U-creator
U dream, we create.

Samsung SDS
S*Pass* V1.1
ST Lite

Samsung SDS Co., Ltd.

SAMSUNG

SAMSUNG SDS

REVISION STATUS

Revision	Date	Description of Change
1.0	Nov 3, 2009	Final version evaluated by KISA
1.0e	Feb 23, 2010	Final version translated into English

Contents

List of Figures

List of Tables

1 ST Introduction

This document is the Security Target (hereafter, 'ST') of SAMSUNG SDS S*Pass* V1.1 which shall be embedded in SPass11 product.

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 S*Pass* V1.1 Security Target Lite
- ST Lite Version: V1.0 (Evaluated ST Version : V1.0)
- Release date : 23rd of February 2010 (3rd of November 2009 for ST)
- Author: SAMSUNG SDS Co., Ltd.
- Evaluation Criteria : Common Criteria for Information Security Evaluation V2.3 (Ministry of Information and Communication Public Notice No. 2009-52)
- Evaluation Assurance Level: EAL4+ (ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_VLA.4)
- PP Compliance: ePassport Protection Profile V1.0[1]
- PP Certification Number : KECS-PP-0084-2008, January 2008
- TOE : SAMSUNG SDS S*Pass* V1.1

1.2 ST Overview

SAMSUNG SDS SPass11 product (hereafter, 'SPass11') is an IC chip package for ePassport assuring high security and optimized performance, and is implemented by embedding TOE in Samsung Electronics S3CC9LC IC chip. S3CC9LC achieved separate CC certification from BSI like below.

- Protection Profile compliance : BSI-PP-0002-2001
- Evaluation assurance level: EAL5 augmented by ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4

SPass11 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 S*Pass* V1.1 (hereafter, 'SPass'*)* which is a combination of the open platform operating system, SAMSUNG SDS MULTOS SM30E R1 (hereafter, 'SM30E') which is implemented upon IC chip and the SPass LDS application V1.1 (hereafter, 'MRTD Application') which is designed to be loaded on MULTOS.

- SM30E is an IC chip operating system which is implemented according to MULTOS V4.21[12] specification (hereafter, 'MULTOS specification') and performs communication with underlying hardware platform, memory management and contains Application Abstract Machine (AAM). Also, SM30E loads and deletes application and handles command and

respond APDU (Application Protocol Data Unit) first. Deleting an application from MULTOS can be prevented if personalization agent dose not allow to issue ADC (Application Delete Certificate).

- MRTD Application is implemented according to the specifications[7][8][9] of International Civil Aviation Organization (hereafter, 'ICAO specification') and EU EAC specification of BSI (hereafter, 'EAC specification').

The key security objectives of the TOE are to protect the TOE itself, TOE data, and important data from the unauthorized exposure or modification.

SM30E provides the following key security features:

- open platform operating system access control functions such as MCD enablement, application load/delete, etc.
- security environment for personalization agent identification/authentication through ROM Key Integration and MISA operation
- separation of applications, integrity Verification of executable code and enablement data
- cryptographic functions: SHA-1 and interfaces for DES/TDES, RSA and ECC provided by IC chip
- self test of open platform operating system per each received command and filtering of undefined commands
- prevention of re-use by deleting or resetting key, random number, SSC securely.

MRTD Application provides the following key security features:

- generation and distribution of BAC, EAC key according to ICAO and EAC specification
- identification/authentication of an Inspection System and access control through BAC, EAC-CA, EAC-TA
- access control of personalization agent and ePassport life cycle management by personalization key authenticaiton.
- Secure Messaging between Inspection System and ePassport after BAC and EAC-CA
- keeping secure value through the CVCA certificate chain Verification and update during EAC-TA.
- providing Verification method for ePassport genuineness to Inspection Systems through AA

1.3 Conformance Claim

The PP that this ST follows claims conformance to

- Information Security System Common Criteria Part1 : Introduction and general model V2.3 , Aug. 2005, CCMB-2005-08-001
- Information Security System Common Criteria Part2 : Security functional requirements V2.3, Aug. 2005, CCMB-2005-08-002
- Information Security System Common Criteria Part3 : Security assurance requirements V2.3, Aug. 2005, CCMB-2005-08-003

as follows

- Part 2 Conformant

- Part 3 Conformant

This ST conforms to the following the Protection Profile.

- Protection Profile compliance: ePassport Protection Profile V1.1[1]
- Protection Profile certification number : KECS-PP-0084-2008
- Package Conformant to EAL4 augmented with ADV_IMP.2, ATE_DPT.2, and AVA_VLA.3

Additionally augmented assurance components to PP in this ST are

- ALC_DVS.2 “Sufficiency of security measures”
- AVA_VLA.4 “Highly resistant”

And the minimum strength of the TOE security function is "SOF-high."

1.4 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 options 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.

1.5 Terms and Definitions

The terms used in this ST have the same meaning as in the PP and CC unless defined..

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.

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.

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 massage unit defined in ISO/IEC 7816-4 IC

External IT Entity

Any IT product or a system, untrusted or trusted, outside of the TOE that interacts with the TOE.

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.

MCD(MULTOS Carrier Device)

ICC that carries MULTOS operating system.

MEL(MULTOS Executable Language)

The instruction set of the Application Abstract Machine, as defined in the MULTOS Developers Reference Manual

MISA(MULTOS Injection Security Application)

MISA stands for MULTOS injection security application and it is a MULTOS application containing transport keys created by the root key management authority for a specific MULTOS implementation. It is designed to inject an initial identity and key into a chip during production. When complete, the chip contains, amongst other management data, an identity (the mcd_id) and a transport key. From this point the card will only accept data encrypted specifically for that card. At the time of manufacture, chips containing the particular MULTOS implementation are identical, apart from unique chip numbers and transit keys.

MSM(MULTOS Security Manager)

Agent generating and managing keys related MULTOS

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 life cycle of MULTOS carrier device. MULTOS employs an end-to-end trust architecture that places the Issuer in control of their card base.

Primitive

Application Programming Application Programming Interface of MULTOS application to analyze AAM in MULTOS .

1.6 ST Organization

Section 1 provides introductory information required for the Protection Profile Identification.

Section 2 defines TOE and describes TOE environment.

Section 3 describes the security aspects of the environment, where the TOE is intended to be used, and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions. It also describes means of the TOE to counter threats technically.

Section 4 describes security objectives for the TOE and environment to deal with identified threats, and supports assumption and Organizational Security Policies.

Section 5 describes security functional requirements and assurance requirements to satisfy security objectives. This section is based on the requirements of the Common Criteria section 2 and 3.

Section 6 explains the TOE security functions implemented.

Section 7 shows compliance to Smartcard Open Platform Protection Profile for Government V1.1.

Section 8 demonstrates that security issues are countered adequately and the IT security requirements for security objectives are complete and adequate.

References contain the materials referenced in this ST.

Abbreviation provides terms and abbreviations frequently used.

2 TOE Description

SPass11 is a packaged dual interface IC chip wafer product of SAMSUNG Electronics S3CC9LC where TOE is contained[1]. TOE comprises of SM30E which complies MULTOS specification and MRTD Application which follows ICAO and EAC specification.

SM30E is an IC chip operating system designed to allow multiple on-card applications to be securely loaded and executed and to provide high level of interoperability and security.

2.1 TOE Overview

The TOE comprises of MULTOS open platform (SM30E) which can manage multiple applications and MRTD Application. SM30E is embedded software on IC chip, communicates with Inspection System and provides run time environment to MRTD Applications. MRTD Application which complies with ICAO and EAC specification is developed separately and loaded as an application on SM30E.

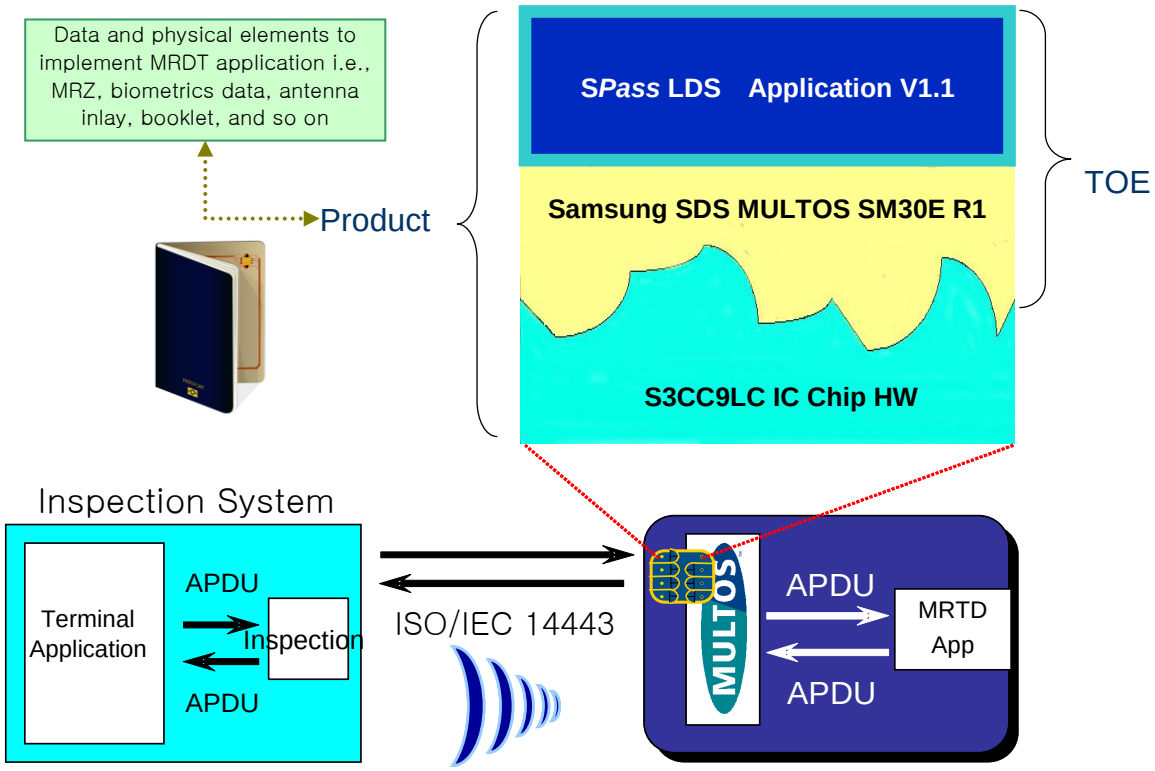


Figure 1. TOE Overview

Details of physical and logical scope of the TOE are described in section 2.6.

2.2 Product Configuration

[1] T=0 and T=1 contact interface hardware controller (UART) is disabled when applied to ePassport .

The TOE (SPass) includes an IC chip operating software, SM30E and an MRTD Application on SM30E and complies with MULTOS specification, ICAO specification and EAC specification. TOE and the underlying hardware are packaged to compose SPass11 product and applied to use as ePassport. As shown in Figure 2, SPass11 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

2.3 TOE Intended Usage

Personalization agent issues ePassport to be used by the holder for international travel. The traveller presents a MRTD to the Inspection System to prove his or her identity. The TOE comprises of the logical parts excluding physical parts of ePassport and complies with Logical Data Structure(hereafter 'LDS') specified by ICAO for Machine Readable Travel Document through contactless interface, that is,

(1) Digital MRZ Data (DG1),
(2) Digital Facial Image (DG2),
(3) Optional biometric reference data, Digital Fingerprint (DG3) or Iris Image(DG4) or both,
(4) Other data according to LDS (from DG5 to DG16),
(5) Document Security Objects (SOD),
(6) Common Data Elements (EF.COM)

and also in order to keep integrity, confidentiality and authentication on each ePassport holder's data,

(1) supports validation method of ePassport to prove that ePassport holder is identical to the printed identification data**,**
(2) communicates securely through Secure Messaging using symmetric key derived from MRZ,
(3) performs access control to the sensitive biometric data like fingerprint using secure communication between the MRTD and Inspection System by means of mutual authentication based on asymmetric key cipher[11].

The logical MRTD is protected by data authentication and secure messaging. Data authentication is enabled by a digital signature (SOD) generated by the DS of the personalization agent and the security features of the MRTD's IC chip (PA, Passive Authentication). The TOE optionally can show that the data stored in the MRTD's IC chip are not fabricated by means of RSA signature (AA, Active Authentication).

ICAO Technical Report [7][9] defines Passive Authentication as a mandatory security mechanism and also defines or mentions Basic Access Control, Active Authentication, and Extended Access Control for the protection of additional biometric information as an optional security meachanism. The

PA Is a security mechanism that TOE environment, that is, Inspection System performs independently of the TOE by reading and verifying SOD of the TOE.

This ST addresses BAC, EAC and AA for the protection of the logical MRTD. TOE supports BAC, EAC and AA mechanism but may not be performed in case personalization agent does not personalize application data to relevant DG's necessary for performing each security mechanism..

For BAC, Inspection System (1) reads the printed data in the MRZ optically (2) authenticates itself as Inspection System to the MRTD's IC chip by means of Document Basic Access Keys derived from MRZ data. After successful authentication, Inspection System is authorized to read data and access DG1, DG2, DG5 ~ DG16, and SOD of logical MRTD by means of secure messaging. .

EAC is implemented according to BSI Technical Guideline TR-03110 v1.11[11]. If both MRTD's IC chip and Inspection System support EAC specification, Advanced ePassport Inspection Procedure will be performed as follows.

(1) After successful BAC, secure messaging starts and Inspection System is allowed to access less sensitive DG such as DG1, DG2, DG14, DG15 and SOD.

(2) After successful key agreement based on DH algorithm by performing EAC-CA, secure messaging restarts with new session key.

(3) PA is performed to verify data authenticity and integrity, and

(4) Inspection System selectively performs AA to verify that the MRTD's IC chip is genuine. Then

(5) Inspection System responses to the challenge from MRTD's IC chip by means of EAC-TA and is granted access to sensitive data (DG3 or DG4).

If either MRTD's IC chip or Inspection System is not compliant to EAC specification, the following Standard ePassport Inspection Procedure will be used.

(1) After successful BAC, secure messaging starts and Inspection System is allowed to access less sensitive DG such as DG1, DG2, DG14, DG15 and SOD.

(2) PA is performed to verify data authenticity and integrity, and

(3) Inspection System selectively performs AA to verify that the MRTD's IC chip is genuine. Then

(4) Inspection System is able to access every DG except sensitive biometric data (DG3 and DG4).

AA is the only method to be able to verify the genuineness of MRTD's IC chip in case either MRTD or Inspection System can not performs the protocol of EAC specification and thus should follow Standard ePassport Inspection Procedure. The procedure of AA is defined in ICAO specification. That is, DS generates asymmetric key pair for AA, when the public key is stored in DG15 according to the X.509 public key information structure and the private key is stored in the secure memory area of MRTD's IC chip. To ensure the genuineness of the MRTD's IC chip, (1) authenticity and integrity of AA public key in DG15 is verified by means of PA, and (2) Inspection System can be assured that the MRTD's IC chip is genuine by Challenge-Response method - verifying digital signature created dynamically by MRTD.

2.4 TOE Operational Environment

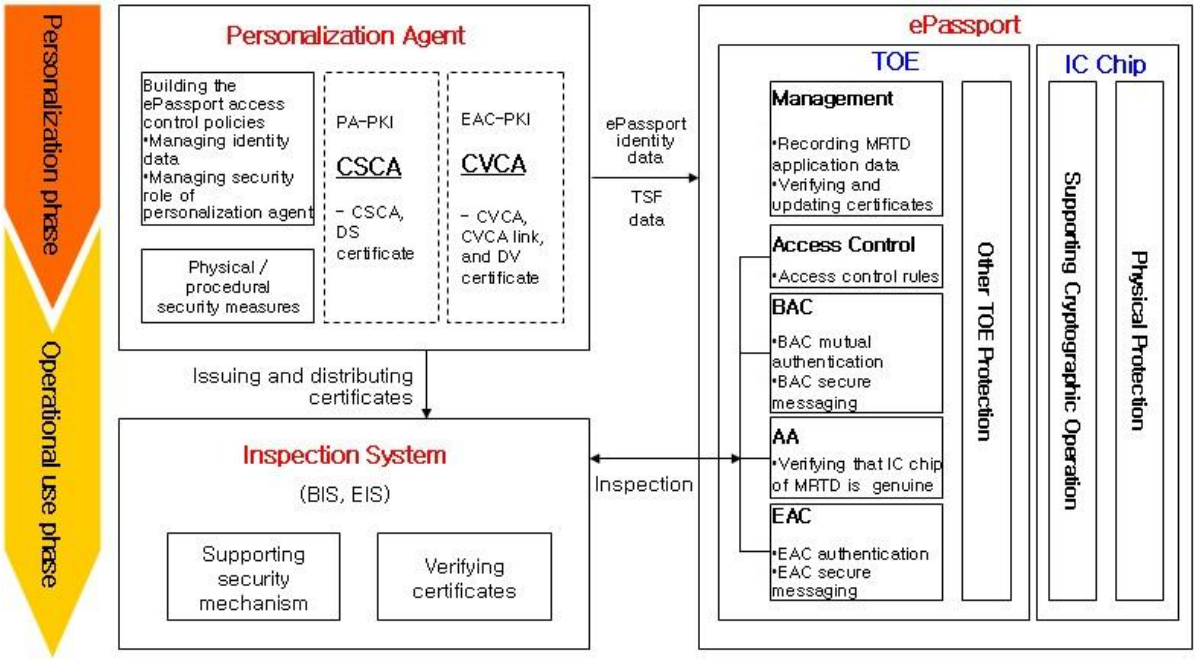


Figure 3. TOE Operational Environment

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

2.5 Security Function of the TOE Environment

The underlying IC chip 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 SM30E enablement data, and (4)MULTOS DES/TDES decryption of application load unit when being loaded onto SM30E in confidential mode.

- Asymmetric key cryptographic operation

  The IC chip provides crypto-processor (Tornado^{TM})[2] and relevant cryptographic library capable of 2048-bit modulus RSA and ECC operations in order that the TOE can perform operations such as (1)digital signature Verification based on RSA or ECDSA for EAC-TA, (2)digital signature generation based on RSA for AA, (3)digital signature Verification based on RSA for application load certificate during loading application onto SM30E, (4)digital signature Verification based on RSA for application delete certificate during deleting application from SM30E, and (5)Asymmetric Hash operation based on RSA for verifying integrity of SPass11 carrying SM30E and its loaded applications.

- Random number generation

  Random number generator 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.

2.6 Scope and Boundary of the TOE

TOE consists of two components to perform the following functions.

- MULTOS Operating System (SM30E)

  SM30E provides the interface with underlying hardware, its memory management and etc. SM30E performs the functions like selecting, loading, and deleting applications and receiving or transferring ADPU command-response pair.

[2] Considering RAM space availability, TOE supports up to 1024-bit modulus in case of RSA.

- MRTD Application

  The MRTD Application comprises of the TOE with implementation of ICAO and EAC specification.

The ePassport is composed of the TOE, TOE-underlying IC chip, inlay, e-cover and the visual data page of the passport book and it is to be used by the holder for international travel after personalization of ePassport application data.

2.6.1 Physical Scope of the TOE

SM30E is masked in ROM area of the underlying IC chip. The MRTD Application is loaded in the EEPROM area. SM30E and the MRTD Application is embedded on the underlying IC chip and constructs SPass11. Packed with antenna inlay and e-cover, SPass becomes a complete ePassport product of Samsung SDS..

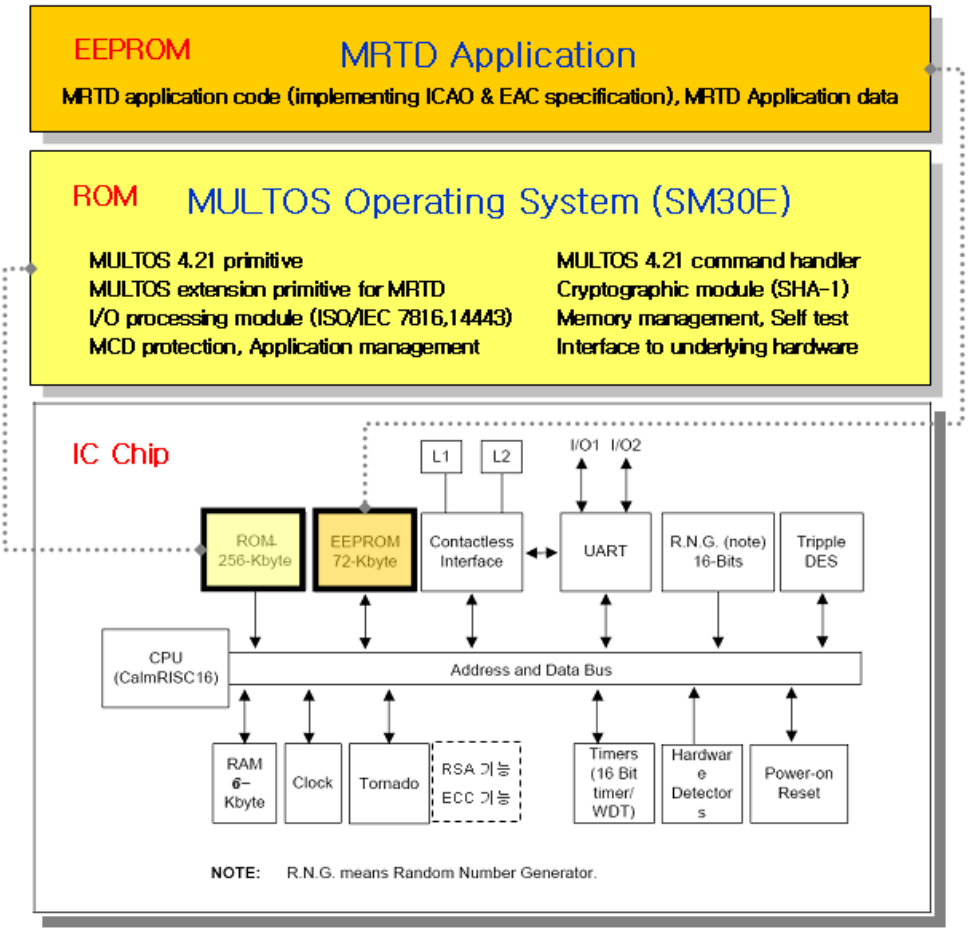


Figure 4. Physical scope of the TOE

ePassport consists of a booklet and an IC chip and antennae 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, SM30E (Samsung SDS MULTOS SM30E R3), and the MRTD Application including MRTD Application data (SDS LDS application V1.1), where underlying IC chip is excluded.

The TOE is implemented in the IC chip which is Samsung Electronics' S3CC9LC 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), SM30E, processes commands and file management according to ISO/IEC 7816-4, 8, 9, executes MRTD Application and provides functions for management of MRTD 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 MRTD Application. SM30E provides cryptographic functions controlling 2048bit segments using run-time firmware library provided by the underlying IC chip.

The MRTD Application is an on-chip application which implements the functions 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 MRTD Application shall contain MRTD holder's sensitive biometric data. The MRTD Application shall be loaded onto the EEPROM using secure mechanism provided by MULTOS[12][14]. It contains data group and security object specified by ICAO and EAC specification and code implementing security protocols such as BAC, AA, EAC-CA and EAC-TA.

The MRTD Application data consists of MRTD user data like MRTD identification information and MRTD TSF data required for security mechanism.

The TOE includes the associated guidance documents such as the administrator guidance (HUUC-0700002-AGD-001), the user guidance (HUUC-0700002-AGD-002), MULTOS manuals published by MAOSCO and SPass personalization guidance.

2.6.2 Logical Scope of the TOE

The TOE communicates with Inspection Systems according to the transmission protocol defined in ISO/IEC 14443-4. The TOE controls reading, writing and personalizing rights to the TOE conducted by Inspection Systems or Personalization Agent. The TOE also performs Secure Messaging, BAC, AA, EAC-CA, EAC TA security mechanism according to ICAO and EAC specification and thus provides data protection and secure management functions. Self test, domain separation and preservation of secure state are provided as well to protect TSF.

The logical scope of the TOE can be defined by the complete set of SM30E commands and MRTD Application commands with their related internal mechanisms.

2.6.2.1 TOE components

MRTD Application provides information security function such as confidentiality, integrity, access control and authentication to protect MRTD user data and MRTD TSF data including identity and authentication information of the MRTD. These information security functions are implemented via

BAC and EAC security mechanisms according to ICAO[7] and EAC[11] specifications. TOE also supports PA security mechanism performed by Inspection System and AA security mechanism[3].

The MRTD Application security features are as below.

a) Cryptographic Support

The MRTD Application ensures that only authorized Inspection System is able to access the user data and TSF data of the TOE and provides message encryption and authentication function to prevent unauthorized disclosure of the TOE while communicating with Inspection System. Hash digest of the user data and TSF data of the TOE is stored, provided to the Inspection System and used to prove that the data has not been modified. According to the ICAO specification, only the Inspection System which can encrypt messages using keys derived from data in MRZ area is allowed to access the user data and TSF data of the TOE and all the data exchanged between the Inspection System and the TOE shall be encrypted with the BAC session key in BAC protocol or EAC session key in EAC-CA protocol. The TOE provides EAC-TA security mechanism based on EAC specification in order that only authorized Inspection Systems can access the sensitive biometric data. The TOE provides digital signature generation functionality about a random number based on the ICAO AA.security mechanism.

b) Data Protection

MRTD Application supports access control policy in order that only an authorized user can access the user data and TSF data of the TOE. After personalization phase, only an authorized user like personalization agent is allowed to have update right to user data and TSF data of the TOE by means of proper authentication with cryptographic key. By means of PA, AA, BAC and EAC security mechanism, an Inspection System can be authorized and obtain rights to read data of the TOE, but update of the user data is never allowed

c) Identification and Authentication

MRTD Application enforces that external IT entity shall establish communication channel after completing identification and authentication itself, and provides countermeasures against consecutive authentication retry which is performed over pre-assigned number. Messages exchanged between the TOE and the Inspection System shall be encrypted to prevent unauthorized disclosure, where MAC is attached to help determine if each message is authorized. MRTD Application enforces authentication mechanism to personalization agent in order that only authorized personalization agent is allowed to access TOE, and enforces BAC and EAC-TA security mechanism in order that only authorized Inspection System is allowed to access TOE. AA security mechanism of the TOE ensures that ePassport is neither forged nor corrupted and thus genuine.

d) Security Management

[3] Out of cryptographic operations, SHA-1 is implemented using only software, but DES/TDES and MAC implementations are using unit block-wise cryptographic operation functions provided by IC chip, and RSA, DH, ECDSA and ECDH are using modular exponentiation operation coprocessor.

MRTD Application limits the capability, availability, and attributes of the TOE functions which shall not be used in operational use phase in order not to be misused, and controls access in order that only authorized entities are allowed to access MRTD application data. All the counters and information relevant to TSF data are discarded securely to prevent replay attack.

The security mechanisms of ePassport are summarized in Table 1.

Table 1. The ePassport Security Mechanisms

Security Mechanisms of the ePassport				IT Security Function of the TOE
Security Mechanism	**Function**	**Cryptography**	**Cryptographic Key/ Certificate Type**	
PA	User Data Authentication	N/A	N/A	Access Control to the SOD - read-rights: BIS, EIS - write-rights: Personalization Agent
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 Authentication Protocol TDES-CBC SHA MAC	BAC Authentication Key (ENC 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 (ENC 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 (ENC Key, MAC Key)	Transmitting messages by creating the MAC after encryption with the BAC session key Receiving messages by decryption it after verifying the MAC with the BAC session key
EAC	EAC-CA	DH, 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 (ENC Key, MAC Key)	Secure messaging by using the EAC session key shared in the EAC-CA

	EAC-TA	RSAPSS ECDSA	CVCA Certificate CVCA Link Certificate DV Certificate IS Certificate	Verifying the IS certificate by using the certificate chain and the link certificate Verifying the digital signature for transmitted messages of the EIS for the EIS authentication

SM30E is a single-thread operating system implemented according to the MULTOS 4.2.1 specification. Only one application can be executed at a certain point of time and parallel processing or multi-tasking mechanism is not supported. When power is supplied, SM30E is executed as follows.

[1] Wait for input from Inspection System

[2] Parse the input

[3] If the input is a MULTOS command, MULTOS processes it and respond to the Inspection System

[4] Otherwise, currently selected application processes the command and respond to the Inspection System

Applications are changed to the form of MULTOS executable language (MEL) while being loaded on SM30E. MEL applications are interpreted by SM30E before being complied and executed by IC chip processor.

SM30E provides applications with the following features:

a) Cryptographic Support

SM30E provides SHA-1 cryptographic function and the interfaces to DES/TEDS, RSA and ECC provided by underlying.

b) Data Protection

SM30E removes residual information securely when withdrawing session keys and random numbers from temporary memory area.

c) Identification and Authentication

SM30E allows personalization agent to load /delete MULTOS application only after successful MCD enablement, and allows to complete loading/deleting[4] MULTOS application only when the KMA's digital signature is verified successfully. The number of failed attempts regarding these key functions is tracked and managed.

d) Security Management

SM30E provides access control function on open platform OS like MCD enablement and application loading/deleting based on the security attributes specified by ROM Key Integration and MISA operation..

e) Platform Protection

SM30E provides application separation function to prevent interference between applications and also provides self-testing function. SM30E interprets commands sent from the inspection system to allow only pre-defined commands to be performed and provides countermeasure

[4] Deletion of applications can be prevented completely by not issuing ADC according to the Personalization Agent's policy

against side-channel attacks using underlying IC chip function. By doing that, attacks that disclose user data or TSF data and bypass TSP shall be prevented even in the environment unexpected during design time

2.7 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

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

   - BAC authentication key : the encryption key and MAC key for BAC mechanism
   - BAC session key : the encryption key and MAC key for BAC mechanism
   - EAC session key : the encryption key and MAC key for EAC mechanism

Table 2. TOE Assets

Category			Description	Storage Space
User Data	ePassport Identity Data	Personal Data of the ePassport holder	Data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16	EF file
		Biometric Data of the ePassport holder	Data stored in EF.DG3 and EF.DG4	
	ePassport Authentication Data		SOD, EAC chip authentication public key, etc.	
	EF.CVCA		In EAC-TA, CVCA digital signature verification key identifier list used by the TOE to authenticate the Inspection System	
	EF.COM		LDS version info., tag list of DG used, etc.	
TSF Data	EAC-CA Private Key		In EAC-CA, Chip Private key used by the TOE to demonstrate Not forged MRTD chip	Secure memory
	AA Private Key		In AA, AA Private Key used by the TOE to generate digital signature to show it's genuine	
	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	Temporary memory
	BAC Session Key		BAC session encryption key, BAC session MAC key	
	EAC Session Key		EAC session encryption key, EAC session MAC key	

3. MUSLTOS 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 MRTD 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[5] (ROM Key Integration procedure).
   - There are Application Load Certificate (ALC) and Application Delete Certificate (ADC) to load/delete the MRTD 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 for Application Loader.
   - Security data injected to secure memory area through MISA (MULTOS Injection Security Application) operation[6] 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
     - MSM Security Attributes: 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 EAL4+.

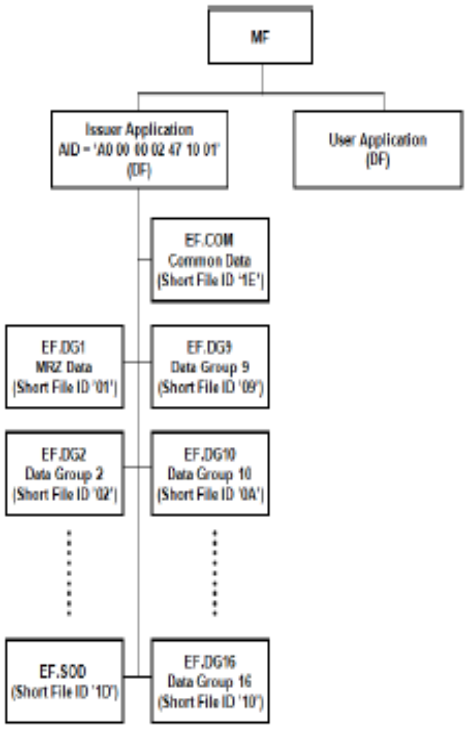
[5] ROM Key Integration procedure

[6] 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.

2.7.1 Content of ePassport User Data

There are MF, DF, and EF structure to be stored ePassport User Data of the TOE in LDS as Table 3 below.

Table 3. Contents of LDS in which the User Data are stored

Category	DG	Content	LDS Structure
Detail(s) in MRZ	DG1	Document(Passport) Type	
		Issuing State	
		Name (of Holder)	
		Document Number	
		Check Digit (of Doc Number)	
		Nationality	
		Date of Birth	
		Check Digit (of DOB)	
		Sex	
		Data of Expiry of Valid Until Date	
		Check Digit (of DOE/VUD)	
		Optional Data	
		Composite Check Digit	
Biometric Data	DG2	Encoded Face information	
	DG3	Encoded Finger(s) information	
	DG4	Encoded Iris(s) information (optional)	
Others	DG5	Displayed Portrait	
	DG6	-	
	DG7	Displayed Signature or Usual mark	
	DG8	-	
	DG9	-	
	DG10	-	
	DG11	Additional Personal Detai(s)	
	DG12	Additional Document Detail(s)	
	DG13		
	DG14	EAC-CA Public Key	
	DG15	AA Digital Signature Verification Key (optional)	
	DG16	Person(s) to Notify	

2.7.2 Types of Certificates in ePassport System

Types of certificates used in the ePassport system are as shown in Table 4.

Table 4. Types of ePassport Certificates

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

Additional certificates for MULTOS feature are as shown in Table 5.

Table 5. 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

2.8 TOE Subject

This section identifies TOE users and the parties concerned in the TOE

Figure 5 shows the overall configuration of the ePassport system.

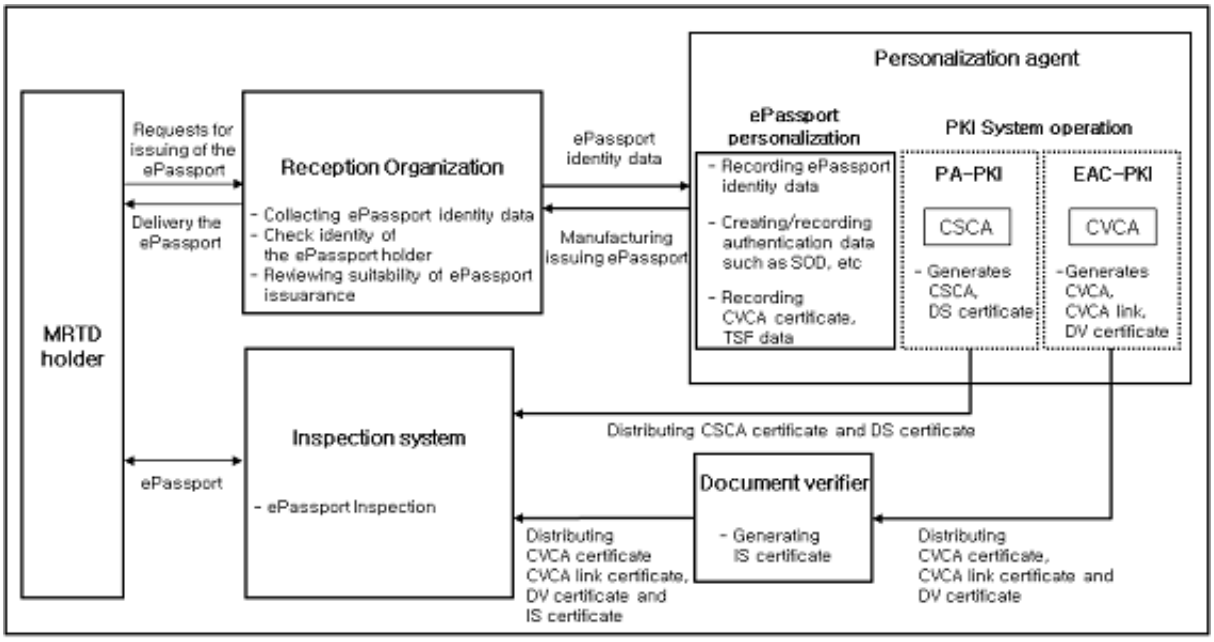


Figure 5 Overall Configuration of the ePassport System

2.8.1 TOE User

■ **Personalization Agent**

The Personalization agent generates document security object (‘SOD’ hereinafter) by digital signature on the user data (identity and authentication data) and records it in the MRTD chip with the ePassport identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the personalization agent is manufactures and issues the ePassport embedded the MRTD chip to the passport. The Personalization agent generates digital signature key for verifying of forgery and corruption of the user data stored in the MRTD chip. Then, in accordance with the Certification Practice Statement (CPS) of the ePassport PKI System the personalization agent generates, issues and manages CSCA certificate and DS certificate. According to the Issuing Policy of the ePassport, the personalization agent generates digital signature key to verifying access-rights to the biometric data of the ePassport holder in case of supporting EAC security mechanism. Then, the personalization agent generates, issues and manages CVCA certificate, CVCA link certificate and DV certificate. For details related to of the ePassport PKI System and certification practice, such as certification server, key generation devices and the physical, procedural security measures, etc., it depends on the Issuing Policy of the ePassport.

■ **Inspection System**

BIS (Basic Inspection System)

A contactless Inspection System with ePassport chip, where PA, BAC, and optionally AA are implemented.

EIS (Extended Inspection System)

A contactless Inspection System with ePassport chip, where PA, BAC, EAC and optionally AA are implemented.

■ **MULTOS Application**

SPass is composed of SM30E, open platform operating system, and MRTD Application thus further applications other than MRTD Application can be loaded to use according to the Personalization Agent's policy, where these are called MULTOS applications. A MULTOS application uses MULTOS standard primitives provided by SM30E.

2.8.2 Party Concerned in the TOE

■ **KMA (Key Management Authority)**

This entity that functions as an MSM (MULTOS Security Manager) defines MULTOS security infrastructure and provides services enforcing security policy. It is regarded as a CA (Certificate Authority) in PKI and a third party trusted by all the users who utilize services based on MULTOS should take this role. KMA generates each MCD enablement data, and is the only organization that issue ALC and ADC. KMA can be often configured as Personalization Agent itself because it shall has similar right to Personalization Agent's.

■ **Application Loader**

The Application Loader executes the technical process that loads applications and each relevant personalization data onto each MCD according to the instruction of the Application Provider, the security policies and processes established by Personalization Agent.

■ **ePassport Applicant (ePassport Holder)**

Users of the service provided by the Personalization Agent through ePassport. After applying an ePassport, one receives ePassport properly issued by issuing policy. A holder of ePassport submits one's ePassport to border control system in order for the Inspection System to check it. During border control, Inspection System and/or relevant persons verify according to each country's ePassport border control policy .

■ **ePassport system**

Reception Organization

Reception Organization identifies ePassport applicant's personal data and biometric data when receiving in cooperation with other related organizations like Police Agency and passes the application to Personalization Agent.

Document Verifier

Document Verifier generate IS certificate using CVCA certificate and DV certificate and provides it to Inspection System.

■ **Developer**

IC chip developer

The IC chip developer performs development of underlying IC chip of the TOE.

MULTOS OS Developer

The MULTOS OS developer performs development of the MULTOS operating system by implementing the requirements specified by the MAOSCO on the chip supplied by an IC Chip Manufacturer.

Application Writer

The Application Writer develops an application according to the requirements and the specifications of the application issuer. The Application Writer should be granted the license by MAOSCO.

Application Provider

The Application Provider manages the components that are required to load an application onto a card such as the application code, application data, key and data for the ePassport Holder. The Application Provider plays a role in supporting the MCD (ePassport) Holder.

■ **Manufacturer**

IC Chip Manufacturer

The IC chip manufacturer is responsible for receiving the ROM code from the MULTOS OS Developer and loads it onto the IC chip. The MULTOS (KMA) supplies the unique transport key and ID for each MCD to a IC Chip Manufacturer.

Module Manufacturer

The Module Manufacturer is responsible for cutting the IC chip wafer and assembling it into the COB (Chip On Board).

e-Cover Manufacturer

The e-Cover Manufacturer produces e-cover by embedding COB module in antenna inlay.

MRTD Manufacturer

MRTD Manufacturer combines ePassport booklet with e-Cover according to requirements of the Personalization Agent. Under the Personalization Agent's permission, MRTD Manufacturer can enable MULTOS OS and load application. MCD enablement data and the Personalization Agent's unique data shall be loaded onto ePassport.

■ **Attacker**

A source of threats trying:

- to identify and trace the movement the MRTD's chip remotely (without knowing or reading the printed MRZ data),
- to read or to manipulate the logical MRTD without appropriate authorization,
- to forge or a copy a genuine MRTD.

2.9 TOE Life Cycle

SPass 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.

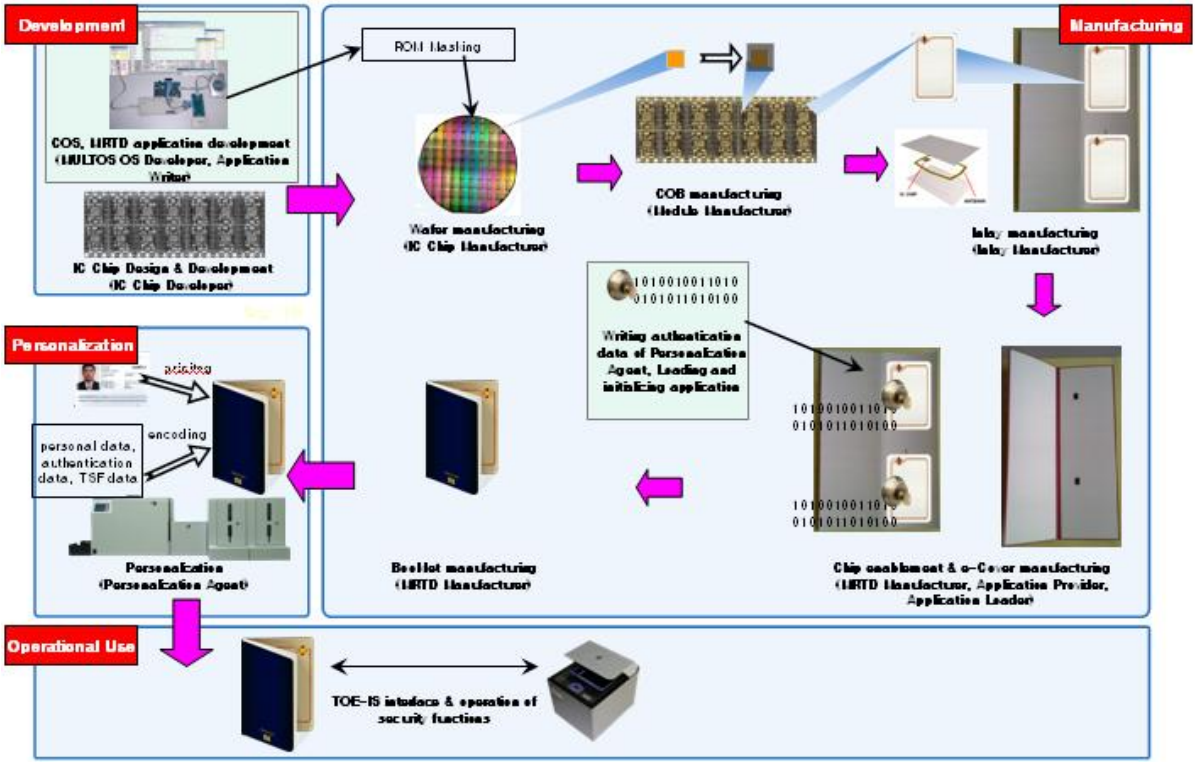


Figure 6. ePassport Life Cycle

Details of lifecycle for ePassport IC chip and the TOE are as shown in Table 6.

Table 6. Life Cycle of the MRTD Chip and the TOE

Phase	Life Cycle of the MRTD Chip	Life Cycle of the TOE	Details
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip dedicated S/W		
		② MULTOS developer to develop TOE (COS, MRTD Application) using IC chip and the dedicated software	TOE development process

Phase 2 (Manufacturing)	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 module, and to perform MISA operation after receiving MISA from KMA (Personalization Agent) ③-3. The Module manufacturer to make COB	③-1. MULTOS developer and KMA (Personalization Agent) to merge KMA public key and relevant information into ROM and to distribute TOE to IC chip manufacturer	TOE distribution process
		④-1. The e-Cover manufacturer to combine each module to antenna inlay and to make e-Cover ④-2. The ePassport manufacturer to enable MCD according to MULTOS security mechanism, and (as the role of the application loader) to load the MRTD Application supplied by the application provider onto EEPROM of MCD ⑤ The ePassport Manufacturer delegated from the personalization agent to write the authentication information of the personalization agent into EEPROM ⑥ The ePassport manufacturer to embed the IC chip in the passport book	TOE installation, generation, and start-up process
Phase 3 (Personalization)		⑦ After first authentication (update of personalization key), the Personalization agent to make room for personalization data in EEPROM and to create SOD by digital signature on ePassport identity data ⑧ The Personalization agent to record the ePassport identity data, the authentication data (including SOD) and the TSF data in the TOE	
(Operational Use)		⑨ The Inspection System to verify the ePassport and to check identity of the ePassport holder by communicating with the TOE	

3 TOE Security Environment

The TOE security environment defines assumptions, threats and organizational security policies in order to determine the scope of the expected operation environment of the TOE.

3.1 Assumptions

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

A. Certificate Verification

The Inspection System, 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 MRTD 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 MRTD for the MRTD 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 MRTD holder if the BAC mutual authentication using the BAC authentication key succeeds. Then, by establishing the BAC secure messaging with the BAC session key, it ensures the confidentiality and integrity of all transmitted data. The BIS verifies the SOD by executing the PA after the BAC. Then, by calculating and comparing a hash value for the personal and authentication data of the MRTD holder, it verifies the forgery and corruption for the personal and authentication data of the MRTD holder. If the BIS supports AA security mechanism as an option, the BIS additionally performs AA and explicitly detects forgery and modification of the TOE via Verification of the digital signature which TOE generates.

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 MRTD 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 MRTD holder. Therefore, the EIS is provided the biometric data of the MRTD holder from the TOE. If the BIS supports AA security mechanism as an option, the BIS explicitly detects forgery and modification of the TOE by performing AA after EAC-CA and PA and before EAC-TA .

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 EAL4+(SOF-high) or higher level. The cryptographic operation supported by the IC chip may be provided in the co-processor of the IC chip or cryptographic libraries loaded in the IC chip.

A.MRZ Entropy

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

Application Notes: In order to 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. However, MRZ entropy may be determined and applied to the TOE in accordance with personalization agent policy and thus strength of function can not be guaranteed.

3.2 Threats

The MRTD 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 security target, the IC chip provides functions of physical protection in order to protect the TOE according to the A. IC chip of the PP. Therefore, the physical threat of the IC chip itself by the high-level threat agent is not considered. Nevertheless, it cannot be ignored that possibility of high-level attacks via logical methods is high.

Therefore, the threat agent to the TOE has the high level of expertise, resources and motivation, and the attacker is likely to find the weakness to be misused.

<Threats to the TOE in the Personalization phase>

T. Application Program Interference

The threat agent may attempt access to the user data and TSF data by exploiting other application pro-grams loaded in the MRTD chip and may deactivate or bypass security functions of the TOE.

T.TSF Data Modification

The threat agent may modify the transmitted TSF data when the Personalization agent records TSF data or attempt access to the stored TSF data by using the external interface through the Inspection System.

<BAC-related Threats in the Operational Use phase>

T. Eavesdropping

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

T. Forgery and Corruption of Personal Data

In order to forge and corrupt the personal data of the MRTD 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 Replay Attack

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[7].

< 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 MRTD 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 MRTD 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.

[7]'T.BAC Authentication Key Disclose' was deleted, so description of its threat was deleted (Refer to 'T.Residual Information').

T.IS Certificate Forgery

In order to obtain the access-rights the biometric data of the MRTD 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. Session Data 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 cipher-text only attack as the same session key is used in each BAC session. When the BAC session key is generated with the same random number used in the BAC mutual authentication, 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 MRTD holder realizing it.

< Threats related to the IC chip Support >

T. Malfunction

In order to bypass security functions or to damage the TOE executable code 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 phrase>

T. Leakage to Cryptographic Key Information

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

T. MRTD Reproduction

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

T. Residual Information

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.

Application Notes : TOE does not use the method generating BAC authentication key and writing in secure memory of MRTD IC chip in the Personalization phase but generates BAC authentication key in Operational Use phase after MRTD personalization. Therefore, 'T.BAC Authentication Key Disclose' is deleted because the disclose threat of BAC authentication key written in secure memory in MRTD IC chip is not need to be considered, and the disclose threat of BAC authentication key from residual information in temporary memory is only considered.

T.IC chip Forgery[8]

The threat agent can forge the MRTD by getting the MRTD user data including SOD and loading the data in the new IC chip.

3.3 Organisational Security Policy

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

P. International Compatibility

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

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

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 MRTD access control policies of the Personalization agent.

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

P. Application Program Loading

[8] Added as the AA-relevant security environment

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

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

P. Personalization Agent

The personalization agent shall issue the ePassport in 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. Open Platform OS Access Control[9]

The TOE shall perform the MCD protection mechanism and the application management mechanism not against the access-control policy of the MULTOS platform.

Application Notes : In MULTOS, the personalization agent generates the unique symmetric key based transport key by MCD and writes it in inactive memory, and generates the unique MSM Control Data, encrypts it with the transport key, and transports it separately in the Personalization phase.

Each MCD allows to load application only in case the MCD successfully installs MSM Controls Data. When loading application data and code can be encrypted before loading according to the policy of personalization agent and loading application is allowed only in case that validity check for modification, removal, insertion, and replay passes successfully with ALC generated by personalization agent.

Deleting loaded applications shall be able to be performed only with valid ADC which the personalization agent generates, and it is only performed when the personalization agent attempts to do in the TOE installing, generating and operating process or the TOE destruction phase [10].

P. MRTD Access Control

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

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

[9] Added to deal with MULTOS-relevant security functions

[10] The application deletion can be blocked as the ADC including the digital signature of Personalization agent is not generated

Table 7. MRTD Access Control Policies

List of Subjects		List of Objects	Objects									
			Personal data of the ePassport holder		Biometric data of the ePassport holder		ePassport Authentication data		EF.CVCA		EF.COM	
		Security Attributes / Security Attributes	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights	Read-Rights	Write-Rights
Subjects	BIS	BAC Authorization	allow	deny	deny	deny	allow	deny	deny	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 MRTD shall execute certification practice to securely generate and manage a digital signature key and to generate, issue, operate, and revocate 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 MRTD 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 of 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 MRTD attached with IC chip is not opened.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

O. Open Platform OS Issuance[11]

The TOE shall activate MCD by enablement processing on the authority of Issuer. During the Manufacturing and Operational use phase, The TOE shall support the process of application loading (or deleting) and shall assure that the initial key can be written into TOE by and authenticated Personalization Agent

Application Notes : Open platform OS issuance includes MCD enablement, load or deletion of MRTD Applications and MULTOS applications authenticated by the personalization agent, writing initial key (used for personalization agent authentication in Personalization phase), etc.

O. Management

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

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

O. Security Mechanism Application Procedures

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

Application Notes : The TOE shall ensure that the application order of PA, BAC and EAC security mechanisms conforms to 2.1.1 Standard MRTD Inspection Procedure and 2.1.2 Advanced MRTD Procedure of the EAC specification and shall not allow requests from the Inspection System that do not correspond to the security mechanism application order. In case of implementation different from procedures of the EAC specification, the ST author shall ensure reliability and secure operation that conforms to the EAC specification.

O. Session Termination

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

[11] Added to deal with MULTOS-relevant security functions

O. Secure Messaging

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

O. Domain Separation

The TOE shall provide means to prevent interference and tampering of the TSF and TSF data by the external IT entities.

Application Notes : The TSF data used inside the TOE shall be stored in secure memory controlled by the COS so that not to be accessed through external interface. Also, the TOE shall separate execution domains between the MRTD Application loaded in the MRTD chip and other application programs.

O. Certificate Verification

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

O. Self-protection

The TOE shall protect itself so that to preserve secure state from attempt of bypassing and modification of TSF executable code and data at start-up.

O. Deleting Residual Information

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

O. Replay Prevention

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

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

O. Access Control

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

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

O.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 MRTD 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 MRTD 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[12]

The TOE can verify own genuineness to the Inspection System as the TOE signs random number transferred from the Inspection System.

4.2 Security Objectives for the Environment

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

OE. Passport Book Manufacturing Security

Physical security measures(security printing, etc.) for the MRTD 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 MRTD holder against the printed identity information page of the MRTD.

OE. Application Program Loading

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

OE. Certificate Verification

The Inspection System, such as the BIS and the EIS, verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and

[12] Added to deal with AA to the PP

corruption of the MRTD 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 MRTD 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 MRTD. The Personalization agent shall deactivate the writing function before the TOE delivery to the Operational Use phase.

OE. Handling Information Leakage

The co-processor of the CI chip or cryptographic libraries loaded in the IC chip used by the TOE shall implement countermeasures to prevent exploiting of leakage information during cryptographic operation for the TSF.

OE. Inspection System

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

OE.IC chip

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

OE.MRZ Entropy

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

OE.PKI

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

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

OE. Range of 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 IC chip is not opened.

5 IT Security Requirements

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

5.1 TOE Security Functional Requirements

The security functional requirements specified in this security target select and use related functional components from Part2 of the CC to satisfy Security Objectives for the TOE in previous section. The security functional requirements specified in this security target consist of the following components from Part2 of the CC, summarized in the following [Table 8].

The strength of function (SOF) for FCS_CKM.1 in this security target is “SOF-high”[13].

Table 8. Security Functional Requirements

Security functional class	Security functional component	
Cryptographic support (FCS)	FCS_CKM.1	Cryptographic key generation (Key Derivation Mechanism)
	FCS_CKM.2(1)	Cryptographic key distribution(KDF Seed Distribution for BAC session key generation)
	FCS_CKM.2(2)	Cryptographic key distribution(KDF Seed Distribution for EAC session key generation)
	FCK_CKM.4	Cryptographic key destruction
	FCS_COP.1(3)	Cryptographic operation(Hash Function)
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control(Open platform OS)
	FDP_ACC.1(2)	Subset access control(MRTD)
	FDP_ACF.1(1)	Security attribute based access control (Open platform OS)
	FDP_ACF.1(2)	Security attribute based access control (MRTD)
	FDP_DAU.1	Basic data authentication
	FDP_RIP.1	Subset residual information protection
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.1(1)	Timing of Authentication (BAC Mutual Authentication)
	FIA_UAU.1(2)	Timing of Authentication (EAC-TA)
	FIA_UAU.1(3)	Timing of Authentication (Personalization Agent Authentication)

[13] FCS_COP.1(1) and FCS_COP.1(2) described as security functional requirements of IT environment are excluded and the strength of function is not applied to FIA_UAU.4 and FMT_MTD.3 whose strength of function are determined by the randomness of IC chip random number generator (IT environment).

	FIA_UAU.1(4)	Timing of Authentication (MULTOS Application Authentication)
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1(1)	Management of security functions behavior(Open platform OS)
	FMT_MOF.1(2)	Management of security functions behavior (MRTD)
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3(1)	Static attribute initialization(Open platform OS)
	FMT_MSA.3(2)	Static attribute initialization (MRTD)
	FMT_MTD.1(1)	Management of TSF data (Certificate Verification Info.)
	FMT_MTD.1(2)	Management of TSF data (SSC Initialization)
	FMT_MTD.1(3)	Management of TSF data (Platform Enablement)
	FMT_MTD.3	Secure TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
	FPT_TST.1	TSF testing

5.1.1 Cryptographic Support

FCS_CKM.1 Cryptographic key generation (Key Derivation Mechanism)

Hierarchical to: No other components.

Dependencies**:** [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.1.1 The TSF shall generate **cryptographic 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 TOE generates the BAC authentication key, BAC session key and EAC session key by using key derivation mechanism.

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

Hierarchical to: No other components.

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

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].

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

Hierarchical to: No other components.

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

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

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

FCS_CKM.4.1 The TSF shall destroy **cryptographic 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].

Application Notes : The ST author shall specify the method to securely destroy the keys generated by the key derivation mechanism. It can be assigned as ‘none’ if there is no standard list for reference.

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

Hierarchical to: No other components

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 The TSF shall perform [hash operation] in accordance with a specified cryptographic algorithm [*SHA-1*] and cryptographic key sizes [none] that meet the following: [*ISO/IEC 10118-3*[14]].

Application Notes : In the key deviation mechanism of the ICAO specification, SHA-1 is used as hash function in order to generate the session key used in the BAC or EAC secure messaging.

5.1.2 User Data Protection

FDP_ACC.1(1) Subset access control (Open platform OS)[15]

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 [open platform OS access control policies] on [subjects, objects, operations defined at [Table 9]].

Table 9. Operations by subject-object of open platform OS

	Subject	Object	Operation
Open platform OS enablement	Personalization agent	MCD	MCD enablement
Application management	Personalization agent	Application of MRTD Application of MULTOS	Loading Deleting

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

Hierarchical to : No other components.

Dependencies : FDP_ACF.1(2) Security attribute based access control (MRTD)

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

a) Subjects

(1) Personalization agent

(2) BIS

(3) EIS

(4) [None]

[14] Satisfying the standard of FIPS 180-2 with this, too

[15] Added to deal with MULTOS-relevant security functions

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 (Open platform OS)[16]

Hierarchical to: No other components.

Dependencies : FDP_ACC.1(1) Subset access control (Open platform OS)

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [open platform OS access control policies] to objects based on the following: [[Table 10], [Table 11], and [Table 12]].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [[Table 10], [Table 11], [Table 12]].

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

FDP_ACF.1.4. The TSF shall explicitly deny access of subjects to objects based on the [[Table 10], [Table 11], [Table 12]].

Table 10. Open Platform OS subject-relevant Security Attributes

Subjects	Security Attributes
Personalization Agent	MCD enablement-rights
	Application load-rights
	Application delete-rights

[16] Added to deal with MULTOS-relevant security functions

Table 11. Object-relevant Security Attributes

Objects	Security Attributes	
	Object's Operation	Security Attributes of Object's Access-Rights
MCD	Enablement-rights	MCD enablement-rights (Detail attributes: MCD enabled flag, MCD_ID)
MRTD Application	Load-rights	Application load-rights (Detail attributes: ALC, AID, MCD Permission, History List)
	Delete-rights	Application delete-rights (Detail attributes: ADC, AID, MCD Permission)
MULTOS Application	Load-rights	Application load-rights (Detail attributes: ALC, AID, MCD Permission, History List)
	Delete-rights	Application delete-rights (Detail attributes: ADC, AID, MCD Permission)

Table 12. MULTOS Detail Security Attribute-relavant Access Rules

Detail security attributes	Governing access rule	Approval access rule	Denial access rule
MCD enabled flag	Demonstrating that MCD is enabled(that is, MSM Control Data of this MCD is installed)	Progressing the MSM Controls Data installaion state if MCD is not enabled.	Stopping the MSM Controls Data installation state if MCD is enabled.
MCD_ID of MCD own and MCD_ID loaded on MSM Controls Data	Demonstrating that MCD_ID of MCD own is identical with MCD_ID loaded on MSM Controls Data.	Progressing the MSM Controls Data installaion state if two MCD_IDs are identical.	Stopping the MSM Controls Data installation state if two MCD_IDs are not identical.
MCD enabled flag	Demonstrating that MCD is enabled(that is, MSM Controls Data of this MCD is installed)	Progressing the application load state if MCD is enabled.	Stopping the application load state if MCD is not enabled.
The unique AID in ALC and AID of the application	Demonstrating that there are other applications having same AID in this	Progressing the application load state if there are	Stopping the application load state if there are

intended to be loaded	MCD	not other applications having same AID	other applications having same AID
Application load Permission and MCD load Permission	Demonstrating that the application load permission is compatible with the MCD permission to be installed when MCD is enabled	Progressing the application load state if two permissions are compatible each other	Stopping the application load state if two permissions are not compatible each other
History list	Deciding that the application is reloaded on this MCD and it was authorized	Progressing the application load state if the application is reloaded and it was authorized	Stopping the application load state if the application is reloaded and it was unauthorized
The unique AID in ADC and AID of the loaded application	Demonstrating that there is any application having AID specified in ADC	Progressing the delete state if there are applications having AID specified in ADC	Stopping the delete state if there is no application having AID specified in ADC
The application delete Permission and the MCD load Permission	Demonstrating that the application delete permission is compatible with MCD permission installed when MCD is enabled	Progressing the application delete state if two permissions are compatible each other	Stopping the application delete state if two permissions are not compatible each other
Application access Permission and Strong Cryptography[17] Flag by each primitive	Checking that the access permission of application includes Strong Cryptography when the application is operated.	Permitting the primitive access if the application access permission includes Strong cryptography	Denying the primitive access if the application access permission does not include Strong cryptography

FDP_ACF.1(2) Security attribute based access control (MRTD)

Hierarchical to: No other components.

Dependencies : FDP_ACC.1(2) Subset access control (MRTD)

FMT_MSA.3 Static attribute initialization

[17] DES/TDES/SEED/AES encryption/decryption, Modular operation(RSA, addition, subtraction, multiplication, and division), ECC operation, SHA-1/SHA256, Asymmetric Hash, and Random Prime Number Generation Primitive, etc are classified to Strong Cryptography Primitive.

FDP_ACF.1.1 The TSF shall enforce the [MRTD access control policy] to objects based on the following: [[Table 13], [Table 14], and [None]].

Table 13. Subject-relevant Security Attributes

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

Table 14. Object-relavant Security Attributes

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

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

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: [None].

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) [None]

FDP_DAU.1 Basic data authentication

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [MRTD IC chip Genuineness Verification Data].

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

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 [*deallocation of the resource from*] the following objects: [

a) BAC session key

b) EAC session key

c) Document basic access key

d) [Random number]

].

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to : No other components.

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

FDP_UCT.1.1 The TSF shall enforce the [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.

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1 The TSF shall enforce the [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. The ST author shall implement additional security mechanism in case of selecting 'replay' in selection operation.

5.1.3 Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when "*an administrator configurable positive integer within [range defined below]*" unsuccessful authentication attempts occur related to [

a) BAC mutual authentication

b) EAC-TA

c) [Personalization agent authorization]

d) [MULTOS application authorization]

].

- One time at a single power-on session in case of BAC mutual authentication and EAC-TA
- One time at a single power-on session in case of MCD enablement, loading application, and deleting application, and maximum 225 times accumulated regardless of a session
- One time at a single power-on session in case of personalization agent authorization

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [user session termination, disablement of pertinent function]**.**

Application Notes 1 : In case of a failure of the BAC mutual authentication or EAC-TA, it is recommended to terminate the BAC or EAC secure messaging. However, the ST author can replace it with another equivalent mechanism. The ST author shall assign the number of unsuccessful authentication attempts by agreeing with the Personalization agent.

Application Notes 2 : MCD enablement is a procedure that will be successfully completed when successfully decrypted is MCD enablement data which is encrypted and transported using MCD-relevant unique transport key only Personalization agent knows and imports to MCD in the manufacturing phase. Therefore, it is a procedure to authenticate Personalization agent implicitly. On the other hand, only the retry counter of the MCD enablement procedure is changeable.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

User	**Security attributes**	**Uses of the security attributes**
Personalization agent	Global Key Certification Key (kck)	kck_pk is a public key of KMA merged into the ROM region of MCD through the ROM key integration, and kck_pk is used to demonstrate the signature of KMA included in ALC/ADC
	MCD unique asymmetric transport key (mkd)	mkd key pair is generated by KMA and stored in the EEPROM region of MCD during the MCD enablement, and it decodes KTU encoded by mkd_pk(public key) to mkd_sk(private key) when

		application is loaded as the Confidential ALU type.
	MCD unique symmetric transport key (tkv)	tkv is stored in the EEPROM region of MCD through MISA operation, and it is used to decode MCD enablement data encoded by KMA in MCD.
	MCD Issuer ID	MCD Issuer ID is unique ID of the personalization agent granted by KMA, it is stored in the EEPROM region of MCD during the MCD enablement and used to compare with MCD Issure ID included in ALC/ADC Permission.

]

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

Hierarchical to : No other components.

Dependencies to : FIA_UAU.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [

a) indication that support the BAC mechanism

b) [none]

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

FIA_UAU.1.2 The TSF shall 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_UAU. 1.1.

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 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 user is authenticated.

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

FIA_UAU.1(3) Timing of authentication (Personalization Agent Authorization)

Hierarchical to : No other components.

Dependencies to : FIA_UAU.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [

a) to perform instructions[18] for collecting basic data

b) to perform the integrity demonstrating instruction[19] about the specified region of TSF execution code

c) to perform the selecting instruction[20] of the MRTD

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

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

FIA_UAU.1(4) Timing of authentication (MULTOS Application Authentication)

Hierarchical to : No other components.

Dependencies to : FIA_UAU.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [

a) to perform the instruction[21] confirming the application ID and keeping memory

b) to perform of the instruction[22] loading each detail component of application

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

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user except the actions stipulated 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) [None]

].

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide [

---

[18] Get Configuration Data, Get Data, Get Manufacturer Data, Get MULTOS Data, Get Purse Type

[19] Check Data

[20] Select File

[21] Open MEL Application

[22] Load Application Signature, Load Code, Load Data, Load DIR File Record, Load FCI Record, Load KTU Ciphertext

a) BAC mutual authentication

b) EAC-TA

c) [Personalization agent authentication]

d) [MULTOS application authentication]

] to support user authentication.

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

a) The BIS or EIS shall succeed the BAC mutual authentication in order to have the BAC authorization and **AA 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 **AA 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) [In order to have MCD enablement-rights, the personalization agent shall have MSM Control Data encrypted with enablement data including MCD_ID of the MCD as transport key.]

d) [The MULTOS application shall succeed the authentication through ALC in order to be loaded on MCD successfully and succeed the authentication through ADC in order to be deleted from MCD successfully.]

].

FIA_UID.1 Timing of identification

Hierarchical to : No other components.

Dependencies : No dependencies

FIA_UID.1.1 The TSF shall allow [

a) to establish the 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 MRTD Application, the TOE identifies it with the Inspection System. From this, the TOE identifies the application with AID(Application Identifier) in case that MULTOS application requires to use TOE interface.

5.1.4 Security Management

FMT_MOF.1(1) Management of security functions behavior(Open platform OS)

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 *determine the behavior of* the functions [loading and deleting applications] to [Personalization agent].

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

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 [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 MRTD Application data in the Personalization phase.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies : [FDP_ACC.1(2) Subset access control(MRTD) or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Open platform 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 [Personalization agent] to specify alternative initial values to override the default values when an object or information is created.

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

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [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 [Personalization agent] to specify alternative initial values to override the default values when an object or information is created.

Application Notes : When generating user data (EF.DG1~16, EF.SOD, EF.COM, EF.CVCA) in the Personalization phase, the Personalization agent shall define security attributes of object's operation and object's access-rights in FDP_ACF.1.1(2).

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

Hierarchical to: No other components.

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

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

a) EAC chip authentication private key

b) initial current date

c) initial CVCA certificate

d) initial CVCA digital signature verification key

e) [AA chip authentication private key[23]]

f) [Personalization agent issuing key]

g) [Life cycle settings]

] to [Personalization agent in the Personalization phase].

Application Notes: The Personalization agent issuing key used to get issuing rights by Personalization agent is generated by updating the Personalization agent initial issuing key generated from FMT_MTD.1(3) 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
FMT_SMR.1 Security roles

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 (Platform enablement)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

[23] Added to deal with AA

FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *generate* the [MSM Controls Data, Personalization agent initial issuing key] to [Personalization agent].

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

a) Function to write user data and TSF data in the Personalization phase

b) Function to verify and update the CVCA certificate, CVCA digital signature verification key and current data in the Operational Use phase

c) [Function to write the Personalization agent initial issuing key in the phase and enablement]

].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

a) Personalization agent

b) [None]

].

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

Application Notes : The Personalization agent is defined as the role to execute a), c) security management function of FMT_SMF.1. The TSF executes security management functions to FMT_MTD.1(2) and b) of FMT_SMF.1. However, the TSF is not defined as the role since it is not a user. The Application loader and MRTD manufacturer can role the security manager in case of being entrusted by the Personalization agent, but security role which the TOE maintains is the Personalization agent.

5.1.5 TSF Protection

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: ADV_SPM.1 Informal TOE security policy model

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) [Failure of inspecting randomness for random number generator provided by IC chip]

].

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) [None]

] if modifications are detected.

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

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Application Notes : The TSF shall separate secure memory not to be affected by interference and tampering from other memory domains. Also, the TSF shall separate the MRTD Application not to be affected by interference and tampering from other application programs.

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: FPT_AMT.1 Abstract machine testing

FPT_TST.1.1 The TSF shall run a suite of self tests *periodically during normal operation* to demonstrate the correct operation of the [*Open platform*].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [*MSM Controls Data*].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.2 Security Functional Requirements for IT Environment

Security functional requirements defined in this ST are selected from CC Part 2 to meet TOE security objectives identified in the previous section, and these consist of components selected from CC Part 2. The following Table presents components of security functional requirements about IT environment used in this ST to meet security objectives about IT environment identified in section 4.

Table 15. Security functional requirements for IT environment

Security Functional Class	Security Functional Component	
Cryptographic Support (FCS)	FCS_COP.1(1)	Cryptographic operation (Symmetric Key Cryptographic Operation)
	FCS_COP.1(2)	Cryptographic operation (MAC)
	FCS_COP.1(4)	Cryptographic operation (Digital signature Verification for Certificates Verification)
	FCS_COP.1(5)[24]	Cryptographic operation (AA Digital signature Generation for Genuineness Verification)
	FCS_COP.1(6)[25]	Cryptographic operation (MULTOS DES)
	FCS_COP.1(7)[26]	Cryptographic operation (MULTOS RSA)
	FCS_COP.1(8)[27]	Cryptographic operation (MULTOS Asymmetric Hash)
Privacy(FPR)	FPR_UNO.1	Unobservability

5.2.1 Cryptographic Support

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

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [message encryption, decryption operation] in accordance with a specified cryptographic algorithm [*TDES*] and cryptographic key sizes [*112 bit*] that meet the following: [*ISO/IEC 18033-3*].

Application Notes : The TOE uses the TDES cryptographic algorithm for the confidentiality protection of the transmitted data of the BAC or EAC secure messaging, for the BAC mutual authentication and

[24] Added to deal with AA

[25] Added to deal with MULTOS OS to the PP

[26] Added to deal with MULTOS OS to the PP

[27] Added to deal with MULTOS OS to the PP

for the BAC key distribution. For operation mode of the cryptographic algorithm used, the CBC mode with IV=0 as defined in ISO/IEC 10116 is used. However, because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

FCS_COP.1(2) Cryptographic operation (MAC)

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [MAC operations] in accordance with a specified cryptographic algorithm [*Retail MAC*] and cryptographic key sizes [*112 bit*] that meet the following: [*ISO/IEC 9797-1*].

Application Notes : The TOE uses the Retail MAC algorithm for the integrity protection of the transmitted data of the BAC or EAC secure messaging and for the BAC mutual authentication. The Retail MAC uses the MAC algorithm 3, the block cipher DES, the sequence message counter and the padding mode 2 defined in ISO/IEC 9797-1. However, because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

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

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [Digital Signature Verification] in accordance with a specified cryptographic algorithm [*RSASSA-PKCS1-v1.5-SHA-256, ECDSA-SHA-224, ECDSA-SHA-256, [RSASSA-PKCS1-v1.5-SHA-1, ECDSA-SHA-1]*] and cryptographic key sizes [1024 bit(RSA), 192 ~ 256 bit(ECDSA)] that meet the following: [*PKCS#1, ISO/IEC 15946-2*].

Application Notes : In Appendix A.3 Terminal Authentication of the EAC specifications, the digital signature algorithm, hash algorithm and digital signature key sizes are defined as of the following. The ST author shall specify the cryptographic key sizes by referring to [Table 16] so that to satisfy the SOF-high. However, because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

Table 16. Detail of Digital Signature in the EAC Specifications

Digital Signature Algorithm	Hash Algorithm	Digital Signature Key Sizes
RSASSA-PKCS1-v1.5	SHA-1, SHA-256	1024,1280,1536,2048,3072 bits
RSASSA-PSS	SHA-1, SHA-256	1024,1280,1536,2048,3072 bits
ECDSA	SHA-1, SHA-224 / SHA-256	160,192,224,256 bits

FCS_COP.1(5)[28] **Cryptographic operation (**AA Digital signature Generation for Genuineness Verification **)**

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [Digital Signature Generation] in accordance with a specified cryptographic algorithm [RSASSA-PKCS1-v1.5-SHA-1] and cryptographic key sizes [1024 bit] that meet the following: [ISO/IEC 9796-2 Digital Signature scheme 1].

Application Notes : Because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

FCS_COP.1 (6) Cryptographic operation (MULTOS DES)

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [decryption of protected code and data region of applications, MSM Controls Data decryption] in accordance with a specified cryptographic algorithm [MULTOS single key DES encryption, MULTOS multiple key DES encryption] and cryptographic key sizes [64 bit(single key), 128 bit(multiple key)] that meet the following: [the following list of standard].

[28] Added to deal with AA to the PP

- MULTOS 4.2.1 Architecture Specification Security Specification (mao-doc-101-003), March, 2006, 5.3.5 MULTOS DES Single Encipher.
- MULTOS 4.2.1 Architecture Specification Security Specification (mao-doc-101-003), March, 2006, 5.3.6 MULTOS DES Multi-key Encipher.

Application Notes : Because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

FCS_COP.1 (7) Cryptographic operation (MULTOS RSA)

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [Digital Signature Verification] in accordance with a specified cryptographic algorithm [Modular Exponentiation] and cryptographic key sizes [1024 ~ 2048 bit(modulus)] that meet the following: [the following list of standard].

- MULTOS 4.2.1 Architecture Specification Security Specification(mao-doc-101-003), March, 2006 , 5.2.1 X^Y MOD(N): exp(mod, exp_parameters, X)

Application Notes : Because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

FCS_COP.1 (8) Cryptographic operation (MULTOS Asymmetric Hash)

Hierarchical to: No other components.

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

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

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

FCS_COP.1.1 IT environment shall perform [MCD code integrity Verification, MSM Controls Data integrity Verification, code integrity of application ALU Verification] in accordance with a specified cryptographic algorithm [Asymmetric Hash] and cryptographic key sizes [768 ~1024 bit (hash modulus)] that meet the following: [the following list of standard].

- MULTOS 4.2.1 Architecture Specification Security Specification (mao-doc-101-003), March, 2006 , 5.1.1 The Asymmetric Hash Function.

Application Notes : Because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip, this requirement is described as a requirement for the IT environment.

5.2.2 Privacy

FPR_UNO.1 Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

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

c) FCS_COP.1(4) Cryptographic operation (Digital signature Verification for Certificate Verification)

d) [FCS_COP.1(5) Cryptographic operation (AA Digital signature Generation for Genuineness Verification)[29]]

e) [FCS_COP.1(6) Cryptographic operation (MULTOS DES)[30]]

f) [FCS_COP.1(7) Cryptographic operation (MULTOS RSA)[31]]

g) [FCS_COP.1(8) Cryptographic operation (MULTOS Asymmetric Hash)[32]]

] on [

a) Document Basic Access Keys

b) BAC Session Keys

c) EAC Session Keys

d) EAC chip authentication private key

e) [AA chip authentication private key[33]]

f) [MCD transport key]

g) [MCD private key]

] by [TSF**].**

Application notes: The external entity may find out and exploit the cryptographic-related data from physical phenomena (change of current, voltage and electromagnetic, etc.) occurred when the IT environment performs cryptographic operations. IT environment provides the means to handle attacks, such as DPA and SPA, etc. However, this requirement is described as a requirement for the IT environment because the TOE satisfies this requirement by using the co-processor of the certified IC chip or cryptographic libraries loaded in the certified IC chip.

---

[29] Added to deal with AA to the PP

[30] Added to deal with MULTOS OS to the PP

[31] Added to deal with MULTOS OS to the PP

[32] Added to deal with MULTOS OS to the PP

[33] Added to deal with AA to the PP

5.3 TOE security assurance requirements

The security assurance requirements for this Security Target consist of the following components from Part 3 of the CC in accordance with MRTD Protection Profile, and evaluation assurance level is EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) added ADV_DVS.2 and AVA_VLA.4 in consideration of the security management system of MULTOS, the open platform OS. The assurance components are augmented follows:

- ADV_IMP.2 Implementation of the TSF
- ADV_DVS.2 Sufficiency of security measures
- ATE_DPT.2 Testing: low-level design
- AVA_VLA.4 Highly resistant

[Table 17] presents a summary of assurance components.

Table 17. TOE Security Assurance Requirements

Assurance class	Assurance components	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.2	Implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: low-level design
	ATE_FUN.1	Functional testing

	ATE_IND.2	Independent testing : sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of the TOE security function evaluation
	AVA_VLA.4	Highly resistant

5.3.1 Configuration Management

ACM_AUT.1 Partial CM automation

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements

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

ACM_CAP.4 Generation support and acceptance procedures

Dependencies:

ACM_SCP.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

Developer action elements

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements

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

ACM_SCP.2 Problem tracking CM coverage

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements

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

5.3.2 Delivery and Operation

ADO_DEL.2 Detection of modification

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements

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

ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies:

AGD_ADM.1 Administrator guidance

Developer action elements

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements

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

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development

ADV_FSP.2 Fully defined external interfaces

Dependencies:

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements

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

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.2 Implementation of the TSF

Dependencies:

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well-defined development tools

Developer action elements

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

Content and presentation of evidence elements

ADV_IMP.2.1C The implementation representation shall unambiguously 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 internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

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_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Dependencies:

ADV_HLD.2 Security enforcing high-level design

ADV_RCR.1 Informal correspondence demonstration

Developer action elements

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements

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

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

Developer action elements

ADV_RCR1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements

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

ADV_SPM.1 Informal TOE security policy model

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements

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

5.3.4 Guidance Documents

AGD_ADM.1 Administrator guidance

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements

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

AGD_USR.1 User guidance

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of the TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements

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

5.3.5 Life Cycle Support

ALC_DVS.2 Sufficiency of security measures

Dependencies: No dependencies.

Developer action elements

ALC_DVS.2.1D The developer shall produce development security documentation.

Content and presentation of evidence 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 provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.2.3C The evidence 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 of evidence 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.1 Well-defined development tools

Dependencies:

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

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

Evaluator action elements

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

5.3.6 Tests

ATE_COV.2 Analysis of coverage

Dependencies:

ADV_FSP.1 Informal 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 of evidence elements

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

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

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.2 Testing: low-level design

Dependencies:

ADV_HLD.2 Security enforcing high-level design

ADV_LLD.1 Descriptive low-level design

ATE_FUN.1 Functional testing

Developer action elements

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

Content and presentation of evidence elements

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

Evaluator action elements

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

ATE_FUN.1 Functional testing

Dependencies: No dependencies.

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 of evidence elements

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

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

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.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Developer action elements

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

Content and presentation of evidence 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 test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment

AVA_MSU.2 Validation of analysis

Dependencies:

ADO_IGS.1 Installation, generation, and start-up procedures

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence

AVA_MSU.2.1C The guidance documentation 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.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements

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

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of the TOE security function evaluation

Dependencies:

ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

Developer action elements

AVA_SOF.1.1D The developer shall perform a strength of the TOE security function analysis for each mechanism identified in the ST as having a strength of the TOE security function claim.

Content and presentation of evidence

AVA_SOF.1.1C For each mechanism with a strength of the TOE security function claim the strength of the TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of the TOE security function claim the strength of the TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements

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

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.4 Highly resistant

Dependencies:

ADV_FSP.1 Informal functional specification

ADV_HLD.2 Security enforcing high-level design

ADV_IMP.1 Subset of the implementation of the TSF

ADV_LLD.1 Descriptive low-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements

AVA_VLA.4.1D The developer shall perform a vulnerability analysis.

AVA_VLA.4.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence

AVA_VLA.4.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.4.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.4.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.6C The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator action elements

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

AVA_VLA.4.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.4.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.4.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.4.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

6 TOE Summary Specification

This section shows TOE security functions to satisfy TOE security functional requirements. TOE security functions provided by SPass can be divided into 5 groups such as Cryptographic Support (CS), Data Protection (DP), Identification and Authentication (IA), Security Management (SM), and Platform Protection (PP). On the other hand, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, and AVA_VLA.4 are augmented to TOE security assurance requirements.

Table 18. TOE Security Functions

SF Group	SF Identifier	Meaning of SF
Cryptographic Support (CS)	CS1	cryptographic key management
	CS2	supporting cryptographic operation
Data Protection (DP)	DP1	data exchange integrity and confidentiality
	DP2	subset residual information protection
	DP3	data authentication based on asymmetric key
Identification and Authentication (IA)	IA1	MULTOS OS authentication mechanism
	IA2	MRTD authentication mechanism
	IA3	contactless communication
	IA4	multiple authentication mechanism
	IA5	authentication failure handling
Security Management (SM)	SM1	MULTOS OS security management
	SM2	MRTD security management
Platform Protection (PP)	PP1	failure with preservation of secure state
	PP2	non-bypassability and domain separation of the TSF
	PP3	integrity Verification by TSF self-testing

Cryptographic Support (CS)

CS1: SPass generates BAC Keys (ENC and MAC), BAC Session Key and EAC Session key. KDF Seed for creating BAC and EAC session key is distributed as specified on ISO/IEC 11770-2, and PKCS#3 for DH or ISO/IEC 15946-3 for ECDH respectively.

CS2: SPass provides hash function compliant to ISO/IEC 10118-3 and interfaces to use DES/TDES, RSA, and ECC that are supported by IC chip.

Data Protection (DP)

DP1: In the process of personalization, SPass provides functions for confidentiality and integrity verification of TSF data. To ensure confidentiality and integrity of data transmitted after successful BAC or EAC-CA, secure messaging according to ICAO and EAC specification is supported in the operational phase.

DP2: SPass removes previously used re by overwriting '0' to the volatile memory area when de-allocating resources to make any previous information content of a resource, such as BAC session key, EAC session key, BAC Keys and random number, unavailable and ensures secure discard of data. SPass securely

DP3: SPass digitally signs a challenge randomly chosen by the Inspection System with AA private key. The Inspection System can verify that the chip is genuine If and only if the returned signature from the chip is correct.

Identification and Authentication (IA)

IA1: Before successful MCD enablement, SPass grant personalization agent to access less-sensitive data such as MCD basic information, IC basic information and etc., Confirming application ID, allocating memory area for application and loading application components is required to load MULTOS application. Application permission, ALU and ALC Verification is following to load application. Successful application permission and ADC Verification is required to delete application as well.

IA2: SPass returns an error, "Security status not satisfied" if the Inspection System tries to access DG without successful BAC to let Inspection System know BAC is mandatory. BAC, EAC-CA must have been successfully executed before starting EAC-TA.

IA3: Contactless interface protocol complies with ISO/IEC 14443-4 is implemented and Inspection System is identified by means of communication channel based on it. SPass processes commands according to ISO/IEC 7816 and responds.

IA4: Successful authentication by MCD enablement and ALC or ADC verification is required for the personalization agent to have rights to load or delete application on SPass. After successful BAC mutual authentication, BIS and EIS is granted BAC rights. BAC, EAC-CA and EAC-TA must have been successfully executed before accessing sensitive biometric data with EAC rights. AA may be performed if Inspection System supports AA.

IA5: User session shall be terminated if each failed attempt count reaches the pre-specified limit of personalization agent authentication, MULTOS application authentication, BAC mutual authentication.

Security Management (SM)

SM1: SPass supports open platform OS access control function by means that MCD enablement and application loading/deletion is controlled based on the security attributes as specified by ROM Key Integration and MISA operation. ROM Key Integration is a security process to inject KMA's public key in a certain area of MCD before releasing ROM image so that KMA's signature included in ALC or ADC can be verified using that KMA's public key. MISA operation a security process that each unique symmetric key which is diversified from the key known only to KMA is stored in the secure memory area of each MCD while manufacturing and then KMA is able to create MSM controls data

which is encrypted with the unique key so that only the relevant MCD which has the identical key can decrypt the MSM controls data thus be enabled.

SM2: SPass controls access rights of personalization agent, BIS and EIS to the ePassport according to each entity's rights. In the process of manufacturing, an authentication based on the challenge-response must have been executed successfully using initial personalization key which is only known to personalization agent before personalization agent is able to write MRTD Application data such as EAC-CA private key, current date, initial CVCA certificate, initial verification key of CVCA digital signature and AA private key in the secure memory area and disable writing function after finishing personalization. SPass generates EAC session key and then initializes SSC to '0' to terminate BAC secure communication channel before establishing EAC secure communication channel. During EAC-TA, expiration date of CVCA link certificate, DV certificate and IS certificate sent by EIS shall be verified by SPass and if necessary, CVCA certificate, digital signature verification key of CVCA, current date and EF.CVCA shall be internally updated to keep values secure**.**

Platform Protection (PP)

PP1: SPass utilizes PP3 to generate and provide unpredictable random number which is secure against replay attack, where a session shall be terminated if the randomness exceeds tolerance. On the other hand, SPass enables Abnormal Condition Detector provided by IC chip in order to terminate a session and to keep reset state until returning back to the normal operational range when TSF is not in the normal operational range. The integrity verification over TSF data and TSF executable code of OS is performed periodically, where the session is terminated to protect platform if failure is detected.

PP2: When receiving commands within the session, only pre-defined combinations of class bytes (CLA) and instruction bytes (INS) shall be executable by SPass to prohibit bypassing policies and conditions to access the TSF data. "Application Pool" block is allocated respectively by SPass for each application during application loading in order that SPass controls applications to be executable within the allocated area to prevent interference or infringement between applications.

PP3: SPass tests the randomness of the random number generated by random number generator each time SPass receives command within the session. To provide random number secure against replay attack, a probabilistic randomness test measure is used based on FIPS 140-2 and X^2 (chi-square) test. On the other hand, prior to performing MCD enablement, integrity verification is performed to confirm the integrity of the specified area of TSF executable code. The checksum of MCD enablement data is calculated and compared to verify integrity of non-volatile memory area each time SPass receives commands within the session.

7 Protection Profile Claims

This section claims that the ST is in compliance with ePassport Protection Profile V1.0.

7.1 Protection Profile Reference

TOE satisfies all the requirements referenced from the following protection profile.

- ePassport Protection Profile V1.0 [1]

7.2 Protection Profile Tailoring

Table 19 shows tailoring of security functional requirements in the ST.

Table 19. Security Functional Requirements Tailoring List

Security Functional Requirements		Performed Operation in ST	Tailoring
FCS_CKM.2(1)	FCS_CKM.2.1	Selection, Selection	
FCS_CKM.2(2)	FCS_CKM.2.1	Selection, Selection	
FCS_CKM.4	FCS_CKM.4.1	Assignment, Assignment	
FCS_COP.1(1)	FCS_COP.1.1	Selection, Selection, Selection	Modified into SFR on IT environment
FCS_COP.1(2)	FCS_COP.1.1	Selection, Selection, Selection	Modified into SFR on IT environment
FCS_COP.1(3)	FCS_COP.1.1	Selection, Selection	
FCS_COP.1(4)	FCS_COP.1.1	Selection, Selection, Assignment, Assignment	Modified into SFR on IT environment
FDP_ACC.1		Iteration	Changed name into FDP_ACC.1(2)
	FDP_ACC.1.1	Assignment, Assignment, Assignment	
FDP_ACF.1		Iteration	Changed name into

			FDP_ACF.1(2)
	FDP_ACF.1.1	Assignment	
	FDP_ACF.1.2	Assignment	
	FDP_ACF.1.3	Assignment	
	FDP_ACF.1.4	Assignment	
FDP_RIP.1	FDP_RIP.1.1	Selection	
FDP_UIT.1	FDP_UIT.1.1	Selection	
	FDP_UIT.1.2	Selection	
FIA_AFL.1	FIA_AFL.1.1	Assignment, Selection, Assignment	supplemented contents for O.Open Platform OS issuance
FIA_UAU.1(1)	FIA_UAU.1.1	Assignment	
FIA_UAU.1(2)	FIA_UAU.1.1	Assignment	
FIA_UAU.4	FIA_UAU.4.1	Assignment	
FIA_UAU.5	FIA_UAU.5.1	Assignment	supplemented contents for O.Open Platform OS issuance
	FIA_UAU.5.2	Refinement, Assignment	supplemented contents for O.Open Platform OS issuance and O.AA
FMT_MOF.1		Iteration	Changed name into FMT_MOF.1(2)
FMT_MTD.1(1)	FMT_MTD.1.1	Assignment	
FMT_SMF.1	FMT_SMF.1.1	Assignment	
FMT_SMR.1	FMT_SMR.1.1	Assignment	
FPR_UNO.1	FPR_UNO.1.1	Assignment, Assignment	Modified into SFR on IT environment
FPT_FLS.1	FPT_FLS.1.1	Assignment	
FPT_ITI.1	FPT_ITI.1.2	Assignment	
FPT_TST.1	FPT_TST.1.1	Selection, Assignment	
	FPT_TST.1.2	Selection, Assignment	

In case of using cryptographic operation and cryptographic library of underlying IC chip, TOE Security Objectives and the TOE Security functional requirements was modified into Security Objectives for the IT Environment and Security functional requirements for the IT Environment. As a result, O.Handling Information Leakage was changed into OE.Handling Information Leakage and FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4), FPR_UNO.1 were changed into Security Objectives for the IT Environment.

Since TOE uses MULTOS open platform operating system, ePassport application is loaded after activating MCD according to MULTOS security management scheme. Thus, ROM key injection and MISA operation are included, module manufacturer is presented, e-Cover manufacture is detailed as well as loading application into EEPROM and authentication required to personalization agent are described in the process of TOE installation, creation and starting (table 6) in the section 2.9

7.3 Protection Profile Augmentations

Protection Profile includes the minimum Security requirements and dose not define implementation model of the TOE. Developers should define additional security environment, security objectives, security requirements for security problems according to implementation model of the TOE.

Since TOE uses MULTOS open platform operating system, ePassport application shall be loaded after activating MCD according to MULTOS security management scheme. Thus as a TOE asset relating to MULTOS OS, MULTOS user data and MULTOS TSF data were added in the section 2.7. In the section 2.8.1, MULTOS application was identified as a TOE user. In the section 3.3 ‘P.Open Platform OS Access Control’ policy was specified and ‘O.Open Platform OS Issuance’ security objective was specified in the section 4.1. In the section 5.1, ‘FDP_ACC.1(1) Subset access control (Open platform OS)’, ‘FDP_ACF.1(1) Security attributes based access control (Open platform OS)’, ‘FIA_ATD.1 User attribute definition’, ‘FIA_UAU.1(4) Timing of authentication (MULTOS Application Authentication)’, ‘FIA_UID.1 Timing of identification’, ‘FMT_MOF.1(1) Management of security functions behavior(Open platform OS)’, ‘FMT_MSA.3(1) Static attribute initialization (Open platform OS)’, ‘FMT_MTD.1(3) MANAGEMENT OF TSF DATA (PLATFORM ENABLEMENT)’, ‘FMT_SMF.1 Specification of Management Functions ’ TOE security functional requirements were added. In the section 5.2 security functional requirements such as FCS_COP.1(6), FCS_COP.1(7), FCS_COP.1(8) relating to MULTOS OS cryptographic operation were modified into security functional requirements for IT environment .

Though AA (Active Authentication) is optional according to EAC specification, this TOE includes AA security mechanism for Inspection Systems which do not support EAC (e.g., non-EU states) to verify genuineness of SOD. As a result, ‘O.AA’ security objective in the section 4., ‘FDP_DAU.1 Basic data authentication’ in the section 5.1 and ‘FCS_COP.1(5) Cryptographic operation (AA Digital signature Generation for Genuineness Verification)’ in the section 5.2 were added.

This ST added TDES authentication into FIA_UAU.1(3) to identify personalization agent authentication mechanism to grant access right to write ePassport application on the IC chip with TOE security functional requirements and security function

The following security assurance requirements (SAR) are augmented to EAL 4 by PP:

- ADV_IMP.2 “Implementation of the TSF”
- ATE_DPT.2 “Testing: low-level design”

- AVA_VLA.3 “Moderately resistant”

The followings are additional security assurance requirements augmented to PP by ST. These refer to the Common Criteria.

- ALC_DVS.2 Sufficiency of security measures
- AVA_VLA.4 Highly resistant

8 Rationale

This section describes the rationale of security objectives and rationale of security requirements.

8.1 Rationale of Security Objectives

The rationale of security objectives 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 20 shows the mapping between security environments and security objectives.

Table 20. Summary of Mappings between Security Environments and Security Objectives

Security Objectives / Security Objectives	TOE Security Objectives														Security Objectives for Environment										
	O.Management	O.Opne Platform OS Issuance	O.Security Mechanism Application Procedures	O.Session Termination	O.Secure Messaging	O.Domain Seperation	O.Certificate Verification	O.Self-protection	O.Deleting Redisual Information	O.Replay Preventation	O.Access Control	O.BAC	O.EAC	O.AA	OE.Passport Book Manufacturing Security	OE.Procedures of Passport Holder Check	OE.Application Program Loading	OE.Certificate Verification	OE.Personalization Agent	OE.handiling Information Leakage	OE.Inspection System	OE.IC chip	OE.MRZ Entropy	OE.PKI	OE.Range of RF Communication
T.Application Program Interference						X											X								
T.TSF Data Modification	X			X	X	X					X								X						
T.Eavesdropping					X																X				
T.Forgery and Corruption of Personal Data				X							X	X									X				
T.BAC Replay Attack										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.Session Data Reuse									X											X				
T.Skimming										X	X	X								X				X
T.Malfunction								X													X			
T.Leakage to Cryptographic Key Information																			X					
T.MRTD Reproduction						X								X	X									
T.Residual Information								X																
T.IC chip Forgery													X											
P.International Compatibility																		X						
P.Security Mechanism Application Procedures			X																	X				
P.Application Program Loading																X								
P.Personalization Agent	X	X																X						
P.Open Platform OS Access Control		X																						
P.MRTD Access Control	X									X	X	X						X		X				
P.PKI							X															X		
P.Range of RF Communication																								X
A.Certificate Verification																	X	X					X	
A.Inspection System																				X				
A.IC chip																					X			
A.MRZ Entropy																						X		

8.1.1 Rationale of the TOE Security Objective

O. Management

This security objective ensures that the TOE provides the means to write user data in EF domain and the means to write TSF data in secure memory only to the authorized Personalization agent in the Personalization phase and prevents unauthorized access using external interface by deactivating the MRTD Application data writing function of the Personalization agent in the Operational Use phase. Therefore, this security objective is required to counter the threats of T. TSF Data Modification and to enforce P. ePassport Access Control and P. Personalization Agent.

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

O. Open Platform OS Issuance

This security objective ensures that the TOE does not load unauthorized application without the Personalization agent's control for the Personalization agent to securely load MRTD Applications in the intended IC chip, that is, the intended MULTOS Open platform OS loaded chip(MCD), in the

Manufacturing phase. Therefore, this security objective is required to enforce P. Open Platform OS Access Control and P. Personalization Agent.

O. Security Mechanism Application Procedures

This security objective is required to enforce the organizational security policies of P. Security Mechanism Application Procedures since the TOE ensures that the application order of the PA, BAC and EAC security mechanisms according to 2.1.1 Standard MRTD Inspection Procedure and 2.1.2 Advanced MRTD Procedure of the EAC specifications and by not allowing requests from the Inspection System that do not correspond to the security mechanism application order.

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

O. Session Termination

This security objective ensures that the TOE prevents continuous authentication attempts of authentication in order for access to forge and corrupt the personal or biometric data of the MRTD holder and terminates session in case modification for the transmitted TSF data is detected. Therefore, this security objective is required to counter the threats of T. Forgery and Corruption of Personal Data, T. Damage to Biometric Data and T. TSF Data Modification.

O. Secure Messaging

This security objective ensures that the TOE establishes the BAC or EAC secure messaging for secure transmission of the personal and biometric data of the ePassport holder to the Inspection System, and provides the confidentiality and integrity for the transmitted personal and biometric data of the ePassport holder. Therefore, this security objective is required to counter the threats of T. Damage to Biometric Data and T. Eavesdropping. Also, this security objective is required to counter the threat of T. TSF Data Modification by establishing secure messaging when the authorized Personalization agent records TSF data in the Personalization phase, therefore providing integrity for TSF data.

O. Domain Separation

This security objective is required to counter the threat of T. Application Program Interference as the TOE provides the means to prevent interference and tampering from external IT entities by separating execution domains between the TSF loaded in the MRTD chip and other application programs.

This security objective is required to counter the threat of T. TSF Data Modification by preventing TSF data modification as the COS blocks an access from external entities when the TOE records the TSF data in secure memory.

This security objective is required to counter the threat of T. IS Certificate Forgery by protecting the CVCA certificate recorded by the Personalization agent in secure memory in order to detect forgery of the CVCA link certificate from external interference and tampering.

This security objective is required to counter the threat of T. MRTD Reproduction because reproduction of TSF data stored in secure memory is not possible even though an attacker reproduces user data in EF domain by manufacturing illegal chip.

O. Certificate Verification

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

This security objective is required to counter the threats of T. Damage to Biometric Data and T. IS Certificate Forgery by determining the status of forgery as the TOE verifies validity of the CVCA link certificate, DV certificate and IS certificate in the EAC-TA.

O. Self-protection

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

O. Deleting Residual Information

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

O. Replay Prevention

This security objective is required to counter the threat of T. BAC Replay Attack 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. Session Data 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 and Corruption of Personal Data, T. Damage to Biometric Data and T. Skimming and enforce the organizational security policies of P. ePassport Access Control by implementing the rules of allowing or denying of Inspection

System to read user data in accordance with the ePassport access control policies by the Personalization agent.

This security objective is required to counter the threats of T. TSF Data Modification 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 policies of P. ePassport Access Control as the TOE implements the BAC security mechanism to control access to the personal data of the MRTD holder, therefore gives the read-rights for the personal data of the MRTD 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 and Corruption of Personal Data and T. Skimming as the TOE allows the read-rights for the personal data of the MRTD holder only to the authorized Inspection System by generating the BAC session key during the BAC mutual authentication and denies access by the Inspection System that does not have the read-rights.

O.EAC

This security objective is required to enforce the organizational security policies of P. ePassport Access Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the MRTD holder, therefore gives the read-rights for the biometric data of the MRTD 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 MRTD 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 as the Inspection System can notice the genuineness by MRTD digital signature authentication in case that the threat agent performs Inspection System and AA by getting MRTD user data and loading it in new IC chip.

8.1.2 Rationale of Security Objective for Environment

OE. Passport Book Manufacturing Security

This security objective for environment is required to counter the threat of T. MRTD Reproduction by ensuring that Physical security measures(security printing, etc.) for the MRTD 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 Passport Holder Check

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

OE. Application Program Loading

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

This security objective for environment is required to counter the threat of T. Application Program Interference by providing the means to prevent interference and tampering for the TSF as an attacker loads any application program to the IC chip through restricting that only the authorized Personalization agent can load application programs.

OE. Certificate Verification

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

OE. Personalization Agent

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

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

OE. Handling Information Leakage

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

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 and Corruption of 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. Session Data Reuse as the Inspection System generate different temporary public key per session to be transmitted to the TOE in the EAC-CA.

OE. IC chip

This security objective for environment is required to support the assumption of A. IC chip as it uses EAL4+(SOF-high) IC chip that generates random number and provides cryptographic operation in order to support security functions of the TOE and provides the malfunction detection and physical protection, etc.

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

OE. MRZ Entropy

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

OE. PKI

This security objective for environment is required to enforce the organizational security policies of P. PKI and supports the assumption of A. Certificate Verification by implementing and operating the MRTD PKI System that executes certification practice according to CPS, such as to generate digital signature key and to generate· issue· distribute of certificates necessary in supporting PA and EAC security mechanisms. Also, this security objective for environment is required to counter the threat of

T. Damage to Biometric Data by generating, issuing and distributing certificates necessary in the EAC through implementation of the EAC-PKI.

OE. Range of RF Communication

This security objective for environment is required to counter the threat of T. Skimming and enforce the organizational security policies of P. Range of 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 MRTD attached with the IC chip is not opened.

8.2 Rationale for Security Requirements

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.

8.2.1 Rationale for Security Functional Requirements of the TOE

The rationale of the 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 21 presents the mapping between the security objectives and the security functional requirements.

Table 21. Mappings between the security objectives and the security functional

Security Functional Requirements \ Security Objectives	TOE Security Objectives													
	O. Management	O.Open platform OS Issuance	O. Security Mechanism Application Procedures	O. Session Termination	O. Secure Messaging	O. Domain Seperation	O. Certificate Verification	O. Self-protection	O. Deleting Residual Information	O. Replay Prevention	O. Access Control	O.BAC	O.EAC	O.AA
FCS_CKM.1												X	X	
FCS_CKM.2(1)										X		X		
FCS_CKM.2(2)													X	
FCS_CKM.4									X					
FCS_COP.1(3)												X	X	
FDP_ACC.1(1)		X												
FDP_ACC.1(2)											X			
FDP_ACF.1(1)		X												
FDP_ACF.1(2)	X		X								X	X	X	
FDP_DAU.1														X

FDP_RIP.1									X	X				
FDP_UCT.1					X					X				
FDP_UIT.1					X					X				
FIA_AFL.1		X	X	X							X	X	X	
FIA_ATD.1		X												
FIA_UAU.1(1)				X							X	X		
FIA_UAU.1(2)			X	X							X		X	
FIA_UAU.1(3)	X	X												
FIA_UAU.1(4)		X												
FIA_UAU.4										X		X	X	
FIA_UAU.5		X	X								X	X	X	X
FIA_UID.1		X										X	X	
FMT_MOF.1(1)		X												
FMT_MOF.1(2)	X										X			
FMT_MSA.1					X						X			
FMT_MSA.3(1)		X												
FMT_MSA.3(2)	X										X			
FMT_MTD.1(1)	X										X			
FMT_MTD.1(2)			X											
FMT_MTD.1(3)		X												
FMT_MTD.3							X			X			X	
FMT_SMF.1	X	X					X							
FMT_SMR.1	X	X												
FPT_FLS.1								X						
FPT_ITI.1				X	X									
FPT_RVM.1								X			X			
FPT_SEP.1						X					X			
FPT_TST.1								X						

FCS_CKM.1 Cryptographic key generation (Key Derivation Mechanism)

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

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

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 by generating KDF seed.

FCS_CKM.2(2) Cryptographic key distribution (KDF Seed Distribution 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#3).

The distribution method defined in this component satisfies the security objective of O. EAC as it is enables to generate EAC session key of FCS_CKM.1 by generating KDF seed.

FCS_CKM.4 Cryptographic key destruction

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

This component satisfies the security objective of O. Deleting Residual Information as it provides the method of destroying the key generated by the TSF and remained in temporary memory with the method defined by the ST author.

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

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

The hash function defined in this component satisfies the security objective of O. BAC and O. EAC as it enables the KDF to generate the BAC and EAC session key.

FDP_ACC.1(1) Subset access control (Open platform OS)

This component defines list of subjects, objects and operations in order to decide a scope of control for the access control policies for OS and applications in case of open platform OS based MRTD.

The open platform OS access control policies defined in this component satisfies the security objective of O. Open Platform OS Access Control as it defines the Personalization agent as subjects, the MCD, MRTD Applications and other applications, etc. as objects and their relationship as operations.

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

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 MRTD holder and MRTD authentication data, etc. as objects and their relationship as operations.

FDP_ACF.1(1) Security attributes based access control(Open platform OS)

In order to enforce the access control policies for OS and application in case of open platform OS based of MRTD, this component defines security attributes of subjects and objects defined in FDP_ACC.1(1) and specifies the ePassport Access Control rules.

Security attributes and the open platform OS access control rules defined in this component satisfy the security objectives of O. Open Platform OS Issuance as only the authorized Personalization agent with the Personalization agent issuing authorization can perform management functions in the Manufacturing phase and the Personalization phase.

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

In order to enforce the ePassport Access Control policies, this component defines security attributes of subjects and objects defined in FDP_ACC.1(2) and specifies the ePassport Access Control rules.

Security attributes and the ePassport Access Control rules defined in this component satisfy the security objectives of O. Management and O. Access Control as only the authorized Personalization agent with the Personalization agent issuing authorization can perform management functions.

Also, this component satisfies the security objectives of O. BAC, O. EAC and O. Access Control because the read-rights for the personal data of the MRTD holder and MRTD authentication data, etc. is allowed only to the subjects holding the BAC authorization and the read-rights for the biometric data of the MRTD 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 Basic data authentication

This component forces the Inspection System to verify genuineness of ePassport by means of verifying a digital signature which is generated by the uniquely assigned TOE private key for the random number sent by the Inspection System, thus ensures that SOD is not cloned and satisfies O.AA.

FDP_RIP.1 Subset residual information protection

This component ensures that previous information is not included when the TSF allocates or de-allocates memory resources for the BAC authentication key, BAC session key, EAC session key and random numbers.

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

FDP_UCT.1 Basic data exchange confidentiality

This component defines the method to protect from disclosure when transmitting objects, such as the personal data and the biometric data of the MRTD 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 MRTD holder, etc. transmitted between the TSF and the Inspection System with the BAC session encryption key, or the biometric data of the MRTD holder, etc. transmitted between the TOE and the Inspection System with the EAC session encryption key. Therefore, this component satisfies the security objective of O. Secure Messaging as the confidentiality of user data is ensured.

This component satisfies the security objective of O. Replay Prevention by ensuring that the BAC session encryption key is not used the same as the BAC authentication key when establishing the BAC secure messaging.

FDP_UIT.1 Data exchange integrity

This component defines the method to protect from modification, deletion, insertion, replay when transmitting objects, such as the personal data and the biometric data of the MRTD 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 MRTD holder, etc. transmitted between the TOE and the Inspection System with the BAC session MAC key, or the biometric data of the MRTD holder, etc. transmitted between the TOE and the Inspection System with the EAC session MAC key. Therefore, this component satisfies the security objective of O. Secure Messaging as the integrity of user data is ensured.

This component satisfies the security objective of O. Replay Prevention by ensuring that the BAC session MAC key is not used the same as the BAC authentication key when establishing the BAC secure messaging.

FIA_AFL.1 Authentication failure handling

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

This component satisfies the security objective of O. Session Termination as the session is terminated if the authentication attempt failure number of the BAC mutual authentication and EAC-TA is surpassed. Also, this component satisfies the security objective of O. Security Mechanism Application Procedures by disabling the unauthorized external IT entity to move on to the next phase of inspection procedures by terminating session if the BAC mutual authentication fails.

In addition, this component satisfies the security objectives of O. BAC, O. EAC and O. Access Control because access to user data is denied by terminating session as BAC mutual authentication or EAC-TA failure is considered that there is no the access-rights for user data.

Also, this component satisfies the security objectives of O. Open Platform OS Issuance not only because session shall be terminated when Personalization agent authentication fails via MCD enablement or ALC/ADC authentication fails for MULTOS application load/deletion, which is regarded as having no relevant right but because access to the relevant operation shall be permanently denied when any of each authentication failure count reaches allowable limit - maximum 255 – accumulatively.

FIA_ATD.1 User attributes definition

This component forces to keep user attributes list required to manage applications according to MULTOS OS scheme before loading/deleting ePassport application, loading/deleting MULTOS application and personalizing ePassport application data, thus enables MCD activation and application management and satisfies O.Open platform OS issuance.

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

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

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

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

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

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

FIA_UAU.1(3) Timing of authentication (Personalization agent authentication)

This component defines the functions the user to be performed before the Personalization agent authentication and executes the authentication for confirming Personalization agent rights for user.

In this component, MCD enablement data encrypted by TDES is successfully decrypted with transport key injected in MISA operation in order to execute MCD enablement and MRTD Application load in the Manufacturing phase, and TDES based challenge-response is executed in order to execute MCD enablement and MRTD Application load in the Personalization phase. This component satisfies the security objectives of O. Open Platform OS Issuance and O. Management as it enables detection by FIA_AFL.1 if the authentication fails and allows the issuing authorization if the authentication succeeds.

FIA_UAU.1(4) Timing of authentication (MULTOS application authentication)

This component defines the functions the user to be performed before the MULTOS application load/deletion and executes the load/deletion right authentication for MULTOS application via ALC/ADC.

In this component, AID identified using FIA_UID.1 is checked if it is not identical to the AID of the previously loaded application and it is identical to the AID that is included in the ALC/ADC, and RSA based KMA digital signature verification is executed. This component satisfies the security objectives of O. Open Platform OS Issuance as it enables detection by FIA_AFL. 1 if the authentication fails and allows the load/deletion rights for applications if the 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 and the EAC-TA, is not replay.

This component satisfies the security objectives of O. Replay Prevention, O. BAC and O. EAC as the TSF executes the BAC mutual authentication and EAC-TA by generating different random numbers used in the BAC mutual authentication and EAC-TA per session and transmitting them to the Inspection System.

FIA_UAU.5 Multiple authentication mechanisms

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.

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 executes AA authentication in case Inspection System supports.

Also in this component, rights to manage applications shall be acquired after successful MCD enablement via Set MSM Controls and rights to load/delete applications shall be acquired after successful ALC/ADC verification thus this component satisfies the security objectives of O. Open Platform OS Issuance.

FIA_UID.1 Timing of identification

This component satisfies the security objectives of O. Open Platform OS Issuance by establishing 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 identifying the user.

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(Open platform OS)

This component satisfies the security objective of O. Open platform OS Issuance as the ability to disable writing function is given only to the Personalization agent in the Personalization phase.

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

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_MSA.1 Management of security attributes

This component requires to restrict the ability of initializing user security attributes only to the TSF as an action to be taken if the TSF detects modification of the transmitted TSF data in FPT_ITI.1.

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

FMT_MSA.3(1) Static attribute Initialization(Open platform OS)

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

This component satisfies the security objectives of O. Open Platform OS Issuance as only the authorized Personalization agent generates open platform OS user data in order to enforce the open platform OS access control policies in the Manufacturing and Operational Use phase and specifies initial values to restrict security attributes of the data.

FMT_MSA.3(2) Static attribute Initialization(MRTD)

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

This component satisfies the security objectives of O. Management and O. Access Control as only the authorized Personalization agent generates user data in order to enforce the ePassport Access Control policies in the Personalization phase and specifies initial values to restrict security attributes of the data.

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

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

This component satisfies the security objectives of O. Management and O. Access Control by enabling only the authorized Personalization agent to have the ability to write TSF data, such as the EAC chip authentication private key, current data, CVCA certificate and CVCA digital signature verification key, etc., in secure memory in the Personalization phase

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

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

This component satisfies the security objective of O. Security Mechanism Application Procedures by initializing SSC (send sequence counter) to '0' in order to terminate the BAC secure messaging after generating the EAC session key and newly establishing the EAC secure messaging.

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

This component restricts that only the Personalization agent enables Open platform, a structure of the TOE.

This component satisfies the security objective of O. Open Platform OS Issuance by preventing unauthorized open platform OS enablement as authorized Personalization agent generates MSM Controls Data.

FMT_MTD.3 Secure TSF Data

This component requires to allow only secure values as the TSF data in order to ensure the secure random numbers and to ensure that valid date of certificates used in EAC-TA has not expired.

This component satisfies the security objective of O. `Replay Prevention because only the secure random numbers are used in order to prevent a replay attack when the TSF generates session key.

Also, the TSF compares the CVCA link certificate provided by the Inspection System with the CVCA certificate stored in the TOE in order for Verification of the IS certificate used in the EAC-TA. If the CVCA certificate update is necessary, the TSF internally updates the CVCA certificate, CVCA digital signature verification key, current dates and EF.CVCA, therefore maintains the TSF data as secure values. This component satisfies the security objectives of O. Certificate Verification and O. EAC because the EAC-TA can be successfully executed by verifying the DV certificate and IS certificate with the secure CVCA certificate.

FMT_SMF.1 Specification of management functions

This component provides the means to manage the MRTD Applications and the MRTD Application data based Open platform in the Manufacturing and Personalization phase.

This component satisfies the security objective of O. Management and O. Open Platform OS Issuance as it defines the MCD enablement and the loading function of applications in the Manufacturing phase, and 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 Security roles

This component defines the role of the Personalization agent to manage the MRTD Applications and the MRTD Application data.

This component satisfies the security objective of O. Management and O. Open Platform OS Issuance as it defines the role of the Personalization agent that executes the MCD enablement

function and the loading function of applications in the Manufacturing phase and that executes the writing function of user data and TSF data in the Personalization phase.

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 and abnormal operating conditions detected by the IC chip, etc.

This component satisfies the security objective of O. Self-protection as it preserves a secure state to prevent the malfunction of the TSF when the modification of integrity of the TSF data or executable code from the self-testing of TPT_TST.1 is detected or the IC chip detects abnormal operating conditions.

FPT_ITI.1 Inter-TSF detection of modification

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

This component satisfies the security objectives of O. Secure Messaging and O. Session Termination by detecting modification of the transmitted TSF data in the 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.

FPT_RVM.1 Non-bypassability of the TSP

This component requires to always invoke the ePassport Access Control function as a reference monitor to protect the TSF from manipulating operation and bypassing access control policy, etc. by untrusted subjects.

This component satisfies the security objectives of O. Self-protection and O. Access Control together with FPT_SEP.1 as the ePassport Access Control function is always invoked, therefore serves the role as a reference monitor in order to protect all subjects, objects and operations included within a scope of control for the ePassport Access Control policies defined in FDP_ACC.1.

–

FPT_SEP.1 TSF Domain Separation

This component defines the security domains in order to protect subjects, objects, operations and the TSF data included within a scope of control of the ePassport Access Control policies from external interference and tampering by untrusted subjects.

This component satisfies the security objectives of O. Access Control and O. Domain Separation by separating domains used by untrusted subjects, such as other application programs, etc. from the domain in which the ePassport Access Control function is executed.

Also, this component satisfies the security objective of O. Domain Separation by separating secure memory domain from other memory domains, therefore protecting the TSF data from external IT entities.

FPT_TST.1 TSF testing

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

This component satisfies the security objective of O. Self-protection by running self-testing under the self-testing execution conditions for TSF parts defined by the ST author, therefore demonstrating the correct operation of the TSF.

Also, this component satisfies the security objective of O. Self-protection by verifying the integrity of TSF data parts defined by the ST author and the TSF executable code stored in the TOE, therefore detecting loss of the TSF data and the executable code.

8.2.2 Rationale of Security Functional Requirements of IT Environment

The rationale of security functional requirements of IT environment demonstrates the followings:

- Each security objective for environment has at least one security functional requirements of IT environment tracing to it.
- Each security functional requirement of IT environment traces back to at least one security objective for environment.

Table 22 presents the mapping between the security objectives and the security functional requirements as follows.

Table 22. Mapping between Security Objectives for Environment and SFR of IT Environment

Security Functional Requirements \ Security Objectives	Security Objectives for Environment	
	OE.Handling Information Leakage	OE.IC chip
FCS_COP.1(1)		X
FCS_COP.1(2)		X
FCS_COP.1(4)		X
FCS_COP.1(5)		X
FCS_COP.1(6)		X
FCS_COP.1(7)		X
FCS_COP.1(8)		X
FPR_UNO.1	X	

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

This component defines TDES cryptographic operation of IC chip used to authenticate the Inspection System that supports the BAC or to protect the transmitted user data from disclosure.

The cryptographic operation of IC chip defined in this component satisfies the security objective for environment of O. IC chip as it ensures confidentiality of user data transmitted between the TOE and the Inspection System by using cryptographic algorithm.

FCS_COP.1(2) Cryptographic operation (MAC)

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

The MAC operation of IC chip defined in this component satisfies the security objective for environment of O. IC chip as it ensures integrity by providing the method to detect modification of user data transmitted between the TOE and the Inspection System.

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

This component defines the method of digital signature Verification via the cryptographic operation of IC chip necessary in the EAC-TA.

The digital signature Verification method via the cryptographic operation of IC chip defined in this component satisfies the security objective for environment of O. IC chip as it verifies the CVCS link certificate, DV certificate and IS certificate provided by the Inspection System to the TOE.

FCS_COP.1(5) Cryptographic operation (AA Digital signature Generation for Genuineness Verification)

This component defines the method of digital signature Verification via the cryptographic operation of IC chip necessary in the AA process.

The method of digital signature Verification via the cryptographic operation of IC chip defined in this component satisfies the security objective for environment of O. IC chip by detecting forgery/modification of MRTD as Inspection System offers random number to the TOE, the TOE responds digital signature with AA private key written in secure memory, and then the Inspection System verifies its genuineness with AA public key from DG15.

FCS_COP.1(6) Cryptographic operation (MULTOS DES)

This component defines the cryptographic operation (MULTOS DES) supported by IC chip additionally used to the access control for OS and applications in case of MULTOS open platform OS based ePassport.

In this component, the cryptographic operation (MULTOS DES) supported by IC chip and defined for MULTOS operation satisfies the security objective for environment of O. IC chip by means that MULTOS enablement data (MSM Controls Data) is decrypted using MULTOS DES resulting in transition to enabled state where application can be loaded and encrypted applications are decrypted using MULTOS DES to authenticate MCD and applications.

FCS_COP.1(7) Cryptographic operation (MULTOS RSA)

This component defines the cryptographic operation (X^Y MOD(N)) supported by IC chip additionally used to the access control for OS and applications in case of MULTOS open platform OS based MRTD.

The cryptographic operation supported by IC chip defined in this component for MULTOS operation satisfies the security objective for environment of O. IC chip by Verification (Asymmetric Hash, X^Y MOD(N)) of digital signature of ALC/ADC during application load/deletion.

FCS_COP.1(8) Cryptographic operation (MULTOS Asymmetric Hash)

This component defines the cryptographic operation (Asymmetric Hash) supported by IC chip additionally used to the access control for OS and applications in case of MULTOS open platform OS based MRTD.

The cryptographic operation supported by IC chip defined in this component for MULTOS operation satisfies the security objective for environment of O. IC chip by Verification (Asymmetric Hash, X^Y MOD(N)) of integrity of the MCD code, the MSM Controls Data, and the Application ALU code.

FPR_UNO.1 Unobservability

This component ensures that external entities are unable to observe the cryptographic-related data, such as the BAC authentication key, BAC session key, EAC session key and EAC chip authentication private key, etc. when the IT environment performs a cryptographic operation supported by the IC chip.

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

8.2.3 Rationale of Assurance Requirements of the TOE

The EAL(Evaluation Assurance Level) of this Security Target was followed the Protection Profile selected as EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VLA.3) by considering the value of assets protected by the TOE and level of threats, etc, and ALC_DVS.2 and AVA_VLA.4 are added by considering the security management system of MULTOS, the open platform OS. This section describes the reason why EAL4+ is selected and the rationale of additional components in assurance level of EAL4

Rationale for EAL4 Level

Assurance requirements of EAL4 are the assurance package requiring systematic design, test and examination. EAL4 is the highest assurance level required in the commercial development phase, and it provides the methodology possible to implement best. The most IC chips are commercially developed and sold, and high assurance level considering the application environment and the protecting asset value. Also, it provides higher assurance than EAL3 by including requirements such as automated configuration management though partly applicable and secure delivery.

This assurance package partially selected assurance components higher than EAL4. Rationale of augmented with assurance components is described as follows.

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

This ST partially selected higher assurance components than the PP selecting assurance components higher than EAL4. Rationale of augmented with assurance components is described as follows.

- **ADV_IMP.2 Implementation of the TSF**
- **ALC_DVS.2 Sufficiency of security measures**
- **ATE_DPT.2 Testing: low-level design**
- **AVA_VLA.4 Highly resistant**

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, since the IC chip is not included in the scope of the TOE, it does not require understanding on hardware structure and advanced specialized equipments, etc. Therefore, considering the resources, motivation and expertise, the TOE must counter attackers possessing moderate attack potential. EAL4 includes AVA_VLA.2 that resistant the low attack potential. Therefore, AVA_VLA.3 is augmented to require execution of systematic vulnerability analysis and resistant to attackers possessing moderate attack potential. However, there still exists direct attack potential to the IC chip by threat agent possessing high attack potential and evaluation and verification for this may be assigned to the IC chip manufacturer and evaluation and verification of the TOE should be performed via independent penetration tests, thus the ST augmented AVA_VLA.4.

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 enable analysis on the entire implementation representation in order to check if the TSF is accurately implemented and defect code does not exist. Also, ATE_DPT.2 is augmented to enable detection of defects not discovered while developing the TOE through testing for subsystems and modules closely related to internal structure of the TSF.

In order to provide high level of assurance regarding physical, procedural, personal and other security measures during ePassport development phase, ALC_DVS.2 was augmented.

8.3 Rationale of Dependency

8.3.1 Dependency of the TOE Security Functional Requirements

Table 23 shows dependency of the TOE functional components.

Table 23. Dependency of the TOE Functional Components

No.	Functional Component	Dependency	Ref. No.
1	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4 FMT_MSA.2	2,3 4 None
2	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4 FMT_MSA.2	1 4 None
3	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4 FMT_MSA.2	1 4 None
4	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_MSA.2	1 None
5	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1 4 None
6	FDP_ACC.1(1)	FDP_ACF.1(1)	8
7	FDP_ACC.1(2)	FDP_ACF.1(2)	9
8	FDP_ACF.1(1)	FDP_ACC.1(1) FMT_MSA.3(1)	8 26
9	FDP_ACF.1(2)	FDP_ACC.1(2) FMT_MSA.3(2)	7 27
10	FDP_DAU.1	-	-
11	FDP_RIP.1	-	-
12	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1(2) or FDP_IFC.1]	None 7
13	FDP_UIT.1	[FDP_ACC.1(2) or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	7 None
14	FIA_AFL.1	FIA_UAU.1	16,17,18,19
15	FIA_ATD.1	-	-
16	FIA_UAU.1(1)	FIA_UID.1	22
17	FIA_UAU.1(2)	FIA_UAU.1(1)	16
18	FIA_UAU.1(3)	FIA_UID.1	None
19	FIA_UAU.1(4)	FIA_UID.1	22
20	FIA_UAU.4	-	-
21	FIA_UAU.5	-	-
22	FIA_UID.1	-	-
23	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	32 33
24	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	32 33
25	FMT_MSA.1	[FDP_ACC.1(2) or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	9 32 33
26	FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	None 33

27	FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	25 33
28	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	32 33
29	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	32 33
30	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	32 33
31	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	EAL4 28
32	FMT_SMF.1	-	-
33	FMT_SMR.1	FIA_UID.1	22
34	FPT_FLS.1	ADV_SPM.1	EAL4
35	FPT_ITI.1	-	-
36	FPT_RVM.1	-	-
37	FPT_SEP.1	-	-
38	FPT_TST.1	FPT_AMT.1	None

FCS_CKM.1, FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP(4) have dependency with FMT_MSA.2, but the dependency in this PP is not satisfied. The target of generating, operating and destroying cryptographic key of FCS is TSF data. Therefore, rather than secure security attributes (FMT_MSA.2), FMT_MTD.3 of secure TSF data is satisfied.

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

FIA_UAU.1(2) has dependency with FIA_UID.1, but the dependency in this ST is not satisfied. Since the EAC-TA is executed after the BAC mutual authentication, FIA_UAU.1(2) depends on FIA_UAU.1(1) and FIA_UAU.1(1) depends on FIA_UID.1. Therefore, indirectly, the dependency is satisfied.

FIA_UAU.1(3) has dependency with FIA_UID.1, and FIA_UID.1 does not need identification requirements because the Personalization agent executes key based authentication. Therefore, the dependency is not satisfied.

FMT_MSA.3(1) has dependency with FMT_MSA.1, but the dependency in this ST is not satisfied. FMT_MSA.3(1) is that the Personalization agent injects operation security attributes and access-right security attributes of subjects described in FDP_ACF.1.1(1) during ROM Key Integration or MISA operation in the Manufacturing phase. Once the injection is terminated, It is impossible to initialize and change security attributes by any means, and FMT_MSA.3(1) does not have dependency with FMT_MSA.1

FPT_TST.1 has dependency with FPT_AMT.1, but the dependency in this PP is not satisfied. FPT_AMT.1 is executed by the IC chip, the TSF underlying abstract machine rather than by the TOE. Therefore, testing if the IC chip is operating normally to support security functions of the TOE is satisfied by security objective for environment of OE. IC chip.

8.3.2 Dependency of Security Functional Requirements for IT Environment

Table 24 shows dependency of security functional requirements for IT environment.

Table 24. Dependency of Security Functional Requirements for IT Environment

No.	Functional Component	Dependency	Ref. No.
1	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
2	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
3	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
4	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
5	FCS_COP.1(6)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
6	FCS_COP.1(7)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
7	FCS_COP.1(8)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	[Table 23] 1 [Table 23] 4 None
8	FPR_UNO.1	-	-

FCS_COP.1(1), FCS_COP.1(2), FCS_COP(4), FCS_COP(5), FCS_COP(6), FCS_COP(7), and FCS_COP(8) have dependency with FMT_MSA.2, but the dependency in this SP is not satisfied. The target of generating, operating and destroying cryptographic key of FCS is TSF data. Therefore, rather than secure security attributes (FMT_MSA.2), FMT_MTD.3 of secure TSF data is satisfied.

8.3.3 Dependency of the TOE Security Assurance Requirements

The dependency of EAL4 provided in Common Criteria is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in [Table 25].

AVA_VLA.3 has dependency with ADV_FSP.1 and ADV_IMP.1. This is satisfied by ADV_FSP.2 and ADV_IMP.2 in hierarchical relationship with ADV_FSP.1 and ADV_IMP.1

Table 25. Dependency of the Added Assurance Components

No.	Assurance Component	Dependency	Ref. No.
1	ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	EAL4 EAL4 EAL4
2	ALC_DVS.2	None	-
3	ATE_DPT.2	ADV_HLD.2 ADV_LLD.1 ATE_FUN.1	EAL4 EAL4 EAL4
4	AVA_VLA.4	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	EAL4 EAL4 1 EAL4 EAL4 EAL4

8.4 Rationale of TOE Summary Specification

8.4.1 Rationale of TOE Security Functions

Table 26 presents the mapping between the security functions and the security functional requirements.

Table 26. Mappings between Security Functions and Security Functional Requirements

Security Functions / SFRs	CS		DP			IA					SM		PP		
	CS 1	CS 2	DP 1	DP 2	DP 3	IA 1	IA 2	IA 3	IA 4	IA 5	SM 1	SM 2	PP 1	PP 2	PP 3
FCS_CKM.1	×														
FCS_CKM.2(1)	×														
FCS_CKM.2(2)	×														
FCS_CKM.4				×											
FCS_COP.1(3)		×													
FDP_ACC.1(1)											×				
FDP_ACC.1(2)												×			
FDP_ACF.1(1)											×				
FDP_ACF.1(2)												×			
FDP_DAU.1					×										
FDP_RIP.1				×											

FDP_UCT.1			×											
FDP_UIT.1			×											
FIA_AFL.1										×				
FIA_ATD.1						×								
FIA_UAU.1(1)							×							
FIA_UAU.1(2)							×							
FIA_UAU.1(3)						×								
FIA_UAU.1(4)						×								
FIA_UAU.4				×										
FIA_UAU.5									×					
FIA_UID.1						×		×						
FMT_MOF.1(1)											×			
FMT_MOF.1(2)												×		
FMT_MSA.1			×									×		
FMT_MSA.3(1)											×			
FMT_MSA.3(2)												×		
FMT_MTD.1(1)												×		
FMT_MTD.1(2)												×		
FMT_MTD.1(3)											×	×		
FMT_MTD.3												×		
FMT_SMF.1											×	×		
FMT_SMR.1											×	×		
FPT_FLS.1													×	
FPT_ITI.1			×	×										
FPT_RVM.1														×
FPT_SEP.1														×
FPT_TST.1														×

8.5 Rationale of Strength of Function

This security target requires ‘SOF-high’ for security functional requirement of FCS_CKM.1.

The key sizes in FCS_CKM.1 shall be selected so that the TOE is resistant to high attack potential. Since keys used in cryptographic operation may be exposed by Brute-Force Attack of attackers, the key length must be selected to handle this situation. Therefore, SOF-high is claimed.

SOF-high is claimed in IT security functional of cryptographic key management(CS1) implementing security functional requirement of FCS_CKM.1. Therefore, consistency for strength of function is achieved.

Nonce should be secure in order to be highly resistant to high level attacks, but generating nonce unpredictable to attackers and resistant to replay attacks is performed by IT security environment, thus TOE does not ensure strength of function of nonce and nonce is out of the scope of strength of function in this ST.

The MRZ used as the seed for BAC the authentication key generation is determined according to Issuing policy of the Personalization agent. Therefore, the TOE does not ensure SOF of the BAC

authentication key. The BAC authentication key does not include in the SOF scope of this security target.

8.6 Rationale of Mutual Support and Internal consistency

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

In '8.3.1 Dependency of the TOE security functional requirements', '8.3.2 Dependency of security functional requirements for IT environment' and '8.3.3 Dependency of the TOE security assurance requirements', the dependency is analyzed as a supportive relationship among security requirements of which it is necessary to depend on other security requirements in order to achieve a security objective because a security requirement is insufficient. In case the dependency was not satisfied, additional rationale is provided.

Also, security functional requirements, although there is no dependency among security functional requirements, are mutually supportive and internally consistency in relation to the TSF operations as of the following.

In the Manufacturing phase, the Personalization agent enables the MCD and loads applications using initialized static attribute or deletes applications if necessary in accordance with issuing policies of the Personalization agent(FMT_MSA.3(1), FMT_MOF.1(1), FMT_MTD.1(3), FMT_SMF.1). The role of the Personalization agent as such is defined as the security role (FMT_SMR.1) and is controlled by the open platform OS access control policies (FDP_ACC.1(1), FDP_ACF.1(1)). The Personalization agent authentication (FIA_UAU.1(3)) and MULTOS application authentication (FIA_UAU.1(4)) are executed according to the authentication mechanism application rules(FIA_UAU.5), and if the authentication is failure, the session is terminated or the functions are disabled(FIA_AFL.1) Therefore, these security requirements are mutually supportive and internally consistent.

In the Personalization phase, the Personalization agent records the MRTD Application data (FMT_MTD.1(1), FMT_MSA.3(2)) and deactivates writing function so that the TOE is not modified by external entities when delivering the TOE to the Operational Use phase(FMT_MOF.1(2), FMT_SMF.1). The role of the Personalization agent as such is defined as the security role (FMT_SMR.1) and is controlled by the ePassport access control policies (FDP_ACC.1(2), FDP_ACF.1(2)). It is separated the execution domain of subjects and objects within the scope of control of the ePassport access control policies from other domains (FPT_SEP.1) and ensured to invoke the access control function at all times as a reference monitor to protect these subjects and objects(FPT_RVM.1). Therefore, these security requirements are mutually supportive and internally consistent.

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

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.

The IC chip must ensure that physical phenomena of current, voltage and electromagnetic waves, etc. occurred when the TSF performs cryptographic operations (FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(4), FCS_COP.1(5), FCS_COP.1(6), FCS_COP.1(7), FCS_COP.1(7)) are not exploited by the threat agents (FPR_UNO.1). The cryptographic-related data created in temporary memory after cryptographic operations must be destroyed to prevent reuse (FCS_CKM.4, FDP_RIP.1). Therefore, these security requirements are mutually supportive and internally consistent.

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

The TSF must execute self-testing under the conditions decided by the ST author (FPT_TST.1). 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.

8.7 Rationale of PP Conformance

In this ST, TOE security objectives and security functional requirements conform to the PP, partial tailoring or augmentation was conducted to specify those of open platform OS as in the section 7.2 and 7.3.

9 Annexes

9.1 References

[1] ePassport Protection Profile V1.0, National Intelligence Service – IT Security Certification Center, KECS-PP-0084-2008, January 2008

[2] Common Criteria for Information Protection System, Ministry of Public Administration and Security, 2009-09-01

[3] Evaluation and Certification Guidance for Information Protection System, Ministry of Public Administration and Security, 2009-09-01

[4] Smart Card Open Platform Protection Profile for Government, the National Intelligence Service, V1.1, 2006-5-17

[5] ISO/IEC 7816 Identification cards : Integrated Circuit 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*, 6th edition, 2006

[8] MRTD Technical Report, Development of a LDS, Rev 1.7, 2004-5-18

[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 Doc9303-Part 1-Sixth Edition, Release 5, ICAO, 2007-02-07

[11] BSI Technical Guideline TR-03110, Advanced Security Mechnisms 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] S3CC9LC 16-bit Microcontroller for SmartCard User's Manual Rev 5.00, January 2010

[14] Samsung SDS SPass V1.0 Security Target, Ver 2.21, 24 August 2008

9.2 Abbreviated terms

AA	Active Authentication
ABEND	Abnormal End (of MEL application execution)
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
CLK	Clock (input to smartcard)
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem (algorithm)
DES	Data Encryption Standard
DG	Data Group
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EBC	Electronic Code Book
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
KTU	Key Transformation Unit
LDS	Logical Data Structure
MAC	Message Authentication Code
MCD	Multos Carrier Device
MEL	Multos Executable Language (application language)
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)

RF	Radio Frequency
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest-Shamir-Aldeman (algorithm)
RST	Reset (input to smartcard)
SFP	Security Function Policy
SOF	Strength of Function
TA	Terminal Authentiation
TSC	TSF Scope of Control
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

U-creator
U dream, we create.

END OF DOCUMENT

Telephone: +82-2-3429-2114
E-mail: sdspr@samsung.com
http://www.sds.samsung.co.kr

삼성SDS SAMSUNG