer)**

Hierarchical to: No other components.

Dependencies: None

FMT\_SMR.1.1 The TSF shall maintain the roles [ MCD Issuer ].

## **6.2.3 TSF Common Security Functional Requirements**

### **<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 at self-testing by FPT\_TST.1

- b) Conditions outside the normal operating of the TSF detected by the IC chip
- c) [None ]

].

### FPT\_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies

FPT\_TST.1.1 The TSF shall run a suite of self tests *during operation* to demonstrate the correct operation of the [ *function to guarantee secure randomness defined in FMT MTD.3* ].

FPT\_TST.1.2 The TSF shall provide **the personalization agent** with the capability to verify the integrity of [ *MSM\_CD, EAC chip authentication private key, active authentication private key, CVCA certificate, CVCA digital signature verification key, personalization agent personalization key, MRTD access condition* ]

FPT\_TST.1.3 The *TSF* shall provide the **personalization agent** with the capability to verify the integrity of TSF

## 6.3 TOE Security Assurance Requirements

Security assurance requirements for this security target document consist of the following components from part 3 of the CC - ePassport protection profile, evaluation level is EAL5+, higher than the protection profile, and had supplemented ALC\_DVS.2, AVA\_VAN.5 considering MULTOS's security management system. The assurance components are augmented follows:

- ADV\_IMP.2 Complete mapping of the implementation representation of the TSF
- ALC\_DVS.2 Sufficiency of security measures
- AVA\_VAN.5 High formulated vulnerability analysis

Assurance components are summarized in the following Table 24.

Table 24. Security Assurance Requirements

Assurance class	Assurance component	
Security target evaluation	ASE_INT.1	ST Introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete semi-formal functional specification with additional

		error information
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
	ADV_TDS.4	Semiformal modular design
	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 analysis	AVA_VAN.5	Advanced methodical vulnerability analysis

### 6.3.1 Security Target

#### ASE\_INT.1 ST Introduction

Dependencies : No dependencies

Developer action elements :

ASE\_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements :

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

ASE\_INT.1.2C The ST reference shall uniquely identify the ST.

ASE\_INT.1.3C The TOE reference shall identify the TOE.

ASE\_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE\_INT.1.5C The TOE overview shall identify the TOE type.

ASE\_INT.1.6C the TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE\_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE\_INT.1.8C The TOE description shall describe the logical scope of the TOE.



Evaluator action elements :

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

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

### **ASE\_CCL.1 Conformance Claim**

Dependencies :

ASE\_INT.1 ST introduction

ASE\_ECD.1 Extended components definition

ASE\_REQ.1 Stated security requirements

Developer action elements :

ASE\_CCL.1.1D The developer shall provide a conformance claim.

ASE\_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements :

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

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

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

ASE\_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

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

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

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

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

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

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

Evaluator action elements :

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

### **ASE\_SPD.1 Security Problem Definition**

Dependencies : No dependencies.

Developer action elements :

ASE\_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements :

ASE\_SPD.1.1C the security problem definition shall describe the threats.

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

ASE\_SPD.1.3C The security problem definition shall describe the OSPs.

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

Evaluator action elements :

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

### **ASE\_OBJ.2 Security Objectives**

Dependencies : ASE\_SPD.1 Security problem definition

Developer action elements :

ASE\_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE\_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements :

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

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

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

ASE\_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE\_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

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

Evaluator action elements :

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

### **ASE\_ECD.1 Extended Components Definition**

Dependencies : No dependencies.

Developer action elements :

ASE\_ECD.1.1D The developer shall provide a statement of security requirements.

ASE\_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements :

ASE\_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE\_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

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

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

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

Evaluator action elements :

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

ASE\_ECD.1.2E The evaluator *shall confirm* that no extended component can be clearly expressed using existing components.

### **ASE\_REQ.2 Derived Security Requirements**

Dependencies :

ASE\_OBJ.2 Security objectives

ASE\_ECD.1 Extended components definition

Developer action elements :

ASE\_REQ.2.1D The developer shall provide a statement of security requirements.

ASE\_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements :

ASE\_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

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

ASE\_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE\_REQ.2.4C All operations shall be performed correctly.

ASE\_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE\_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE\_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE\_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE\_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements :

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

### **ASE\_TSS.1 TOE Summary Specification**

Dependencies :

ASE\_INT.1 ST introduction

ASE\_REQ.1 Stated security requirements

ADV\_FSP.1 Basic functional specification

Developer action elements :

ASE\_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements :

ASE\_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements :

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

ASE\_TSS.1.2E The evaluator *shall confirm* that the TOE summary specification is consistent with the TOE overview and the TOE description.

## **6.3.2 Development**

### **ADV\_ARC.1 Security Architecture Description**

Dependencies :

ADV\_FSP.1 Basic functional specification

ADV\_TDS.1 Basic design

Developer action elements :

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

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

ADV\_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements :

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

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

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

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

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

Evaluator action elements :

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

#### **ADV\_FSP.5 Complete Semiformal Functional Specification with Additional Error Information**

Dependencies :

ADV\_TDS.1 Basic design

ADV\_IMP.1 Implementation representation of the TSF

Developer action elements :

ADV\_FSP.5.1D The developer shall provide a functional specification.

ADV\_FSP.5.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements :

ADV\_FSP.5.1C The functional specification shall completely represent the TSF.

ADV\_FSP.5.2C The functional specification shall describe the TSFI using a semi-formal style.

ADV\_FSP.5.3C The functional specification shall describe the purpose and method of use for all TSFI.

ADV\_FSP.5.4C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV\_FSP.5.5C The functional specification shall describe all actions associated with each TSFI.

ADV\_FSP.5.6C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV\_FSP.5.7C The functional specification shall describe all error messages that do not result from an invocation of a TSFI.

ADV\_FSP.5.8C The functional specification shall provide a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.

ADV\_FSP.5.9C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements :

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

ADV\_FSP.5.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

## **ADV\_IMP.2 Complete Mapping of the Implementation Representation of the TSF**

Dependencies :

ADV\_TDS.3 Basic modular design

ALC\_TAT.1 Well-defined development tools

ALC\_CMC.5 Advanced support

Developer action elements :

ADV\_IMP.2.1D The developer shall make available the implementation representation for the entire TSF.

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

Content and presentation elements: ADV\_IMP.2.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV\_IMP.2.2C The implementation representation shall be in the form used by the development personnel.

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

Evaluator action elements :

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

## **ADV\_TDS.4 Semiformal Modular Design**

Dependencies :

ADV\_FSP.5 Complete semi-formal functional specification with additional error information

Developer action elements :

ADV\_TDS.4.1D The developer shall provide the design of the TOE.

ADV\_TDS.4.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements :

ADV\_TDS.4.1C The design shall describe the structure of the TOE in terms of subsystems.

- ADV\_TDS.4.2C The design shall describe the TSF in terms of modules, designating each module as SFR-enforcing, SFR-supporting, or SFR-non-interfering.
- ADV\_TDS.4.3C The design shall identify all subsystems of the TSF.
- ADV\_TDS.4.4C The design shall provide a semiformal description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.
- ADV\_TDS.4.5C The design shall provide a description of the interactions among all subsystems of the TSF.
- ADV\_TDS.4.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.
- ADV\_TDS.4.7C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its purpose and relationship with other modules.
- ADV\_TDS.4.8C The design shall describe each SFR-enforcing and SFR-supporting module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing or SFR-supporting modules.
- ADV\_TDS.4.9C The design shall describe each SFR-non-interfering module in terms of its purpose and interaction with other modules.
- ADV\_TDS.4.10C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
- Evaluator action elements :ADV\_TDS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV\_TDS.4.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

## **ADV\_INT.2 Well-Structured Internals**

Dependencies :

- ADV\_IMP.1 implementation representation of the TSF
- ADV\_TDS.3 Basic modular design
- ALC\_TAT.1 Well-defined development tools

Developer action elements :

- ADV\_INT.2.1D The developer shall design and implement the entire TSF such that it has well-structured internals.
- ADV\_INT.2.2D The developer shall provide an internals description and justification.

Content and presentation elements :

- ADV\_INT.2.1C The justification shall describe the characteristics used to judge the meaning of “well-structured”.
- ADV\_INT.2.2C The TSF internals description shall demonstrate that the entire TSF is well-structured.

Evaluator action elements :

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

ADV\_INT.2.2E The evaluator shall perform an internal analysis on the TSF.

### 6.3.3 Guidance Documents

#### AGD\_OPE.1 Operational User Guidance

Dependencies :

ADV\_FSP.1 Basic functional specification

Developer action elements :

AGD\_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements : AGD\_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

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

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

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

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

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

AGD\_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements :

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

#### AGD\_PRE.1 Preparative Procedures

Dependencies : No dependencies.

Developer action elements :

AGD\_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements :



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

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

Evaluator action elements :

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

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

### 6.3.4 Lifecycle Support

#### ALC\_CMC.4 Production Support, Acceptance Procedures and Automation

Dependencies :

ALC\_CMS.1 TOE CM coverage

ALC\_DVS.1 Identification of security measures

ALC\_LCD.1 Developer defined life-cycle model

Developer action elements :

ALC\_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC\_CMC.4.2D The developer shall provide the CM documentation.

ALC\_CMC.4.3D The developer shall use a CM system.

Content and presentation elements :

ALC\_CMC.4.1C The TOE shall be labelled with its unique reference.

ALC\_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC\_CMC.4.3C The CM system shall uniquely identify all configuration items.

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

ALC\_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC\_CMC.4.6C The CM documentation shall include a CM plan.

ALC\_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

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

ALC\_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC\_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements :

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

### **ALC\_CMS.5 Development Tools CM Coverage**

Dependencies : No dependencies.

Developer action elements :

ALC\_CMS.5.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements :

ALC\_CMS.5.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information.

ALC\_CMS.5.2C The configuration list shall uniquely identify the configuration items.

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

Evaluator action elements :

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

### **ALC\_DEL.1 Delivery Procedures**

Dependencies : No dependencies.

Developer action elements :

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

ALC\_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements :

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

Evaluator action elements :

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

### **ALC\_DVS.2 Sufficiency of Security Measures**

Dependencies : No dependencies.

Developer action elements :

ALC\_DVS.2.1D The developer shall produce and provide development security documentation.

Content and presentation elements :

ALC\_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC\_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator action elements :

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

ALC\_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

### **ALC\_LCD.1 Developer Defined Life-Cycle Model**

Dependencies : No dependencies.

Developer action elements :

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

ALC\_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements :

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

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

Evaluator action elements :

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

### **ALC\_TAT.2 Compliance with Implementation Standards**

Dependencies :

ADV\_IMP.1 Implementation representation of the TSF

Developer action elements :

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

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

ALC\_TAT.2.3D The developer shall describe and provide the implementation standards that are being applied by the developer.

Content and presentation elements :

ALC\_TAT.2.1C Each development tool used for implementation shall be well-defined.

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

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

Evaluator action elements :

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

ALC\_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

### 6.3.5 Testing

#### ATE\_COV.2 Analysis of Coverage

Dependencies :

ADV\_FSP.2 Security-enforcing functional specification

ATE\_FUN.1 Functional testing

Developer action elements :

ATE\_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements :

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

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

Evaluator action elements :

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

#### ATE\_DPT.3 Testing: Modular Design

Dependencies :

ADV\_ARC.1 Security architecture description

ADV\_TDS.4 Semiformal modular design

ATE\_FUN.1 Functional testing

Developer action elements :

ATE\_DPT.3.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements :

ATE\_DPT.3.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems and modules in the TOE design.

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

ATE\_DPT.3.3C The analysis of the depth of testing shall demonstrate that all TSF modules in the TOE design have been tested.

Evaluator action elements :

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

### **ATE\_FUN.1 Functional Testing**

Dependencies :

ATE\_COV.1 Evidence of coverage

Developer action elements :

ATE\_FUN.1.1D The developer shall test the TSF and document the results.

ATE\_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements :

ATE\_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

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

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

ATE\_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements :

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

### **ATE\_IND.2 Independent Testing - Sample**

Dependencies :

ADV\_FSP.2 Security-enforcing functional specification

AGD\_OPE.1 Operational user guidance

AGD\_PRE.1 Preparative procedures

ATE\_COV.1 Evidence of coverage

ATE\_FUN.1 Functional testing

Developer action elements :

ATE\_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements :

ATE\_IND.2.1C The TOE shall be suitable for testing.

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

Evaluator action elements :

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

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

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

### 6.3.6 Vulnerability Analysis

#### AVA\_VAN.5 Advanced Methodical Vulnerability Analysis

Dependencies :

ADV\_ARC.1 Security architecture description

ADV\_FSP.4 Complete functional specification

ADV\_TDS.3 Basic modular design

ADV\_IMP.1 Implementation representation of the TSF

AGD\_OPE.1 Operational user guidance

AGD\_PRE.1 Preparative procedures

ATE\_DPT.1 Testing : basic design

Developer action elements :

AVA\_VAN.5.1D The developer shall provide the TOE for testing.

Content and presentation elements :

AVA\_VAN.5.1C The TOE shall be suitable for testing.

Evaluator action elements :

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

AVA\_VAN.5.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA\_VAN.5.3E The evaluator shall perform an independent, methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA\_VAN.5.4E The evaluator shall conduct penetration testing based on the identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by an attacker possessing High attack potential.

## **6.4 Security Requirements Rationale**

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

### **6.4.1 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 25 presents the mapping between the security objectives and the security functional requirements.

Table 25. Mappings between Security Objectives and Security Functional Requirements

Security Objectives Security Functional Requirements	TOE Security Objectives																
	O.Management	O.Personalization_Agent_Authentication	O.Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.BAC	O.EAC	O.AA	O.MCD_Authentication	O.MCD_Issuer_Authentication	O.MCD_Management	O.MCD_Access_Control	O.Secure_State
FCS_CKM.1(1)									X	X							
FCS_CKM.1(2)		X															
FCS_CKM.2(1)							X		X								
FCS_CKM.2(2)										X							
FCS_CKM.4							X										
FDP_ACC.1(1)								X									
FDP_ACF.1(1)	X		X						X	X	X						
FDP_DAU.1(1)												X					
FDP_RIP.1							X	X									
FDP_UCT.1					X			X									
FDP_UIT.1					X			X									
FIA_AFL.1(1)			X	X					X	X	X						
FIA_AFL.1(2)		X															
FIA_UAU.1(1)				X					X	X							
FIA_UAU.1(2)			X	X					X		X						
FIA_UAU.1(3)	X	X							X								
FIA_UAU.4		X						X		X	X						
FIA_UAU.5		X	X						X	X	X	X					
FIA_UID.1(1)		X								X	X						
FMT_MOF.1(1)	X								X								
FMT_MOF.1(2)	X					X			X								
FMT_MSA.1(1)						X			X								
FMT_MSA.3(1)	X								X								
FMT_MTD.1(1)	X								X								
FMT_MTD.1(2)			X														
FMT_MTD.1(3)	X								X								
FMT_MTD.1(4)	X								X								
FMT_MTD.3						X		X			X						
FMT_SMF.1(1)	X					X											
FMT_SMR.1(1)	X	X															



Security Objectives	TOE Security Objectives																
	O.Management	O.Personalization_Agent_Authentication	O.Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.BAC	O.EAC	O.AA	O.MCD_Authentication	O.MCD_Issuer_Authentication	O.MCD_Management	O.MCD_Access_Control	O.Secure_State
FPT_ITC.1					X												
FPT_ITI.1				X	X												
FDP_ACC.1(2)																X	
FDP_ACF.1(2)																X	
FDP_DAU.1(2)												X					
FDP_ETC.2																X	
FIA_AFL.1(3)													X				
FIA_UAU.1(4)													X				
FIA_UID.1(2)													X				
FMT_MSA.1(2)															X		
FMT_MSA.1(3)															X		
FMT_MSA.2															X		
FMT_MSA.3(2)															X		
FMT_SMF.1(2)															X		
FMT_SMR.1(2)													X	X			
FPT_FLS.1																	X
FPT_TST.1																	X

< Security Functional Requirements of ePassport >

**FCS\_CKM.1(1) Cryptographic Key Generation (Key Derivation Mechanism)**

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

**FCS\_CKM.1(2) Cryptographic Key Generation (Personalization Key Generation)**

This component requires generating the 112 bit TDES Personalization authentication key, Personalization SM Key and Personalization session key to support Personalization agent authentication method which provides an equivalent security level as BAC. Therefore, this component satisfies the security objective of O.Personalization\_Agent\_Authentication.

### **FCS\_CKM.2(1) Cryptographic Key Distribution (KDF Seed Distribution for BAC Session Key Generation)**

This component defines the method to distribute seed of key derivation mechanism necessary in generating the BAC session key to the Inspection System (ISO/IEC 11770-2 Key Establishment Mechanism 6).

The distribution method defined in this component satisfies the security objective of O.Replay\_Prevention as it uses random numbers and O.BAC as it enables to generate the BAC session key of FCS\_CKM.1(1) by generating KDF seed.

### **FCS\_CKM.2(2) Cryptographic Key Distribution (KDF Seed Distribution for EAC Session Key Generation)**

This component defines the method to distribute seed of key derivation mechanism necessary in generating the EAC session key to the Inspection System (DH key distribution protocol of PKCS#2, ECDH key distribution protocol of ISO/IEC 15946-3).

The distribution method defined in this component satisfies the security objective of O.EAC as it enables to generate EAC session key of FCS\_CKM.1(1) by generating KDF seed.

### **FCS\_CKM.4 Cryptographic Key Destruction**

This component satisfies the security objective of O.Deleting\_Residual\_Info as it provides the method of destroying the keys which are generated by the TSF in accordance with the key derivation mechanism of FCS\_CKM.1(1), FCS\_CKM.1(2) and remained in temporary memory.

### **FDP\_ACC.1(1) Subset Access Control (ePassport)**

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

The ePassport access control policies defined in this component satisfies the security objective of O.Access\_Control as it defines the Personalization Agent, BIS and EIS as subjects, the personal data and biometric data of the ePassport holder, ePassport authentication data, EF.CVCA and EF.COM, etc. as objects and their relationship as operations.

### **FDP\_ACF.1(1) Security Attribute based Access Control (ePassport)**

In order to enforce the ePassport access control policies, this component defines security attributes of subjects and objects defined in FDP\_ACC.1(1) and specifies the ePassport access control rules.

This component provides the method of managing the personal data of ePassport holder only to the authorized personalization agent by allowing write-rights for the personal data of the ePassport holder to the subject who has the issuing-authorization.. Therefore the security objective of O.Management is satisfied

This component satisfies the security objective of O.Access\_Control by providing access control functions as follows. The read-rights for the personal data of the ePassport holder and ePassport authentication data, etc. is allowed only to the subjects holding the BAC authorization and the read-rights for the biometric data of the ePassport holder is allowed only to the subjects holding the

EAC authorization. Read, write and delete operations on the object defined in FDP\_ACF.1(1) is allowed only to the subjects holding the personalization agent authorization and deleting is allowed when the Operational mode is Initialized. Also, this component denies accessing all the objects if the Operational mode does not allow the action.

This component satisfies the security objectives of O.BAC and O.EAC, because the read-rights for the personal data of the ePassport holder and ePassport authentication data, etc. is allowed only to the subjects holding the BAC authorization and the read-rights for the biometric data of the ePassport holder is allowed only to the subjects holding the EAC authorization.

The explicitly deny rules of FDP\_ACF.1.4 defined in this component satisfy the security objective of O.Security\_Mechanism\_Application\_Procedures because the application order of security mechanisms is ensured as access by the Inspection System is denied when the order of transmitted instructions specified in 2.1 Inspection Procedures of the EAC specifications is violated.

#### **FDP\_DAU.1(1) Basic Data Authentication (Active Authentication)**

This component provides BIS/EIS with a digital signature which is generated by signing the random number transmitted from Inspection System with uniquely assigned Active Authentication private key for ensuring the genuineness of MRTD chips, thus proves that the MRTD chip is genuine and satisfies the security objective of O.AA.

#### **FDP\_RIP.1 Subset Residual Information Protection**

This component ensures that previous information is not included when the TSF deallocates memory resources for the BAC session key, EAC session key, random numbers and Active Authentication Private Key.

This component satisfies the security objective of O.Deleting\_Residual\_Info as it ensures that previous information of the BAC session key, EAC session key, random numbers and Active Authentication Private Key is not available when destroying those keys according to the method of destruction defined in FCS\_CKM.4. Also, this component satisfies the security objective of O.Replay\_Prevention by ensuring that previous information of BAC session key, EAC session key, random numbers and Active Authentication Private Key is not available.

#### **FDP\_UCT.1 Basic Data Exchange Confidentiality**

This component defines the method to protect from disclosure when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies.

This component establishes the BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session encryption key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session encryption key. In addition, if personalization agent decides to apply secure messaging, this component establishes secure messaging by performing cryptographic operations for the user data of the ePassport which are transmitted to the TOE with the Personalization session key. Therefore confidentiality of the user data is ensured and the security objective of O.Secure\_Messaging is satisfied.

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

#### **FDP\_UIT.1 Data Exchange Integrity**

This component defines the method to protect from modification, deletion, insertion, replay when transmitting objects, such as the personal data and the biometric data of the ePassport holder within the scope of the ePassport access control policies.

This component establishes the BAC or EAC secure messaging by performing cryptographic operations for the personal data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the BAC session MAC key, or the biometric data of the ePassport holder, etc. transmitted between the TOE and the Inspection System with the EAC session MAC key.

In addition, if Personalization agent decides to apply secure messaging, this component generates MACs of user data with personalization agent session key which are transmitted to the TOE during writing user data of the ePassport, thus ensures integrity of user data and satisfies the security objective of O.Secure\_Messaging.

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

#### **FIA\_AFL.1(1) Authentication Failure Handling (Inspection System Authentication Failure)**

This component detects 1 unsuccessful BAC mutual authentication or EAC-TA attempt within a challenge and a single power-on session and requires to terminate a user session.

Session is terminated if BAC authentication fails within a single power-on session. EAC secure messaging established by successful EAC-CA is retained if EAC-TA fails within a single power-on session to protect data transmitted. Therefore the security objective of O.Session\_Management is satisfied.

This component satisfies the security objective of O.Security\_Mechanism\_Application\_Procedures since it disables the unauthorized external entity to move on to the next phase of inspection procedures by terminating session if the BAC mutual authentication fails.

The security objective of O.Access\_Control is satisfied because the access to user data is denied if BAC mutual authentication or EAC-TA fails.

In addition, this component satisfies the security objectives of O.BAC and O.EAC because accessing user data is denied by terminating session if BAC mutual authentication fails and secure messaging established by successful EAC-CA is retained if EAC-TA fails.

#### **FIA\_AFL.1 (2) Authentication Failure Handling (Personalization Agent Authentication Failure)**

This component requires to detect when 10 accumulated unsuccessful attempts of personalization agent authentication is reached and to change the Operational mode to Terminate.

This component satisfies the security objective of O.Personalization\_Agent\_Authentication as it denies any access to the TOE by changing the Operational mode to Terminated when 10 unsuccessful attempts related to personalization agent authentication are accumulated regardless of sessions.

Thus, this component provides an enhanced authentication failure handling method than BAC failure handling.

#### **FIA\_UAU.1(1) Timing of Authentication (BAC Mutual Authentication)**

This component defines the functions to be performed by BIS before the BAC mutual authentication when the Operational Mode of TSF is Personalized and requires the BAC mutual authentication for BIS.

In this component, the BAC mutual authentication is executed in order to enable the Inspection System identified in FIA\_UID.1 to execute the indication function to support the BAC mechanism and to read the personal data of the ePassport holder. This component satisfies the security objectives of O.Session\_Management, O.BAC and O.Access\_Control as it enables detection by FIA\_AFL.1, if the authentication fails and allows the read-rights for the personal data of the ePassport holder if the authentication succeeds.

#### **FIA\_UAU.1(2) Timing of Authentication (EAC-TA)**

This component defines the functions to be performed by EIS before the EAC-TA when the Operational Mode of TSF is Personalized and requires execution of the EAC-TA for EIS.

In this component, only the Inspection System of which the BAC mutual authentication succeeded in FIA\_UAU.1(1) can execute EAC-CA and reading of user data (exception of the biometric data of the ePassport holder). To read the biometric data of the ePassport holder, the EAC-TA shall be executed. This component satisfies the security objectives of O.Security\_Mechanism\_Application\_Procedures, O.Session\_Management, O.EAC and O.Access\_Control as it enables detection by FIA\_AFL.1(1) if authentication fails and allows the read-rights for the biometric data of the ePassport holder if authentication succeeds.

#### **FIA\_UAU.1(3) Timing of Authentication (Personalization Agent Authentication)**

This component defines the functions to be performed by personalization agent before the authorization when the Operational Mode of TSF is Initialized and requires the personalization agent authentication.

This component satisfies the security objective of O.Personalization\_Agent\_Authentication as it gives issuing authorization to the personalization agent by authenticating the system as not BIS but personalization agent with the method based on TDES which is similar to BAC provided by TSF. Also, the security objectives of O.Access\_Control and O.Management are satisfied as it enables authentication failure detection by FIA\_AFL.1(2), and retains the authorized personalization agent by giving the issuer authorization if authentication succeeds.

#### **FIA\_UAU.4 Single-Use Authentication Mechanisms**

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

This component satisfies the security objectives of O.Replay\_Prevention, O.BAC, O.EAC and O.Personalization Agent authentication as the TSF executes the BAC mutual authentication,

EAC-TA and Personalization Agent authentication by generating different random numbers used in the BAC mutual authentication and EAC-TA per session and transmitting them to the Inspection System.

#### **FIA\_UAU.5 Multiple Authentication Mechanisms**

This component defines multiple authentication mechanisms and the rules of applying authentication mechanism according to type of user data to be accessed by the Inspection System.

If the external entity is identified as personalization agent by applying personalization agent authentication mechanism, not with BAC or EAC-TA mechanism, object security attributes according to the Personalization agent issuing authorization are given. Also, it ensures that the user holds the personalization agent issuing authorization only if personalization agent authentication succeeds, thus the security objectives of O.Personalization\_Agent\_Authentication and O.Access\_Control are satisfied.

This component satisfies the security objectives of O.Security\_Mechanism\_Application\_Procedures, O.Access\_Control, O.BAC, O.EAC and O.AA as the Inspection System holds the BAC authorization by succeeding in BAC mutual authentication and the EAC authorization by succeeding in the EAC-CA, EAC-TA and certificate verification after the BAC mutual authentication according to authentication mechanism application rules and the Inspection System performs Active Authentication if it supports the mechanism.

#### **FIA\_UID.1(1) Timing of Identification (ePassport User Identification)**

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

The security objective of O.Personalization\_Agent\_Authentication is satisfied because this component identifies an external entity which requests to select the ePassport application after establishing the communication channel according to ISO/IEC 14443 as a personalization agent and provides the process to handle the personalization agent authentication request.

This component satisfies the security objectives of O.BAC and O.EAC as the external entity is identified with the Inspection System, if an external entity to establish the communication channel request to use the MRTD application.

#### **FMT\_MOF.1(1) Management of Security Functions Behavior (Suspending writing function)**

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

This component satisfies the security objectives of O.Management and O.Access\_Control by deactivating the writing function of the personalization agent in the Personalization phase so that the TOE in the Operational Use phase cannot record any data.

#### **FMT\_MOF.1(2) Management of Security Functions Behavior (Suspending EAC and Secure Messaging)**

This component defines that the ability to disable EAC and secure messaging of Personalization phase is given only to the personalization agent in the Personalization phase.

This component ensures that the TOE is managed securely by providing the method to disable EAC if DG3/DG4 is not used due to the issuing policy of the Personalization agent and the method to disable Secure Messaging only to the authorized personalization agent and denying the access to the DG3/DG4 when EAC is disabled. Therefore, this component satisfies the security objectives of O.Management and O.Access\_Control.

The security objective of O.Secure\_Messaging is satisfied because this component performs the functions defined in FDP\_UIT.1, FDP\_UCT.1, FPT\_ITI.1 and FPT\_ITC.1 when the personalization agent requests secure messaging in the Personalization phase and disables the functions only if the personalization agent does not request the secure messaging.

### **FMT\_MSA.1(1) Management of Security Attributes (ePassport)**

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

This component satisfies the security objectives of O.Secure\_Messaging and O.Access\_Control as the integrity is ensured and access to the MRTD application data is blocked by resetting the previously given security attributes of the personalization agent or the Inspection System as an action to be taken if the TSF detects modification of the transmitted TSF data.

### **FMT\_MSA.3(1) Static Attribute Initialization (MRTD Object Security Attributes)**

This component requires the TSF in place of personalization agent to specify initial values in order to restrict default values for security attributes when an object is created in Personalization phase.

This component satisfies the security objectives of O.Management and O.Access\_Control because initial values which are restricted to object security attributes defined FDA\_ACF.1(1) are specified by TSF in place of personalization agent when generating user data object and the means of management are provided by relating the initial values to the generated object when the authorized personalization agent requests to generate object.

### **FMT\_MTD.1(1) Management of TSF Data (Certificate Verification Information and Authentication Key)**

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

This component satisfies the security objectives of O.Management and O.Access\_Control by enabling only the authorized personalization agent to have the ability to write TSF data, such as the EAC chip authentication private key, initial current data, initial CVCA certificate, initial CVCA digital signature verification key and active authentication private key, etc., in secure memory in the Personalization phase

### **FMT\_MTD.1(2) Management of TSF Data (SSC Initialization)**

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

This component satisfies the security objective of O.Security\_Mechanism\_Application\_Procedures by initializing SSC (send sequence counter) to '0' in order to terminate the BAC secure messaging after generating the EAC session key and newly establishing the EAC secure messaging.

#### **FMT\_MTD.1(3) Management of TSF Data (Operational Mode Management)**

This component restricts that only the personalization agent queries and updates the Operational Mode of TSF.

This component provides means to query and update Operational Mode only to the authorized personalization agent for managing allowed command list based on Operational Mode. Therefore this component satisfies the security objective of O.Management and O.Access\_Control.

#### **FMT\_MTD.1(4) Management of TSF Data (Generating and Storing BAC Authentication Key)**

This component restricts that TSF in place of authorized personalization agent generates and stores BAC authentication key.

This component satisfies the security objectives of O.Management and O.Access\_Control because the means to manage TSF data are provided as generating BAC authentication key by TSF when personalization agent request to write DG1 and TSF data for BAC mutual authentication to give BIS BAC authorization are managed.

#### **FMT\_MTD.3 Secure TSF Data**

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

This component satisfies the security objective of O.Replay\_Prevention because only the secure random numbers are used in order to prevent a replay attack when the TSF generates session key or performs AA security mechanism.

Also, the TSF compares the CVCA link certificate provided by the Inspection System with the CVCA certificate stored in the TOE in order for verification of the IS certificate used in the EAC-TA. If the CVCA certificate update is necessary, the TSF internally updates the CVCA certificate, CVCA digital signature verification key, current dates and EF.CVCA, therefore maintains the TSF data as secure values. This component satisfies the security objectives of O.Certificate\_Verification and O.EAC because the EAC-TA can be successfully executed by verifying the DV certificate and IS certificate with the secure CVCA certificate.

#### **FMT\_SMF.1(1) Specification of Management Functions (ePassport Security Management)**

This component satisfies the security objective of O.Management as it provides the method to write initial personalization key or personalization key and to disable EAC in manufacturing or personalization phase.

The security objective of O.Management is satisfied as it defines the writing function of user data and TSF data in the Personalization phase.



Also, this component satisfies the security objective of O.Certificate\_Verification as it provides the function for the TSF to update the CVCA certificate, the CVCA digital signature verification key and current dates, etc. by itself in the Operational Use phase.

#### **FMT\_SMR.1(1) Security Roles (Personalization Agent)**

This component defines the role of the personalization agent to manage the ePassport application data.

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

This component defines the role of personalization agent and relates it to the authorized user according to FIA\_UAU.1(3), thus satisfies the security objective of O.Personalization\_Agent\_Authentication.

#### **FPT\_ITC.1 Inter-TSF Confidentiality during Transmission**

This component defines the behavior of Inter-TSF confidentiality during transmission.

This component satisfies the security objective of O.Secure\_Messaging as it performs the management behavior as specified in FMT\_MSA.1(1) by encrypting TSF data while sending them and decrypts TSF data while receiving them in the personalization and operational use phase

#### **FPT\_ITI.1 Inter-TSF Detection of Modification**

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

This component satisfies the security objectives of O.Secure\_Messaging and O.Session\_Management by detecting modification of the transmitted TSF data in the Personalization and Operational Use phases and by performing an action to be taken, such as terminating the related communication channels, deleting the related session key and management actions specified in FMT\_MSA.1, etc., if modifications are detected.

### **< Security Functional Requirements of MULTOS >**

#### **FDP\_ACC.1(2) Subset Access Control (MULTOS)**

This component defines list of subjects, objects and operations in order to decide a scope of control for the ALU access control policies performed by the MCD Issuer.

This component satisfies the security objective of O.MCD\_Access\_Control as it decides a scope of control by defining the subjects (process which takes the role of the MCD Issuer), objects (MULTOS application) and operations (Loading, executing and deleting).

#### **FDP\_ACF.1(2) Security Attribute based Access Control (MULTOS)**

In order to enforce the process which takes the role of the MCD Issuer to perform access control on ALU, this component defines security attributes of subjects and objects defined in FDP\_ACC.1(2) and specifies the access control rules.

This component satisfies the security objective of O.MCD\_Access\_Control because the subjects and objects security attributes of MULTOS access control are defined according to FDP\_ACC.1(2) and it allows/denies access by defining access control rules of loading/executing/deleting ALU for the MCD Issuer based on the defined subjects and objects.

#### **FDP\_DAU.1(2) Basic Data Authentication (MCD Authentication)**

This component requires that it shall be proved to the MCD Issuer that MCD owns TSF data which are injected by the MCD Issuer in the manufacturing phase.

This component satisfies the security objective of O.MCD\_Authentication as it proves to the MCD Issuer that MCD has TSF data injected in the manufacturing phase to confirm the validity of key information required for proving the integrity of TSF execution code.

#### **FDP\_ETC.2 Export of User Data with Security Attributes**

This component requires to export user data with part of MULTOS security attributes to ensure MULTOS access control policies.

The MCD Issuer selects the MULTOS application to be loaded/deleted and loads/deletes the appropriate MULTOS application. This component enables the MCD Issuer to load/delete the selected MULTOS application by providing security attributes such as MCD Permission, KTU encryption public key, MCD public key certificate to the external entity. Therefore, this component satisfies the security objective of O.MCD\_Access\_Control.

#### **FIA\_AFL.1 (3) Authentication Failure Handling (MCD Issuer Authentication Failure)**

This component enforces to detect when 10 accumulated unsuccessful attempts related to the MCD Issuer authentication is surpassed and disable MCD permanently.

This component satisfies the security objective of O.MCD\_Issuer\_Authentication as it disables MCD permanently when 10 unsuccessful the MCD Issuer authentication attempts are accumulated.

#### **FIA\_UAU.1(4) Timing of Authentication (MCD Issuer Authentication)**

This component requires the MCD Issuer identified according to FIA\_UID.1(2) to perform the MCD Issuer authentication by MCD enablement.

This component allows MCD authentication before authenticating the MCD Issuer that the MCD Issuer first authenticates TOE and TSF authenticates the MCD Issuer. The MCD Issuer authentication is indirectly performed by proof of possession.

This component performs the MCD Issuer authentication indirectly by proof of possession that the MCD Issuer first authenticates TOE and TSF authenticate the MCD Issuer by allowing MCD authentication prior to the MCD Issuer authentication.

#### **FIA\_UID.1(2) Timing of Identification (MCD Issuer Identification)**

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

This component supports the MCD Issuer authentication by requesting the identification of the user as the MCD Issuer. The identification is performed with the MCD Issuer authentication method selected by the user before authenticating the user to the MCD Issuer. Therefore, the component satisfied the security objective of O.MCD\_Issuer\_Authentication.

#### **FMT\_MSA.1(2) Management of Security Attributes (MSM\_CD)**

This component requires to restrict the ability of setting subject security attributes defined in FDP\_ACF.1(2) only to the MCD Issuer as an action to be taken during MULTOS enablement to force MULTOS access control policies.

This component satisfies the security objective of O.MCD\_Management as it provides the means for setting security attributes such as MCD Permission, KTU encryption public key to the MCD Issuer in accordance with FMT\_SMR.1(2).

#### **FMT\_MSA.1(3) Management of Security Attributes (ALC, ADC Certificate Verification)**

This component requires to restrict the ability of verifying security attributes of ALC and ADC only to the MCD Issuer as an action to be taken if application is loaded or deleted according to MULTOS access control policies.

This component satisfies the security objective of O.MCD\_Management as it ensures that the means to verify ALC and ADC certificates with kck\_pk defined as MULTOS access control security attribute are provided to the MCD Issuer in accordance with FMT\_SMR.1(2).

#### **FMT\_MSA.2 Secure Security Attributes**

This component ensures that TSF shall verify ALD and ADC with the MCD Issuer public key according to MULTOS access control policies.

This component satisfies the security objective of O.MCD\_Management as it only allows that secure values are accepted for ALC and ADC. This is achieved by verifying correctness of the certificate, such as Permission accordance, certificate format, etc.

#### **FMT\_MSA.3(2) Static Attribute Initialization (MULTOS Security Attributes)**

This component requires the MCD Issuer to specify optional initial values in order to restrict default values of the security attributes according to MULTOS access control policies when loading or deleting applications on MCD.

ALU security attributes are implemented with ADC and ALC App Permission provided by the MCD Issuer as ALU security attributes in accordance with FMT\_SMR.1(2). This component satisfies the security objective of O.MCD\_Management as it provides functions to manage MULTOS access control security attributes by implementing ALU security attributes.

#### **FMT\_SMF.1(2) Specification of Management Functions (MCD Management)**

This component enforces TSF to perform ALC or ADC verification and subject security attributes management defined in FDP\_ACF.1(2)

This component satisfies O.MCD\_Management as it provides the means to manage security attributes of subjects and objects that are the scope of access control.

#### **FMT\_SMR.1(2) Security Roles (MCD Issuer)**

This component defines the role of the MCD Issuer to manage the MCD.

This component provides the means for MCD management as it relates the authorized user by the MCD Issuer authentication defined in FIA\_UAU.1(4) to the security role of the MCD Issuer. Therefore this component satisfies the security objective of O.MCD\_Issuer\_Authentication and O.MCD\_Management

### **<Common Security Functional Requirements of TSF>**

#### **FPT\_FLS.1 Failure with Preservation of Secure State**

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

This component satisfies the security objective of O.Secure\_State as it preserves a secure state to prevent the malfunction of the TSF when the modification of integrity of the TSF data or TSF is detected; the randomness-test failure detected from the self-testing of FPT\_TST.1 or the IC chip detects abnormal operating conditions.

#### **FPT\_TST.1 TSF Testing**

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

This component runs self randomness-test on random numbers generated by IC chip to ensure the security of random number during initial start-up, thus preserves a secure state of TOE. Also, this component preserves a secure state providing the tools to verify the integrity of TSF and parts of TSF data. Therefore the security objective of O.Secure\_State is satisfied.

## **6.4.2 Security Assurance Rationale**

The security assurance level of this ST is selected as EAL5+(ADV\_IMP.2) considering the asset value and threat level which TOE protects, and ALC\_DVS.2 and AVA\_VAN.5 are augmented as well considering the security scheme of the open platform operating system, MULTOS. This sections describes the reason why EAL5+ is selected and the rationale for the augmented components to the EAL5 assurance level.

### **Rationale of the EAL5 Assurance Level**

The EAL5 assurance package requires semi-formal design and test while EAL4 requires systematic design, test and review

EAL5 allows a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

TOE has been developed with the intention of being used in domestic area and overseas as well, thus are forced to provide high level security independently assured by planned development. And some personalization agents require highly strict application of a development method based on security engineering to the TOE. Therefore the TOE and this ST are designed to follow EAL5 to satisfy all these cases.

#### **Rationale of the Augmented Components to the EAL5 Assurance Level**

This ST selected EAL5 which is wholly higher than PP that partially selected higher assurance component that EAL4, and then partially selected assurance components that are higher than EAL5. The rationale of the augmented with assurance components are 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**

The TOE is an operating system and application program operated in the MRTD chip. Therefore, it largely depends on the IC chip in terms of cryptographic operation function and physical security. To ensure the secure MRTD chip, the reliability and secure operation of not only the TOE, but also the IC chip must be verified. The TOE is developed by using publicly available standard implementation specifications. Therefore, it is easy to obtain information related to design and operation of the TOE. Also, TOE is easily accessed as it is used in open environment and it is difficult to trace an attack. However, it requires verifying the security of the ePassport IC chip as a whole though since the IC chip is not included in the scope of the TOE, it does not require understanding on hardware structure and advanced specialized equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing high attack potential. AVA\_VAN.4 is augmented to PP considering execution of systematic vulnerability analysis and resistant to attackers possessing moderate attack potential. However, with high probability, ePassport can be a target to attack by threat agent possessing high attack potential like a huge gangsters as it is an identification document used worldwide, therefore independent and advanced evaluation and verification is augmented to counter these threat and it follows that AVA\_VAN.5 is augmented with the appropriate assistance from the security functionality of the underlying IC chip .

It is difficult to correct of defects even if defects are occurred after issuing the ePassport loaded with the IC chip and this may be exploited by attackers. Therefore, ADV\_IMP.2 is augmented to analyze

completely in order to check if the TSF is accurately implemented and defect code does not exist, and ALC\_DVS.2 is augmented to assure high level development security in terms of physical, procedural, personal, and other security measures in the phase of development based on MULTOS.

### 6.4.3 Rationale of Dependency

#### < Dependency of TOE Security Functional Requirements >

Table 26 shows dependency of TOE functional components.

Table 26. Dependency of TOE Functional Components

No.	SFR of ST	Dependency as specified by CC Part 2	Dependency of ST (Refer to Column 1)
1	FCS_CKM.1(1)	[FCS_CKM.2 and FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	3,4 5
2	FCS_CKM.1(2)	[FCS_CKM.2 and FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	None 5
3	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 5
4	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 5
5	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.1]	1,2
6	FDP_ACC.1(1)	FDP_ACF.1	7
7	FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	6 23
8	FDP_DAU.1(1)	-	-
9	FDP_RIP.1	-	-
10	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	None 6
11	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	6 None
12	FIA_AFL.1(1)	FIA_UAU.1	14,15
13	FIA_AFL.1(2)	FIA_UAU.1	16
14	FIA_UAU.1(1)	FIA_UID.1	19
15	FIA_UAU.1(2)	FIA_UID.1	14
16	FIA_UAU.1(3)	FIA_UID.1	19
17	FIA_UAU.4	-	-
18	FIA_UAU.5	-	-
19	FIA_UID.1(1)	-	-
20	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	29 30
21	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	29 30
22	FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	6 29 30
23	FMT_MSA.3(1)	FMT_MSA.1	22 30

No.	SFR of ST	Dependency as specified by CC Part 2	Dependency of ST (Refer to Column 1)
		FMT_SMR.1	
24	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	29 30
25	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	29 30
26	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	29 30
27	FMT_MTD.1(4)	FMT_SMF.1 FMT_SMR.1	29 30
28	FMT_MTD.3	FMT_MTD.1	24
29	FMT_SMF.1(1)	-	-
30	FMT_SMR.1(1)	FIA_UID.1	19
31	FPT_ITC.1	-	-
32	FPT_ITI.1	-	-
33	FDP_ACC.1(2)	FDP_ACF.1	34
34	FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	33 43
35	FDP_DAU.1(2)	-	-
36	FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	33
37	FIA_AFL.1(3)	FIA_UAU.1	38
38	FIA_UAU.1(4)	FIA_UID.1	39
39	FIA_UID.1(2)	-	-
40	FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	33 44 45
41	FMT_MSA.1(3)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	33 44 45
42	FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	33 41 45
43	FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	41 45
44	FMT_SMF.1(2)	-	-
45	FMT_SMR.1(2)	FID_UID.1	39
46	FPT_FLS.1	-	-
47	FPT_TST.1	-	-

Security functional components such as FDP\_UCT.1, FDP\_UIT, FIA\_UAU.1(2) that does not meet dependency accept the rationale of dependency of the PP. That is, FDP\_UCT.1 and FDP\_UIT.1 have dependency with FTP\_ITC.1 or FTP\_TRP.1, but it is not included. FDP\_UCT.1 and FDP\_UIT.1 require secure messaging between inspection system and TOE. Since the secure messaging between both is the unique channel, it is not necessary to be logically separated from other communicational channels. Therefore, in this ST, requirements of FTP\_ITC.1 are not defined as in the PP.

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

Among augmented security functional components in ST, FCS\_CKM.1(2) does not meet the dependency. Since personalization agent can generate an identical key by exchanging random number based on the previously distributed issuing key in the manufacturing phase according to the pre-defined scheme by TOE, it is not necessary to distribute personalization authentication key and session key. Therefore, in this ST, FCS\_CKM.2 to require cryptographic key distribution is not required.

< **Dependency of TOE Security Assurance Requirements** >

The dependency of EAL5 provided in Common Criteria is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in Table 27. Dependency of the Augmented Assurance Component.

ADV\_IMP.2 shall have dependency with ALC\_CMC.5 but, ADV\_IMP.2 is augmented to enable analysis on the entire implementation representation in order to check if the TSF is accurately implemented and defect code does not exist. And since the configuration management at ALC\_CMC.5 level which provides automated measure to identify if the changes in configuration items affect other configuration items is determined to be not necessarily required and thus not augmented into the PP. Therefore, this ST follows PP as it selected.

AVA\_VLA.5 has dependency with ADV\_FSP.2, ADV\_IMP.1 and ATE\_DPT.1. This is satisfied by ADV\_FSP.4, ADV\_IMP.2 and ATE\_DPT.3 in hierarchical relationship with ADV\_FSP.2, ADV\_IMP.1 and ATE\_DPT.1.

Table 27. Dependency of the Augmented Assurance Component

No	Assurance Component	Dependency	Ref. No.
1	ADV_IMP.2	ADV_TDS.3 ALC_TAT.1 ALC_CMC.5	EAL4 EAL4 None
2	ALC_DVS.2	None	-
3	ATE_DPT.3	ADV_ARC.1 ADV_TDS.4 ATE_FUN.1	EAL5 EAL5 EAL5



4	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 3
---	-----------	---	--

#### 6.4.4 Rationale of Mutual Support and Internal Consistency

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

In 6.4.3 ‘Dependency of TOE security functional requirements’ and ‘Dependency of TOE security assurance requirements’, the dependency is analyzed as a supportive relationship among security requirements of which it is necessary to depend on other security requirements in order to achieve a security objective because a security requirement is insufficient. In case the dependency was not satisfied, additional rationale is provided.

In the manufacturing phase, the MCD Issuer performs MCD authentication (FMT\_MSA.1(2), FMT\_MSA.3(2), FDP\_DAU.1(2)) and loads applications or deletes applications if necessary in accordance with issuing policies of The personalization agent (FMT\_MSA.1(3), FMT\_MSA.2, FMT\_SMF.1(2)) using initialized static attributes. The role of the MCD Issuer as such is defined as the security role (FMT\_SMR.1(2)) and is controlled by the open platform OS, MULTOS, access control policies(FDP\_ACC.1(2), FDP\_ACF.1(2), FDP\_ETC.2), when the MCD Issuer is identified(FIA\_UID.1(2)), MCD Issuer authentication(FIA\_UAU.1(4)) is conducted, and if the authentication results in failure 10 times cumulatively regardless of the session, the MCD shall be disabled permanently(FIA\_AFL.1(3)). Therefore, these security requirements are mutually supportive and internally consistent.

In the personalization phase, TSF performs ePassport personalization agent authentication (FIA\_UAU.1(3)). TSF changes the operational mode into ‘Terminated’ if the authentication fails 10 times cumulatively regardless of the session(FIA\_AFL.1(2)). The authentication relevant data used in the ePassport personalization agent authentication procedure shall use random number to prevent replay attack(FIA\_UAU.4) Once succeeding in authentication, the ePassport personalization agent records the ePassport application data (FMT\_MTD.1(1)), when TSF enforces to initialize the security attributes (FMT\_MSA.3(1)) of operation and access right of specified objects and generate BAC authentication key to store (FMT\_MTD.1(4)) on behalf of The personalization agent in the personalization phase. ePassport personalization agent can prevent all the TSF data from unauthorized disclosure during transmission in the personalization phase (FPT\_ITC.1) and can detect integrity inconsistency of the transmitted TSF data(FPT\_ITI.1). ePassport personalization agent can deactivate EAC functionality in accordance with the personalization policy and also deactivate secure messaging during personalization in case the physical, personal, procedural security measures are in operation equivalent to the secure messaging during personalization(FMT\_MOF.1(2)). ePassport personalization agent deactivates writing function so that the TOE is not modified by external entities when delivering the TOE to the operational use phase(FMT\_MOF.1(1), FMT\_SMF.1). The role of The personalization agent as such is defined as the security role (FMT\_SMR.1(1)) and is controlled by the

ePassport access control policies (FDP\_ACC.1(1), FDP\_ACF.1(1)). Therefore, these security requirements are mutually supportive and internally consistent.

The TSF, after identifying the inspection system (FIA\_UID.1(1)), executes the BAC mutual authentication (FIA\_UAU.1(1)) and the EAC-TA (FIA\_UAU.1(2)) according to authentication mechanism application rules (FIA\_UAU.5). If the Inspection System fails in authentication, the session shall be terminated (FIA\_AFL.1(1)). The random numbers must be used to prevent reuse of authentication-relevant data used in authentication (FIA\_UAU.4). In order to ensure the secure random numbers shall be used and the secure certificates shall be used in the EAC-TA, the certificates must be verified and updated (FMT\_MTD.3). Therefore, these security requirements are mutually supportive and internally consistent.

In the personalization phase, ePassport personalization agent queries and changes (FMT\_MTD.1(3)), and enforces to initialize the security attributes (FMT\_MSA.3(1)) of operation and access right of specified objects on behalf of The personalization agent in the personalization phase. Therefore, these security requirements are mutually supportive and internally consistent.

The TSF must initialize SSC to 0 (FMT\_MTD.1(2)) in order to indicate the channel termination when terminating the BAC secure messaging (FDP\_UCT.1 and FDP\_UIT.1) established in order to protect the transmitted user data. Therefore, these security requirements are mutually supportive and internally consistent.

IC Chip provides the security function to prevent that physical phenomena of current, voltage and electromagnetic waves, etc. occurred when the TSF performs cryptographic operations are not exploited by the threat agents ((FCS\_COP.1(1), FCS\_COP.1(2), FCS\_COP.1(4)), FPR\_UNO.1). The cryptographic-related data created in temporary memory after cryptographic operations must be destroyed to prevent reuse (FCS\_CKM.4, FDP\_RIP.1). Therefore, these security requirements are mutually supportive and internally consistent.

TSF shall prevent all the TSF data from unauthorized disclosure during transmission in the operational use phase (FPT\_ITC.1) and terminate session (FPT\_ITI.1) and reset the access right of the inspection system(FMT\_MSA.1(1)) once detecting integrity inconsistency of the transmitted TSF data. Therefore, these security requirements are mutually supportive and internally consistent.

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

## 7 TOE Summary Specification

This section shows TOE security functions to satisfy TOE security functional requirements, and defines TOE assurance measure to satisfy TOE assurance requirements. Detailed content of TSF will be described in TOE specification.

### 7.1 TOE Security Function

This Section describes Security Function supported by TOE to satisfy Security Functional Requirements defined in '5.1 TOE Security Functional Requirements'. TOE is composed of 10 subsystems like

Table 28 Countermeasure against TOE Subsystem & SFRs and these subsystems satisfy Security Functional Requirements by associated action.

TOE is composed of the following 3 layers.

- Hardware Abstraction Layer
- Extended MULTOS Layer
- Application Layer

### **Hardware Abstraction Layer**

DS controls underlying IC chip functions directly and it is a subsystem which executes Hardware Abstraction Layer's movement. DS is composed of components (module group) like SS(Start-up & Shutdown), IO(Input & Output), HW(Hardware Driver), CR(Command Router).

### **Extended MULTOS Layer**

It is a layer which executes most of TOE's logical functions and it is composed of MULTOS layer which execute normal MULTOS functions and ePassport Layer which moved ePassport specific functions from EEPROM to ROM. MULTOS Layer is composed of Core service subsystem which supplies MM, CF, US and a subsystem which executes external interface like AM, CH. ePassport Layer is composed of type of subsystems like SS, IA, SM which handle external interface through ER

### **Application Layer**

It is a part of ER subsystem and composed of LDS applications. It is physically added to EEPROM area by MULTOS application load command. After loading, it saves ePassport's TSF Data and calls code which executes ePassport Security Function through Interface with lower layers.

Table 28 Countermeasure against TOE Subsystem & SFRs

Subsystem SFR	ER	SS	IA	SM	AM	CH	MM	CF	US	DS
FCS_CKM.1(1)		O	O							
FCS_CKM.1(2)			O							
FCS_CKM.2(1)			O	O						
FCS_CKM.2(2)			O							
FCS_CKM.4		O	O							
FDP_ACC.1(1)	O	O								
FDP_ACF.1(1)	O	O								
FDP_DAU.1(1)			O							
FDP_RIP.1		O	O							
FDP_UCT.1	O			O						
FDP_UIT.1	O			O						
FIA_AFL.1(1)			O							
FIA_AFL.1(2)			O							
FIA_UAU.1(1)	O		O	O						
FIA_UAU.1(2)	O		O					O		
FIA_UAU.1(3)	O		O							
FIA_UAU.4			O					O		
FIA_UAU.5			O							
FIA_UID.1(1)	O									
FMT_MOF.1(1)		O								
FMT_MOF.1(2)	O	O								
FMT_MSA.1(1)			O							
FMT_MSA.3(1)		O								
FMT_MTD.1(1)		O	O							
FMT_MTD.1(2)			O							
FMT_MTD.1(3)		O	O							
FMT_MTD.1(4)		O								
FMT_MTD.3		O	O					O		
FMT_SMF.1(1)	O	O	O							
FMT_SMR.1(1)		O	O							
FPT_ITC.1	O			O						
FPT_ITI.1	O		O	O						
FDP_ACC.1(2)					O	O	O			
FDP_ACF.1(2)					O	O	O			
FDP_DAU.1(2)						O				
FDP_ETC.2						O			O	
FIA_AFL.1(3)						O				
FIA_UAU.1(4)						O				
FIA_UID.1(2)										O
FMT_MSA.1(2)						O				
FMT_MSA.1(3)						O	O			
FMT_MSA.2						O				
FMT_MSA.3(2)						O	O			
FMT_SMF.1(2)						O				
FMT_SMR.1(2)						O				
FPT_FLS.1					O			O		O
FPT_TST.1	O		O	O		O	O	O		O

(O:SFR-enforcing, △:SFR-supporting, Others: SFR-non-interfering)

The following shows subsystem's role to supply ePassport related security characteristics.

- ePassport personalization agent certification and authentication key/session key generation  
ER calls IA to execute ePassport personalization agent certificate mechanism by identifying user. IA checks certification failed count and stops certification process and make operational mode to Termination if the accumulated certification failed count is over.  
IA generates personalization agent's authentication key from personalization key by support of CF and generates data to verify the certification data from personalization agent's authentication key.  
IA defines whether success or failure by comparing certification data from DS with data from CF with a support of US.  
IA generates personalization agent's session key from personalization key by support of CF and record in temporary memory area requires DS to use personalization agent's session key when external IT subject requires personalization agent's secure channel and SM controls it.
- ePassport User Data personalization  
ER calls subsystem according to the kind of personalization target's data after checks ePassport personalization agent's subject authority.  
SS calls CF to record CVCA public key to EEPROM and verify certificate signature about CVCA public key. SS records information needed for verifying certificate chain like CVCA public key.  
SS records active authentication private key, EAC-CA chip certificate private key, personalization key with a support of DS.  
SS records ePassport user data to EEPROM as the ePassport access control rule by support of DS. When DG1 is recorded in EEPROM, MRZ is generated from recorded value and BAC authentication key is generated with a support of CF.  
SS controls operational mode to supply command access control functions based on operational mode.
- BAC authentication and ePassport reading  
ER calls IA by applying authentication rule and execute BAC mutual authentication mechanism to authenticate BIS by identifying user.  
IA authenticates BIS by realizing BAC authentication mechanism specified in ePassport standard with a support of CF. If authentication is succeeded, set BIS subject authority to BAC authority with a support of DS. And generate BAC session key for the BAC secure channel.  
SS searches files required for the permission of BIS reading authority of ePassport owner's basic information from file table and checks BA authority of DG file. If BAC authority is agreed then required length of data will be transmitted to outside via DS.
- Active authentication  
AA defines whether support AA or not by checking existence of active authentication public key from DG15 by support of SS. IA requires CF random number for AA realization. IA

receive SHA1 calculation result from CF and requires generation of RSA based signature to organize AA authentication data. IA transmit RSA based signature to outside via DS.

- EAC-CA

IA realizes BIS standard EAC-CA mechanism and supports Inspection system. And generates EAC session key for the EAC secure channel and initializes SSC by support of CF.

- EAC-TA and biometrics reading

ER calls IA by applying authentication rule and executes EAC-TA mechanism to identify user and authenticate EIS by .

IA authenticates EIS by realizing BIS standard specified EAC authentication mechanism by support of CF.

IA executes certificate construction analysis by support of US and establish CVCA public key or DV public key for the certificate chain verification. IA verifies certificate signature by using established public key and by support of CF. If verification of the signature is succeeded then read access authority for the DG3/DG4 included in certificate and establish EAC subject authority. If certificate type is link certificate then update CVCA public key and current date by support of DS.

If EAC authentication is succeeded, IA establishes EIS subject authority to EAC authority by support of DS. If not initialize subject authority setting to prevent access for the DG3/DG4 and maintain EAC secure channel.

SS searches files required for the permission of EIS reading authority of ePassport owner's bio information from file table and checks EAC authentication is succeeded and DG3/DG4 access authority is included in certificate. If EAC authority is agreed then required length of DG3/DG4 data will be transmitted to outside via DS.

The following shows subsystem's role to supply MULTOS related security characteristics.

- MCD Authentication

CH generates proving data possible to authenticate the ownership for the key information by support of CF's A\_Hash operation to authenticate MCD has tkf(TSF key information for integrity verification) from Security Data and transmit to outside via DS.

- The MCD Issuer authentication and subject security attribute setting.

CH authenticates the MCD Issuer by means of symmetric key crypto which is same security level with TDES by support of CF. CF calculates A\_Hash and call US to compare with value transmitted from the MCD Issuer. CH receives data verification result about US from CF and estimates whether the authentication was succeeded or failed

If authentication is failed, then increase authentication failure number and inspect authentication fail reaction condition. If the condition is satisfied, inactivate MCD permanently.

If authentication is succeeded then CH sets the MCD Issuer 's subject attribute by support of DS' EEPROM write function.

- MULTOS Access Control and Security Attribute Management.

CH inspects free space by support of MM to load MULTOS Application and checks MCD subject's security attribute is included in MULTOS Application security attribute.

CH verifies ALC signature by support of CF and if it is Protected ALU then verifies ALU signature with ALC's public key by support of CF.

If it is Confidential ALU then CH decrypt MULTOS Application Code and Data with crypto key from KTU decrypt by support of CF and save to EEPROM by support of DS.

CH confirms MCD subject's security attribute is included in MULTOS Application security attribute to delete MULTOS Application and verify ADC signature and delete that MULTOS Application from EEPROM by support of DS.

CH finds, select and activates MULTOS Application's executive code and data to run MULTOS Application and protect from other MULTOS Application's interference.

The following shows subsystem's role to supply common related security characteristics.

- Secure start-up and IC chip's security characteristic use
  - If electric power is connected, DS checks former shutdown status and if there was a abnormal shutdown then transmit failure message and stop execution
  - DS establishes register value required to use IC chip's security characteristic during initializing module for the communication channel generation.
  - DS verifies security of random number used for ePassport security mechanism.
- TSF secure operation guarantee
  - CH and CF supply integrity verification method for TSF during MCD certificate process.
  - SS supplies integrity verification method for TSF Data during personalization.
  - If randomness verification of RNG output was failed, then CF maintains secure status by making DS stop TSF execution.
  - If transmitted TSF Data integrity verification was failed. then SS maintains secure status by making DS stop TSF execution to DS.
  - If IC chip detects abnormal execution environment, then DS maintains secure status by stopping TSF execution.

## 7.2 Assurance Measures

This section defines assurance measures which is required in accordance with EAL5+ TOE security assurance requirement. The augmented assurance requirements are ADV\_IMP.2, ALC\_DVS.2, and AVA\_VAN.5.

The assurance measures will be provided as specified in the following table.

Table 29. TOE Assurance Measures

Assurance Class	Assurance Component	Assurance Measure
Security Objectives Specifications	ASE_INT.1	SP20-ASE-001 & attached
	ASE_CCL.1	SP20-ASE-001 & attached



Evaluation	ASE_SPD.1	SP20-ASE-001 & attached
	ASE_OBJ.2	SP20-ASE-001 & attached
	ASE_ECD.1	SP20-ASE-001 & attached
	ASE_REQ.2	SP20-ASE-001 & attached
	ASE_TSS.1	SP20-ASE-001 & attached
Development	ADV_ARC.1	SP20-ADV-001 & attached
	ADV_FSP.5	SP20-ADV-011 & attached
	ADV_IMP.2	SP20-ADV-021 & attached
	ADV_TDS.4	SP20-ADV-041 & attached
	ADV_INT.2	SP20-ADV-031 & attached
Guidance Documents	AGD_OPE.1	SP20-AGD-001 ~ 004 & attached
	AGD_PRE.1	SP20-AGD-001 ~ 004 & attached SP20-ALC-001 & attached
Lifecycle Support	ALC_CMC.4	SP20-ALC-001 & attached
	ALC_CMS.5	SP20-ALC-001 & attached
	ALC_DEL.1	SP20-ALC-001 & attached
	ALC_DVS.2	SP20-ALC-001 & attached
	ALC_LCD.1	SP20-ALC-001 & attached
	ALC_TAT.2	SP20-ALC-001 & attached
Tests	ATE_COV.2	SP20-ATE-001 & attached
	ATE_DPT.3	SP20-ATE-001 & attached
	ATE_FUN.1	SP20-ATE-001 & attached
	ATE_IND.2	ePassport sample, Emulation board, Test Tool
Vulnerability Assessment	AVA_VAN.5	SP20-AVA-001 ePassport sample, Emulation board, Test Tool

## 8 References

- [1] ePassport Protection Profile V2.1, National Intelligence Service , KECS-PP-0163a-2009, 2010-06-10
- [2] Common Criteria for Information Protection System, Ministry of Public Administration and Security, 2009-52
- [3] Evaluation and Certification Guidance for Information Protection System, Ministry of Public Administration and Security, 2009-9-1
- [4] Smart Card Open Platform Protection Profile, the National Intelligence Service, V2.0, 2008-4-24
- [5] ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts
- [6] ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards
- [7] ICAO Doc 9303 *Machine Readable Travel Documents Part 1 Machine Readable Passports*, 6<sup>th</sup> edition, 2006
- [8] ISO/IEC JTC1/SC17 Supplement to Doc 9303, Release 6, ICAO, 2007-9-21
- [9] MRTD Technical Report, PKI for MRTD Offering ICC Read-Only Access, Ver 1.1, 2004-10-1
- [10] ISO/IEC JTC1/SC17 Supplement to Doc 9303, Release 7, ICAO, 2008-11-19
- [11] BSI Technical Guideline TR-03110, Advanced Security Mechanisms for MRTD – Extended Access Control, Ver 1.11, 2008. 02. 21
- [12] MULTOS Architecture Specification - High Level Design[HLD]; IFD/MULTOS Interface[IFS]; Security Architecture[SEC]; Application Abstract Machine[AAM]; Data Dictionary[DD], Ver 4.2.1, March 2006
- [13] S3CT9KW 16-bit Microcontrollers for SmartCard User's Manual, July 2009
- [14] TORNADO-2Mx2 RSA/ECC Library API Manual v1.3, 2009-08-17
- [15] Samsung SDS SPass V2.0 Security Target, SP20-ASE-001
- [16] Samsung SDS SPass V2.0 Security Architecture, SP20-ADV-001
- [17] Samsung SDS SPass V2.0 Functional Specification, SP20-ADV-011
- [18] Samsung SDS SPass V2.0 Implementation Representation, SP20-ADV-021
- [19] Samsung SDS SPass V2.0 TSF Internals, SP20-ADV-031
- [20] Samsung SDS SPass V2.0 TOE Design, SP20-ADV-041
- [21] Samsung SDS SPass V2.0 Terms and Abbreviations, SP20-PMS-002
- [22] Samsung SDS MULTOS ATR Definition v2.1, October 2009
- [23] MAO-DOC-REF-006 MULTOS Developers Reference Manual v1.42, July 2004
- [24] MAO-DOC-REF-008 Guide to Loading and Deleting Applications v2.20, Jan 2000
- [25] MAO-DOC-REF-009 Guide to Generating Application Load Units v2.51, Dec 2002

## 9 Terms and Abbreviation

### 9.1 Terms

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

#### **Object**

Entity in the TSC(TSF Scope of Control), that contains or receives information, and upon which subjects perform operation

#### **DV : Document Verifier**

The CA(Certification Authority) that generates and issues the IS certificate

#### **Personalization Agent**

The agent receives the ePassport identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, The personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI.

#### **Personalization Key**

The symmetric key which the personalization agent uses to get issuing authorization and to write TSF data securely. It refers to the personalization authentication key and the personalization secure messaging key

#### **Personalization Authentication Key**

The symmetric key which the personalization agent uses to get issuing authorization by external authentication.

#### **Personalization Secure Messaging Key**

The symmetric key which the personalization agent uses to write TSF data securely with secure messaging

#### **SOD (Document Security Object)**

The SOD refers to the ePassport identity data and the ePassport authentication data recorded in the Personalization phase by the personalization agent that is signed by the personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and encoded with DER method.

#### **Ciphertext Only Attack**

Attack by the threat agent to attempt decryption based on the collected cipher text

#### **Encryption Key**

Key used in the symmetric cryptographic algorithm for data encryption(TDES) in order to prevent the data disclosure

#### **ePassport PKI**

Unique data signed on the ePassport by the personalization agent with digital signature generation key issued in the ePassport PKI System in order to issuance and check of the electronically processed passport

#### **ePassport PKI System**

System to provide certification practice, such as issuance of certificates necessary in passport's digital signature and management of certification-related records, etc.

**Reverse Engineering**

To identify and reproduce the basic design concept and applied technologies of product through detailed analysis of the completed product

**External IT Entity**

Any IT product or a system, untrusted or trusted, outside of the TOE that interacts with the TOE.

**Certificate**

The electronic data by a digital signature on the digital signature verification key by the CA in order to check and demonstrate that the digital signature generation key belongs only to the person who holds the key

**ePassport**

The passport embedded the contactless IC chip in which identity and other data of the ePassport holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO).

**User Data**

Including the ePassport identity data and the ePassport authentication data

**ePassport Identity Data**

Including personal data of the ePassport holder and biometric data of the ePassport holder

**Personal Data of the ePassport Holder**

Visually identifiable data printed on identity information page of the of ePassport and other identity data stored in the MRTD chip in the LDS structure

**Biometric data of the ePassport holder(Sensitive Data)**

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

**ePassport Application Data**

Including user data and TSF data of the MRTD

**ePassport Application**

Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc.

**ePassport Authentication Data**

The data stored in the MRTD chip with the LDS format to support ePassport security mechanisms that includes the PA SOD, the EAC chip authentication public key and the active authentication public key, etc.

**MRTD Chip**

The contactless IC chip that includes the MRTD application and the IC chip operating system necessary in operation of the MRTD application and that supports communications protocol by ISO/IEC 14443

**TSF Data**

The data stored in the secure memory of the MRTD chip to support ePassport security mechanisms

**Initial Personalization Key**

Initially shared personalization key between the personalization agent and the manufacturer doing the TOE initialization delegated by the personalization agent

**Abstract Machine**

An hardware/firmware platform, or it could be some known and assessed hardware/software combination acting as a virtual machine. Underlying abstract machine is OS if TOE is application, but it is firmware or hardware if TOE is OS.

**KDM (Key Derivation Mechanism)**

The mechanism to generate the encryption key and the MAC key by using hash algorithm from the Seed

**KDF ( Key Derivation Function)**

The function to generate the encryption key and the MAC key by using hash algorithm from the Seed

**Inspection**

Procedure in which immigration office checks identity of the ePassport holder by inspecting the MRTD chip presented by the ePassport holder, therefore verifying genuine of the MRTD chip

**IS (Inspection System)**

As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the ePassport inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands.

**Active Authentication**

The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values

**Active Authentication Private Key**

The private key based on the asymmetric key which the TOE uses to sign random number during AA Authentication

**Active Authentication Public Key**

The public key based on the asymmetric key which IS uses to verify the signed values of the TOE during AA authentication

**ADC(Application Delete Certificate)**

An application delete certificate contains permission for an application to be deleted from one or more MULTOS. The certificate contains the application ID (AID) of the application to be deleted. To delete an application the certificate is presented to a MCD. The MCD checks the certificate, and if valid, will delete the application.

**AAM(Application Abstract Machine)**

The software module of MULTOS OS which manages the operation of MULTOS application programs(MEL application program) and the logical memory spaces which application programs requires

**ALC(Application Load Certificate)**

An Application Load Certificate contains permission for an application to be loaded to one or more MULTOS. The certificate contains ROM ID, application ID (AID), product ID, enablement dates, application provider public key and so on of the application to be loaded. To load an application the

certificate is presented to a MCD. The MCD checks the certificate, and if valid, will load the application.

***ALU(Application Load Unit)***

A unit in which applications are loaded to MULTOS cards as. An application load unit consists of code and data.

***APDU(Application Protocol Data Unit)***

For communication between application on IC chip and external program protocol message unit defined in ISO/IEC 7816-4 IC

***BAC (Basic Access Control)***

The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the secure messaging for the MRTD chip and the IS

***BAC Mutual Authentication***

The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol

***BAC Session Keys***

The BAC session encryption key and the BAC session MAC key for generated by using the KDM from random numbers for generating session keys shared in the BAC mutual authentication

***BAC Secure Messaging***

The communication channel to provide the confidentiality and the integrity of transmitted data by encryption the transmitted data with the BAC session encryption key and generating, therefore transmitting after generating message authentication value with the BAC session MAC key

***BAC Authentication Keys(Document Basic Access Keys)***

The BAC authentication encryption key and the BAC authentication MAC key generated by using the KDM from the MRZ (passport No., passport No. check digit, date of birth, date of birth check digit, valid date, valid date check digit) for mutual authentication of the MRTD chip and the IS

***BIS : BAC Inspection System***

The IS implemented with the BAC and the PA security mechanisms and the AA as an option

***Chip Authentication***

The mechanism with which the ePassport certified implicitly to the Inspection System by DH key agreement mechanism and generates the secure messaging in EAC according to the BSI

***CSCA Certificate***

The certificate to demonstrate validity of the digital signature verification key for the digital signature generation key of the PA-PKI root CA by signature on the digital signature verification key with digital signature generation key of the PA-PKI root CA

***CVCA Link Certificate***

The certificate that includes digital signature value that the EAC-PKI root CA with the digital signature generation key that corresponds to the previous CVCA certificate after generating a new CVCA certificate before expiring the valid date of the CVCA certificate

***CVCA Certificate***

The certificate that includes digital signature value by the EAC-PKI root CA with digital signature generation key of the EAC-PKI root CA on the digital signature verification key in order to demonstrate validity of the CVCA link certificate and the DV certificate

***DG(Data Group)***

The data unit stored inside of ePassport according to the LDS of ePassport

***DS (Document Signer) Certificate***

The certificate of the personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism

***DV Certificate***

The certificate that includes digital signature value on the digital signature verification key of the IS with the digital signature generation key of the DV in order to demonstrate validity of the digital signature verification key of the IS

***EAC (Extended Access Control)***

The security mechanisms consisted with the EAC-CA for chip authentication and the EAC-TA for the IS authentication in order to enable only the EAC supporting Inspection System (EIS) to read the biometric data of the ePassport holder for access control to the biometric data of the ePassport holder stored in the MRTD chip

***EAC Session Keys***

The session key used to establishing secure messaging to protect transmission of the biometric data of the ePassport holder that consist of the EAC session encryption key and the EAC session MAC key generated by using the KDF of which keys shared with the EIS through the Ephemeral-Static DH key distribution protocol in the EAC-CA are used as seed

***EAC Chip Authentication Public Key and EAC Chip Authentication Private Key***

Set of the DH keys used by the MRTD chip to authenticate itself to the EAC supporting IS in the EAC-CA that contain data recorded by the personalization agent in the Personalization phase

***EIS : EAC Inspection System***

The IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option

***EAC-CA (EAC-Chip Authentication)***

The security mechanism to implement the Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) to enable the MRTD chip authentication by the EIS through key checking for the EAC chip authentication public key and private key of the MRTD chip and temporary public key and private key of the EIS

***CVCA ( Country Verifying Certification Authority)***

The root CA that generates and issues the CVCA certificate, the CVCA link certificate and the DV certificate by securely generating digital signature key in the EAC-PKI to support the EAC security mechanisms, which includes the version information of EF.COM LDS and the tag information of the data groups

***EAC-TA (EAC-Terminal Authentication)***

The security mechanism that The EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements chal-

challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS

**e-Cover**

The e-Cover refers to the sheet including IC chip and antenna inlay in the ePassport.

**EF.COM**

Including the LDS version info. data groups tag information

**EF.CVCA**

The EF format file to specify the read-right and the list of the CVCA digital signature verification key identifier necessary in verification of the CVCA certificate validity in the EAC-TA

**Grandmaster Chess Attack**

Attack by masquerading as the MRTD chip using the IC chip to hookup the communication channel between the MRTD chip and the IS

**IC Chip (Integrated Circuit Chip)**

The important semiconductor to process smart card functionality, and the processing unit including four functional units(mask ROM, EEPROM, RAM, and I/O port)

**ICAO-PKD**

The DS certificate storage operated and managed by the ICAO that online distributes in case the domestic/ overseas IS requests the DS certificate of the corresponding country

**IS Certificate**

Certificate used by the MRTD chip to verify the digital signature transmitted by the IS in the EAC-TA. The DV performs a digital signature on the digital signature verification key of the EIS with the digital signature generation key.

**KMA(Key Management Authority)**

Agent to generate MULTOS enablement data, ALC and ADC as a MULTOS security manager.

**KTU(Key Transformation Unit)**

A Key Transformation Unit (KTU) is required when loading Confidential Application Load Units. The purpose of the KTU is to protect the keys used in making the ALU confidential. The KTU will normally be created as part of the data preparation / ALU generation process. During application loading the KTU is used by the card to decrypt the confidential ALU.

**LDS (Logical Data Structure)**

Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip

**Secure Attribute of LDS Application Program**

An attribute to represent the lifecycle(operational mode) of ePassport application and the application status of BAC or EAC, which stored in LDS application program

**MAC Key (Key for Message Authentic Code)**

Key used by symmetric cryptographic algorithm according to ISO9797 to generate the message authentication code in order to prevent data forgery and corruption

**MCD(MULTOS Carrier Device)**

ICC that carries MULTOS operating system.

**MCD Unique Symmetric Transfer Key**

A transfer key based on the symmetric-key cryptosystem stored in EEPROM of MCE by MISA operation and used to decrypt MSM\_CD encrypted with KMA in MCD



***MCD Unique Asymmetric Transfer Key***

A transfer key based on a public-key cryptosystem generated by KMA and stored EEPROM of MCD during MCD enablement. When the KTU is encrypted with the public key of asymmetric transfer key and is loaded to application program in Confidential ALU, it is decrypted with the private key of asymmetric transfer key.

***MEL(MULTOS Executable Language)***

The instruction set of the application abstract machine, as defined in the MULTOS developers reference manual.

***MRTD(Machine Readable Travel Document)***

Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes

***MRZ(Machine Readable Zone)***

A fixed standard area located on the data page of MRTD, including the formatted necessary data and optional data for machine-read with OCR .

***MSM(MULTOS Security Manager)***

Agent generating and managing keys related MULTOS.

***MSM\_CD (MSM Controls Data)***

Enablement data to activate MULTOS to be able to load, delete and execute applications.

***MULTOS(Multi-Application Operating System)***

A name of operating system usually implemented on ICC to operate multiple application in a highly secure manner. It also implies the scheme of management and operation for the lifecycle of MULTOS carrier device. MULTOS employs an end-to-end trust architecture that places the Issuer in control of their card base.

***PA (Passive Authentication)***

The security mechanism to demonstrate that identity data recorded in the ePassport has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the ePassport access control policy.

***CSCA (Country Signing Certification Authority)***

The root CA that generates and issues the CSCA certificate and the DV certificate by securely generating the digital signature key in the PA-PKI to support the PA security mechanisms

***Primitive***

Application Programming Application Programming Interface of MULTOS application to analyze AAM in MULTOS.

***Probing***

Attack to search data by inserting probing pin in the IC chip

***Terminal Authentication***

The mechanism with which the ePassport certified implicitly to the Inspection System by eSignature verification based on a public-key cryptosystem and generates the Secure Messaging in EAC according to the BSI

## 9.2 Abbreviations

AA	Active Authentication
ABEND	Abnormal End (of MEL application execution)
ADC	Application Delete Certificate
AIS	Active Inspection System
ALC	Application Load Certificate
ALU	Application Load Unit
AM	Abstract Machine (Software Module)
ATR	Answer To Reset
AU	Application Unit
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CLK	Clock (input to smartcard)
COS	Card Operating System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem (algorithm)
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie-Hellman
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EBC	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIS	Extended Inspection System
HW	Hardware
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IFD	Interface Device
IO	Input/Output
IS	Inspection System
ISO	International Organization for Standardization

IT	Information Technology
KDF	Key Derivation Function
KDM	Key Derivation Mechanism
KTU	Key Transformation Unit
LDS	Logical Data Structure
MAC	Message Authentication Code
MCD	Multos Carrier Device
MEL	Multos Executable Language (application language)
MF	Master File
MISA	MSM Injection Security Application
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MSM	Multos Security Manager
OTP	One-Time Programmable (memory)
PA	Passive Authentication
PCD	Proximity Coupling Device
PICC	Proximity Card
PIS	Passive Inspection System
PKI	Public Key Infrastructure
PP	Protection Profile
PPS	Protocol and Parameters Selection (ref ISO7816)
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read-Only Memory
RSA	Rivest-Shamir-Aldeman (algorithm)
RST	Reset (input to smartcard)
SFI	Short File ID
SFP	Security Function Policy
SFR	Security Function Requirement
SOD	Security Object of Document
SOF	Strength of Function
SPA	Simple Power Analysis
SSC	Send Sequence Counter
ST	Security Target
TA	Terminal Authentication
TDES	Triple-DES
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Subsystem, TSF Subsystem

END OF DOCUMENT

Phone: +82-2-3429-2114

E-mail: [sdspr@samsung.com](mailto:sdspr@samsung.com)

<http://www.sds.samsung.co.kr>

**SAMSUNG SDS**

