SPass NX V1.0 R3
on S3CT9KW/S3CT9KC/S3CT9K9

Security Target
Public version

Samsung SDS

REVISION STATUS

Revision	Date	Author	Description of Change
1.02	2013.04.10	JH Lee	Final release

Contents

List of Figures

List of Tables

1 ST Introduction

This document is the Security Target (hereafter, 'ST') of SAMSUNG SDS SPass NX V1.0 R3 on S3CT9KW /S3CT9KC/S3CT9K9 which shall be embedded in SPNX10 product and developed by SAMSUNG SDS.

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

1.1 ST Reference

- Title : SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9 Security Target (Public Version)
- Version : V1.02
- Release date : 10th of April, 2013
- Author : SAMSUNG SDS Co., Ltd.
- Evaluation criteria : Common Criteria for Information Technology Security Evaluation V3.1r4 [CC_PAS]
- Evaluation assurance level : EAL5+ (ADV_IMP.2, ALC_DVS.2, AVA_VAN.5)
- PP compliance : ePassport Protection Profile V2.1[PP]
- PP certification number : KECS-PP-0163a-2009

1.2 TOE Reference

- Developer : SAMSUNG SDS Co., Ltd
- TOE name : SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9

  (hereafter 'S3CT9KW/S3CT9KC/S3CT9K9' is abbreviated to 'S3CT9Kx')
- TOE element
  - SPass NX V1.0
  - S3CT9Kx : Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional Secure RSA/ECC V2.2 Library including specific IC Dedicated Software
  - User Manual (SPNX-AGD-101, SPNX-AGD-102, SPNX-AGD-103)
- TOE version : Release 3

1.3 TOE Overview

1.3.1 TOE Type

The TOE that defined in this ST is IC chip operating system (COS), the application of machine readable travel documents (MRTD application) and hardware elements of the IC chip of machine readable travel documents (S3CT9Kx). S3CT9Kx has separately achieved Common Criteria certification from BSI as follows and since the IC chip operating system with MRTD application is embedded on that, the TOE is the composition TOE that follows CCDB-2012-04-001. The TSF of IC chip used by the TOE is described in the section 7.1.

PP compliance	BSI-PP-0035-2007
Certified TOE name	Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software
Certification number	ANSSI-CC-2012/70
Certified cryptographic library version	Secure RSA/ECC Library v2.2, TRNG Library v2.0
Evaluation Assurance Level	EAL5+ (ALC_DVS.2, AVA_VAN.5)

The MRTD application satisfies the ICAO's Machine Readable Travel Documents, DOC 9303 Part 1 Volume 2[DOC9303] and the BSI's Advanced Security Mechanisms Machine Readable Travel Documents – Extended Access Control V1.11 2008.02 [EAC].

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

1.3.2 MRTD System

The Figure 1 shows the overall configuration of the MRTD system.

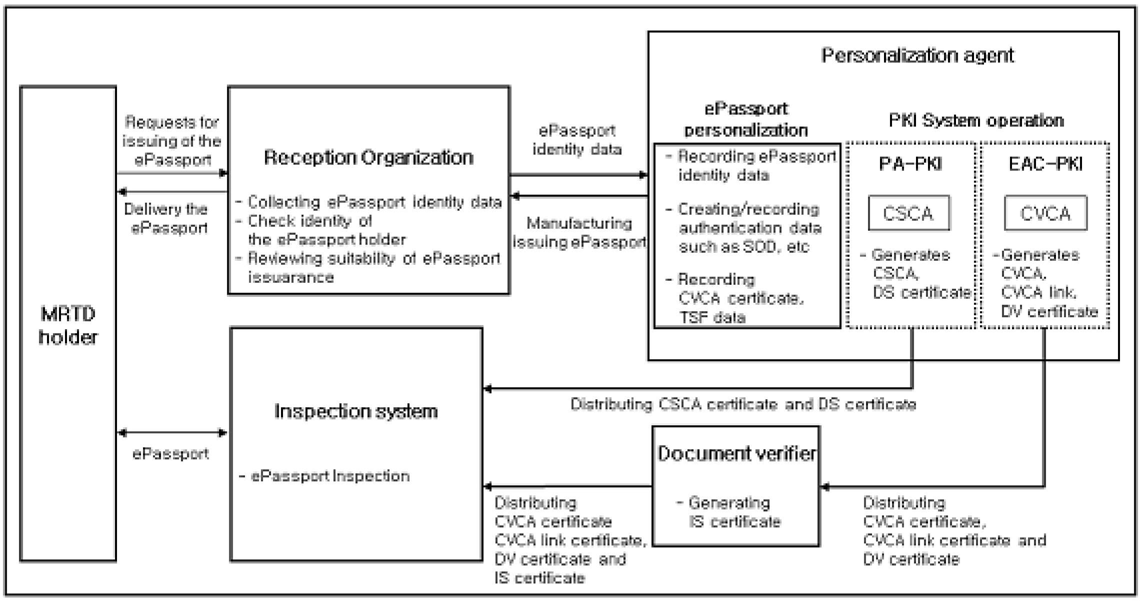

MRTD holder
Requests for issuing of the ePassport
Delivery the ePassport
ePassport
Reception Organization
- Collecting ePassport identity data
- Check identity of the ePassport holder
- Reviewing suitability of ePassport issuarance
ePassport identity data
Manufacturing issuing ePassport
Personalization agent
ePassport personalization
- Recording ePassport identity data
- Creating/recording authentication data such as SOD, etc
- Recording CVCA certificate, TSF data
PKI System operation
PA-PKI
CSCA
- Generates CSCA, DS certificate
EAC-PKI
CVCA
-Generates CVCA, CVCA link, DV certificate
Inspection system
- ePassport Inspection
Distributing CSCA certificate and DS certificate
Document verifier
- Generating IS certificate
Distributing CVCA certificate CVCA link certificate, DV certificate and IS certificate
Distributing CVCA certificate, CVCA link certificate and DV certificate

Figure 1. Overall Configuration of the MRTD System

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

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

The Personalization agent generates document security object('SOD' hereafter) by digital signature on the user data (identity and authentication data) and records it in the MRTD chip with the MRTD identity data sent from the reception organization. Also, after recording the TSF data in secure memory, the personalization agent manufactures and issues the MRTD embedded the MRTD chip to the passport. Details of data recorded in the MRTD will be described in 1.4.2 Logical Scope of the TOE.

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 MRTD PKI System the personalization agent generates, issues and manages CSCA certificate and DS certificate. According to the Issuing Policy of the MRTD, the personalization agent generates digital signature key to verifying access-rights to the biometric data of the MRTD 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 MRTD 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 MRTD.

The Document verifier generates IS certificate by using CVCA and DV certificates, then provides these certificates to Inspection System.

Types of certificates used in the MRTD system are as shown in Table 1 below.

Table 1. Types of Certificates

Usage	MRTD 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	EAC-PKI	CVCA	CVCA certificate

of the biometric data of the MRTD holder			CVCA link certificate
		Document verifier	DV certificate
		EAC supporting Inspection System	IS certificate

1.3.3 Life Cycle and Environment of the TOE

The ST identifies the life cycle of of the TOE and the operational environment of the TOE as follows.

<Life Cycle of the TOE>

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

Table 2. TOE Life Cycle

Phase	Life Cycle of the IC Chip	Life Cycle of the Embedded S/W
Phase 1 (Development)	① The IC chip developer to design the IC chip and to develop the IC chip Dedicated S/W	
		② The S/W developer to develop the TOE (COS, MRTD application) by using the IC chip and the Dedicated S/W
Phase 2 (Manufacturing)	③ The IC chip manufacturer to mask the TOE in the ROM, to record the IC chip identifier and to produce the IC chip	
		④ The MRTD manufacturer to create user data storage space according to the LDS format or the ICAO document and to record it in EEPROM ⑤ The MRTD manufacturer to record identification and authentication information of the MRTD Personalization agent in the EEPROM ⑥ The MRTD manufacturer to embed the IC chip in the passport book

Phase 3 (Personalization)		⑦ The Personalization agent to create SOD by a digital signature on the MRTD identity data ⑧ The Personalization agent to record the MRTD i dentity data, the authentication data (including S OD) and the TSF data in the TOE
Phase 4 (Operational Use)		⑨ The Inspection System to verify the MRTD and t o check identity of the MRTD holder by communi cating with the TOE

The initialization of the TOE can be conducted after both manufacturing the inlay sheet and manufacturing the cover sheet depending on the personalization agent’s policy.

The life cycle of the TOE is subdivided for Embedded S/W with 3 steps of Kernel Mode and 3 steps of Application Mode that is activated only in Operational Use mode of the kernel. Here manufacturer means the TOE developer or an MRTD manufacturer delegated by the TOE developer.

<TOE Operational Environment>

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

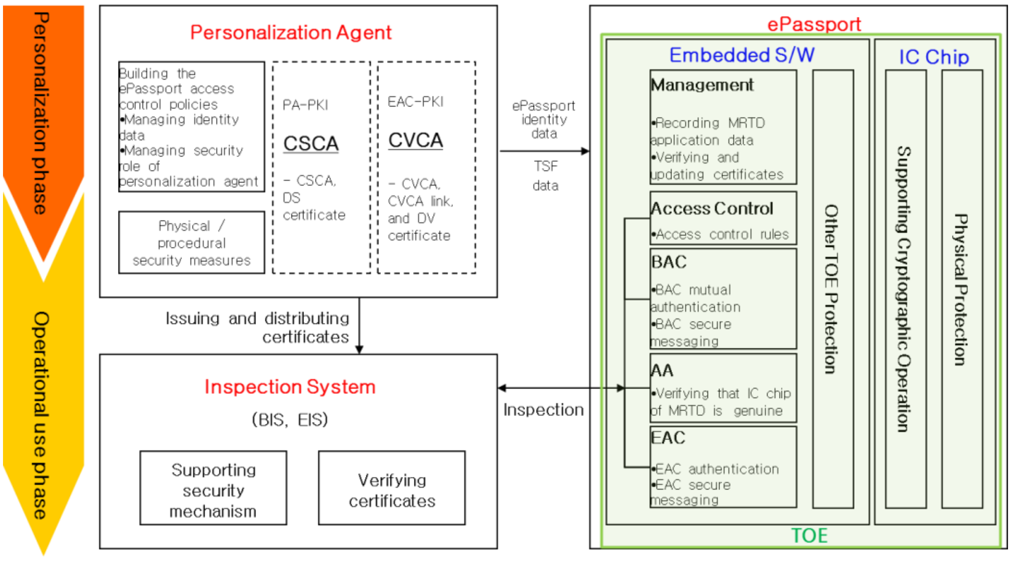

Personalization phase
Operational use phase
Personalization Agent
Building the ePassport access control policies
•Managing identity data
•Managing security role of personalization agent
Physical / procedural security measures
PA-PKI
CSCA
- CSCA, DS certificate
EAC-PKI
CVCA
- CVCA, CVCA link, and DV certificate
ePassport identity data
TSF data
Issuing and distributing certificates
Inspection System
(BIS, EIS)
Supporting security mechanism
Verifying certificates
Inspection
ePassport
Embedded S/W
Management
•Recording MRTD application data
•Verifying and updating certificates
Access Control
•Access control rules
BAC
•BAC mutual authentication
•BAC secure messaging
AA
•Verifying that IC chip of MRTD is genuine
EAC
•EAC authentication
•EAC secure messaging
Other TOE Protection
IC Chip
Supporting Cryptographic Operation
Physical Protection
TOE

Figure 2. TOE Operational Environment

1.3.4 TOE Security Characteristics

<Security Mechanism>

The TOE provides security characteristics such as the confidentiality, the integrity, the access control and the authentication, in order to protect the TSF data and the user data of the MRTD identity data and the MRTD authentication data, etc. These security characteristics are implemented with the BAC mechanism of the ICAO document and the EAC mechanism of the EAC specifications. Also, the TOE provides the SOD to the BIS and the EIS and the Inspection System detects forgery and corruption of the user data through the verification of the digital signature of the SOD.

BAC
The BAC (basic access control) is to provide the confidentiality and the integrity for the personal data of the MRTD holder by secure messaging when controlling access to the personal data of the MRTD holder stored in the TOE and transmitting it to the Inspection System with read-rights. The BAC includes the BAC mutual authentication, the BAC key distribution and the BAC secure messaging. The TOE generate random values by either generate the BAC authentication key from the MRZ data of DG1 or using the stored BAC authentication key and the BAC-supporting Inspection System by using BAC authentication key generated from reading optically the MRZ. Then, the TOE and the Inspection System perform encryption the generated random number and exchange them. The TOE and the BAC-supporting Inspection System execute the BAC mutual authentication by checking the exchanged random number. The session is ended in case of the mutual authentication failure. The TOE, in order to secure transmission of the personal data of the MRTD holder after checking the read-rights of the Inspection System for the personal data of the MRTD holder through the BAC mutual authentication, establishes the BAC secure messaging by encrypting with the BAC session key shared through the BAC key distribution and generating the MAC.
EAC
The EAC (extended access control) is to provide the confidentiality and the integrity for the biometric data of the MRTD holder by secure messaging when controlling access to the biometric data of the MRTD holder stored in the TOE and transmitting it to the Inspection System with read-rights. The EAC includes the EAC-CA, the EAC secure messaging and the EAC-TA. The EAC-CA is to implement the ephemeral-static DH key distribution protocol for the EAC session key distribution and the chip authentication. The TOE transmits the EAC chip authentication public key so that the Inspection System authenticates itself and executes key distribution protocol by using temporary public key received from the Inspection System. The session is ended in case of the EAC-CA failure. In case of the successful EAC-CA, the TOE establishes the EAC secure messaging by using the EAC session key. The EAC-TA is for the TOE to implement challenge-response authentication protocol based on the digital signature in order to authenticate the EAC-supporting Inspection System. The TOE authenticates the Inspection System, verifying the value of the digital signature by the Inspection System in temporary public key used for the EAC-CA, by using the IS certificate. The TOE, when receiving the CVCA link certificate, the DV certificate and the IS certificate from the EAC-supporting Inspection System, verifies the CVCA link certificate by using the CVCA digital signature verification key in secure memory. Then, by checking valid date of the CVCA link certificate, the TOE updates the CVCA digital signature verification key and the current date if necessary. After verifying the IS certificate and checking that it is a suitable certificate, the TOE allows access of the EAC-supporting Inspection System to read the biometric data of the MRTD holder and transmits the data through the EAC secure messaging.
AA
AA(active authentication) is to provide the capability to generate evidence that can be used as a

guarantee of the valid binding between MRTD IC chip and the stored user data by the mechanism that the Inspection System verifies the digital signature signed by the TOE including the random number sent by the Inspection System. The AA private key of the TOE used as the signing key is stored in the secure memory that are not accessiable via external interfaces, the Inspection System requests TOE to generate digital signature and verifies it using AA public key in the DG15 after establishing BAC secure communication channel TOE.

The Inspection System can deny the MRTD holder to pass the border in case verification of the digital signature comes to fail.

Table 3 summarized the MRTD security mechanisms.

Table 3. The MRTD Security Mechanisms

The MRTD Security Mechanisms				IT Security characteristic of the TOE
Security Mechanism	Security characteristic	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-PKCS1-v1.5	AA Private Key (used to generate digital signature) AA Public Key (used by BIS, EIS)	TOE generates a digital signature to card nonce and terminal nonce and Inspection System verifies it to ensure that the IC chip is genuine
BAC	BAC Mutual authentication	Symmetric key-based entity authentication protocol TDES-CBC SHA MAC	BAC Authentication Key (encryption key, MAC key)	The TOE verifies if the Inspection System has access-rights, by decryption and MAC operation for the transmitted value of the Inspection System. The TOE transmits the value to the Inspection System after encryption and MAC operation for authentication.
	BAC Key Distribution	Symmetric key-based key distribution protocol TDES-CBC SHA MAC	BAC Session Key (encryption key, MAC key)	Generating BAC session key by using KDF from the exchanged key-sharing random number on the basis of the TDES-based key distribution protocol
	BAC Secure messaging	Secure Messaging	BAC Session Key (encryption key, MAC key)	Transmitting messages by creating the MAC after encryption with the BAC session key Receiving messages by decryption it after verifying the MAC with the BAC session key

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

<TOE Access Control and Security Management>

The TOE provides access control rules and management functions for the MRTD application data based on security attributes of the user in the phases of the Personalization and the Operational Use.

The TOE provides only the authorized personalization agent to writing function on the user data and TSF data in the Personalization phase. Also, the TOE provides the access control function on the read-rights of the user data based on the access-rights of the Inspection System given through execution of security mechanisms in the Operational Use phase.

The TOE allows only the authorized personalization agent to manage the security attributes of user, user data and TSF data in the phases of the Personalization and the Operational Use and defines it as security role. Also, the TSF executes itself some security management functions, such as updating the CVCA certificate and the current date and initializing the identifier for secure messaging, etc.

<Other TOE Protection>

The TOE executes the functions to detect and handle for modification of the TSF data transmitted and run self-testing to verify the integrity of the stored TSF data and TSF. Also, if detecting failures through self-testing or abnormal operation in the IC chip, the TOE preserves a secure state so that to prevent the types of failures in the TSF(malfunction).

The TOE ensures not to obtain the cryptographic-related data by exploiting physical phenomena of the cryptographic operation (change of current, voltage and electromagnetic, etc.).

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The physical scope of the TOE is defined as Figure 3 in the ST.

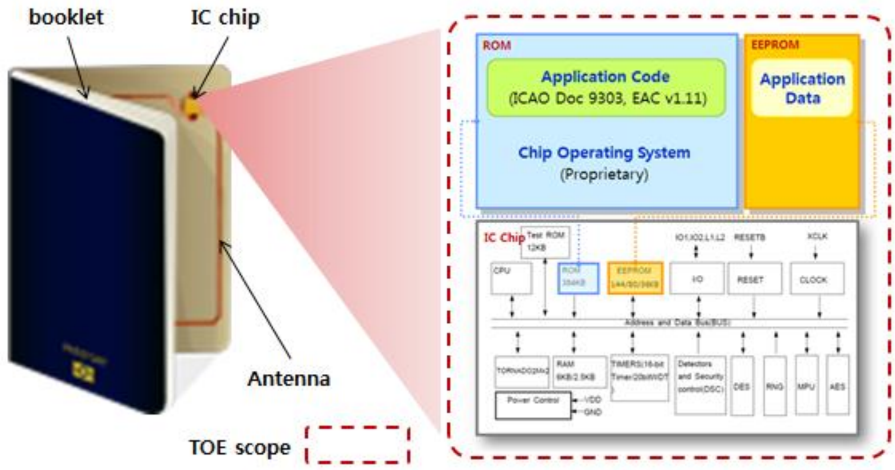


Figure 3. Physical Scope of the TOE

The MRTD refers to the passport book and the MRTD chip and the antenna embedded in the cover of the passport book[1]. The MRTD chip includes the IC chip operating system, the MRTD application, the MRTD application data and the IC chip elements. The IC chip elements consist of CPU, co-processor, I/O port, memory (RAM, ROM, EEPROM) and contactless interface, etc.

In this ST, TOE is defined with the IC chip operating system (COS), the MRTD application, the MRTD application data and the IC chip hardware elements. TOE is Samsung Electronics Secure IC chip S3CT9Kx that contains proprietary IC chip operating system(Embedded S/W) including an MRTD application, where S3CT9Kx includes CPU that conducts TOE execution code, TDES accelerator and Tornado coprocessor. In particular, RSA and ECC are provided as a cryptographic library of Tornado and in the scope of the IC chip TOE.

The COS provides functions for execution of MRTD application and management of the MRTD application data, such as commands processing and files management, etc. defined in ISO/ IEC 7816-4, 8 and 9. In this protection profile accepts both opened or closed IC chip operating systems.

The MRTD chip application is IC chip application that implements the function to store and process the MRTD identity data according to LDS(Logical Data Structure) format defined in the ICAO document and security mechanism to securely protect the function. Also, the MRTD application is added the EAC security mechanism by the EAC specifications, because the biometric data of the MRTD holder is included in the MRTD identity data.

The MRTD application data consists of the user data, such as the MRTD identity data, etc., and the TSF data required in the security mechanism

The IC chip S3CT9Kx as a component of the TOE where Embedded S/W is contained achieved a separate common criteria certificate from BSI and its cryptographic library provides security functions as follows.

- Symmetric key cryptographic operation

[1] TOE carrier can be the cover of the passport as well as various form factors like ID-1 and ID-3 defined in the ISO/IEC 7816 depending on the policy of the personalization agent and is combined with antenna inlay.

The IC chip provides AES 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)128 bit AES message encryption and decryption for initialization authentication and personalization agent authentication and (4)112 bit AES-CMAC calculation for Secure Messaging according to initialization authentication and personalization agent authentication.

- Asymmetric key cryptographic operation

  The IC chip provides crypto-processor (Tornado^{TM}) and relevant cryptographic library capable of 2048-bit modulus RSA and 512-bit ECC operations in order that the TOE can perform operations such as (1)key exchange and agreement based on DH or ECDH, (2)digital signature verification based on RSA or ECDSA for EAC-TA, (3)digital signature generation based on RSA for AA.

- One-way hash functions

  The IC chip's cryptographic library provides on-way hash functions of SHA-224, SHA-256, SHA-384, SHA-512 in order that the TOE can perform operations such as (1)KDF calculation which derives symmetric key used to perform Secure Messaging of BAC/EAC, (2)digital signature generation and verification based on RSA/ECDSA, (3)KDF calculation which derives symmetric key used to perform Secure Messaging of initialization or personalization. (Note: SHA-1 is implemented in the COS.)

- Random number generation

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

- 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.

TOE and TOE components are identified in the following Table 4.

Table 4. TOE and TOE Component Identification

Category (Form)	Name	Explanation
Product (MRTD IC chip in the form of COB or wafer)	SPNX	Physical products of the TOE delivered to customers in the form of wafer or COB package containing TOE

TOE	SPass NX V1.0 R3 on S3CT9Kx	Combination of COS, MRTD application and IC chip
TOE Component (HW)	S3CT9Kx	Revision 2
TOE Component (SW)	SPass NX V1.0	SPass NX V1.0 Release 3
TOE Component (Document)	User Guidance	Inspection System Guidance
		Initialization Guidance
		Personalization Guidance

1.4.2 Logical Scope of the TOE

TOE consists of 13 subsystems operating on the underlying IC chip.

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

<Asset>

In order to protect the TOE assets of Table 5, the TOE provides security functions, such as the confidentiality, the integrity, the authentication and the access control, etc.

Table 5. TOE Assets

Category			Description
User Data	MRTD Identity Data	Personal Data of the MRTD holder	Data stored in EF.DG1, EF.DG2, EF.DG5~EF.DG13 and EF.DG16
		Biometric Data of the MRTD holder	Data stored in EF.DG3 and EF.DG4
	MRTD 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 Chip Authentication Private Key		In EAC-CA, Chip Private key used by the TOE to demonstrate Not forged MRTD chip
	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

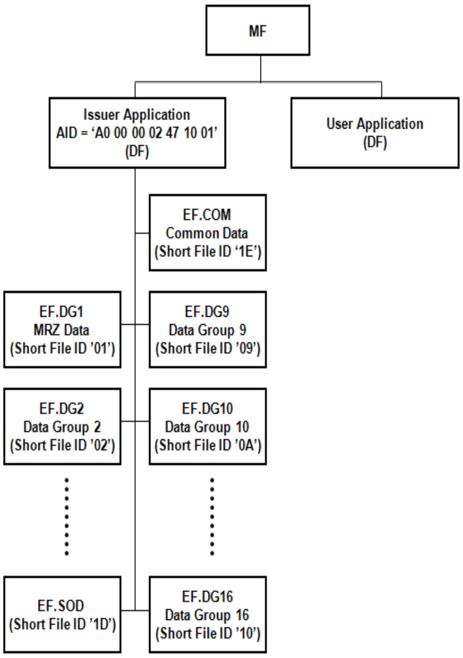
	Current Date	In personalization phase, Date of issuing the MRTD is recorded. However, In operational use phase, the TOE internally updates it as the latest date among issuing dates of CVCA link certificate, DV certificate or Issuing State IS certificate.
	BAC Authentication Key	BAC authentication encryption key, BAC authentication MAC key
	Initialization Key	Initialization authentication encryption key, Initialization authentication MAC key,
	Personalization Key	Personalization agent authentication encryption key, Personalization agent authentication MAC key,
	Operational Mode	TOE operational mode indicating credential
	MRTD Access Condition	Attributes assigned by personalization agent to allow up to BAC or up to EAC after MRTD personalization phase
	Initialization Data	TSF data credentials set by initialization (including Personalization Key, Operational Mode, MRTD Access Condition)
	BAC Session Key	BAC session encryption key, BAC session MAC key
	EAC Session Key	EAC session encryption key, EAC session MAC key
	Initialization Session Key	Initialization session encryption key, Initialization session MAC key
	Personalization Session Key	Personalization session encryption key, Personalization session MAC key

Application Notes : In order to support the EAC, the Personalization agent generates the EAC chip authentication public and private key and records them in the TOE. The CVCA digital signature verification key is updated through the CVCA link certificate according to the EAC specifications. However, the first CVCA digital signature verification key for verifying the CVCA link certificate shall be recorded in secure memory of the MRTD chip in the personalization phase. When The CVCA digital signature verification key is updated, the invalidation or deleting the existing CVCA digital signature verification key depends on the Issuing policy of the MRTD.

The LDS in which the user data are stored defines MF, DF and EF file structure. Table 6 shows the content of EF.DG1~EF.DG16 in which parts of the user data are stored.

Table 6. Contents of the LDS in which the User Data are Stored

Category	DG	Content	LDS Structure
Detail(s) Recorded	DG1	Document Type	
		Issuing State	

in MRZ		Name (of Holder)	
		Document Number	
		Check Digit – Doc Number	
		Nationality	
		Date of Birth	
		Check Digit - DOB	
		Sex	
		Data of Expiry or Valid Until Date	
		Check Digit DOE/VUD	
		Composite Check Digit	
Encoded Identification Features	DG2	Encoded face	
	DG3	Encoded finger(s)	
	DG4	Encoded Eye(s)	
Others	DG5	Displayed Portrait	
	DG6	-	
	DG7	Displayed Signature	
	DG8	-	
	DG9	-	
	DG10	-	
	DG11	Additional Personal Detail(s)	
	DG12	Additional Document Detail(s)	
	DG13	-	
	DG14	EAC Chip Authentication Public Key	
	DG15	AA Digital Signature Verification Key (optional)	
	DG16	Person(s) to Notify	

1.5 Conventions

ST uses some English terms and abbreviations to present clear meaning. The notation, formatting and conventions used in this ST are consistent with the Common Criteria for Information Technology Security Evaluation (hereafter referred to as "CC").

The CC allows several operations to be performed on functional requirements: assignment, iteration, refinement and selection. Each of these operations is used in this ST.

Iteration

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

Selection

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

Refinement

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

Assignment

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

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

1.6 ST Organization

Section 1 provides introductory material required for the ST and PP references and the summary of TOE.

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

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

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

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

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

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

Section 8 contains the materials referenced in this ST.

Section 9 defines the terms and abbreviations used in this ST.

2 Conformance Claim

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

2.1 Common Criteria Conformance

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

<Common Criteria Identification>

- Common Criteria for Information Technology, Part 1: Introduction and general model, version 3.1r4, 2012.9, CCMB-2012-09-001[CC1]
- Common Criteria for Information Technology, Part 2: Security functional components version 3.1r4, 2012.9, CCMB-2012-09-002[CC2]
- Common Criteria for Information Technology, Part 3: Security assurance components, version 3.1r4, 2012.9, CCMB-2012-09-003[CC3]

<Common Criteria Conformance>

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

2.2 Protection Profile Conformance

This ST conforms to the following PP.

- Title : ePassport Protection Profile
- Protection Profile Version : V2.1
- Certification Number : KECS-PP-0163a-2009
- Assurance Package : EAL4 augmented with(ADV_IMP.2, ATE_DPT.2, AVA_VAN.4)
- Type of conformance : demonstrable conformance

One of the TOE components, IC chip S3CT9Kx, claims Security IC Platform PP[PP_IC] and is certified as follows. ST lite, cetification report, maintenance reports of the S3CT9Kx can be found in the CCRA web site.

PP Conformance	BSI-PP-0035-2007
Ceritifcate Number	ANSSI-CC-2012/70
Evaluation Assurance Level	EAL5+ (ALC_DVS.2, AVA_VAN.5)

2.3 Package Conformance

This ST conforms to the following package.

- Assurance package : EAL5+(ADV_IMP.2, ALC_DVS.2, AVA_VAN.5)

2.4 Conformance Claim Rationale

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

2.4.1 The Consistency of the TOE Type

The type of TOE in the PP is the software including IC chip operating system (COS) and the application of machine readable travel documents (MRTD application) with the exception of hardware elements of the chip of machine readable travel documents (MRTD chip). The MRTD application includes the MRTD security mechanisms such as BAC, EAC and the MRTD access controls.

The type of TOE in this ST is the composition of the Embedded S/W which executes chip operating system with MRTD application and the IC chip hardware elements which claims [PP_IC]. The chip operating system implements the MRTD security mechanisms such as BAC, EAC and MRTD access control as well as AA and the personalization agent authentication.

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

2.4.2 The Consistency of the Security Problem Definition

<The Re-establishment of the Security Problem Definition>

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

Table 7. List of the Re-establishment of the Security Problem Definition

PP	ST	Description of reestablishment	Rationale
T.BAC_Authentication_Key_Disclose	T.BAC_Authentication_Key_Disclose	The BAC authentication key is generated by the personaliza-tion agent and is stored in the secure memory in the Personalization phase.	Selected the method that The Personalization Agent generates and stores the BAC authentication key out of the 2 methods proposed in the PP. Revised the application note according to this change.
T.Residual_Info	T.Residual_Info	”BAC authentication key” removed “Initialization authentication key, Initialization session key, personalization authentication key, personalization session key” added	BAC Authentication Key is stored in the secure memory and is not stored in the temporary memory. Thus it is not a residual information. Keys are added according to the authentication mechanism of initialization and personalization. This is more restrictive thus it satisfies “demonstrable conformance”.
P.Application_Install	P.Application_Install	Application notes modified	TOE is not an ‘open platform’ type thus it is described that initialization of application means install of application and subjects are also described. This is more restrictive thus it satisfies “demonstrable conformance”

PP	ST	Description of reestablishment	Rationale
A.Inspection_System	A.Inspection_System	Added AA support	Modified to make the inspection system support AA because the TOE provides AA security mechanism. This is more restrictive thus it satisfies “demonstrable conformance”.
A.IC_Chip	P.IC_Chip	IC chip is changed from TOE underlying platform to TOE component Changed from Assumption to Organizational Security Policy	TOE is a composite TOE meaning IC chip is included in the scope of the TOE thus IC chip is changed to TOE component and PP requires IC chip with appropriate level certificate shall be used in terms of policy thus OSP replaces Assumption.
A.MRZ_Entropy	A.MRZ_Entropy	Application notes modified	Raised the threat agent from moderate-level to high-level thus more restrictive.

<The Augmentation to the Security Problem Definition>

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

Table 8. List of Augmentation to the Security Problem Definition

Augmentation	Rationale
T.IC_Chip_Forgery	Adding a threat of IC chip forgery attack augments security object thus enhances the security attributes and restricts the security problem definition in the PP.
P.The_Issuing_Policy_of_the_MRTD	Additional OSPs for applying the MRTD personalization policy such as disabling EAC and secure communication channel do not weaken the security attributes in the PP thus the security problem is equivalent.
A.Process-Sec-IC	Accepted Assumption from the ST of the underlying IC chip assumes IC hip shall be delivered and protected in a secure manner during manufacturing phase and personaization phase, thus restricts the security problem definition in the PP
A.Plat-Appl	Accepted Assumption from the ST of the underlying IC chip assumes Embedded S/W shall be designed under the certified guidance of the IC chip, thus restricts the security problem definition in the PP
A.Resp-Appl	Accepted Assumption from the ST of the underlying IC chip assumes Embedded S/W shall maintain self application data in a secure manner, thus the security problem is equivalent.
A.Key-Function	Accepted Assumption from the ST of the underlying IC chip assumes the functionality relevant to cryptographic keys implemented in the Embedded S/W shall not allow information leakage attack, thus the security problem is equivalent.

2.4.3 Security Objectives Rationale

<The Re-establishment of the Security Objectives>

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

Table 9. List of Re-establishment of the Security Objectives

PP security objectives	ST security objectives	Reestablishment	Rationale
O.Management	O.Management	Augmented TOE management including initialization during the manufactruing phase	TOE management methods including initialization in the manufacturing phase are additionally defined. This is more restrictive thus it satisfies "demonstrable conformance".
O.Session_Termination	O.Session_Management	Maintain EAC communica-tion channel instead of session termination even if the EAC-TA fails Change the name	EAC specification mandates maintaining the EAC secure messaging channel generated by successful EAC-CA to protect the transmission data even if the EAC-TA fails.
O.Secure_Messaging	O.Secure_messaging	Augmented secure messaging in the personalization phase	Augmenting a purpose in order to add a function for the policy to protect the transmission data to enhance security in the manufacturing phase and in the personalization phase
O.Replay_Prevention	O.Replay_Prevention	Modified the application note, additional authentica-tion data which requires a random number	The coverage of authentication data whichrequires replay prevention is widened for AA and personalization agent authentication are added.
O.Security_Mechanism_Application_Procedures	O.Security_Cechanism_Application_Procedures	Augmented AA	AA is augmented according to ICAO/EAC specifications. This is more restrictive thus it satisfies "demonstrable conformance".
O.Handling_Info_Leakage	O.Handling_Infor_Leakage	Modified application note according to the intention of the composite evaluation	Countermeasures are described in the application note. This is more restrictive thus it satisfies "demonstrable conformance".
OE.IC_Chip	O.IC_Chip	Change to security objectives for the TOE	As a composite TOE, IC chip is included in the TOE scope thus security characteristics of IC chip should be changed to security objectives for the TOE.

<The Augmentation to the Security Objectives>

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

Table 10. List of the Augmentation to the Security Objectives

Augmentation	Rationale
O.Personalization_Agent_Authentication	Augmenting the relevant objective in order to provide authentication method of MRTD personalization agent and thus restricts the security objectives in the PP
O.Initialization_Authentication	Augmenting the relevant objective in order to provide authentication method of TOE initialization and thus restricts the security objective in the PP
O.AA	Augmenting the security attribute of the TOE for verification of genuineness enhances the security properties of the PP and thus conforms more restrictively.

2.4.4 The Rationale for the Consistency of Security Function Requirements

<The Re-establishment of the SFR>

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

Table 11. List of Re-establishment of the SFR

SFR		Operation performed in this ST	Description on re-establishment
FCS_CKM.1	-	iteration	Renamed to FCS_CKM.1(1)
	dependencies	refinement	FCS_CKM.2, FCS_COP.1 refinement
	FCS_CKM.1.1	refinement	TSF generates keys on behalf of manufacturers & personalization agents, refinement on the application notes
FCS_CKM.2(1)	dependencies	refinement	FCS_CKM.1 refinement
	FCS_CKM.2.1	selection, selection	applied operations to meet the security objectives
FCS_CKM.2(2)	dependencies	refinement	FCS_CKM.1 refinement
	FCS_CKM.2.1	selection, selection, refinement	refinement on the application notes
FCS_CKM.4	dependencies	refinement	FCS_CKM.1 refinement
	FCS_CKM.4.1	assignment, assignment	applied operations to meet the security objectives
FCS_COP.1(1)	dependencies	refinement	FCS_CKM.1 refinement
	FCS_COP.1.1	(selection+assignment), (selection+assignment), (selection+assignment), refinement	applied operations to meet the security objectives, refinement on the application notes
FCS_COP.1(2)	dependencies	refinement	FCS_CKM.1 refinement
	FCS_COP.1.1	(selection+assignment), (selection+assignment), (selection+assignment), refinement	applied operations to meet the security objectives, refinement on the application notes
FCS_COP.1(3)	FCS_COP.1.1	selection, (selection+assignment)	applied operations to meet the security objectives, refinement on the application notes

SFR		Operation performed in this ST	Description on re-establishment
FCS_COP.1(4)	dependencies	refinement	FCS_CKM.1 refinement
	FCS_COP.1.1	selection, (selection+assignment), assignment, assignment	applied operations to meet the security objectives, refinement on the application notes
FDP_ACC.1	FDP_ACC.1.1	assignment, assignment, assignment	applied operations to meet the security objectives
FDP_ACF.1	FDP_ACF.1.1	assignment	applied operations to meet the security objectives
	FDP_ACF.1.2	assignment	applied operations to meet the security objectives
	FDP_ACF.1.3	assignment	applied operations to meet the security objectives
	FDP_ACF.1.4	assignment	applied operations to meet the security objectives
FDP_RIP.1	FDP_RIP.1.1	deletion, assignment, selection, refinement	deleted BAC authentication key from the objectives list, refinement on the application notes
FDP_UCT.1	FDP_UCT.1.1	refinement	refinement on the application notes
FDP_UIT.1	FDP_UIT.1.1	selection	applied operations to meet the security objectives
	FDP_UIT.1.2	selection, refinement	applied operations to meet the security objectives, refinement on the application notes
FIA_AFL.1	-	iteration	Renamed to FIA_AFL.1(1)
	dependencies	refinement	FIA_UAU.1 refinement
	FIA_AFL.1.1	assignment, (selection+assignment)	applied operations to meet the security objectives
	FIA_AFL.1.2	selection, refinement	applied operations to meet the security objectives, refinement on the method of handling authentication fails
FIA_UAU.1(1)	dependencies	refinement	FIA_UID.1 refinement
	FIA_UAU.1.1	refinement, assignment	refinement on timing/objective of security function execution, applied operations to meet the security objectives
	FIA_UAU.1.2	refinement	user refinement
FIA_UAU.1(2)	FIA_UAU.1.1	refinement, assignment	refinement on timing/objective of security function execution, applied operations to meet the security objectives
	FIA_UAU.1.2	refinement	user refinement
FIA_UAU.4	FIA_UAU.4.1	assignment	applied operations to meet the security objectives
FIA_UAU.5	FIA_UAU.5.1	assignment	applied operations to meet the security ob-

SFR		Operation performed in this ST	Description on re-establishment
			jectives
	FIA_UAU.5.2	refinement, assignment	refinement including AA security mechanism, applied operations to meet the security objectives
FIA_UID.1	-	iteration	Renamed to FIA_UID.1(1)
	FIA_UID.1.2	refinement	refinement on the application notes
FMT_MOF.1	-	iteration	Renamed to FMT_MOF.1(1)
	FMT_MOF.1.1	refinement	refinement to MRTD Personalization Agent
FMT_MSA.3	FMT_MSA.3.2	refinement	refinement to TSF on behalf of Personalization Agent, refinement on the application notes
FMT_MTD.1(1)	component name	refinement	changed identification information of iteration component to 'the certificate verification information and the authentication key'
	FMT_MTD.1.1	assignment, refinement	applied operations to meet the security objectives, augmented application notes
FMT_MTD.3	dependencies	refinement	FMT_MTD.1 refinement
	FMT_MTD.3.1	assignment, refinement	applied operations to meet the security objectives, refinement to the high-level attack potential
FMT_SMF.1	FMT_SMF.1.1	refinement, assignment	refinement on security management functions in the manufacturing, personalization and operational use phase, applied operations to meet the security objectives
FMT_SMR.1	dependencies	refinement	FIA_UID.1 refinement
	FMT_SMR.1.1	assignment	applied operations to meet the security objectives
FPR_UNO.1	FPR_UNO.1.1	assignment, assignment, refinement	applied operations to meet the security objectives, refinement on the application notes
FPT_FLS.1	FPT_FLS.1.1	assignment	applied operations to meet the security objectives
FPT_ITI.1	FPT_ITI.1.2	assignment, refinement	applied operations to meet the security objectives, refinement on the application notes
FPT_TST.1	FPT_TST.1.1	selection, assignment, selection	applied operations to meet the security objectives
	FPT_TST.1.2	selection, assignment	applied operations to meet the security objectives
	FPT_TST.1.3	selection	applied operations to meet the security objectives

FCS_CKM.1(1), FDP_RIP.1 and FMT_MSA.3 are restrictively refined to reflect that TSF generates BAC authentication keys on behalf of MRTD Personalization Agent after writing DG1 in the personalization phase and writes them in the secure memory of EEPROM and do not write in the volatile memory during the BAC mutual authentication procedure.

Application notes of FDP_UCT.1 and FDP_UIT.1 are refined to reflect the function that can select Secure Messaging during transceiving MRTD user data by the Personalization Agent.

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

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

The security management functions of the MRTD's operational use phase in FMT_SMF.1 and the application notes on FCS_CKM.2(2), FIA_UID.1(1), FPT_ITI.1 are refined to reflect the implementational characteristic of the TOE.

<The Augmentation to the Security Functional Requirement>

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

Table 12. List of the Additional SFR

Additional SFR	Rationale
FCS_CKM.1(2)	Augmented to generate the key used for the authentication mechanism of intiailization and personalization agent because each authentication mechanism is augmented.
FCS_CKM.2(3)	Defined additional SFR on distribution method of KDF Seed values to generate the session keys used for initialization and personalization according to each authentication mechanism
FCS_COP.1(5)	This SFR if added to reflect AA mechanism to prove genuineness of the TOE because AA mechanism is augmented.
FCS_RNG.1	This SFR is added because it is relevant to meet O.IC_Chip under composite TOE evaluation.
FDP_DAU.1	This SFR is added since the AA security mechanism is added to the security objective. The MRTD personalization agent provides the function to detect the forged IC chip thus the SFR in this ST accepts the PP restrictively
FIA_AFL.1(2)	This SFR is augmented to provide counteractions to the failures of initialization and personalization agent authentication as these are augmented. This accepts the PP restrictively because the counteractions are stronger than those to BAC authentication failure.
FIA_UAU.1(3)	This SFR is added for the requirement of the method to authenticate a user as the personalization agent to connect and maintain the security role of the personalization agent to user and grant the subject right to the user. This accepts the PP restrictively because it augments personalization agent authentication.
FIA_UAU.1(4)	This SFR is added for the requirement of the method to authenticate a user as the manufacturer to connect and maintain the security role of the manufacturer to user and grant the

Additional SFR	Rationale
	subject right to the user. This accepts the PP restrictively because it augments initialization authentication.
FIA_UID.1(2)	This SFR is added to allow various communication protocol without limiting communication protocols when manufacturers are identified.
FMT_MOF.1(2)	EAC is unnecessary and disabled when DG3/DG4 are not available according to the policy of the personalization agent. The level of security is equivalent to that of the PP since disabling the EAC is only applicable when DG3/DG4 are not available and the access to DG3/DG4 are explicitly denied when the EAC is disabled so the MRTD access control policy is conformed. The PP does not require the secure messaging in personalization phase, but this ST added this SFR in order to provide the secure messaging and disable it if the personalization environment is secure and does not require the secure messaging.
FMT_MTD.1(3)	This SFR is added since the TOE distinguishes the personalization phase and the operational use phase to manage the MRTD more securely and defines modes of operation and provides management functions in order to implement the command access control according to the phases. This SFR is also added to reflect the function that writes initialization data to the secure memory to initialize TSF in the manufacturing phase. This enhances the security and thus accepts the PP restrictively.
FMT_MTD.1(4)	This SFR is added since the TOE is selected as a subject generates the BAC authentication key among the two options in the PP and the TSF generates and stores the BAC authentication key automatically after the DG1 is written successfully.
FPT_ITC.1	This SFR is added to provide optional function that enhances the security of transmitted data in the manufacturing and personalization phase
FPT_PHP.3	This SFR is added because it is relevant to meet O.IC_Chip under composite TOE evaluation.

2.4.5 The Consistency of the Security Assurance Requirements

This ST specifies CC EAL5 augmented with (ADV_IMP.2, ALC_DVS.2, AVA_VAN.5) to assure the secure operation of the TOE is not compromised and counter the high-level threat agent. This assurance package maintains “demonstrable conformance” of the security assurance requirements of the PP since this is a superset including the assurance package of the PP - EAL 4 augmented with(ADV_IMP.2, ATE_DPT.2, AVA_VAN.4) – and ADV_FSP.5, ADV_TDS.4, ALC_DVS.2 ALC_CMS.5, ALC_TAT.2, ATE_DPT.3 and AVA_VAN.5 in this assurance package are hierarachical to each of ADV_FSP.4, ADV_TDS.3, ALC_DVS.1, ALC_CMS.4, ALC_TAT.1, ATE_DPT.2 and AVA_VAN.4 in the EAL4 assurance package and thus maintain “demonstrable conformance” of the security assurance requirements of the PP. And ADV_INT.2 is augmented to describe well-structured TSF internals that is required in the EAL 5 or higher.

<Additional Security Assurance Requirements>

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

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

- ATE_DPT.2 “Testing: Security-enforcing modules”
- AVA_VAN.4 “Methodical vulnerability analysis”

The ST augments again the following security assurance requirements (SAR) to the PP. This augmentation is in accordance with the CC.

- ADV_FSP.5 “Complete semi-formal functional specification with additional error information”
- ADV_INT.2, “Well-structured internals”
- ADV_TDS.4, “Semiformal modular design”
- ALC_DVS.2 “Sufficiency of security measures”
- ALC_CMS.5 “Development tools CM coverage”
- ALC_TAT.2 “Compliance with implementation standards”
- ATE_DPT.3 “Testing: modular design”
- AVA_VAN.5 “Advanced methodical vulnerability analysis”

3 Security Problem Definition

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

3.1 Threats

The 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 ST, the TOE consists of the Embedded S/W and the IC chip. Therefore, the threat agent has high-level expertise, resources, motivation.

<Threats to the TOE in the Personalization Phase>

T. TSF_Data_Modification

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

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

T. Eavesdropping

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

T. Forgery_Corruption_Personal_Data

In order to forge and corrupt the personal data of the 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_Authentication_Key_Disclose

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

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

T. BAC_ReplayAttack

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

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

<EAC-related Threats in the Operational Use Phase>

T. Damage_to_Biometric_Data

The threat agent may disclose, forge and corrupt the biometric data of the 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.

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. SessionData_Reuse

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

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

T. Skimming

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

<Threats related to IC Chip Support>

T. Malfunction

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

<Other Threats in the Operational Use Phase>

T. Leakage_CryptographicKey_Info

By using electric power and wave analysis devices, the threat agent may obtain key information used in cryptographic technique applied to the 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_Info

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

T. IC_Chip_Forgery

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

3.2 Organisational Security Policies

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

P. International_Compatibility

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

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

P. Security_Mechanism_Application_Procedures

The TOE shall ensure the order of security mechanism application according to the type of the Inspection System so that not to violate the 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 MRTD Inspection Procedure and 2.1.2 Advanced MRTD Procedure of the EAC specifications.

P. Application_Program_Install

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

Application Notes : The application program installing is implemented during initialization in the TOE which can be conducted by the manufacturer.

P. 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 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. MRTD_Perso_Policy

The TOE shall deactivate the EAC if the Personalization_agent does not store the biometric data into the MRTD.

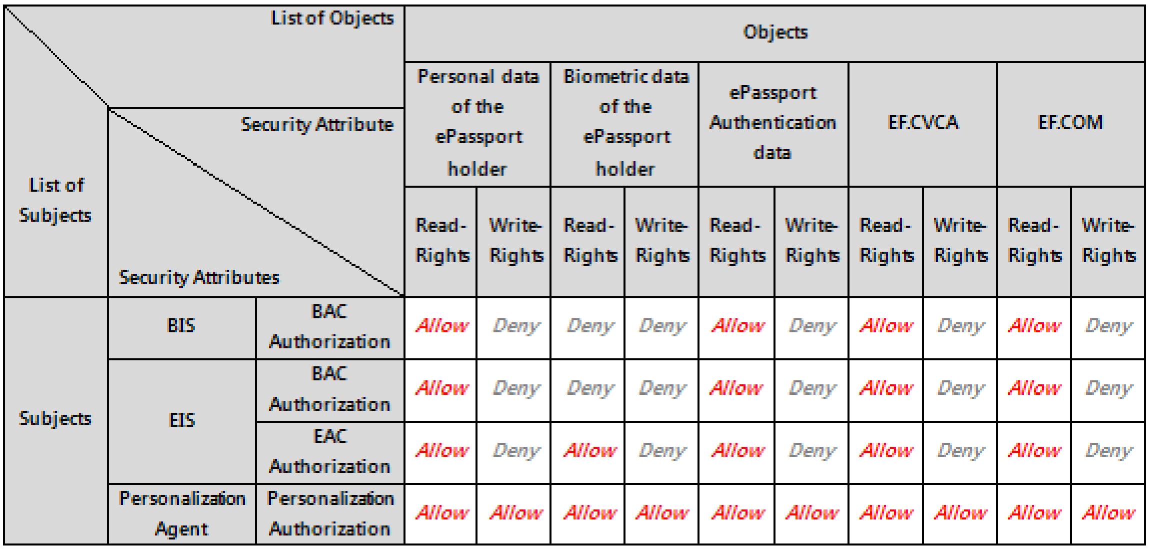
The TOE shall provide the way to deactivate the secure communication channel if it is not required because the issuing environment is insulated from the outside so that the security of transmission data is assured.

P. MRTD_Access_Control

The Personalization Agent and 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 document and EAC specifications.

Table 13. MRTD Access Control Policy



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

P. PKI

The Issuing State of the MRTD 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 MRTD 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_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.

P. IC_Chip

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

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

3.3 Assumption

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

A. Certificate_Verification

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

Application Notes : The methods of the Inspection System to verify the certificate chain for the PA and to distribute the IS certificate and the digital signature generation key may depend on the Issuing policy of the MRTD. Therefore, the ST author can define security environment according to the Issuing policy of the MRTD.

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 the AA security mechanism as an option, it verifies the forgery and corruption for the personal and authentication data of the MRTD holder explicitly by performing the AA and verifying the digital signature which is generated by the TOE.

As the EIS supports the BAC, EAC and PA security mechanisms, it obtains the read-rights for the personal, authentication and biometric data of the 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 EIS supports the AA security mechanism as an option, it verifies the forgery and corruption for the personal and authentication data of the MRTD holder explicitly by performing the AA and verifying the digital signature which is generated by the TOE after performing the EAC-CA and the PA.

A. MRZ_Entropy

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

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

<Assumptions from the ST of IC chip>

The followings are augmented using the assumptions applied in the [ST_IC].

A.Process-Sec-IC (Protection during Packaging, Finishing and Personalisation)

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

A.Plat-Appl (Usage of Hardware Platform)

The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

A.Resp-Appl (Treatment of User Data)

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

A.Key-Function (Usage of Key-dependent Functions)

Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks.

4 Security Objectives

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

4.1 Security Objectives for the TOE

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

O. Management

The TOE shall provide the means to manage the MRTD application initialization data in the manufacturing phase to the authorized Manufacturer.

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

O.Personalization_Agent_Authentication

The TOE shall provide the authentication means, which have the equivalent level to BAC, to connect only the authorized Personalization Agent to issuing management role and subject security attributes. However, it shall provide stronger level of countermeasure to authentication failures than BAC's. It shall also generate personalization session keys to be used for creating a secure channel in the personalization phase.

O.Initialization_Authentication

The TOE shall provide the authentication means, which have the equivalent level to BAC, to allow only the authorized Manufacturer to initialize. However, it shall provide stronger level of countermeasure to authentication failures than BAC's. It shall also generate initiallization session keys to be used for creating a secure channel in the manufacturing phase.

O.Security_Mechanism_Application_Procedures

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

Application Notes : The TOE shall ensure that the application order of PA, AA, BAC, and EAC security mechanisms conforms to 2.1.1 Standard MRTD Inspection Precedure and 2.1.2 Advanced MRTD Precedure of the EAC specifications 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 specifications, the ST author shall ensure reliability and secure operation that conforms to the EAC specifications.

O.Session_Management

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

O.Secure_Messaging

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

O.Certificate_Verification

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

O.Secure_State

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

O.Deleting_Residual_Info

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

O.Replay_Prevention

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

Application Notes : The TOE shall generate the transmitted data to the Inspection System in the BAC mutual authentication and EAC-TA to be different per session and shall not use the BAC authentication key as the BAC session key. Also, the TOE shall not provide critical information necessary to derive session key by generating the BAC session key with the same random number used in the BAC mutual authentication. The transmitted value to Inspection System shall be different for each session during initialization authentication or personalization agent authentication, and authenticaiton keys or random numbers used to generate them for each mechanism shall not be used when generating session keys so as not to provide information indicating them. The random number generated in the active authentication and the random number used in Persionalization agent authentication shall be differenctly generated per session.

O.Access_Control

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

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

O.Handling_Info_Leakage

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

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

O.AA

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

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.IC_Chip

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

4.2 Security Objectives for the Environment

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

OE.MRTD_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_MRTD_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_Install

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

OE.Certificate_Verification

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

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

OE.MRZ_Entropy

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

OE.PKI

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

OE.Range_RF_Communication

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

<Security Objectives for environment from the ST of the IC chip>

The followings are augmented using Security Objectives for environment applied in the [ST_IC].

OE. Plat-Appl (Usage of Hardware Platform)

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

OE.Resp-Appl (Treatment of User Data)

Security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as required by the security needs of the specific application context. For example, the Smartcard Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.

OE.Process-Sec-IC (Protection during composite product manufacturing)

Security procedures shall be used after TOE delivery up to delivery to the “consumer“ to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.

4.3 Security Objectives Rationale

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

The rationale of security objectives demonstrates the following:

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

Table 14 shows the mapping between Security Problem Definition and Security Objectives.

Table 14. The mapping between Security Problem Definition and Security Objectives

Security Objectives / Security Problem Definition	TOE Security Objectives																Security Objectives for the Environment								
	O.Management	O.Personalization _Authentication	O.Initialization_Authentication	O Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Secure_State	O.Deleting_Residua_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.AA	O.BAC	O.EAC	O.IC_Chip	OE.MRTD_Manufacturing_Security	OE.Procedures_of_MRTD_Holder_Check	OE.Application_Program_Install	OE.Certificate_Verification	OE.Personalization_Agent	OE.Inspection_System	OE.MRZ_Entropy	OE.PKI	OE. Range_RF_Communication
T.TSF_Data_ Modification	X	X			X	X					X										X				
T.Eavesdropping						X																X			
T.Fogery_Corruption_Personal Data					X						X			X								X			
T.BAC_Authentication_Key_Disclose	X				X						X							X							
T.BAC_ReplayAttack										X															
T.Damage_to_Biometric_Data					X	X	X				X				X					X		X		X	
T. EAC-CA_Bypass				X														X		X		X			
T. IS_Certificate_Forgery	X	X					X													X					
T. SessionData_Reuse										X												X			
T. Skimming											X			X	X							X			X
T.Malfunction								X								X									
T.Leakage_CryptographicKey_Info												X				X									
T. MRTD_Reproduction																	X	X							
T.Residual_Info									X																
T.IC_Chip_Forgery													X												
P.International_Compatibility																					X				
P.Security_Mechanism_Application_Procedures				X																		X			
P.Application_Program_Install	X		X			X													X						
P.Personalization_Agent	X	X																			X				
P.MRTD_Perso_Policy	X	X				X																			
P.MRTD_Access_Control	X										X			X	X						X	X			
P. PKI							X																	X	
P.Range_RF_Communication																									X
P.IC_Chip																X									
A.Certificate_Verification																				X	X			X	
A.Inspection System																						X			
A.MRZ_Entropy																							X		

The following table shows the mapping between Security Problem Definition and Security Objectives coming from [IC_ST]

Security Problem Definition from the IC chip	Security Objectives from the IC chip
A.Process-Sec-IC	OE.Process-Sec-IC
A.Plat-Appl	OE.Plat-Appl
A.Resp-Appl	OE.Resp-Appl
A.Key-Function	OE.Plat-Appl, OE.Resp-Appl

4.3.1 Security Objective Rationale for the TOE

<MRTD-relevant Security Objectives>

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 LDS application data writing function of the personalization agent in the Operational Use phase. Therefore, this security objective is required to counter the threats of T.TSF_Data_Modification and T.BAC_Authentication_Key_Disclose and to enforce the organizational security policies of P.MRTD_Access_Control and P.Personalization_Agent.

Also, this security objective provides the manufacturer with the means to manage TOE including initialization of MRTD application in the Initialization phase, therefore is required to counter the OSP of P.Application_Program_Install, and 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.

This security objective provides the means to manage EAC disablement when personalizing MRTD excluding MRTD biometric information according to the issuing policy, therefore contributes to enforce the organizational security policy of P.MRTD_Personalization_Policy.

O.Personalization_Agent_Authentication

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

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

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

O.Initialization_Authentication

This security objective ensure that the TOE provides the means to authorize user as manufacturer for granting management to select options, initialize function talbes and initialize EEPROM, etc., therefore is required to counter the OSP of P.Application_Program_Install.

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

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

O.Security_Mechanism_Application_Procedures

This security objective is required to enforce the organizational security policy of P.Security_Mechanism_Application_Procedures since the TOE ensures that the application order of the PA, BAC and EAC security mechanisms according to 2.1.1 Standard 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_Management

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

Also, this security objective ensures that the TOE detects the BAC or EAC-TA failure of whom attempts access to read, maintains the BAC or EAC secure channel, and reduces attack chances, therefore is required to counter the threat of T.BAC_Authentication_Key_Disclosure and T.Damage_to_Biometric_Data.

O.Secure_Messaging

This security objective ensures that the TOE establishes the BAC or EAC secure messaging for secure transmission of the personal and biometric data of the MRTD holder to the Inspection System, and provides the confidentiality and integrity for the transmitted personal and biometric data of the MRTD holder. Therefore, this security objective is required to counter the threats of T.Damage_to_Biometric_Data and T.Eavesdropping. Also, this security objective ensures that the TOE establishes the secure messaging when the authorized Personalization Agent wirtes TSF data, and provides integrity of TSF data. Therefore, this security objective is required to counter the threat of T.TSF_Data_Modification.

This security objective ensures that the secure messaging shall be created to provide confidentiality and integrity for initialization data when the Manufacturer initializes MRTD application. Therefore, theis security objective contributes to enforce the organizational security policy of P.Application_Program_install.

Also, this security objective ensures that if the Personalization Agent requests the secure messaging the TOE handles it, and that if the Personalization Agent does not request it, the TOE deactives the secure messaging. Therefore, this security objective contributes to enforce the organizational security policy of P.MRTD_Personalization_Policy.

O.Certificate_Verification

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

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

O.Secure_State

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

O.Deleting_Residual_Info

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

O.Replay_Prevention

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

O.Access_Control

This security objective is required to counter the threats of T. Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data and T.Skimming and enforce the organizational security policy of P.MRTD_Access_Control by implementing the rules of allowing or denying of Inspection System to read user data in accordance with the MRTD access control policies by the personalization agent.

This security objective is required to counter the threats of T.TSF_Data_Modification and T.BAC_Authentication_Key_Disclose as it allows the authorized personalization agent has the write-rights of the MRTD application data in the Personalization phase and denies the access by personalization agent in the Operational Use phase.

O.Handling_Info_Leakage

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

O.AA

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

O.BAC

This security objective is required to enforce the organizational security policy of P.MRTD_Access_Control as the TOE implements the BAC security mechanism to control access to the personal data of the MRTD holder, therefore grants 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_Corruption_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 policy of P.MRTD_Access_Control as the TOE implements the EAC-CA and EAC-TA to control access to the biometric data of the MRTD holder, therefore grants 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.IC_Chip

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

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

4.3.2 Security Objective Rationale for Operating Environment

OE.MRTD_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_MRTD_Holder_Check

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

OE.Application_Program_Install

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

OE.Certificate_Verification

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

OE.Personalization_Agent

This security objective for environment is required to enforce the organizational security policies of P.International_Compatibility and P.Personalization_Agent by ensuring that the TOE is delivered to the Operational Use phase after securely issuing the 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 policy of P.MRTD_Access_Control as it defines the role of the personalization agent. Also, this security objective for environment is required to support the assumption of A.Certificate_Verification because the personalization agent makes certificates necessary in the PA and EAC support available to the Inspection System.

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

OE.Inspection_System

This security objective for environment is required to support the assumption of A.Inspection System and enforce the organizational security policies of P.Security_Mechanism_Application_Procedures and P.MRTD_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 MRTD access control policies of the personalization agent and by ensuring that information used in communication with the TOE is securely destroyed after session termination.

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

This security objective for environment is required to counter the threats of T. Forgery_Corruption_Personal Data, T.Damage_to_Biometric_Data, T.Skimming and T.EAC-CA_Bypass as the Inspection System supports the BAC mutual authentication, EAC and PA.

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

OE.MRZ_Entropy

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

OE.PKI

This security objective for environment is required to enforce the organizational security policy of P. PKI and supports the assumption of A.Certificate_Verification by implementing and operating the MRTD PKI System that executes certification practice according to CPS, such as to generate digital signature key and to generate, issue, and distribute of certificates necessary in supporting PA and

EAC security mechanisms. Also, this security objective for environment is required to counter the threat of T.Damage_to_Biometric_Data by generating, issuing and distributing certificates necessary in the EAC through implementation of the EAC-PKI.

OE.Range_RF_Communication

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

<Rationale of the Security Objects for environment from the ST of the IC Chip>

OE. Plat-Appl (Usage of Hardware Platform)

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

OE.Resp-Appl (Treatment of User Data)

This security objective for environment supports the assumption of A.Resp-Appl and A.Key-Function by requiring Embedded S/W developer to handle sensitive application data such as cryptographic keys in accordance with the security requirement considering the context of application program.

OE.Process-Sec-IC (Protection during composite product manufacturing)

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

5 Definition of Extended Component

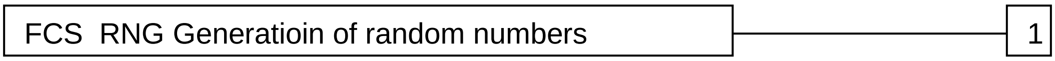
ST defines FCS_RNG as follows that is declared in the ST of the IC chip.

FCS_RNG Generation of random numbers

Family behaviour

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

Component levelling:



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

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

6 Security Requirements

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

ST follows external entities such as the Personalization agent, BIS, EIS, MRTD IC Chip are specified in PP.

This ST defines all subjects, objects, operation, security attributes employed in security requirements as Table 15 as does in the PP. Also, it defines SSC(Send Sequence Counter) with session security attributes related to establishing secure messaging.

Table 15. Definition of Subject, Object, related Security Attributes and Operation

<table>
<tr><th>Subject</th><th>Subject Security Attributes</th><th>Object</th><th>Object Security Attributes</th><th>Operation</th></tr>
<tr>
<td colspan="2">
<table>
<tr><th>S bje ts</th><th>Security attributes</th></tr>
<tr><td>BIS</td><td>BAC authorization</td></tr>
<tr><td>EIS</td><td>BAC authorization,
EAC authorization</td></tr>
<tr><td>Personalization agent</td><td>Personalization agent issuing authorization</td></tr>
</table>
</td>
<td colspan="2">
<table>
<tr><th rowspan="2">Objects</th><th colspan="2">Security attributes</th></tr>
<tr><th>Security attributes of object's operation</th><th>Security attributes of object's access-rights</th></tr>
<tr><td rowspan="2">Personal data of the MRTD holder</td><td>Read-rights</td><td>BAC authorization,
EAC authorization</td></tr>
<tr><td>Write-rights</td><td>Personalization agent issuing authorization</td></tr>
<tr><td rowspan="2">Biometric data of the MRTD holder</td><td>Read-rights</td><td>EAC authorization</td></tr>
<tr><td>Write-rights</td><td>Personalization agent issuing authorization</td></tr>
<tr><td rowspan="2">MRTD authentication data</td><td>Read-rights</td><td>BAC authorization,
EAC authorization</td></tr>
<tr><td>Write-rights</td><td>Personalization agent issuing authorization</td></tr>
<tr><td rowspan="2">EF.CVCA</td><td>Read-rights</td><td>BAC authorization,
EAC authorization</td></tr>
<tr><td>Write-rights</td><td>Personalization agent issuing authorization</td></tr>
<tr><td rowspan="2">EF.COM</td><td>Read-rights</td><td>BAC authorization,
EAC authorization</td></tr>
<tr><td>Write-rights</td><td>Personalization agent issuing authorization</td></tr>
</table>
</td>
<td>- Read
- Write</td>
</tr>
</table>

6.1 Terms and Definitions

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

Table 16 Terms and Definitions Relevant to SFR

Terms	Definitions
Initialization authentication key	Symmetric keys such as encryption key and MAC key for initialization authentication that are used for the manufacturer to acquire initialization-right and to conduct initialization of TSF data in a secure manner
Initialization session key	Symmetric keys such as encryption key and MAC key generated in accordance with KDF using random number generated during initialization authentication for initialization session that are used for each session by the authorized manufacturer to generate secure messaging in the manufacturing phase
Personalization authentication key	Symmetric keys such as encryption key and MAC key personalization agent authentication that are used for the personalization agent to acquire personalization-right and to conduct TSF data writing in a secure manner
Personalization session key	Symmetric keys such as encryption key and MAC key generated in accordance with KDF using random number generated during personalization agent authentication for personalization session that are used for each session by the personalization agent to generate secure messaging in a secure manner
AA private key	The private key stored in the TOE seucre memory and used to generate digital signature for AA security mechanism
AA public key	The public key read from the DG15 in the TOE and used to verify digital signature for AA security mechanism

.

6.2 TOE Security Functional Requirements

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

<Cryptographic Support>

FCS_CKM.1(1) Cryptographic Key Generation (Key Derivation Mechanism)

Hierarchical to: No other components.

Dependencies: [**FCS_CKM.2(1)** Cryptographic key distribution (KDF Seed Distribution for BAC session key generation) and

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

FCS_COP.1 Cryptographic operation(One-way hash function)]

FCS_CKM.4 Cryptographic key destruction

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

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

FCS_CKM.1(2) Cryptographic Key Generation (Initialization and Personalization Key Derivation Mechanism)

Hierarchical to: No other components.

Dependencies: [**FCS_CKM.2(3)** Cryptographic key distribution (KDF Seed Distribution for initialization and personalization session key generation) or

FCS_COP.1(3) Cryptographic operation(One-way hash function)]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate **initialization session key of Manufacturer and personalization session key of Personalization agent** in accordance with a specified cryptographic key generation algorithm [Appendix 5.1 Key Derivation Mechanism] and specified cryptographic key sizes [128 bit] that meet the following: [the ICAO specification].

FCS_CKM.2(1) Cryptographic Key Distribution(KDF Seed Distribution for BAC Session Key Generation)

Hierarchical to: No other components

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

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

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

FCS_CKM.4 Cryptographic key destruction

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

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

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

Hierarchical to: No other components

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

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

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

FCS_CKM.4 Cryptographic key destruction

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

Table 17 Cryptographic Key Distribution Standard and Method

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

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

Table 18 Cryptographic Key Distribution Standard and Method

Standard	Key Length
DH	1280, 1536, 2048 bits
ECDH	192, 224, 256, 320, 384, 512 bits

FCS_CKM.2(3) Cryptographic Key Distribution(KDF Seed Distribution for Initialization and Personalization Session Key Generation)

Hierarchical to: No other components

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

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

FCS_CKM.1(2) Cryptographic key generation(Initialization and Personalization Key Derivation Mechanism)]

FCS_CKM.4 Cryptographic key destruction

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

Application Notes : The TOE uses AES accelerator and SHA-256 cryptographic library are supported by IC chip, for KDF Seed for the Initialization and Personalization session key generation.

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other components

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

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

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

FCS_CKM.1(2) Cryptographic key generation (initialization and personalization Key-derivation mechanism)]

FCS_CKM.4.1 The TSF shall destroy **encryption keys and MAC keys** in accordance with a specified cryptographic key destruction method [deleting memory data physically by overwriting] that meets the following: [none].

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

Hierarchical to: No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism) and
FCS_CKM.1(2) Cryptographic key generation (initialization and personalization Key-derivation mechanism)]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [message encryption, decryption operation] in accordance with [*[specified cryptographic algorithms in Table 19]*] and cryptographic key sizes [*[specified in Table 19]*] that meet the following: [*[specified standards in Table 19]*].

Table 19 Symmetric Key Cryptographic Standards and Specifications

Standard	Cryptographic Algorithm	Cryptographic Key Size
ISO/IEC 18033-3 4.1	TDES	112 bit
ISO/IEC 18033-3 5.1	AES	128 bit

Application Notes : The TOE uses the TDES cryptographic algorithm for the confidentiality protection of the transmitted data of the BAC or EAC secure messaging, for the BAC mutual authentication and for the BAC key distribution. The TOE uses the AES cryptographic algorithm for the confidentiality protection of the transmitted data of the initialization or personalization secure messaging, for the initialization or personalization agent authentication and for the initialization or personalization authentication key and session key distribution.

FCS_COP.1(2) Cryptographic operation (MAC)

Hierarchical to: No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(1) Cryptographic key generation(Key Derivation Mechanism) and
FCS_CKM.1(2) Cryptographic key generation (initialization and personalization Key-derivation mechanism)]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [MAC operation] in accordance with [*[specified cryptographic algorithms in]*] and cryptographic key sizes [*[specified in Table 20]*] that meet the following: [*[specified standards in Table 20]*].

Table 20 MAC Standards and Specifications

Standard	Cryptographic Algorithm	Cryptographic Key Size
ISO/IEC 9797-1	Retail MAC	112 bit
NIST SP 800-38B	AES-CMAC	128 bit

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. And the TOE uses the AES-CMAC algorithm for the integrity protection of the transmitted data of the initialization or personalization secure messaging.

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(1) Cryptographic key generation(Key Derivation Mechanism) and

FCS_CKM.1(2) Cryptographic key generation (initialization and personalization Key-derivation mechanism)]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Hash operation] in accordance with [*SHA-1,[SHA-224,SHA-256, SHA-384, SHA-512]*] and cryptographic key sizes [None] that meet the following: [*ISO/IEC 10118-3*].

Application Notes : In the key derivation mechanism of the ICAO document, the SHA-1 implemented in the COS is used as a hash function in order to generate the session key used in the BAC or EAC secure messaging. An the SHA-256 provided by IC chip is used as a hash function in order to generate the session key used in the initialization or personalization secure messaging and to protect the integrity of the transmitted data of the initialization or personalization secure messaging, SHA-224, SHA-384, SHA-512 to be used are also provided by IC chip.

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

Hierarchical to: No other components

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

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

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

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [digital signature verification] in accordance with [*RSASSA-PKCS1-v1.5-SHA-256*, *RSASSA-PSS-SHA-256*, *ECDSA-SHA-224*, *ECDSA-SHA-256*, *[RSASSA-PKCS1-v1.5-SHA-1, RSASSA-PSS-SHA-1, ECDSA-SHA-1, ECDSA-SHA-384, ECDSA-SH-512]*] and cryptographic key sizes [1280 ~ 2048 bit (RSA), 192 ~ 512 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 TOE specifies the cryptographic key sizes specified in the following Table so that to counter attackers possessing high attack potential required by AVA_VAN.5. SHA-1 implemented in the COS as well as SHA-224, SHA-384, and SHA-512 provided by IC chip are used as the one-way hash functions.

Table 21. Details of Digital Signature in the EAC Specifications

Digital Signature Algorithm	Hash Algorithm	Digital Signature Key Sizes
RSASSA-PKCS1-v1.5	SHA-1, SHA-256	1280,1536,2048 bits
RSASSA-PSS	SHA-1, SHA-256	1280,1536,2048 bits
ECDSA	SHA-1, SHA-224 / SHA-256, SHA-384, SHA-512	192,224,256,320,384,512 bits

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

Hierarchical to: No other components

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

FCS_COP.1.1 The TSF shall perform [digital signature generation] in accordance with [RSASSA-PKCS1-v1.5-SHA-1] and cryptographic key sizes [1280 ~ 2048 bit] that meet the following: [ISO/IEC 9796-2 Digital Signature scheme 1].

Application Notes : ICAO document defines digital signature algorithms, hash algorithms, digital signature key lengths for AA. The TOE specifies the cryptographic key sizes specified in the following Table so that to counter attackers possessing high attack potential required by AVA_VAN.5. SHA-1 implemented in the COS is used as the one-way hash function.

Table 22. Details of Digital Signature in the AA Specifications

Digital Signature Algorithm	Hash Algorithm	Digital Signature Key Sizes
RSASSA-PKCS1-v1.5	SHA-1	1280 ~ 2048 bits

FCS_RNG.1 Random Number Generation

Hierarchical to: No other components

Dependencies : No dependencies

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

FCS_RNG.1.2 The TSF shall provide random numbers that meet *AIS31 version 1 Functional Classes and Evaluation Methodology for Physical Random Number Generators, 25 September 2001, Class P2*.

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

<User Data Protection>

FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

a) Subjects

(1) Personalization Agent

(2) BIS

(3) EIS

(4) [None]

b) Objects

(1) Personal data of the MRTD holder

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

(2) The biometric data of the MRTD holder

: EF.DG3, EF.DG4

(3) MRTD authentication data

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

(4) EF.CVCA

(5) EF.COM

(6) [None]

c) Operations

(1) Read

(2) Write

(3) [None]

].

FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [MRTD access control policy] to objects based on the following: [Table 23, Table 24, and [None]].

Table 23. Subject-relevant Security Attributes

Subjects	Security Attributes
BIS	BAC authorization
EIS	BAC authorization, EAC authorization
Personalization Agent	Personalization Agent Issuing authorization

Table 24. 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 LDS Application by FIA_UID.1 when the BAC mutual authentication succeeds.

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

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

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

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

b) [None]

].

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

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

a) Explicitly deny access of subjects to objects if instructions order of the Inspection System is not correct in order to ensure the application order of security mechanisms according to 2.1 Inspection Procedures of the EAC specifications

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

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

d) Explicitly deny access of the different operational mode to all objects

FDP_DAU.1 Basic Data Authentication

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

Application Notes: TSF provides AA security mechanism up to maximum 2048 bits for RSA.

FDP_RIP.1 Subset Residual Information Protection

Hierarchical to: No other components.

Dependencies: No dependencies

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

a) BAC session key

b) EAC session key

c) [Random number

d) Initialization session key

e) Personalization session key

f) Active authentication private key]

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

FDP_UCT.1 Basic Data Exchange Confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 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. **When the personalization agent is successfully authenticated, MRTD user data can be protected via encryption with personalization agent session 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. **When the personalization agent chooses Secure Messaging after successful personalization agent authentication, MRTD user data can be protected from disclosure using personalization agent session key.**

<Identification and Authentication>

FIA_AFL.1(1) Authentication Failure Handling(Inspection System Authentication Failure)

Hierarchical to: No other components.

Dependencies: **FIA_UAU.1(1)** Authentication(BAC mutual Authentication), **FIA_UAU.1(2)** Authentication(EAC-TA)

FIA_AFL.1.1 The TSF shall detect when "*[one at a single session given same random number]*" unsuccessful authentication attempts occur related to [

a) BAC mutual authentication

b) EAC-TA

c) [None]

].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts *has been met or surpassed*, the TSF shall perform [**the following Table 25**].

Table 25. Authentication Failure Handling for Authentication Mechanism

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

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

FIA_AFL.1 (2) Authentication Failure Handling(Initialization Authentication and Personalization agent authentication Failure)

Hierarchical to: No other components.

Dependencies: **FIA_UAU.1(3)** Timing of Authentication(Personalization agent authentication), **FIA_UAU.1(4)** Timing of Authentication(Initialization Authentication)

FIA_AFL.1.1 The TSF shall detect when "*[maximum retrial counter specified in below Table]*" unsuccessful authentication attempts occur related to [

a) Initialization Authentcation

a) Personalization Authentcation

]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [perform the failure handling action specified in below Table]

Table 26. Authentication Failure Handling for Authentication Mechanism (2)

	Maximum Retrial Counter	Counter Actions to Authentication Failure
Initialization Authentication	Cumulatively 16, regardless of the number of sessions	· Change the operational mode of the kernel to Terminated
Personalization Agent Authentication	Cumulatively 10, regardless of the number of sessions	· Change the operational mode of the application to Disabled · Reset TSF data and user data to ‘0‘

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

Hierarchical to: No other components.

Dependencies to: **FIA_UID.1(1)** Timing of identification(MRTD user identification)

FIA_UAU.1.1 **When operational mode of the application is Operational Use**, the TSF shall allow [

a) indication of the BAC mechanism support

b) [none]

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

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

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

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

Hierarchical to: No other components.

Dependencies to: **FIA_UAU.1(1)** Timing of authentication(BAC Mutual Authentication)

FIA_UAU.1.1 **When operational mode of the application is Operational Use,** the TSF shall allow [

a) to perform EAC-CA

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

c) [to perform AA]

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

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

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

Hierarchical to: No other components.

Dependencies to: **FIA_UID.1(1)** Timing of identification (MRTD user identification)

FIA_UAU.1.1 **When operational mode of the kernel is Personalization**, the TSF shall allow [to select and to execute MRTD application] on behalf of the user to be performed before the **MRTD personalization agent** is authenticated.

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

FIA_UAU.1(4) Timing of Authentication (Initialization Authentication)

Hierarchical to: No other components.

Dependencies to: **FIA_UID.1(2)** Timing of identification (initialization user identification)

FIA_UAU.1.1 **When operational mode of the kernel is Initialization**, the TSF shall allow [to select and to execute MRTD application] on behalf of the user to be performed before the **manufacturer** is authenticated.

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

FIA_UAU.4 Single-Use Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

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

a) BAC mutual authentication

b) EAC-TA

c) [Initialization authentication

d) Personalization agent authentication]

FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide [

a) BAC mutual authentication

b) EAC-TA

c) [Initialization authentication

d) Personalization agent authentication]

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

a) The BIS or EIS shall succeed the BAC mutual authentication in order to have the

BAC authorization and **active authentication in case that Inspection System supports**.

b) The EIS, in order to have the EAC authorization, shall succeed the BAC mutual authentication, EAC-CA and EAC-TA and **active authentication in case that Inspection System sup-**

ports and include the read-rights of biometric data in all of the CVCA certificate, DV certificate and IS certificate. For this, the TSF shall provide the EAC-CA.

c) [To get initialization permission, the manufacturer should authenticate successfully.

d) To get personalization permission, the personalization agent should authenticate successfully]

].

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

FIA_UID.1(1) Timing of Identification(MRTD User Identification)

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

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

FIA_UID.1(2) Timing of Identification(Initialization User Identification)

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [to establish the communication channel based on the user's specification] 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 send commands with regard to initialization, the TOE identifies it as the Manufacturer.

<Security Management>

FMT_MOF.1(1) Management of Security Functions Behavior(Suspending write function)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to *disable* the functions [writing] to [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_MOF.1(2) Management of Security Functions Behavior(Suspending EAC and Secure Messaging)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions (MRTD)
FMT_SMR.1 Security roles (Personalization Agent)

FMT_MOF.1.1 The TSF shall restrict the ability to *disable* the functions [

a) EAC

b) Secure Messaging in the personliazation phase

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

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

FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

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

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

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

FMT_MSA.3 Static Attribute Initialization

Hierarchical to: No other components.

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

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

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

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

FMT_MTD.1(1) Management of TSF Data (Certificate Verification Information and Authentication Key)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions(MRTD Issuing Management)
FMT_SMR.1 Security roles(Personalization Agent)

FMT_MTD.1.1 The TSF shall restrict the ability to [_write in secure memory_] the [

a) EAC chip authentication private key

b) initial current date

c) initial CVCA certificate

d) initial CVCA digital signature verification key

e) [active authentication private key, personalization authentication key]

] to [personalization agent in the Personalization phase].

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

FMT_MTD.1(2) Management of TSF Data (SSC initialization)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions(MRTD Issuing Management)
FMT_SMR.1 Security roles(Personalization Agent)

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

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

FMT_MTD.1(3) Management of TSF Data(Operational Mode Management)

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to [operate specified below] the [TSF data specified below] to [the authroized roles specified below].

Table 27. TSF Data Operations for Each Authorized Role

TSF Data	Operations	Authroized Roles
Operational Mode	Inquiry, Alter	Manufacturer in Manufacturing phase, Personalization agent in Personalization phase
Initialization Data	Write in secure memory	Manufacturer in Manufacturing phase

Application Notes : Manufacturer in Manufacturing phase means Embedded S/W developer, but can be an MRTD manufacturer delegated by Embedded S/W developer.

FMT_MTD.1(4) Management of TSF Data (Generating and Storing BAC Authentication Key)

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to *[generate and store]* the [BAC Authentication Key] to [TSF].

Application Notes : The TSF automatically calculates BAC authentication key using personalized MRZ and store it after writing DG1 file.

FMT_MTD.3 Secure TSF Data

Hierarchical to: No Other Components.

Dependencies: **FMT_MTD.1(1)** Management of TSF data(Certificate verification information and authentication key)

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

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

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 and **TSF data management such as MRTD subject and object security attribute and SSC initialization**

c) [Function to decide to enable EAC in the Personalization phase

d) Halt security function such as writing, EAC and Secure Messaging in the Personalization phase

e) Managing operational mode

f) Initialization of secure memory area with initialization data in Manufacturing phase

g) BAC authentication key generation and storage in the Personalization

].

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: **FIA_UID.1(1)** Timing of Identification(MRTD User Identification), **FIA_UID.1(2)** Timing of Identification(Initialization User Identification)

FMT_SMR.1.1 The TSF shall maintain the roles [

a) Personalization agent

b) [Manufacturer]

].

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

Application Notes: In the function to security management defined by FMT_SMF.1, the personalization agent performs a),c),d), Manufacturer performs f), Manufacturer and Personalization agent in Manufacturing phase performs e) and the TSF performs b),g). However the TSF is not a user thus is not defined as security roles.

<Privacy>

FPR_UNO.1 Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

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

d) [FCS_COP.1(5) Cryptographic operation (Digital Signature Generation for AA)]

] on [

a) BAC authentication key

b) BAC session key

c) EAC session key

d) EAC chip authentication private key

e) [AA chip authentication priviate key

f) Initialization authentication key

g) Initialization session key

h) Personalization authentication key

i) Personalization session key]

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

<TSF Protection>

FPT_ITC.1 Inter-TSF Confidentiality during Transmission

Hierarchical to: No other components.

Dependencies: None

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

Application Notes: Secure Messaging is provided optionally according to the manufacturing environment and Secure Messaging is provided including encryption optionally according to the personalization agent's policy in the personalization phase.

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) Deletion of Personalization agent session key

f) Termination of initialization communication channel

g) Deletion of Initialization session key]

] if modifications are detected.

Application Notes: The Strength of Retail MAC is equivalent to the secure Retail MAC specified in FCS_COP.1(2) or more. **The TSF shall provide means to protect integrity of initialization data from alteration, deletion, and insertion using initialization session key. The TSF shall provide means to protect integrity of TSF data from alteration, deletion, and insertion using personalization session key in Personalization phase according to the personalization agent's policy. Secure Messaging shall be conducted in Operational Use phase.**

FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

Dependencies: No dependencies

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

a) Failure detected at self-testing by FPT_TST.1

b) Conditions outside the normal operating of the TSF detected by the IC chip

c) [None]

].

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies

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

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

FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests *during operation* to demonstrate the correct operation of the [*function to guarantee secure random numbers defined in FMT_MTD.3*].

FPT_TST.1.2 The TSF shall provide **the personalization agent** with the capability to verify the integrity of [*EAC chip authentication private key, active authentication private key, CVCA certificate, CVCA digital signature verification key, personalization authentication key, MRTD access condition, current data, BAC authentication key*]

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

6.3 TOE Security Assurance Requirements

Security assurance requirements for this security target document consist of the following components from part 3 of the CC like PP, evaluation level is EAL4+ (ADV_IMP.2, ALC_DVS.2, ALC_CMS.5, ALC_TAT.2, ATE_DPT.2, AVA_VAN.5). Assurance components are summarized in the following Table 28.

The assurance components are augmented as follows:

· ADV_IMP.2	“Complete mapping of the implementation representation of the TSF”
· ALC_DVS.2	“Sufficiency of security measures“
· ALC_CMS.5	“Development tools CM coverage“
· ALC_TAT.2	“Compliance with implementation standards “
· ATE_DPT.2	“Testing: security enforcing modules”

- AVA_VAN.5 “High formulated vulnerability analysis”

Table 28. Security Assurance Requirements

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

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements Rationale

The rationale of TOE security functional requirements demonstrates the followings :

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

Table 29 presents the mapping between the security objectives and the security functional requirements.

Table 29. Mappings between Security Objectives and Security Functional Requirements

Security Objectives / Security Functional Requirements	TOE Security Objectives															
	O. Management	O.Personalization_Agent_Authentication	O.Initialization_Authentication	O.Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Secure State	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.AA	O.BAC	O.EAC	O.IC_Chip
FCS_CKM.1(1)														X	X	
FCS_CKM.1(2)		X	X													
FCS_CKM.2(1)										X				X		
FCS_CKM.2(2)															X	
FCS_CKM.2(3)		X	X							X						
FCS_CKM.4									X							
FCS_COP.1(1)		X	X			X								X		X
FCS_COP.1(2)		X	X			X								X		X
FCS_COP.1(3)		X	X											X	X	X
FCS_COP.1(4)							X								X	X
FCS_COP.1(5)													X			X
FCS_RNG.1																X
FDP_ACC.1											X					
FDP_ACF.1	X			X							X			X	X	
FDP_DAU.1													X			
FDP_RIP.1									X	X						
FDP_UCT.1						X				X						
FDP_UIT.1						X				X						
FIA_AFL.1(1)				X	X						X			X	X	
FIA_AFL.1(2)		X	X													
FIA_UAU.1(1)					X						X			X		
FIA_UAU.1(2)				X	X						X				X	

Security Objectives / Security Functional Requirements	TOE Security Objectives															
	O. Management	O.Personalization_Agent_Authentication	O.Initialization_Authentication	O.Security_Mechanism_Application_Procedures	O.Session_Management	O.Secure_Messaging	O.Certificate_Verification	O.Secure State	O.Deleting_Residual_Info	O.Replay_Prevention	O.Access_Control	O.Handling_Info_Leakage	O.AA	O.BAC	O.EAC	O.IC_Chip
FIA_UAU.1(3)	X	X									X					
FIA_UAU.1(4)	X		X								X					
FIA_UAU.4		X	X							X				X	X	
FIA_UAU.5		X	X	X							X		X	X	X	
FIA_UID.1(1)		X												X	X	
FIA_UID.1(2)			X													
FMT_MOF.1(1)	X										X					
FMT_MOF.1(2)	X					X					X					
FMT_MSA.1						X					X					
FMT_MSA.3	X										X					
FMT_MTD.1(1)	X										X					
FMT_MTD.1(2)				X												
FMT_MTD.1(3)	X										X					
FMT_MTD.1(4)	X										X					
FMT_MTD.3							X			X					X	X
FMT_SMF.1	X						X									
FMT_SMR.1	X	X														
FPR_UNO.1												X				X
FPT_ITC.1						X										
FPT_ITI.1					X	X										
FPT_FLS.1								X								X
FPT_PHP.3																X
FPT_TST.1								X								

6.4.2 Security Assurance Requirements Rationale

The security assurance level of this ST is selected as EAL5+(ADV_IMP.2, ALC_DVS.2, AVA_VAN.5) considering the asset value and threat level which TOE protects.

EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in commodity planned development and require a high level of independently assured security in a planned development and require a rrigrous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

ST augmented assurance components partially higher than EAL5 as follows.

- ADV_IMP.2 “Complete mapping of the implementation representation of the TSF”
- ALC_DVS.2 “Sufficiency of security measures“
- AVA_VAN.5 “High formulated vulnerability analysis”

6.4.3 Rationale of Dependency

<Dependency of TOE Security Functional Requirements>

Table 30 shows dependency of TOE functional components.

Table 30. Dependency of TOE Functional Components

No.	SFR of ST	Dependency as specified by CC Part 2	Dependency of ST (Refer to Column 1)
1	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	3,4 6
2	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS.CKM.4	5 6
3	FCS_CKM.2(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 6
4	FCS_CKM.2(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	1 6
5	FCS_CKM.2(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	2 6
6	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	1,2
7	FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1,2 6
8	FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1,2 6
9	FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None 6
10	FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	1 6
11	FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None 6
12	FCS_RNG.1	-	-
13	FDP_ACC.1	FDP_ACF.1	14
14	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	13 32
15	FDP_DAU.1	-	-

No.	SFR of ST	Dependency as specified by CC Part 2	Dependency of ST (Refer to Column 1)
16	FDP_RIP.1	-	-
17	FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	None 13
18	FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	13 None
19	FIA_AFL.1(1)	FIA_UAU.1	21,22
20	FIA_AFL.1(2)	FIA_UAU.1	23,24
21	FIA_UAU.1(1)	FIA_UID.1	27
22	FIA_UAU.1(2)	FIA_UAU.1(1)	21
23	FIA_UAU.1(3)	FIA_UID.1	27
24	FIA_UAU.1(4)	FIA_UID.1	28
25	FIA_UAU.4	-	-
26	FIA_UAU.5	-	-
27	FIA_UID.1(1)	-	-
28	FIA_UID.1(2)	-	-
29	FMT_MOF.1(1)	FMT_SMF.1 FMT_SMR.1	38 39
30	FMT_MOF.1(2)	FMT_SMF.1 FMT_SMR.1	38 39
31	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	13 38 39
32	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	31 39
33	FMT_MTD.1(1)	FMT_SMF.1 FMT_SMR.1	38 39
34	FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	38 39
35	FMT_MTD.1(3)	FMT_SMF.1 FMT_SMR.1	38 39
36	FMT_MTD.1(4)	FMT_SMF.1 FMT_SMR.1	38 39
37	FMT_MTD.3	FMT_MTD.1	33
38	FMT_SMF.1	-	-
39	FMT_SMR.1	FIA_UID.1	27
40	FPR_UNO.1	-	-
41	FPT_FLS.1	-	-
42	FPT_ITC.1	-	-
43	FPT_ITI.1	-	-
44	FPT_PHP.3	-	-
45	FPT_TST.1	-	-

<Dependency of TOE Security Assurance Requirements>

The dependency of EAL5 provided in Common Criteria is already satisfied. Therefore, the rationale for this is omitted. The dependency of the augmented security assurance requirements is as shown in Table 31.

ADV_IMP.2 has dependency with ALC_CMC.5, but PP does not augment ALC_CMC.5 as ADV_IMP.2 is augmented to analyze completely if TSF is implemented correctly and has no fault code thus ALC_CMC.5 is not necessarily required that provides automatic method to identify if a configuration change affects other configuration list.

ALC_DVS.2 has no dependency.

AVA_VAN.5 has dependency with ADV_IMP.1 and ATE_DPT.1. This is satisfied by ADV_IMP.2 and ATE_DPT.3 with hierarchical relationship.

Table 31 Dependency of the Augmented Assurance Component

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

7 TOE Summary Specification

This section shows TOE security functionality to satisfy TOE security functional requirements, and defines TOE assurance measures to satisfy TOE assurance requirements. Detailed contents of TSF will be described in TOE specification.

7.1 TOE Security Functionality

<TSF of IC chip used in the TOE>

Among TSFs of the IC chip specified in [ST_IC], the following security functions are used in the TOE. The security function, de-synchronization and signal-to-noise ratio reduction mechanisms, provided by the IC chip is used when 3DES, AES, RSA, DH, ECDSA, ECDH provided by the IC chip are used in accordance with the guidance of [SAN].

Table 32 TSF of IC chip used in the TOE

TSF of the IC chip	Relevant SFR of the IC chip	TSF of the IC chip summary	Relevant TOE security functionality
TOE's Detectors	FPT_FLS.1	Security detector functions that detect and perform counter actions to abnormal conditions such as abnormal frequency, abnormal voltage, abnormal temperature, light, inner insulation removal, active shield removal, power glitch which can compromise the secure state of the IC chip.	7.1.11
Active Shield	FPT_PHP.3 FDP_ITT.1 FPT_ITT.1	Unbypassable shielding functions that prevent physical penetration attacks from being realized	7.1.11
Memory Encryption	FDP_IFC.1	Security functions that prevent data stored in the IC chip secure memory and transmitted internally from being analyzed.	7.1.11
De-synchronization and signal-to-noise ratio reduction mechanisms	FDP_ITT.1 FPT_ITT.1	Security functions such as Internal Variable Clock, Random Current Generator, Random Wait Generator that make probing attacks and side-channel attacks more difficult.	7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.1.8, 7.1.9
TRNG	FCS_RNG.1	AIS31 Class P2-compliant TRNG provision	7.1.1, 7.1.5, 7.1.6, 7.1.8, 7.1.10
3DES	FCS_COP.1	Secure 3DES cryptographic operation provision	7.1.5, 7.1.9
AES	FCS_COP.1	Secure AES cryptographic operation provision	7.1.1, 7.1.11

RSA (DH)	FCS_COP.1	Secure RSA (DH) cryptographic operation provision	7.1.4, 7.1.6, 7.1.7, 7.1.8
ECDSA	FCS_COP.1	Secure ECDSA cryptographic operation provision	7.1.4, 7.1.6, 7.1.8
ECDH	FCS_COP.1	Secure ECDH cryptographic operation provision	7.1.7
SHA	FCS_COP.1	Secure SHA cryptographic operation provision	7.1.1, 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.1.11

7.1.1 Initialization/Personalization Agent Authentication and Generation of Authentication Key/Session Key of Each Mechanism

CS shall perform initialization authentication mechanism and IA shall perform personalization agent authentication mechanism applying authentication rule to identify users. CS and SS shall check authentication failure retrial counter before each authentication is performed, and stop each authentication procedure and initialize in case the retrial counter exceeds the maximum counter. In case initialization or personalization agent authentication fail, initialization session keys or personalization authentciation and session keys are destructed with assistance of CS or IA for each.

7.1.2 Identification of MRTD Application (AID : A0000002471001)

COS application containing MRTD Application ID shall be activated by Select File command and thereafter receive commands following APDU handling by CR. MRTD Application shall interprete the receiving commands via ER and process them.

7.1.3 Management of TOE Initialization and Operational Mode

Only when Manufacturer acquires initialization permission via initialization authentication in the manufacturing phase, CS shall receive initialization data following initialization request of Manufacturer and install MRTD TSF data such as MRTD operational mode, MRTD access conditions and personalization authentication keys while initializing MRTD application. CS shall change the operational mode of the Kernel to Operational Use and that of the application to Personalization where MRTD application can be personalized via the request of Manufacturer

SS shall change the operational mode of the MRTD application. The mode of the MRTD application can be changed only when personalization permission is acquired through personalization agent authentication of IA and consists of 3 modes. Change to Operational Use shall be conducted after user data are assured to be personalized and in case of change to Disabled, user data and MRTD TSF data shall be deleted with assistance of HW.

ER shall check the operational mode of the MRTD application and control updates on MRTD user data and MRTD TSF data.

7.1.4 Personalization of MRTD User Data and TSF Data

SS shall be able to change MRTD access condition to ‘EAC disabled‘ according to personalization agnet’s request, and call CF to verify certificate for CVCA public key before writing it in the nonvolatile memory. SS shall write information required to verify certificate chain such as CVCA public key in the nonvlatile memory with assistance of HW.

SS shall write AA priate key, EAC-CA private key and personalization authentication keys in the nonvolatile memory with assistance of HW. When DG1 is written in the nonvolatile memory, MRZ shall be generated from DG1 and BAC authentication keys are generated with the assistance of CF to be written permanently with assistance of CF

SS shall perform to personalize of MRTD user data and TSF data and MRTD access condition after checking personalization permission is acquired.

7.1.5 BAC and MRTD Access

ER shall call IA applying authentication rule in order that BAC is performed to authenticate BIS via user identification. IA shall authenticate BIS via implementing BAC in accordance with ICAO specifications with assistance of CF. After successful authentication, the BIS subject right shall be set to BAC right with assistance of HW and BAC session keys shall be generated for BAC secure messaging.

All the intermediate values calculated during operation shall be disappeared when a session is terminated or power is not supplied, or destructed in a secure manner when authentication fails.

After successful BAC authentication, BIS shall be able to access every data group except DG3 and DG 4 via secure messaging within the relevant session.

7.1.6 AA

After credentials from Internal Authenticate command with secure messaging are received by the TOE securely, IA shall assemble the message F using RND.IFD received through IO and CR to be signed in accordance with Apendix A6.1.3 Active Authentication procedure of the ICAO document and sign using AA private key.

The digital signature shall be transmitted to the inspection system via IO as the data of the response message and used to check genuineness of the IC chip in accordance with Apendix A6.1.3 Active Authentication procedure of the ICAO document.

When AA fails, the session shall be terminated and the residual information shall be destructed.

7.1.7 EAC-CA

IA shall generate EAC session keys required for EAC secure messaging with assistance of CF and initialize SSC. SSC shall be set to ‘0‘ after derivation of the session keys using the shared secret key as KDF seed value.

7.1.8 EAC-TA

ER shall call IA applying authentication rule in order that EAC is performed to authenticate EIS via user identification.

IA shall assign CVCA or DV public key to verify certificate chain after parsing the certificate with assistance of US. IA shall verify the certificate using the assigned public keys with assistance of CF. IA shall check the cerficiate structure received by CR with assistance of UF and verify the cerificate using the assigned public keys with assistance of CF.

After successful EAC authentication, IA shall assign EIS subject right to EAC right with assistance of HW. After EAC fails, subject right shall be initialized to prevent accessing DG3/DG4 but the EAC secure messaging shall be maintained.

SS shall search the requested file from the file table in order to allow EIS to read MRTD holder's sensitive biometric data, and check if EAC authentication succeeded and access permission to DG3/DG4 is included in the certificate. In case EAC permission is matched, the requested length of DG3/DG4 data shall be transmitted outside via IO.

7.1.9 Secure Messaging after Personalization Agent Authentication, BAC or EAC-CA

TOE shall implement secure messaging using session keys and SSC in order to protect command/response APDU and data exchanged in the communication channel after BAC or EAC-CA.

ER shall protect residual information by destructing BAC or EAC session keys and SSC via filling with '0' with assistance of IA. ER shall request SM to check secure messaging. SM shall check the structure of the received commands with assistance of, increase SSC with assistance of IA, and verify the received MAC using functions of CF. BAC or EAC session keys and SSC shall be destructed via filling with '0' with assistance of IA and BAC or EAC permission of the inspection system shall be initialized.

Secure messaging shall be implemented using personalization session key and SSC after successful personalization agent authentication in the Personalization phase. ER shall verify secure messaging with assistance of SM, and initialize session information including personalization permission of the personalization agent in case of the verification failure.

7.1.10 Secure Start-up and Use of IC chip's Security Features

BL shall check the previous state of termination upon power supply and stop continuing in case abnormal termination is detected. IO shall assign registers values required to use the IC chip security features such as UART considering the communicaiton type (e.g. ISO/IEC 14443A) when initializing modules required to create the communication channel, and perform to assign the communicationi speed and to transmit the initial response.

BL shall use the statistic test provided by the IC chip to check randomness of the manipulated random numbers provided by the IC chip per every power-up to keep the security of the random numbers to be used in the MRTD security mechanisms. A separate randomness test shall be peformed using the library provided by the IC chip per every generation of the random numbers by HW.

7.1.11 Assurance of TSF Secure Operation

SS and CF shall provide means to check integrity on the TSF via 'Check Data' command process. CS in the manufacturing phase and SS in the personalization phase shall provide means to check integrity on the TSF via secure messaing where AES and SHA provided by the IC chip shall be used.

BL shall test randomness of the random numbers per each power-up or each generation via HW and shall stop TSF execution to maintain the secure state in case the test fails.

SS shall stop TSF execution to maintain the secure state in case the integrity check of the TSF data via secure messaing fails.

HW shall stop TSF execution to maintain the secure state in case abnormal conditions are detected using the security functions such as active shield and security detector provided by the IC chip.

TSF shall maintain the secure operation against the observation attacks such as SPA and DPA using countermeasures provided by the IC chip.

7.2 Assurance Measures

This section defines assurance measures which is required in accordance with EAL5+ TOE security assurance requirement. The augmented assurance requirements are ADV_IMP.2, ALC_DVS.2, and AVA_VAN.5.

The assurance measures will be provided as specified in the following table.

Table 33. TOE Assurance Measures

Assurance Class	Assurance Component	Assurance Measure
Security Target Specifications Evaluation	ASE_INT.1	SPNX-ASE-101
	ASE_CCL.1	SPNX-ASE-101
	ASE_SPD.1	SPNX-ASE-101
	ASE_OBJ.2	SPNX-ASE-101
	ASE_ECD.1	SPNX-ASE-101
	ASE_REQ.2	SPNX-ASE-101
	ASE_TSS.1	SPNX-ASE-101
Development	ADV_ARC.1	SPNX-ADV-101 & attached
	ADV_FSP.5	SPNX-ADV-111, SPNX-ADV-112, SPNX-ADV-113
	ADV_IMP.2	SPNX-ADV-121
	ADV_TDS.4	SPNX-ADV-131, SPNX-ADV-132, SPNX-ADV-133
	ADV_INT.2	SPNX-ADV-141
Guidance Documents	AGD_OPE.1	SPNX-AGD-101, SPNX-AGD-102, SPNX-AGD-103
	AGD_PRE.1	SPNX-AGD-101, SPNX-AGD-102, SPNX-AGD-103, SPNX-ALC-101 & attached
Lifecycle Support	ALC_CMC.4	SPNX-ALC-101, SPNX-ALC-102 & attached
	ALC_CMS.5	SPNX-ALC-101, SPNX-ALC-102 & attached
	ALC_DEL.1	SPNX-ALC-101, SPNX-ALC-102 & attached
	ALC_DVS.2	SPNX-ALC-101, SPNX-ALC-102 & attached
	ALC_LCD.1	SPNX-ALC-101, SPNX-ALC-102 & attached
	ALC_TAT.2	SPNX-ALC-101, SPNX-ALC-102 & attached
Tests	ATE_COV.2	SPNX-ATE-101 & attached
	ATE_DPT.3	SPNX-ATE-101 & attached
	ATE_FUN.1	SPNX-ATE-101 & attached
	ATE_IND.2	MRTD samples, Emulation board, Test Tool(HW, SW)
Vulnerability Assessment	AVA_VAN.5	MRTD samples, Emulation board, Test Tool (HW, SW)

8 References

8.1 Externel References

CC1	Common Criteria for Information Technology Seuciryt Evaluation, Part 1 : Introduction and general model, Version 3.1r4, September 2012, CCMB-2012-09-001
CC2	Common Criteria for Information Technology Seuciryt Evaluation, Part 2 : Security functional components, Version 3.1r4, September 2012, CCMB-2012-09-002
CC3	Common Criteria for Information Technology Seuciryt Evaluation, Part 3 : Security assurance components, Version 3.1r4, September 2012, CCMB-2012-09-003
CC4	Common Methodology for Information Technology Security Evaluation, Version 3.1r4, September 2012, CCDB-2012-09-004
PP	MRTD Protection Profile V2.1, National Intelligence Service, KECS-PP-0163a-2009, 2010-06-10
PP_IC	Security IC Platform Protection Profile Version 1.0, BSI-PP-0035-2007, 2007-06-15
CC_PAS	Common Criteria for Information Protection System, Ministry of Public Administration and Security, 2009-52
CC_GUIDE	Evaluation and Certification Guidance for Information Protection System, Ministry of Public Administration and Security, 2009-9-1
ISO7816	ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts
ISO14443	ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards
DOC9303	ICAO Doc 9303 Machine Readable Travel Documents Part 1 Machine Readable Passports, 6th edition, 2006
ISO_SUP	ISO/IEC JTC1/SC17 Supplement to Doc 9303, Release 10, ICAO, 2007-9-21
EAC	BSI Technical Guideline TR-03110, Advanced Security Mechnisms for MRTD – Extended Access Control, Ver 1.11, 2008. 02. 21
ST_IC	Security Target Lite of Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software, Version 2.2, 2012-09-26
NIST_CMAC	NIST Special Publication 800-38B

8.2 Internel References

IC_TOR	TORNADO-2Mx2 RSA/ECC Library API Manual v2.10, 2012-04-19
SEC-ICC	S3CT9XX 16-bit CMOS Microcontroller for SmartCard User's Manual, November 2011
TRNG_AN	S3CT9Kx AIS31 TRNG library application note Revision 1.2, 2012-07-02
SEC-ICC-ER	User's Manual Errata Version 2.00, November 2011

SAN	S3CT9Kx Security Application Note V2.2, 2012-07-03

9 Terms and Abbreviation

9.1 Terms

The terms that are used in this document and defined in the CC as well are to have the same meaning as in the CC.

Terms	Definitions
AA (Active Authentication)	The security mechanism with which the MRTD chip demonstrates its genuine to the IS by signing random number transmitted from the IS and the IS verifies genuine of the MRTD chip through verification with the signed values
BAC (Basic Access Control)	The security mechanism that implements the symmetric key-based entity authentication protocol for mutual authentication of the MRTD chip and the IS and the symmetric key-based key distribution protocol to generate the session keys necessary in establishing the secure messaging for the MRTD chip and the IS
BAC authentication key	The BAC authentication encryption key and the BAC authentication MAC key generated by using the KDM from the MRZ (passport No., passport No. check digit, date of birth, date of birth check digit, valid date, valid date check digit) for mutual authentication of the MRTD chip and the IS
BAC Mutual authentication	The mutual authentication of the MRTD chip and the IS according to the ISO 9798-2 symmetric key-based entity authentication protocol
BAC Secure messaging	The communication channel to provide the confidentiality and the integrity of transmitted data by encryption the transmitted data with the BAC session encryption key and generating, therefore transmitting after generating message authentication value with the BAC session MAC key
BAC Session Key	The BAC session encryption key and the BAC session MAC key for generated by using the KDM from random numbers for generating session keys shared in the BAC mutual authentication
Biometric data of the MRTD holder	Fingerprint and/ or iris data of MRTD holder stored in the MRTD chip in the LDS structure
BIS (BAC Inspection System)	The IS implemented with the BAC and the PA security mechanisms
Certificate	The electronic data by a digital signature on the digital signature verification key by the CA in order to check and demonstrate that the digital signature generation key belongs only to the person who

	holds the key
Ciphertext Only Attack	Attack by the threat agent to attempt decryption based on the collected ciphertext
CSCA (Country Signing Certification Authority)	The root CA that generates and issues the CSCA certificate and the DV certificate by securely generating the digital signature key in the PA-PKI to support the PA security mechanisms
CSCA Certificate	The certificate to demonstrate validity of the digital signature verification key for the digital signature generation key of the PA-PKI root CA by signature on the digital signature verification key with digital signature generation key of the PA-PKI root CA
CVCA (Country Verifying Certification Authority)	The root CA that generates and issues the CVCA certificate, the CVCA link certificate and the DV certificate by securely generating digital signature key in the EAC-PKI to support the EAC security mechanisms
CVCA Certificate	The certificate that includes digital signature value by the EAC-PKI root CA with digital signature generation key of the EAC-PKI root CA on the digital signature verification key in order to demonstrate validity of the CVCA link certificate and the DV certificate
CVCA Link Certificate	The certificate that includes digital signature value that the EAC-PKI root CA with the digital signature generation key that corresponds to the previous CVCA certificate after generating a new CVCA certificate before expiring the valid date of the CVCA certificate
DS (Document Signer) Certificate	The certificate of the Personalization agent signed with the digital signature generation key of the PA-PKI root CA used by the IS to verify the SOD of the PA security mechanism
DV (Document Verifier)	The CA(Certification Authority) that generates and issues the IS certificate
DV Certificate	The certificate that includes digital signature value on the digital signature verification key of the IS with the digital signature generation key of the DV in order to demonstrate validity of the digital signature verification key of the IS
EAC-CA (EAC-chip Authentication)	The security mechanism to implement the Ephemeral-Static DH key distribution protocol (PKCS#3, ANSI X.42, etc.) to enable the MRTD chip authentication by the EIS through key checking for the EAC chip authentication public key and private key of the MRTD chip and temporary public key and private key of the EIS

EAC-TA (EAC-terminal Authentication)	The security mechanism that The EIS transmits values digital signature with the digital signature generation key of its own to the temporary public key used in the EAC-CA and the MRTD chip by using the IS certificate, verifies the digital signature. This security mechanism implements challenge-response authentication protocol based on digital signature through which the MRTD chip authenticates the EIS.
EAC (Extended Access Control)	The security mechanisms consisted with the EAC-CA for chip authentication and the EAC-TA for the IS authentication in order to enable only the EAC supporting Inspection System (EIS) to read the biometric data of the MRTD holder for access control to the biometric data of the MRTD holder stored in the MRTD chip
EAC Chip Authentication Public Key and EAC Chip Authentication Private key	Set of the DH keys used by the MRTD chip to authenticate itself to the EAC supporting IS in the EAC-CA that contain data recorded by the Personalization agent in the Personalization phase.
EAC Inspection System (EIS: EAC Inspection System)	The IS to implement the BAC, the PA and the EAC security mechanisms and the AA as an option
EAC Session Key	The session key used to establishing secure messaging to protect transmission of the biometric data of the MRTD holder that consist of the EAC session encryption key and the EAC session MAC key generated by using the KDF of which keys shared with the EIS through the Ephemeral-Static DH key distribution protocol in the EAC-CA are used as Seed
EF.COM	Including the LDS version info. Data Groups tag information
EF.CVCA	The EF format file to specify the read-right and the list of the CVCA digital signature verification key identifier necessary in verification of the CVCA certificate validity in the EAC-TA
Encryption Key	Key used in the symmetric cryptographic algorithm for data encryption in order to prevent the data disclosure
MRTD	The passport embedded the contactless IC chip in which identity and other data of the MRTD holder stored according to the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO).
MRTD authentication data	The data stored in the MRTD chip with the LDS format to support MRTD security mechanisms that includes the PA SOD, the EAC chip authentication public key and the AA chip authentication public key, etc.
MRTD identity data	Including personal data of the MRTD holder and biometric data of

	the MRTD holder
MRTD PKI	Unique data signed on the MRTD by the Personalization agent with digital signature generation key issued in the MRTD PKI System in order to issuance and check of the electronically processed passport
MRTD PKI System	System to provide certification practice, such as issuance of certificates necessary in passport's digital signature and management of certification-related records, etc.
Grandmaster Chess Attack	Attack by masquerading as the MRTD chip using the IC chip to hookup the communication channel between the MRTD chip and the IS
ICAO-PKD	The DS certificate storage operated and managed by the ICAO that online distributes in case the domestic/ overseas IS requests the DS certificate of the corresponding country
Inspection	Procedure in which immigration office checks identity of the MRTD holder by inspecting the MRTD chip presented by the MRTD holder, therefore verifying genuine of the MRTD chip
IS (Inspection System)	As an information system that implements optical MRZ reading function and the security mechanisms (PA, BAC, EAC and AA, etc.) to support the MRTD inspection, the IS consists with a terminal that establishes the RF communication with the MRTD chip and the system that transmits commands to the MRTD chip through this terminal and processes responses for the commands.
IS Certificate	Certificate used by the MRTD chip to verify the digital signature transmitted by the IS in the EAC-TA. The DV performs a digital signature on the digital signature verification key of the EIS with the digital signature generation key.
KDF (Key Derivation Function)	The function to generate the encryption key and the MAC key by using hash algorithm from the Seed
KDM (Key Derivation Mechanism)	The mechanism to generate the encryption key and the MAC key by using hash algorithm from the Seed
LDS (Logical Data Structure)	Logical data structure defined in the ICAO document in order to store the user data in the MRTD chip
MAC Key (Key for Message Authentic Code)	Key used by symmetric cryptographic algorithm according to ISO9797 to generate the message authentication code in order to prevent data forgery and corruption
MRTD	Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes

MRTD Application	Program for loaded in the MRTD chip that is programmed by the LDS of the ICAO document and provides security mechanisms of BAC, PA and EAC, etc.
MRTD Application Data	Including user data and TSF data of the MRTD
MRTD Chip	The contactless IC chip that includes the MRTD application and the IC chip operating system necessary in operation of the MRTD application and that supports communications protocol by ISO/IEC 14443
PA (Passive Authentication)	The security mechanism to demonstrate that identity data recorded in the MRTD has not been forgery and corruption as the IS with the DS certificate verifies the digital signature in the SOD and hash value of user data according to read-right of the MRTD access control policy.
Personal data of the MRTD holder	Visually identifiable data printed on identity information page of the of MRTD and other identity data stored in the MRTD chip in the LDS structure
Personalization agent	The agent receives the MRTD identity data from the Reception organization and generates the SOD by digital signature on the data. After recording them in the MRTD chip, the personalization agent generates TSF data and stores it in the secure memory of the MRTD chip. The agent also operates PA-PKI and/ or EAC-PKI.
Probing	Attack to search data by inserting probing pin in the IC chip
Reverse Engineering	To identify and reproduce the basic design concept and applied technologies of product through detailed analysis of the completed product
SOD (Document Security Object)	The SOD refers to the MRTD identity data and the MRTD authentication data recorded in the Personalization phase by the Personalization agent that is signed by the Personalization agent with the digital signature generation key. The SOD is an object implemented with signed data type of 'RFC 3369 cryptographic message syntax, 2002.8' and encoded with DER method.
TSF Data	The data stored in the secure memory of the MRTD chip to support MRTD security mechanisms
User Data	Including the MRTD identity data and the MRTD authentication data

9.2 Abbreviations

AA	Active Authentication
ABEND	Abnormal End (of MEL application execution)

AM	Abstract Machine (Software Module)
ATR	Answer To Reset
BAC	Basic Access Control
BIS	Basic Inspection System
CA	Chip Authentication
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CLK	Clock (input to smartcard)
COS	Card Operating System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem (algorithm)
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DES	Data Encryption Standard
DF	Dedicated File
DG	Data Group
DH	Diffie-Hellman
DPA	Differential Power Analysis
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EBC	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIS	Extended Inspection System
HW	Hardware
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
IFD	Interface Device
IO	Input/Output
IS	Inspection System
ISO	International Organization for Standardization
IT	Information Technology

KDF	Key Derivation Function
KDM	Key Derivation Mechanism
LDS	Logical Data Structure
MAC	Message Authentication Code
MF	Master File
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
OTP	One-Time Programmable (memory)
PA	Passive Authentication
PCD	Proximity Coupling Device
PICC	Proximity Card
PKI	Public Key Infrastructure
PP	Protection Profile
PPS	Protocol and Parameters Selection (ref ISO7816)
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read-Only Memory
RSA	Rivest-Shamir-Aldeman (algorithm)
RST	Reset (input to smartcard)
SFI	Short File ID
SFP	Security Function Policy
SFR	Security Function Requirement
SOD	Security Object of Document
SOF	Strength of Function
SPA	Simple Power Analysis
SSC	Send Sequence Counter
ST	Security Target
TA	Terminal Authentiation
TDES	Triple-DES
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Subsystem, TSF Subsystem

ICSP
Intelligent Convergence Solution Provider

END OF DOCUMENT

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

smart answer SAMSUNG SDS SAMSUNG