LG CNS

XSmart e-Passport V1.4 EAC with SAC on M7892

Security Target

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

[Table of Contents]

REFERENCED DOCUMENTS 3

1. INTRODUCTION 5

1.1. SECURITY TARGET REFERENCE 5
1.2. TOE REFERENCE 5
1.3. TOE OVERVIEW 6

2. CONFORMANCE CLAIMS 18

2.1. CC CONFORMANCE CLAIM 18
2.2. PP CLAIM 18
2.3. PACKAGE CLAIM 18
2.4. CONFORMANCE RATIONALE 19

3. SECURITY PROBLEM DEFINEION 20

3.1. INTRODUCTION 20
3.2. ASSUMPTIONS 26
3.3. THREATS 28
3.4. ORGANIZATIONAL SECURITY POLICIES 33

4. SECURITY OBJECTIVES 37

4.1. SECURITY OBJECTIVES FOR THE TOE 37
4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 41
4.3. SECURITY OBJECTIVE RATIONALE 45

5. EXTENDED COMPONENTS DEfiNITION 49

6. SECURITY REQUIREMENTS 55

6.1. SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE 58
6.2. SECURITY ASSUARANCE REQUIREMENTS FOR THE TOE 87
6.3. SECURITY REQUIREMENTS RATIONALE 87

7. TOE SUMMARY SPECIFICATION. 98

7.1. TOE SECURITY FUNCTIONS BY THE SOFTWARE 98
7.2. TOE SECURITY FUNCTIONS BY IC CHIP 98

8. GLOSSARY AND ACRONYMS 101

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Referenced Documents

[CC]	Common Criteria for Evaluation of IT Security, Version 3.1r4, CCBM-2012-09-0041
[CEM]	Common Criteria Methodology for Evaluation of IT Security , Version 3.1r4, CCBM-2012-09-004
[CCMB]	CCMB-2012-09-002, Version 3.1, Revision 4, Common Criteria for Information Technology Security Evaluation
[PACE-PP-0068]	Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011, Version 1.0, November 2011
[EAC-PP-0056]	Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012(Version 1.3.0, 20th January 2012)
[ICPP]	Security IC Platform Protection Profile; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007, Version 1.0, June 2007
[BAC-PP-0055]	Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0055, Version 1.10, 25th March 2009
[ICST]	Security Target Lite M7892 B11 Recertification including optional Software Libraries RSA - EC - SHA-2 - Toolbox, Version 0.3, October 13, 2015
[GPCS]	GlobalPlatform Card Specification, Version 2.1.1, GlobalPlatform Inc., March 2003
[MRTD]	Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, 2006 (this includes the latest supplemental for ICAO Doc 9303 which also should be considered)
[EAC]	Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents –Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), October 2010
[SAC]	ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010
[KM]	ISO/IEC 11770-3: Information technology . Security techniques . Key management -- Part 3: Mechanisms using asymmetric techniques, 2008
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11
[ISO7816]	ISO/IEC 7816: Identification cards . Integrated circuit cards, Version Second Edition, 2008
[PKCS]	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised, November 1, 1993

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

[ECC-TR]	Bundesamt für Sicherheit in der Informationstechnik (BSI), Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, 17.04.2009
[AIS31]	Functionality classes and evaluation methodology for physical random number generators AIS31, Version 2.1, 2011-12-02

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

1. Introduction

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

1.1. Security Target Reference

Subject	XSmart e-Passport V1.4 EAC with SAC on M7892 Security Target
ST Identification	XSMART e-Passport V1.4_ASE(EAC with SAC)_V1.5.docx
Version	V1.5
Author	LG CNS
Evaluation Criteria	Information Protection System Common Criteria V3.1r4
Evaluation Assurance Level	EAL5+ (ALC_DVS.2, ATE_DPT.3, AVA_VAN.5)
Protection Profile	BSI-CC-PP-0056-V2-2012 (Version 1.3.2, 05th December 2012)
Keywords	MRTD, ICAO, BSI,e-Passport

Table 1 Reference of Security Target

1.2. TOE Reference

TOE Name	XSmart e-Passport V1.4 EAC with SAC on M7892
Component of TOE	- XSmart e-Passport V1.4 -User Guide for Management (XSmart e-Passport V1.4_AGD(EAC with SAC)_V1.4) -Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013,SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)
TOE code identification	Hex code -e-Passport_V14_CLFX2400P.hex (implemented on 78CLFX2400P) -e-Passport_V14_CLFX3000P.hex(implemented on 78CLFX3000P) -e-Passport_V14_CLFX4000P.hex(implemented on 78CLFX4000P)
IC Chip	Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013,SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)
IC Chip reference	BSI-DSZ-CC-0782-V2-2015

Table 2 Reference of TOE

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

1.3. TOE Overview

This document is the security target regarding the XSmart e-Passport V1.4 on Infineon SLE7892 IC Chip(referred to as **"XSmart e-Passport V1.4"** hereafter), which is the composite TOE composed of a COS in charge of the chip operating system and an IC chip as a part of hardware. TOE supports Basic Access Control and Active Authentication according to [MRTD].

XSmart e-Passport V1.4 is the composed of HAL(Hardware Abstraction Layer), AML(Application Middle Layer), LDS layer and IC Chip H/W.

- HAL(Hardware Abstraction Layer) actually performs I/O handling according to ISO/IEC 7816 and ISO/IEC 14443 and memory management through the chip interface. It supports the DES/RSA/AES/ECC security function using H/W Crypto Library.

- AML(Application Middle Layer) that lies in the middle of HAL and LDS layer provides useful function required for key management, transaction, encryption mechanism.

- LDS layer supports [MRTD],[EAC],[SAC] functions defined in each spec. After the first e-passport program is loaded in FLASH area, it is activated through the installation and issuance process.

- SLE 78CLFX2400P/3000P/4000P are the contact/contactless IC chips from Infineon Technologies that have been certified by the Common Criteria from BSI.
  - Protection Profile: Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035-2007
  - TOE : Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software(firmware)
  - Certification Number : BSI-DSZ-CC-0782-V2-2015
  - Assurance level: CC EAL 6+ (ALC_FLR.1)
  - Certified cryptography library: RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

1.3.1. TOE definition

The Target of Evaluation (TOE) is an electronic travel document representing a contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [SAC] (which means amongst others according to the Logical Data Structure (LDS) defined in [MRTD])and additionally providing the Extended Access Control according to the 'ICAO Doc 9303' [MRTD] and BSI TR-03110 [EAC], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment(PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [PACE-PP-0068].

The TOE comprises of at least

- the circuitry of the contactless/contact chip incl. all IC dedicated software
- Hardware abstraction layer for IC chip (HAL)
- The Application middle layer for MRTD application (AML)
- the MRTD application (LDS)
- the associated guidance documentation

1.3.2. TOE usage and security features for operational

A State or Organisation issues travel documents to be used by the holder for international travel. The traveller presents a travel document to the inspection system to prove his or her identity. The travel document in context of this security target contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the travel document's chip according to LDS in case of contactless machine reading. The authentication of the traveller is based on (i) the possession of a valid travel document personalised for a holder with the claimed identity as given on the biographical data page and (ii) biometrics using the reference data stored in the travel document. The issuing State or Organisation ensures the authenticity of the data of genuine travel documents. The receiving State trusts a genuine travel document of an issuing State or Organisation

For this security target the travel document is viewed as unit of

(i) the **physical part of the travel document** in form of paper and/or plastic and

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

chip. It presents visual readable data including (but not limited to) personal data of the travel document holder

(a) the biographical data on the biographical data page of the travel document surface,

(b) the printed data in the Machine Readable Zone (MRZ) and

(c) the printed portrait.

(ii) the **logical travel document** as data of the travel document holder stored according to the Logical Data Structure as defined in [MRTD] as specified by ICAO on the contact based or contactless integrated circuit. It presents contact based / contactless readable data including (but not limited to) personal data of the travel document holder

(a) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(b) the digitized portraits (EF.DG2),

(c) the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both1

(d) the other data according to LDS (EF.DG5 to EF.DG16) and

(e) the Document Security Object (SOD).

The issuing State or Organisation implements security features of the travel document to maintain the authenticity and integrity of the travel document and their data. The physical part of the travel document and the travel document's chip are identified by the Document Number.

The physical part of the travel document is protected by physical security measures (e.g. watermark, security printing), logical (e.g. authentication keys of the travel document's chip) and organisational security measures (e.g. control of materials, personalisation procedures) [MRTD]. These security measures can include the binding of the travel document's chip to the travel document.

The logical travel document is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organisation and the security features of the travel document's chip.

The ICAO defines the baseline security methods Passive Authentication and the optional advanced security methods Basic Access Control to the logical travel document, Active Authentication of the travel document's chip, Extended Access Control to and the Data

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Encryption of sensitive biometrics as optional security measure in the ICAO Doc 9303 [MRTD], and Password Authenticated Connection Establishment [SAC]. The Passive Authentication Mechanism is performed completely and independently of the TOE by the TOE environment.

This security target addresses the protection of the logical travel document (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Extended Access Control Mechanism. This security target addresses the Chip Authentication Version 1 described in [EAC] as an alternative to the Active Authentication stated in [MRTD].

The confidentiality by Basic Access Control is a mandatory security feature that shall be implemented by the TOE, too. Nevertheless this is not explicitly covered by this security target as there are known weaknesses in the quality (i.e. entropy) of the BAC keys generated by the environment. Therefore, the MRTD has additionally to fulfill the 'Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control' BSI-CC-PP-0055 [BAC-PP-0055]. Due to the fact that [BAC-PP-0055] does only consider extended basic attack potential to the Basic Access Control Mechanism (i.e. AVA_VAN.3) the MRTD has to be evaluated and certified separately.

The confidentiality by Password Authenticated Connection Establishment (PACE) is a mandatory security feature of the TOE. The travel document shall strictly conform to the 'Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (EAC PP)' [EAC-PP-0056]. Note that [EAC-PP-0056] considers high attack potential.

For the PACE protocol according to [SAC], the following steps shall be performed:

(i) the travel document's chip encrypts a nonce with the shared password, derived from the MRZ resp. CAN data and transmits the encrypted nonce together with the domain parameters to the terminal.

(ii) The terminal recovers the nonce using the shared password, by (physically) reading the MRZ resp. CAN data.

(iii) The travel document's chip and terminal computer perform a Diffie-Hellmann key agreement together with the ephemeral domain parameters to create a shared secret. Both parties derive the session keys KMAC and KENC from the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

shared secret.

(iv) Each party generates an authentication token, sends it to the other party and verifies the received token.

After successful key negotiation the terminal and the travel document's chip provide private communication (secure messaging) [EAC], [SAC].

The security target requires the TOE to implement the Extended Access Control as defined in [EAC]. The Extended Access Control consists of two parts (i) the Chip Authentication Protocol Version 1 and (ii) the Terminal Authentication Protocol Version 1 (v.1). The Chip Authentication Protocol v.1 (i) authenticates the travel document's chip to the inspection system and (ii) establishes secure messaging which is used by Terminal Authentication v.1 to protect the confidentiality and integrity of the sensitive biometric reference data during their transmission from the TOE to the inspection system. Therefore Terminal Authentication v.1 can only be performed if Chip Authentication v.1 has been successfully executed. The Terminal Authentication Protocol v.1 consists of (i) the authentication of the inspection system as entity authorized by the receiving State or Organisation through the issuing State, and (ii) an access control by the TOE to allow reading the sensitive biometric reference data only to successfully authenticated authorized inspection systems. The issuing State or Organisation authorizes the receiving State by means of certification the authentication public keys of Document Verifiers who create Inspection System Certificates

1.3.3. TOE life-cycle

The TOE life-cycle is described in terms of the four life-cycle phases. (With respect to the [ICPP], the TOE life-cycle is additionally subdivided into 7 steps.)

<u>Phase 1 "Development"</u>

(Step1) The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC Dedicated Software and the guidance documentation associated with these TOE components.

(Step2) The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC Dedicated Software and develops the IC Embedded Software (operating system), the e-Passport application and the guidance documentation associated with these TOE components.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

The manufacturing documentation of the IC including the IC Dedicated Software and the Embedded Software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC Embedded Software in the non-volatile programmable memories, the e-Passport application and the guidance documentation is securely delivered to the travel document manufacturer.

Phase 2 "Manufacturing"

(Step3) In a first step the TOE integrated circuit is produced containing the travel document's chip Dedicated Software and the parts of the travel document's chip Embedded Software in the non-volatile non-programmable memories (ROM). The IC manufacturer writes the IC Identification Data onto the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer. The IC is securely delivered from the IC manufacture to the travel document manufacturer.
If necessary the IC manufacturer adds the parts of the IC Embedded Software in the non-volatile programmable memories (for instance EEPROM).

(Step4 optional) The travel document manufacturer combines the IC with hardware for the contact based / contactless interface in the travel document unless the travel document consists of the card only.

(Step5) The travel document manufacturer (i) adds the IC Embedded Software or part of it in the non-volatile programmable memories (for instance EEPROM or FLASH) if necessary, (ii) creates the e-Passport application, and (iii) equips travel document's chips with pre-personalization Data

The pre-personalised travel document together with the IC Identifier is securely delivered from the travel document manufacturer to the Personalisation Agent. The travel document manufacturer also provides the relevant parts of the guidance documentation to the Personalisation Agent.

Phase 3 "Personalisation of the travel document"

(Step6) The personalisation of the travel document includes (i) the survey of the travel document holder's biographical data, (ii) the enrolment of the travel document holder biometric reference data (i.e. the digitized portraits and the optional biometric reference

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

data), (iii) the personalization of the visual readable data onto the physical part of the travel document, (iv) the writing of the TOE User Data and TSF Data into the logical travel document and (v) configuration of the TSF if necessary. The step (iv) is performed by the Personalisation Agent and includes but is not limited to the creation of (i) the digital MRZ data (EF.DG1), (ii) the digitized portrait (EF.DG2), and (iii) the Document security object.
The signing of the Document security object by the Document signer [MRTD] finalizes the personalisation of the genuine travel document for the travel document holder. The personalised travel document (together with appropriate guidance for TOE use if necessary) is handed over to the travel document holder for operational use.

Phase 4 "Operational Use"

(Step7) The TOE is used as a travel document's chip by the traveller and the inspection systems in the "Operational Use" phase. The user data can be read according to the security policy of the issuing State or Organisation and can be used according to the security policy of the issuing State but they can never be modified.

1.3.4. Non-TOE hardware/software/firmware required by the TOE

There is no explicit non-TOE hardware, software or firmware required by the TOE to perform its claimed security features. The TOE is defined to comprise the chip and the complete operating system and application. Note, the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete travel document, nevertheless these parts are not inevitable for the secure operation of the TOE.

1.3.5. TOE SCOPE

This security target includes native e-passport program and IC chip hardware with firmware and crypto library

1.3.5.1. Physical scope of TOE

This picture illustrates the physical scope of TOE.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

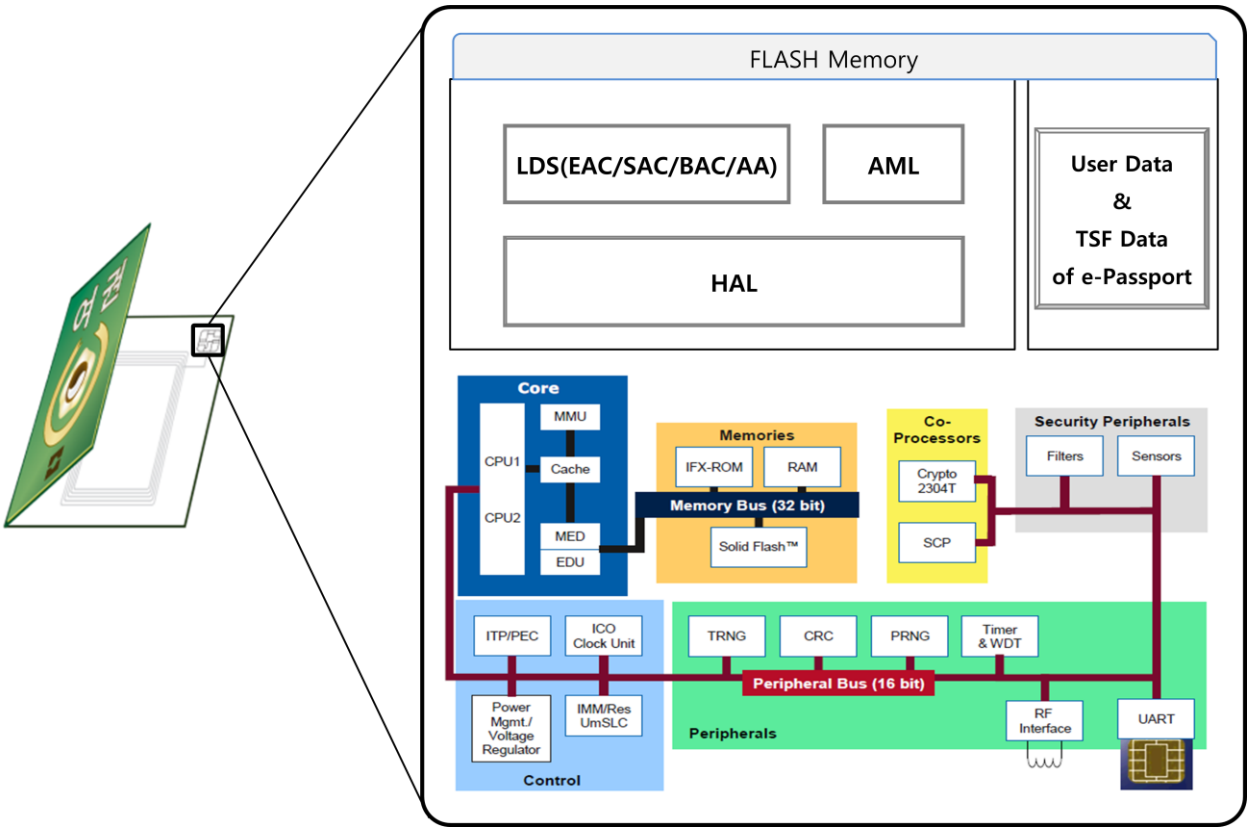


Figure. Physical scope of TOE

The physical scope of TOE includes the IC chip in the passport booklet, e-Passport application with user data and TSF data.
The components of IC chip as are CPU, Crypto Co-Processor, I/O, Memory (RAM, FLASH), and various H/W functions.

This security target address the Extended Access Control and Supplemental Access Control.

In IC Chip's flash area, after e-Passport application is installed, flash area is changed to locked state.(non-programmable state)
Also, e-passport data like biometric data (face, fingerprint) and TSF data (keys for authentication, seed key for BAC, CA private key) are saved in the flash area

Infineon SLE 78CLFX2400P/3000P/4000P which is the composition element of the IC chip, is a product certified with CCRA EAL 6+ assurance level, and the composition elements included in the authentication are IC chip hardware and cryptographic calculation software

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

library as shown in the following.

IC Chip hardware

- 16 bit microprocessor(CPU)
- 8KB RAM
- ROM : Not user available, H/W only)
- FLASH : 240KB(2400P), 300KB(3000P), 404KB(4000P)
- Memory Protection Unit(MPU), Random Number Generator(RNG), Timer(TIM), Crypto co-processor
- RF interface, address and data bus(ADBUS)

Software library for cryptographic operation

- 3DES , AES, RSA/ECC library
- True Random Number Generator (TRNG)
- Hash function(SHA-224, SHA-256, SHA-384, SHA-512)

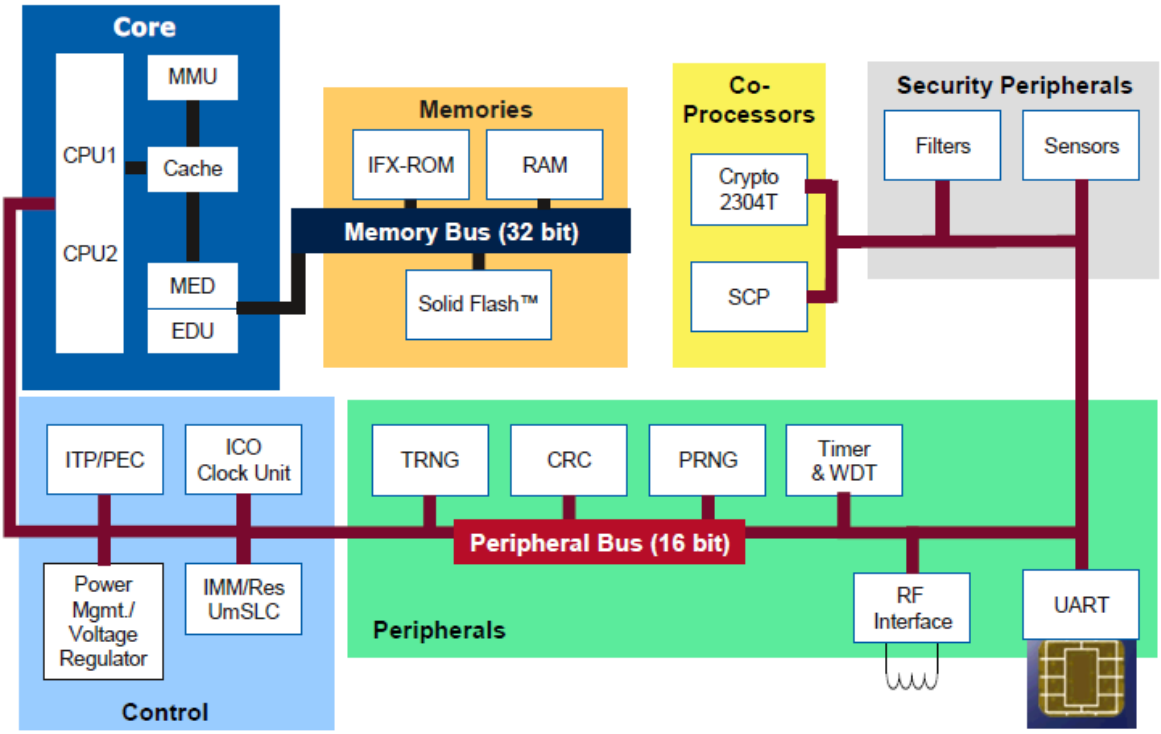


Figure. IC Chip H/W diagram

The IC chip hardware provide SCP module used in the symmetric key encryption according to DES and AES standards, Crypto 2304T Crypto module used in the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

asymmetric key encryption, physical security measures such as shield, temperature sensor, voltage sensor, and filter, and non-determinant hardware random number generator.
The firmware provides IC chip hardware management function such as flash download or hardware testing. The cryptographic calculation software library provides calculations such as digital signature generation/verification for hash value, ECDH key exchange, ECC/RSA key pair generation, and ECC/RSA public key verification.

SCP(Symmetric Crypto)

- TDES encryption and decryption
- Retail MAC and Full Triple DES MAC generation/verification
- AES encryption and decryption

Crypto@2404T

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

SHA-2 library
This library provides SHA-224, SHA-256, SHA-384, SHA-512.

1.3.5.2. Logical scope of TOE

TOE communicates with the inspection system according to the communication protocol defined in ISO/IEC 14443-4. TOE implements the security mechanism EAC and SAC defined in [EAC],[SAC]

This picture illustrates the logical scope of TOE.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

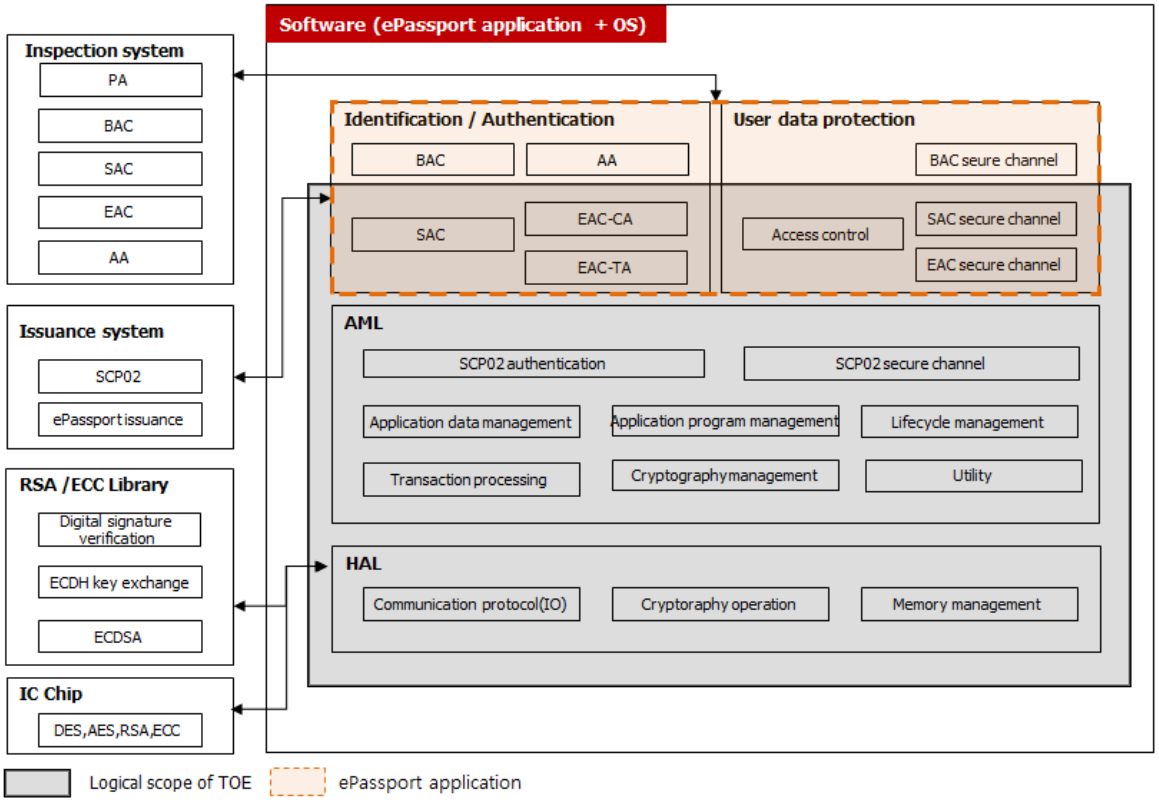


Figure. Logical scope of TOE

e-Passport application(LDS)

e-passport application program is an IC chip application program which implements the function for storing/processing e-passport identity information and the security mechanism to securely protect it according to the LDS (Logical Data Structure) format in [MRTD]. e-passport application program provides security management function for e-passport application program to the authenticated Personalization agent through SCP02 security mechanism provided in the card manager, and permits access to e-passport user data through SAC and EAC secure messaging only when the access rights were acquired through BAC secure messaging.

Application Middle Layer(AML)

AML is a middle layer for electronic passport application, in conjunction with HAL, to support the functions of logic necessary for the key management, transaction and encryption operations.

Hardware Abstraction Layer(HAL)

HAL is the hardware-dependent IC chip implementation like IC chip booting, hardware resource management, algorithm operation using crypto library, security configuration

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

setting of the IC chip. For SHA-1, it is implemented as a separate software, only the portion that is used as part of the electronic passport is the TOE scope.

Physical attack countermeasures

To prevent a variety of physical attack from the outside, IC Chip protection is enabled. Upon detecting a security violation, OS responds as card response stop, delay of card response, card termination.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

2. Conformance Claims

2.1. CC Conformance Claim

This security target claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1 Revision 4, September 2012 [CC-1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 [CC-2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012 [CC-3]

as follows

- Part 2 extended,
- Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1 Revision 4, July 2012[CEM] has to be taken into account.

2.2. PP Claim

The conformance of this ST to the Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control with PAC(EAC PP), BSI-CC-PP-0056-V2-2012 (Version 1.3.2, 05th December 2012)[EAC-PP-0056] is claimed.

2.3. Package Claim

This security target is conforming to assurance package EAL5 augmented with ALC_DVS.2 , AVA_VAN.5. defined in defined in [CC-3].

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

2.4. Conformance rationale

This ST claims strict conformance to the [EAC-PP-0056].

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

3. Security Problem Definition

3.1. Introduction

Asset

The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in PP [PACE-PP-0068], chap. 7)

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	user data stored on the TOE	All data (being not authentication data) stored in the context of the e-Passport application of the travel document as defined in [SAC] and being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [SAC]). This asset covers 'User Data on the MRTD's chip', 'Logical MRTD Data' and 'Sensitive User Data' in [BAC-PP-0055].	Confidentiality[1] Integrity Authenticity
2	user data transferred between the TOE and the terminal connected (i.e. an authority represented by Basic Inspection System with PACE)	All data (being not authentication data) being transferred in the context of the e-Passport application of the travel document as defined in [SAC] between the TOE and an authenticated terminal acting as Basic Inspection System with PACE (in the sense of [SAC]). User data can be received and sent (exchange Û {receive, send}).	Confidentiality[2] Integrity Authenticity

[1] Though not each data element stored on the TOE represents a secret, the specification [SAC] anyway requires securing their confidentiality: only terminals authenticated according to [SAC] can get access to the user data stored. They have to be operated according to P.Terminal.

[2] Though not each data element being transferred represents a secret, the specification [SAC] anyway requires securing their confidentiality: the secure messaging in encrypt-then-authenticate mode is required for all messages according to [SAC].

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

3	travel document tracing data	Technical information about the current and previous locations of the travel document gathered unnoticeable by the travel document holder recognising the TOE not knowing any PAC E password. TOE tracing data can be provided / gathered.	Unavailability[3]

Logical travel document sensitive User Data

: Sensitive biometric reference data (EF.DG3,EF.DG4)

All these primary assets represent User Data in the sense of the CC

Application note : Due to interoperability reasons the 'ICAO Doc 9303' [MRTD] requires that Basic Inspection Systems may have access to logical travel document data DG1, DG2, DG5 to DG16. The TOE is not in certified mode, if it is accessed using BAC [MRTD]. Note that the BAC mechanism cannot resist attacks with high attack potential (cf. [BAC-PP-0055]). If supported, it is therefore recommended to used PACE instead of BAC. <u>If nevertheless BAC has to be used, it is recommended to perform Chip Authentication v.1 before getting access to data (except DG14), as this mechanism is resistant to high potential attacks</u>

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
4	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
5	Genuineness of the TOE	Property of the TOE to be authentic in order to provide claimed security functionality in a proper way.	Availability

[3] represents a prerequisite for anonymity of the travel document holder

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

		This asset also covers 'Authenticity of the MRTD's chip' in [BAC-PP-0055].	
6	TOE internal secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.	Confidentiality Integrity
7	TOE internal non-secret cryptographic material	Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material (Document Security Object SOD containing digital signature) used by the TOE in order to enforce its security functionality.	Integrity Authenticity
8	travel document communication establishment authorisation data	Restricted-revealable [4] authorisation information for a human user being used for verification of the authorisation attempts as authorised user (PACE password). These data are stored in the TOE and are not to be send to it.	Confidentiality Integrity

The secondary assets represent TSF and TSF-data in the sense of the CC.

A sensitive asset is the following more general one.

Authenticity of the travel document's chip

The authenticity of the travel document's chip personalised by the issuing State or Organisation for the travel document holder is used by the traveller to prove his possession of a genuine travel document.

Due to strict conformance to PACE PP, this ST also includes all assets listed in [PACE-PP-0068], chap 3.1 Subjects and external entities

External Entity No.	Subject No.	Role	Definition
1	1	travel document holder	A person for whom the travel document Issuer has personalised the travel document[5].

[4] The travel document holder may reveal, if necessary, his or her verification values of CAN and MRZ to an authorised person or device who definitely act according to respective regulations and are trustworthy.
[5] i.e. this person is uniquely associated with a concrete electronic Passport

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

			This entity is commensurate with 'MRTD Holder' in [BAC-PP-0055]. Please note that a travel document holder can also be an attacker(s. below)
2	-	travel document presenter (traveller)	A person presenting the travel document to a terminal[6] and claiming the identity of the travel document holder. This external entity is commensurate with 'Traveller' in [BAC-PP-0055]. Please note that a travel document presenter can also be an attacker (s. below).
3	2	Terminal	A terminal is any technical system communicating with the TOE through the contactless/contact interface. The role 'Terminal' is the default role for any terminal being recognised by the TOE as not being PACE authenticated ('Terminal' is used by the travel document presenter). This entity is commensurate with 'Terminal' in [BAC-PP-0055].
4	3	Basic Inspection System with PACE (BIS-PACE)	A technical system being used by an inspecting authority[7] and verifying the travel document presenter as the travel document holder (for e-Passport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder). BIS-PACE implements the terminal's part of the PACE protocol and authenticates itself to the travel document using a shared password (PACE password) and supports Passive Authentication. See also par. 1.2.5 above.
5	-	Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [MRTD]. This role is usually delegated to a Personalisation Agent.
6	-	Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel document and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (CCSCA) having to be distributed by strictly secure diplomatic means, see. [MRTD], 5.5.1.

[6] In the sense of[SAC]
[7] concretely, by a control officer

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

7	4	Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i) establishing the identity of the travel document holder for the biographic data in the travel document, (ii) enrolling the biometric reference data of the travel document holder, (iii) writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [MRTD], (iv) writing the document details data, (v) writing the initial TSF data, (vi) signing the Document Security Object defined in [MRTD] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. This entity is commensurate with 'Personalisation agent' in [BAC-PP-0055].
8	5	Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase[8]. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer. This entity is commensurate with 'Manufacturer' in [BAC-PP-0055].
9	-	Attacker	A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the assets having to be maintained. The attacker is assumed to possess an at most high attack potential. Please note that the attacker might 'capture' any subject role recognised by the TOE. This external entity is commensurate with 'Attacker' in [BAC-PP-0055].
10	-	Country Verifying Certification Authority	The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing State or Organisation with respect to the protection of sensitive biometric reference data stored in the travel document. The CVCA represents the country specific root of the PKI of Inspection Systems and creates the Document Verifier Certificates within this PKI. The updates of the public key of the

[8] cf. also par. 1.2.3 in sec. 1.2.3 above

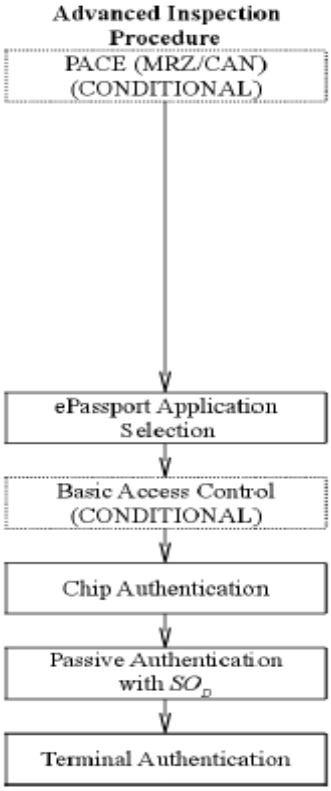
Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

			CVCA are distributed in the form of Country Verifying CA Link-Certificates
11	-	Document Verifier	The Document Verifier (DV) enforces the privacy policy of the receiving State with respect to the protection of sensitive biometric reference data to be handled by the Extended Inspection Systems. The Document Verifier manages the authorization of the Extended Inspection Systems for the sensitive data of the travel document in the limits provided by the issuing States or Organizations in the form of the Document Verifier Certificates.
-	-	Terminal	A terminal is any technical system communicating with the TOE either through the contact interface or through the contactless interface
-	-	Inspection system(EIS)	travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder. The Extended Inspection System (EIS) performs the Advanced Inspection Procedure and therefore (i) contains a terminal for the communication with the travel document's chip, (ii) implements the terminals part of PACE and/or BAC; (iii) gets the authorization to read the logical travel document either under PACE or BAC by optical reading the travel document providing this information. (iv) implements the Terminal Authentication and Chip Authentication Protocols both Version 1 according to [EAC] and (v) is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data. Security attributes of the EIS are defined by means of the Inspection System Certificates. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the BIS, PACE must be used.
-	-	Attacker	Additionally to the definition from PACE PP [PACE-PP-0068], chap 3.1 the definition of an attacker is refined as followed: A threat agent trying (i) to manipulate the logical travel document without authorization, (ii) to read sensitive biometric reference data (i.e. EF.DG3, EF.DG4), (iii) to forge a genuine travel document, or (iv) to trace a travel document.

Subjects and external entities[9]

[9] This table defines external entities and subjects in the sense of [CC]. Subjects can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates . for each of the respective external entity . an 'image' inside and 'works' then with this TOE internal image (also called subject in [CC]). From this point of view, the TOE itself

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved



Advanced Inspection System

3.2. Assumptions

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

A.Insp_Sys (Inspection Systems for global interoperability)

The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [SAC] and/or BAC [BAC-PP-0055]. be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

perceives only 'subjects' and, for them, does not differ between 'subjects' and 'external entities'. There is no dedicated subject with the role 'attacker' within the current security policy, whereby an attacker might 'capture' any subject role recognised by the TOE

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Justification:

The assumption A.Insp_Sys does not confine the security objectives of the [PACE-PP-0068] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

A.Auth_PKI (PKI for Inspection Systems)

The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

Justification:

This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [PACE-PP-0068] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

This ST includes the assumption from the PACE PP [PACE-PP-0068], chap 3.4, namely A.Passive_Auth.

A.Passive_Auth (PKI for Passive Authentication)

The issuing and receiving States or Organizations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organization runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organizations. It is assumed that the Personalization Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [MRTD].

3.3. Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE.

The TOE in collaboration with its IT environment shall avert the threats as specified below.

T.Read_Sensitive_Data (Read the sensitive biometric reference data)

Adverse action:

An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip. The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [8]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

Threat agent:

having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document

Asset:

confidentiality of logical travel document sensitive user data (i.e. biometric reference)

T.Counterfeit (Counterfeit of travel document chip data)

Adverse action:

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document.

The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

Threat agent:

having high attack potential, being in possession of one or more legitimate travel documents

Asset:

authenticity of user data stored on the TOE

This ST includes all threats from the PACE PP [PACE-PP-0068], chap 3.2, namely T.Skimming, T.Eavesdropping, T.Tracing, T.Abuse-Func, T.Information_Leakage, T.Phys-Tamper, T.Forgery and T.Malfunction, below :

T.Skimming (Skimming travel document / Capturing Card-Terminal Communication)

Adverse action :

An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless/contact interface of the TOE.

Threat agent :

having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset:

confidentiality of logical travel document data

Application Note : MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder.

T.Eavesdropping (Eavesdropping on the communication between the TOE and the PACE terminal)

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Adverse action:

An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.

Threat agent:

having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset:

confidentiality of logical travel document data

T.Tracing (Tracing travel document)

Adverse action:

An attacker tries to gather TOE tracing data (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.

Threat agent:

potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset:

privacy of the travel document holder

Application Note : This Threat completely covers and extends "T.Chip-ID" from BAC PP [MRTD].

Application Note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication or Active Authentication), a threat like T.Counterfeit (counterfeiting travel document)[10] cannot be averted by the current TOE.

T.Forgery (Forgery of Data)

Adverse action:

An attacker fraudulently alters the User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected in

[10] Such a threat might be formulated like: 'An attacker produces an unauthorised copy or reproduction of a genuine travel document to be used as part of a counterfeit Passport: he or she may generate a new data set or extract completely or partially the data from a genuine travel document and copy them on another functionally appropriate chip to imitate this genuine travel document. This violates the authenticity of the travel document being used for authentication of an travel document presenter as the travel document holder'.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

Threat agent:

having high attack potential

Asset:

integrity of the travel document

T.Abuse-Func (Abuse of Functionality)

Adverse action:

An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE or (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.

Threat agent:

having high attack potential, being in possession of one or more legitimate travel documents

Asset:

integrity and authenticity of the travel document, availability of the functionality of the travel document

Application Note: Details of the relevant attack scenarios depend, for instance, on the capabilities of the test features provided by the IC Dedicated Test Software being not specified here.

T.Information_Leakage (Information Leakage from travel document)

Adverse action:

An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected. The information leakage may be inherent in the normal operation or caused by the attacker.

Threat agent:

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

having high attack potential

Asset:

confidentiality of User Data and TSF-data of the travel document

Application Note: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

T.Phys-Tamper (Physical Tampering)

Adverse action:

An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

Threat agent:

having high attack potential, being in possession of one or more legitimate travel documents

Asset:

integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Application Note: Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that,

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

T.Malfunction due to Environmental Stress

Adverse action:

An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent:

having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation

Asset:

integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Application note: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

3.4. Organizational Security Policies

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

P.Sensitive_Data (Privacy of sensitive biometric reference data)

The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

P.Personalisation (Personalisation of the travel document by issuing State or)Organisation only

The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

This ST includes all OSPs from the PACE PP [PACE-PP-0068], chap 3.3, namely P.Pre-Operational, P.Card_PKI, P.Trustworthy_PKI, P.Manufact and P.Terminal.

P.Manufact (Manufacturing of the travel document's chip)

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

P.Pre-Operational (Pre-operational handling of the travel document)

1.) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
2.) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE.
3.) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. <u>before</u> they are in the operational phase.
4.) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

P.Card_PKI (PKI for Passive Authentication (issuing branch))

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Application Note: The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

1.) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (C_{CSCA}) .
2.) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (C_{CSCA}) having to be made available to the travel document Issuer by strictly secure means, see [MRTD], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (C_{DS}) and make them available to the travel document Issuer, see [MRTD], 5.5.1.
3.) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

P.Trustworthy_PKI (Trustworthiness of PKI)

The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document

P.Terminal (Abilities and trustworthiness of terminals)

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

1.) The related terminals (basic inspection system, cf. above) shall be used by terminal operators and by travel document holders as defined in [MRTD].
2.) They shall implement the terminal parts of the PACE protocol [SAC], of the Passive Authentication [MRTD] and use them in this order[11]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3.) The related terminals need not to use any own credentials.

[11] This order is commensurate with [SAC]

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

4.) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [MRTD]).

5.) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

4. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

4.1. Security Objectives for the TOE

The following TOE security objectives address the protection provided by the TOE independent of TOE environment

OT.Sens_Data_ConfConfidentiality of sensitive biometric reference data
The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

OT.Chip_Auth_Proof Proof of the travel document's chip authenticity
The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [EAC]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

Application note: The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [MRTD] and (ii) the hash value of DG14 in the Document

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Security Object signed by the Document Signer.

OT.Data_Integrity (Integrity of Data)

The TOE must ensure integrity of the User Data and the TSF-data stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying).The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Data_Authenticity (Authenticity of Data)

The TOE must ensure authenticity of the User Data and the TSF-data stored on it by enabling verification of their authenticity at the terminal-side[12].The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[13].

OT.Data_Confidentiality (Confidentiality of Data)

The TOE must ensure confidentiality of the User Data and the TSF-data by granting read access only to the PACE authenticated BIS-PACE connected. The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

OT.Tracing (Tracing travel document)

The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

Application note: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)[14]

[12] Verification of SO_D

[13] Secure messaging after the PACE authentication, see also[SAC]

[14] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

cannot be achieved by the current TOE.

OT.Prot_Abuse-Func (Protection against Abuse of Functionality)

The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

OT.Prot_Inf_Leak (Protection against Information Leakage)

The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines
- by forcing a malfunction of the TOE and/or
- by a physical manipulation of the TOE

Application note: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

OT.Prot_Phys-TamperProtection against Physical Tampering

The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software by means of

- measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis)
- manipulation of the hardware and its security functionality, as well as
- controlled manipulation of memory contents (User Data, TSF-data)

with a prior

- reverse-engineering to understand the design and its properties and functionality.

---

the authenticity of the travel document as a whole device as issued by the travel document Issuer (issuing PKI branch of the travel document Issuer) by means of the Passive and Chip Authentication as defined in [MRTD]'.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

OT.Prot_Malfunction Protection against Malfunctions

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.

The following TOE security objectives address the aspects of identified threats to be countered involving TOE's environment.

OT.Identification Identification of the TOE

The TOE must provide means to store Initialisation[15] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

OT.AC_PersAccess Control for Personalisation of logical MRTD

The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [MRTD] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

Application note: The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

Application Note:

The cryptographic processor and RSA / ECC cryptographic library that is mounted on the IC chip must implement countermeasures to prevent abuse of information leakage while cryptographic processings.

[15] Amongst other, IC Identification data

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

4.2. Security Objectives for the Operational Environment

Issuing State or Organisation

The issuing State or Organisation will implement the following security objectives of the TOE environment.

OE.Auth_Key_Travel_Document (Travel document Authentication Key)

The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.

Justification:

This security objective for the operational environment is needed additionally to those from [PACE-PP-0068] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 .

OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)

The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of travel document holders to authorized receiving States or Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.

Justification:

This security objective for the operational environment is needed additionally to those from [PACE-PP-0068] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Protection Profile and not in [PACE-PP-0068].

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Receiving State or Organisation

The receiving State or Organisation will implement the following security objectives of the TOE environment.

OE.Exam_Travel_Document (Examination of the physical part of the travel document)

The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [SAC] and/or the Basic Access Control [MRTD]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.

Justification:

This security objective for the operational environment is needed additionally to those from [PACE-PP-0068] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [PACE-PP-0068] and therefore also counters T.Forgery and A.Passive_Auth from [PACE-PP-0068]. This is done because a new type of Inspection System is introduced in this ST as the Extended Inspection System is needed to handle the additional features of a travel document with Extended Access Control

OE.Prot_Logical_Travel_Document (Protection of data from the logical travel document)

The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.

Justification:

This security objective for the operational environment is needed additionally to those

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

from [PACE-PP-0068] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)
The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.

Justification:
This security objective for the operational environment is needed additionally to those from [PACE-PP-0068] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

This ST includes all Security Objectives of the TOE environment from the PACE PP [PACE-PP-0068], chap. 4.2.

Travel document Issuer as the general responsible
The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

OE.Legislative_Compliance Issuing of the travel document
The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations

Travel document Issuer and CSCA: travel document's PKI (issuing) branch
The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application Note 20 above):

OE.Passive_Auth_Sign (Authentication of travel document by Signature)
The travel document Issuer has to establish the necessary public key infrastructure as

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (CCSCA). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [MRTD]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [MRTD]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DSs must sign exclusively correct Document Security Objects to be stored on travel document.

OE.Personalisation (Personalisation of travel document)

The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enroll the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [MRTD], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [MRTD] (in the role of a DS).

Terminal operator: Terminal's receiving branch

OE.TerminalTerminal operating

The terminal operators must operate their terminals as follows:

1.) The related terminals (basic inspection systems, cf. above) are used by terminal operators and by travel document holders as defined in [MRTD].
2.) The related terminals implement the terminal parts of the PACE protocol [SAC], of the Passive Authentication [SAC] (by verification of the signature of the Document Security Object) and use them in this order[16]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating

[16] This order is commensurate with [SAC]

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

ephemeral keys for Diffie-Hellmann).

3.) The related terminals need not to use any own credentials.

4.) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [MRTD]).

5.) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Travel document holder Obligations

OE.Travel_Document_HolderTravel document holder Obligations

The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

4.3. Security Objective Rationale

The following table provides an overview for security objectives coverage

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_Pers2	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Tracing	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Identification	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion	OE.Auth_Key_Travel_Document	OE.Authoriz_Sens_Data	OE.Exam_Travel_Document	OE.Prot_Logical_Travel_Document	OE.Ext_Insp_Systems	OE.Personalisation	OE.Passive_Auth_Sign	OE.Terminal	OE.Travel_Document_Holder	OE.Legislative Compliance
T.Read_Sensitive_Data	x													x			x					
T.Counterfeit		x											x		x							
T.Skimming3				x	x	x															x	
T.Eavesdropping						x																
T.Tracing							x														x	
T.Abuse-Func								x														
T.Information_Leakage									x													
T.Phys-Tamper											x											
T.Malfunction												x										
T.Forgery			x	x	x			x			x				x			x	x	x		

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

P.Sensitive_Data	x													x			x					
P.Personalisation			x							x								x				
P.Manufact										x												
P.Pre-Operational			x							x								x				x
P.Terminal															x					x		
P.Card_PKI																			x			
P.Trustworthy_PKI																			x			
A.Insp_Sys															x	x						
A.Auth_PKI														x			x					
A.Passive_Auth															x				x			

security objectives rationale

The OSP **P.Personalisation** "Personalisation of the travel document by issuing State or Organisation only" addresses the (i) the enrolment of the logical travel document by the Personalisation Agent as described in the security objective for the TOE environment **OE.Personalisation** "Personalisation of logical travel document", and (ii) the access control for the user data and TSF data as described by the security objective **OT.AC_Pers** "Access Control for Personalisation of logical travel document". Note the manufacturer equips the TOE with the Personalisation Agent Key(s) according to **OT.Identification** "Identification and Authentication of the TOE". The security objective **OT.AC_Pers** limits the management of TSF data and the management of TSF to the Personalisation Agent.

The OSP **P.Sensitive_Data** "Privacy of sensitive biometric reference data" is fulfilled and the threat **T.Read_Sensitive_Data** "Read the sensitive biometric reference data" is countered by the TOE-objective **OT.Sens_Data_Conf** "Confidentiality of sensitive biometric reference data" requiring that read access to EF.DG3 and EF.DG4 (containing the sensitive biometric reference data) is only granted to authorized inspection systems. Furthermore it is required that the transmission of these data ensures the data's confidentiality. The authorization bases on Document Verifier certificates issued by the issuing State or Organisation as required by **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data". The Document Verifier of the receiving State has to authorize Extended Inspection Systems by creating appropriate Inspection System certificates for access to the sensitive biometric reference data as demanded by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems".

The OSP **P.Terminal** "Abilities and trustworthiness of terminals" is countered by the security objective **OE.Exam_Travel_Document** additionally to the security objectives from PACE PP [pace-pp-0068]. **OE.Exam_Travel_Document** enforces the terminals to

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

perform the terminal part of the PACE protocol.

The threat **T.Counterfeit** "Counterfeit of travel document chip data" addresses the attack of unauthorized copy or reproduction of the genuine travel document's chip. This attack is thwarted by chip an identification and authenticity proof required by **OT.Chip_Auth_Proof** "Proof of travel document's chip authentication" using an authentication key pair to be generated by the issuing State or Organisation. The Public Chip Authentication Key has to be written into EF.DG14 and signed by means of Documents Security Objects as demanded by **OE.Auth_Key_Travel_Document** "Travel document Authentication Key". According to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" the General Inspection system has to perform the Chip Authentication Protocol Version 1 to verify the authenticity of the travel document's chip.

The threat **T.Forgery** "Forgery of data" addresses the fraudulent, complete or partial alteration of the User Data or/and TSF-data stored on the TOE or/and exchanged between the TOE and the terminal. Additionally to the security objectives from PACE PP [PACE-PP-0068] which counter this threat, the examination of the presented MRTD passport book according to **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" shall ensure its authenticity by means of the physical security measures and detect any manipulation of the physical part of the travel document.

The examination of the travel document addressed by the assumption **A.Insp_Sys** "Inspection Systems for global interoperability" is covered by the security objectives for the TOE environment **OE.Exam_Travel_Document** "Examination of the physical part of the travel document" which requires the inspection system to examine physically the travel document, the Basic Inspection System to implement the Basic Access Control, and the Extended Inspection Systems to implement and to perform the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip. The security objectives for the TOE environment **OE.Prot_Logical_Travel_Document** "Protection of data from the logical travel document" require the Inspection System to protect the logical travel document data during the transmission and the internal handling. The assumption **A.Passive_Auth** "PKI for Passive Authentication" is directly covered by the security objective for the TOE environment **OE.Passive_Auth_Sign** "Authentication of travel document by Signature" from PACE PP [PACE-PP-0068] covering the necessary procedures for the Country Signing CA Key Pair and the Document Signer Key Pairs. The implementation of the signature verification procedures is covered by

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

OE.Exam_Travel_Document "Examination of the physical part of the travel document".

The assumption **A.Auth_PKI** "PKI for Inspection Systems" is covered by the security objective for the TOE environment **OE.Authoriz_Sens_Data** "Authorization for use of sensitive biometric reference data" requires the CVCA to limit the read access to sensitive biometrics by issuing Document Verifier certificates for authorized receiving States or Organisations only. The Document Verifier of the receiving State is required by **OE.Ext_Insp_Systems** "Authorization of Extended Inspection Systems" to authorize Extended Inspection Systems by creating Inspection System Certificates. Therefore, the receiving issuing State or Organisation has to establish the necessary public key infrastructure.

The following table provides an overview for security objectives coverage.

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.

.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

5. Extended Components Definition

This protection profile uses components defined as extensions to CC part 2. Most of them are drawn from [MRTD].

Definition of the Family FAU_SAS

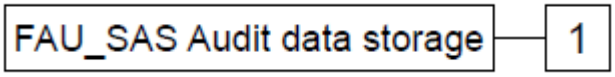
To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

FAU_SAS Audit data storage

Family behaviour

his family defines functional requirements for the storage of audit data.

Component leveling:



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components

Dependencies: No dependencies

FAU_SAS.1.1 The TSF shall provide [assignment: authorised users] with the capability to store [assignment: list of audit information] in the audit records.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Definition of the Family FIA_API

To describe the IT security functional requirements of the TOE a sensitive family (FIA_API) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove their identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity	1

FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: There are no actions defined to be auditable.

FIA_API.1Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [assignment: authorized user or role].

Definition of the Family FCS_RND

To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

keys unlike the component FCS_CKM.1.

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 Generation of random numbers	1

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 Quality metric for random numbers
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Definition of the Family FMT_LIM

The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

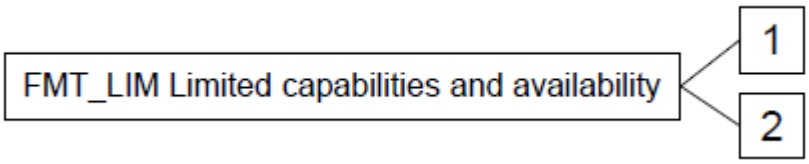
FMT_LIM Limited capabilities and availability

Family behaviour

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management : FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit : FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced [assignment: Limited capability and availability policy].

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FMT_LIM2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced [assignment: Limited capability and availability policy].

Application note:
The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced

or conversely

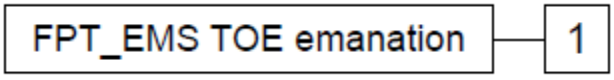
(ii) the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

Definition of the Family FPT_EMS

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 .

FPT_EMS TOE emanation
Family behaviour
This family defines requirements to mitigate intelligible emanations.
Component levelling:



FPT_EMS.1 emanation has two constituents:

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management : FPT_EMS.1
There are no management activities foreseen.

Audit : FPT_EMS.1
There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

6. Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph C.4 of Part 1 [CC] of the CC. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word "refinement" in bold text and the added/changed words are in **bold text**. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are underlined text with "<" like <this >.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized with "<" like <*this*>.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

The definition of the subjects "Manufacturer", "Personalisation Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations "write", "modify", "read" and "disable read access" are used in accordance with the general linguistic usage. The operations

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

"store", "create", "transmit", "receive", "establish communication channel", "authenticate" and "re-authenticate" are originally taken from [CCMB] part 2. The operation "load" is synonymous to "import" used in [CCMB] part 2.

Definition of security attributes:

Security attribute	Values	meaning
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [EAC]); Terminal is authenticated as Country Verifying Certification Authority after successful CA v.1 and TA v.1
	DV (domestic)	roles defined in the certificate used for authentication (cf. [EAC]); Terminal is authenticated as domestic Document Verifier after successful CA v.1 and TA v.1
	DV (foreign)	roles defined in the certificate used for authentication (cf. [EAC]); Terminal is authenticated as foreign Document Verifier after successful CA v.1 1 and TA v.1
	IS	roles defined in the certificate used for authentication (cf. [EAC]); Terminal is authenticated as Extended Inspection System after successful CA v.1 and TA v.1
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [EAC])
	DG3 (Fingerprint)	Read access to DG3: (cf. [EAC])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [EAC])

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [PP-PACE-0068].

Name	Data
Public Key (PK_{CVCA})	Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [EAC] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii)

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [KM].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organisation signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.
Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified by an Extended Inspection System of the receiving State or Organisation with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE

Application note:

The Country Verifying Certification Authority identifies a Document Verifier as "domestic" in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as "foreign" in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document's

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

point of view the domestic Document Verifier belongs to the issuing State or Organisation

6.1. Security Functional Requirements for the TOE

This section on security functional requirements for the TOE is divided into sub-section following the main security functionality.

6.1.1. Class FCS Cryptographic Support

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below (Common Criteria Part 2). The iterations are caused by different cryptographic key generation algorithms to be implemented and key to be generated by the TOE.

FCS_CKM.1/CA Cryptographic key generation - Diffie-Hellman for Chip Authentication session keys

Hierarchical to: No other components.

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

FCS_CKM.1.1/CA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <*ECDH*> and specified cryptographic key sizes <*224, 256, 320, 384*> that meet the following: <based on an ECDH protocol compliant to [ECC-TR]>

Application note:
FCS_CKM.1/CA implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [EAC].

Application note:
The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [EAC]. This protocol may be based on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [ECC-TR], for details). The shared secret value is used to derive the Chip Authentication Session Keys used for

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

encryption and MAC computation for secure messaging (defined in Key Derivation Function [EAC]).

Application note:
The SHA-1 function is supported by OS, not by H/W library.
It is for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 may use SHA-1 (cf. [EAC]). The TOE may Protocol v.1 (cf. [EAC] for details).

Application note:
The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [PACE-PP-0068] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1. Concerning the Chip Authentication keys FCS_CKM.4 is also fulfilled by FCS_CKM.1/CA

FCS_CKM.1/DH_PACE Cryptographic key generation - Diffie-Hellman for PACE session keys

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]: fulfilled by FCS_CKM.2/DH.
fulfilled by FCS_CKM.2/DH.
Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.
FCS_CKM.4 Cryptographic key destruction: fulfilled by CS_CKM.4

FCS_CKM.1.1/DH_PACE The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm <ECDH comp liant to [ECC-TR]>and specified cryptographic key sizes <*224, 256, 320, 384, 512* > that meet the following: [SAC]

Application note :

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

The TOE generates a shared secret value K with the terminal during the PACE protocol, see [SAC]. This protocol may be based on the ECDH compliant to TR-03111 [ECC-TR] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [SAC] and [ECC-TR] for details). The shared secret value K is used for deriving the AES or DES session keys for message encryption and message authentication (PACE-KMAC, PACE-KEnc) according to [SAC] for the TSF required by FCS_COP.1/PACE_ENC and FCS_COP.1/PACE_MAC.

Application note:
FCS_CKM.1/DH_PACE implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [SAC].

FCS_CKM.4 Cryptographic key destruction- Session keys

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, orFCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method <*overwriting with zero or new key value*> that meets the following: <*none* >

Application note:
The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1.

FCS_COP.1/CA_ENC Cryptographic operation - Symmetric Encryption / Decryption

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

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FCS_COP.1.1/CA_ENC The TSF shall perform <*secure messaging - encryption and decryption* > in accordance with a specified cryptographic algorithm <*see table below*> and cryptographic key sizes <*see table below*> that meet the following: <*see table below* >

algorithm	key size	standard
3DES in CBC mode	112	FIPS PUB 197
AES in CBC mode	128, 192, 256	ISO/IEC 18033-3

Application note:
This SFR requires the TOE to implement the cryptographic primitives (e.g. Triple-DES and/or AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA..

FCS_COP.1/CA_MAC Cryptographic operation -MAC

Hierarchical to: No other components.

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

FCS_COP.1.1/CA_MAC The TSF shall perform <*secure messaging - message authentication code*> in accordance with a specified cryptographic algorithm <*see table below*> and cryptographic key sizes <*see table below*> that meet the following: <*see table below*>

algorithm	key size	standard
3DES Retail-MAC	112	ISO/IEC 9797-1
AES CMAC	128, 192, 256	NIST 800-38B

Application note:
This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FCS_CKM.1/CA. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

FCS_COP.1/PACE_ENC Cryptographic operation - Encryption / Decryption AES / 3DES

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]: fulfilled by FCS_CKM.1/DH_PACE
FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4.

FCS_COP.1.1/ PACE_ENC

The TSF shall perform *<secure messaging - encryption and decryption>* in accordance with a specified cryptographic algorithm *<see table below >* in CBC mode and cryptographic key sizes *<see table below>* bit that meet the following: compliant to [SAC]

algorithm	key size
3DES	112
AES	128, 192, 256

Application note:
This SFR requires the TOE to implement the cryptographic primitive AES or 3DES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KEnc)..

FCS_COP.1/PACE_MAC Cryptographic operation - MAC

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]: fulfilled by FCS_CKM.1/DH_PACE

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4..

FCS_COP.1.1/ PACE_MAC

The TSF shall perform *<secure messaging - message authentication code>* in accordance with a specified cryptographic algorithm *<see table below>* and cryptographic key sizes <*see table below>* bit that meet the following: compliant to [SAC] .

algorithm	key size
Retail-MAC	112
CMAC	128, 192, 256

Application note:
This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE (PACE-KMAC). Note that in accordance with [SAC] the (two-key) Triple-DES could be used in Retail mode for secure messaging.

FCS_COP.1/SIG_VER Cryptographic operation - Signature verification by travel document

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/SIG-VER

The TSF shall perform *<digital signature verification>* in accordance with a specified cryptographic algorithm <*ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256>* and cryptographic key sizes <*224, 256, 320, 384>* that meet the following: <*[ECC-TR] >*

Application note:
The ST writer shall perform the missing operation of the assignments for the signature algorithms key lengths and standards implemented by the TOE for the Terminal

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Authentication Protocol v.1 (cf. [EAC]). The signature verification is used to verify the card verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet : <*[AIS31]* >

Application note:

This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE.

6.1.2. Class FIA Identification and Authentication

The Table below provides an overview on the authentication mechanisms used

Name	SFR for the TOE
Authentication Mechanism for Personalisation Agents	FIA_UAU.4/PACE
Chip Authentication Protocol v.1	FIA_API.1, FIA_UAU.5/PACE, FIA_UAU.6/EAC
Terminal Authentication Protocol v.1	FIA_UAU.5/PACE
PACE protocol	FIA_UAU.1/PACE FIA_UAU.5/PACE FIA_AFL.1/PACE
Passive Authentication	FIA_UAU.5/PACE

Overview on authentication SFR

Note the Chip Authentication Protocol Version 1 as defined in this security target includes

- the asymmetric key agreement to establish symmetric secure messaging keys between the TOE and the terminal based on the Chip Authentication Public Key and the Terminal Public Key used later in the Terminal Authentication Protocol Version 1,

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

- the check whether the TOE is able to generate the correct message authentication code with the expected key for any message received by the terminal.

The Chip Authentication Protocol v.1 may be used independent of the Terminal Authentication Protocol v.1. But if the Terminal Authentication Protocol v.1 is used the terminal shall use the same public key as presented during the Chip Authentication Protocol v.1.

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)" as specified below (Common Criteria Part 2).

FIA_UID.1/PACE Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_UID.1.1/PACE The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [SAC] ,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS
4. to carry out the Chip Authentication Protocol v.1 according to [EAC]
5. to carry out the Terminal Authentication Protocol v.1 according to [EAC]
6. *<to select e-Passport Application by SELECT COMMAND>.*

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

Application note:

The SFR FIA_UID.1/PACE in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to PACE PP.

Application note:

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 "Personalisation of the travel document". The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

Application note:
User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).

Application note:
In the life-cycle phase 'Manufacturing' the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC. Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role 'Personalisation Agent', when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

The TOE shall meet the requirement "Timing of authentication (FIA_UAU.1)" as specified below (Common Criteria Part 2).

FIA_UAU.1/PACE Timing of identification

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

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

FCS_UAU.1.1/PACE The TSF shall allow
1. to establish the communication channel,
2. carrying out the PACE Protocol according to [SAC] ,
3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS,
4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version according to [EAC]
6. to carry out the Terminal Authentication Protocol Version 1 according to [EAC]
7. *< to select ePassport Application by SELECT COMMAND>.*

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

Application note:
The SFR FIA_UAU.1/PACE. in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to PACE PP.

The TOE shall meet the requirements of "Single-use authentication mechanisms (FIA_UAU.4)" as specified below (Common Criteria Part 2).

FIA_UAU.4/PACE Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE

Hierarchical to: No other components.
Dependencies: No dependencies

FCS_UAU.4.1/PACE The TSF shall prevent reuse of authentication data related to
1.PACE Protocol according to [SAC] ,
2.Authentication Mechanism based on <Triple- DES and AES>
3.Terminal Authentication Protocol v.1 according to [EAC] .

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Application note:
The SFR FIA_UAU.4.1 in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to PACE PP. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [PACE-PP-0068].

Application note:
The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

The TOE shall meet the requirement "Multiple authentication mechanisms (FIA_UAU.5)" as specified below (Common Criteria Part 2)..

FIA_UAU.5/PACE Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies

FCS_UAU.5.1/PACE The TSF shall provide
1. PACE Protocol according to [SAC] ,
2. Passive Authentication according to [MRTD]
3. Secure messaging in MAC-ENC mode according to [SAC] ,
4. Symmetric Authentication Mechanism based on <Triple-DES, AES>
5. Terminal Authentication Protocol v.1 according to [EAC] , to support user authentication.

FCS_UAU.5.2/PACE The TSF shall authenticate any user's claimed identity according to the following rules:
1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

with the terminal by means of the PACE protocol.

2. The TOE accepts the authentication attempt as Personalisation Agent by < SCP02 Mutual Authentication [GPCS] E.2>.
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1 19.
5. <*none*>.

Application note:
The SFR FIA_UAU.5.1/PACE in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

The TOE shall meet the requirement "Re-authenticating (FIA_UAU.6)" as specified below (Common Criteria Part 2).

FIA_UAU.6/PACE Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.
Dependencies: No dependencies

FCS_UAU.6.1/PACE The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PAC E protocol shall be verified as being sent by the PACE terminal.

Application note:
The PACE protocol specified in [SAC] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

FIA_UAU.6/EAC Re-authenticating of Terminal by the TOE

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_UAU.6.1/EAC The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below (Common Criteria Part 2 extended).

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_API.1.1 The TSF shall provide a *<Chip Authentication Protocol Version 1 according to [EAC]>* to prove the identity of the *<TOE>*.

FIA_AFL.1/PACE Authentication failure handling - PACE authentication using non-blocking authorisation data

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FIA_AFL.1.1/PACE The TSF shall detect when *<1>* unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password .

FIA_AFL.1.1/PACE When the defined number of unsuccessful authentication attempts has been met, the TSF shall <*accumulates the delay time>.*

6.1.3. Class FDP User Data Protection

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below (Common Criteria Part 2).

FDP_ACC.1/TRM Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/TRM The TSF shall enforce the Access Control SFP on terminals gaining access to the User Data and data stored in EF.SOD of the logical travel document.

Application note:
The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below (Common Criteria Part 2).

FDP_ACF.1/TRM 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/TRM The TSF shall enforce the *< Access Control SFP>* to objects based on the following:
1.Subjects:
a.Terminal,

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

b.BIS-PACE
c.Extended Inspection System
2.Objects:
a.data in EF.DG1, EF.DG2 and EF.DG5 to EF.DG16, EF.SOD and EF.COM of the logical travel document ,
b.data in EF.DG3 of the logical travel document ,
c.data in EF.DG4 of the logical travel document ,
d.all TOE intrinsic secret cryptographic keys stored in the travel document
3.Security attributes:
a.PACE Authentication
b.Terminal Authentication v.1
c.Authorisation of the Terminal.

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: A BIS-PACE is allowed to read data objects from FDP_ACF.1.1/TRM according to [SAC] after a successful PACE authentication as required by FIA_UAU.1/PACE.

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

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
1.Any terminal being not authenticated as PACE authenticated BIS-PACE is not allowed to read, to write, to modify, to use any User Data stored on the travel document.
2.Terminals not using secure messaging are not allowed to read, to write, to modify, to use any data stored on the travel document.
3.Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 3 (Fingerprint) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2b) of FDP_ACF.1.1/TRM.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

4. Any terminal being not successfully authenticated as Extended Inspection System with the Read access to DG 4 (Iris) granted by the relative certificate holder authorization encoding is not allowed to read the data objects 2c) of FDP_ACF.1.1/TRM.
5. Nobody is allowed to read the data objects 2d) of FDP_ACF.1.1/TRM.
6. Terminals authenticated as CVCA or as DV are not allowed to read data in the EF.DG3 and EF.DG4.

Application note:
The SFR FDP_ACF.1.1/TRM in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by additional subjects and objects. The SFRs FDP_ACF.1.2/TRM and FDP_ACF.1.3/TRM in the current ST cover the definition in PACE PP [PACE-PP-0068]. The SFR FDP_ACF.1.4/TRM in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by 3) to 6).These extensions do not conflict with the strict conformance to PACE PP.

Application note :
The relative certificate holder authorization encoded in the CVC of the inspection system is defined in [EAC]. The TOE verifies the certificate chain established by the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate (cf. FMT_MTD.3). The Terminal Authorization is the intersection of the Certificate Holder Authorization in the certificates of the Country Verifying Certification Authority, the Document Verifier Certificate and the Inspection System Certificate in a valid certificate chain.

Application note:
Please note that the Document Security Object (SOD) stored in EF.SOD (see [MRTD]) does not belong to the user data, but to the TSF data. The Document Security Object can be read out by Inspection Systems using PACE, see [SAC].

Application note:
FDP_UCT.1/TRM and FDP_UIT.1/TRM require the protection of the User Data transmitted from the TOE to the terminal by secure messaging with encryption and message authentication codes after successful Chip Authentication Version 1 to the Inspection System. The Password Authenticated Connection Establishment, and the Chip

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Authentication Protocol v.1 establish different key sets to be used for secure messaging (each set of keys for the encryption and the message authentication key).

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

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

1. Session Keys (immediately after closing related communication session) ,
2. the ephemeral private key ephem - SK_{PICC}- PACE (by having generated a DH shared secret K),
3. *<none>*.

The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" as specified below (Common Criteria Part 2).

FDP_UCT.1/TRM Basic data exchange confidentiality -MRTD

Hierarchical to: No other components.

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

FDP_UCT.1.1/TRM The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from unauthorised disclosure.

The TOE shall meet the requirement "Data exchange integrity (FDP_UIT.1)" as specified below (Common Criteria Part 2).

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FDP_UIT.1/TRM Data exchange integrity

Hierarchical to: No other components.

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

FDP_UIT.1.1/TRM The TSF shall enforce the Access Control SFP to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

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

6.1.4. Class FTP Trusted Path/Channels

FTP_ITC.1/PACE Inter-TSF trusted channel after PACE

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1/PACE The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/PACE The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE The TSF shall ~~initiate~~ enforce communication via the trusted channel for any data exchange between the TOE and the Terminal.

Application note:

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

The trusted IT product is the terminal. In FTP_ITC.1.3/PACE, the word "initiate" is changed to 'enforce", as the TOE is a passive device that can not initiate the communication. All the communication are initiated by the Terminal, and the TOE enforce the trusted channel.

6.1.5. Class FAU Security Audit

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies

FAU_SAS.1.1 The TSF shall provide the Manufacturer with the capability to store the Initialisation and Pre-Personalisation Data in the audit records.

Application note:
The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialisation and/or Pre-personalisation Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA, FMT_MTD.1/INI_DIS). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

6.1.6. Class FMT Security Management

The SFR FMT_SMF.1 and FMT_SMR.1/PACE provide basic requirements on the management of the TSF data

The TOE shall meet the requirement "Security roles (FMT_SMR.1)" as specified below (Common Criteria Part 2)

FMT_SMR.1/PACE Security roles

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

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

FMT_SMR.1.1/PACE The TSF shall maintain the roles
1.Manufacturer ,
2.Personalisation Agent,
3.Terminal,
4.PACE authenticated BIS-PACE,
5.Country Verifying Certification Authority,
6.Document Verifier,
7.Domestic Extended Inspection System
8.Foreign Extended Inspection System.

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

Application note:
The SFR FMT_SMR.1.1/PACE in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by 5) to 8). This extension does not conflict with the strict conformance to PACE PP.

Application note:
The SFR FMT_LIM.1 and FMT_LIM.2 address the management of the TSF and TSF data to prevent misuse of test features of the TOE over the life-cycle phases.

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

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:
1. Initialization,
2. Pre-personalization,
3. Personalization,

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

4. Configuration.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced:

<Deploying test features after TOE delivery do not allow>

1. User Data to be manipulated and disclosed,
2. TSF data to be disclosed or manipulated,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capailability

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:

<Deploying Test Features after TOE Delivery does not allow:>

1. User Data to be manipulated and disclosed,
2. TSF data to be disclosed or manipulated
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. sensitive User Data (EF.DG3 and EF.DG4) to be disclosed.

Application note:

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

The formulation of "Deploying Test Features …" in FMT_LIM.2.1 might be a little bit misleading since the addressed features are no longer available (e.g. by disabling or removing the respective functionality). Nevertheless the combination of FMT_LIM.1 and FMT_LIM.2 is introduced to provide an optional approach to enforce the same policy.
Note that the term "software" in item 4 of FMT_LIM.1.1 and FMT_LIM.2.1 refers to both IC Dedicated and IC Embedded Software.

Application note:
The following SFR are iterations of the component Management of TSF data (FMT_MTD.1). The TSF data include but are not limited to those identified below.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below (Common Criteria Part 2). The iterations address different management functions and different TSF data.

FMT_MTD.1/CVCA_INI Management of TSF data - Initialization of CVCA Certificate and Current Date

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ CVCA_INI

The TSF shall restrict the ability to *<write>* the
1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date,
4. *<none>*

To *<the Personalization Agent>*.

Application note:
The ST writer shall perform the missing operation in the component FMT_MTD.1.1/CVCA_INI. The initial Country Verifying Certification Authority Public Key may be written by the Personalisation Agent (cf. [EAC]). The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FMT_MTD.1/CVCA_UPD Management of TSF data - Country Verifying Certification Authority

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/ CVCA_UPD

The TSF shall restrict the ability to *<update>* the
1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate

to Country Verifying Certification Authority

Application note:
The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf. [EAC]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3) is provided by the terminal (cf. [EAC]).

FMT_MTD.1/DATE Management of TSF data - Current date

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1/DATE

The TSF shall restrict the ability to <modify> the *<Current date>* to
1.Country Verifying Certification Authority,
2.Document Verifier,
3.Domestic Extended Inspection System.

Application note:
The authorized roles are identified in their certificate (cf. [EAC]) and authorized by validation of the certificate chain (cf. FMT_MTD.3). The authorized role of the terminal is part of the Certificate Holder Authorization in the card verifiable certificate provided by the terminal for the identification and the Terminal Authentication v.1 (cf. to [EAC]).

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FMT_MTD.1/CAPK Management of TSF data - Chip Authentication Private Key

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/CAPK The TSF shall restrict the ability to < load> the <*Chip Authentication Private Key* > to *<the Personalization Agent>*.

Application note:

The verb "load" means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory.

FMT_MTD.1/ KEY_READ Management of TSF data - Key Read

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1/ KEY_READ The TSF shall restrict the ability to <read> the

1.PACE passwords ,

2.Chip Authentication Private Key,

3.Personalisation Agent Keys

to none.

The TOE shall meet the requirement "Secure TSF data (FMT_MTD.3)" as specified below (Common Criteria Part 2):

FMT_MTD.1/INI_ENA Management of TSF data - Writing Initialisation and Pre-personalisation Data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1

FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FMT_MTD.1.1/INI_ENA The TSF shall restrict the ability to write the Initialisation Data and Pre-personalisation Data to the Manufacturer.

Application note:
Manufacturer means integrated circuit and the travel document Manufacturer completing the IC to the travel document. The Manufacturer is the default user of the TOE during the manufacturing life cycle phase . The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
This entity is commensurate with 'Manufacturer' in [BAC-PP-0055].

FMT_MTD.1/INI_DIS Management of TSF data - Reading and Using Initialisation and Pre-personalisation Data

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

FMT_MTD.1.1/INI_DIS The TSF shall restrict the ability to read out the Initialisation Data and the Pre-personalisation Data to the Personalisation Agent.

Application note:
The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

FMT_MTD.1/PA Management of TSF data - Personalisation Agent

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions: fulfilled by FMT_SMF.1
FMT_SMR.1 Security roles: fulfilled by FMT_SMR.1/PACE

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FMT_MTD.1.1/PA The TSF shall restrict the ability to write the Document Security Object (SO_D) to the Personalisation Agent.

Application note:
By writing SOD into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

FMT_MTD.3 Secure TSF data

Hierarchical to: No other components.
Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1/ The TSF shall ensure that only secure values of the certificate chain are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control.

Refinement:
The certificate chain is valid if and only if

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,**
3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE**.

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

Application note:
The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE and FIA_UAU.5/PACE. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM..

6.1.7. Class FPT Protection of the Security Functions

The TOE shall prevent inherent and forced illicit information leakage for User Data and TSF Data. The security functional requirement FPT_EMS.1 addresses the inherent leakage. The SFRs "Limited capabilities (FMT_LIM.1)", "Limited availability (FMT_LIM.2)" together with the SAR "Security architecture description" (ADV_ARC.1) prevent bypassing, deactivation and manipulation of the security features or misuse of TOE functions.

The TOE shall meet the requirement "TOE Emanation (FPT_EMS.1)" as specified below (Common Criteria Part 2 extended):

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.
Dependencies: No Dependencies

FPT_EMS.1.1 The TOE shall not emit *<Power consumption of IC chip>* in excess of *<unnecessary information>* enabling access to

1. Chip Authentication Session Keys
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem SK_{PICC}-PACE,
4. *<Transport key>*[17],
5. Personalisation Agent Key(s),

[17] For delivery to Personalization Agent safely, Transport key is stored during pre-personalization by Manufacturer. It is used to protect TOE from being abused without authentication of Personalization Agent

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

6. Chip Authentication Private Key and
7. *<EF.DG3, EF.DG4>*

FPT_EMS.1.2 The TSF shall ensure any users are unable to use the following interface smart card circuit contacts to gain access to

1. Chip Authentication Session Keys
2. PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem SK_{PICC}-PACE,
4. *<Transport key>*,
5. Personalisation Agent Key(s) and
6. Chip Authentication Private Key and
7. *<EF.DG3, EF.DG4>*.

Application note:
The SFR FPT_EMS.1.1 in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2 in the current ST covers the definition in PACE PP [PACE-PP-0068] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to PACE PP.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.
Dependencies: No Dependencies

FPT_FLS.1 The TSF shall preserve a secure state when the following types of failures occur:

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1,
3. *<none>*.

FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No Dependencies

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FPT_TST.1.1 The TSF shall run a suite of self tests < during initial start-up , *at reset*> to demonstrate the correct operation of the TSF.

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

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

Application note:
If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorised user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3 may be executed during initial start-up by the 'authorised user' Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1 in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.
Dependencies: No Dependencies

FPT_TST.1.1 The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Application note:
The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

6.2. Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL5 augmented by the following components:

- ALC_DVS.2 (Sufficiency of security measures),
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

The following table provides an overview for security functional requirements coverage (SFRs from PACE PP [PACE-PP-0068] are marked in italic letters and SFRs from PACE PP [PACE-PP-0068] which are extended in EAC PP are marked in bold letters)

	OT.Sens_Data_Conf	OT.Chip_Auth_Proof	OT.AC_PersAccess	OT.Data_Integrity	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Tracing	OT.Prot_Phys-Tamper	OT.Prot_Malfuntion
FAU_SAS.1			X				X					
FCS_CKM.1/DH_PACE				X	X	X						
FCS_CKM.1/CA	X	X	X	X	X	X						
FCS_CKM.4	X		X	X	X	X						
FCS_COP.1/PACE_ENC						X						
FCS_COP.1/CA_ENC	X	X	X	X		X						
FCS_COP.1/PACE_MAC				X	X							
FCS_COP.1/CA_MAC	X	X	X	X								
FCS_COP.1/SIG_VER	X		X									
FCS_RND.1	X		X	X	X	X						
FIA_AFL.1/PACE										X		
FIA_UID.1/PACE	X		X	X	X	X						
FIA_UAU.1/PACE	X		X	X	X	X						
FIA_UAU.4/PACE	X		X	X	X	X						
FIA_UAU.5/PACE	X		X	X	X	X						
FIA_UAU.6/PACE				X	X	X						
FIA_UAU.6/EAC	X		X	X	X	X						
FIA_API.1		X										
FDP_ACC.1/TRM	X		X	X		X						
FDP_ACF.1/TRM	X		X	X		X						

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FDP_RIP.1				X	X	X						
FDP_UCT.1/TRM	X			X		X						
FDP_UIT.1/TRM				X		X						
FMT_SMF.1		X	X	X	X	X	X					
FMT_SMR.1/PACE		X	X	X	X	X	X					
FMT_LIM.1								X				
FMT_LIM.2								X				
FMT_MTD.1/INI_ENA			X				X					
FMT_MTD.1/INI_DIS			X				X					
FMT_MTD.1/CVCA_INI	X											
FMT_MTD.1/CVCA_UPD	X											
FMT_MTD.1/DATE	X											
FMT_MTD.1/CAPK	X	X		X								
FMT_MTD.1/PA			X	X	X	X						
FMT_MTD.1/KEY_READ	X	X	X	X	X	X						
FMT_MTD.3	X											
FPT_EMS.1			X						X			
FPT_TST.1									X			X
FPT_FLS.1									X			X
FPT_PHP.3				X					X		X	
FTP_ITC.1/PACE				X	X	X				X		

Coverage of Security Objective for the TOE by SFR

The security objective **OT.Identification** "Identification of the TOE" addresses the storage of Initialisation and Pre-Personalisation Data in its non-volatile memory, whereby they also include the IC Identification Data uniquely identifying the TOE's chip. This will be ensured by TSF according to SFR FAU_SAS.1. The SFR FMT_MTD.1/INI_ENA allows only the Manufacturer to write Initialisation and Pre-personalisation Data (including the Personalisation Agent key). The SFR FMT_MTD.1/INI_DIS requires the Personalisation Agent to disable access to Initialisation and Pre-personalisation Data in the life cycle phase 'operational use'. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.AC_Pers** "Access Control for Personalisation of logical travel document" addresses the access control of the writing the logical travel document. The justification for the SFRs FAU_SAS.1, FMT_MTD.1/INI_ENA and FMT_MTD.1/INI_DIS arises from the justification for OT.Identification above with respect to the Pre-personalisation Data. The write access to the logical travel document data are defined by the SFR FIA_UID.1/PACE, FIA_UAU.1/PACE, FDP_ACC.1/TRM and FDP_ACF.1/TRM in the same way: only the successfully authenticated Personalisation Agent is allowed to write the data of the groups EF.DG1 to EF.DG16 of the logical travel document only once. FMT_MTD.1/PA covers the related property of OT.AC_Pers (writing SO_D and, in generally,

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

personalisation data). The SFR FMT_SMR.1/PACE lists the roles (including Personalisation Agent) and the SFR FMT_SMF.1 lists the TSF management functions (including Personalisation). The SFRs FMT_MTD.1./KEY_READ and FPT_EMS.1 restrict the access to the Personalisation Agent Keys and the Chip Authentication Private Key.

The authentication of the terminal as Personalisation Agent shall be performed by TSF according to SFR FIA_UAU.4/PACE and FIA_UAU.5/PACE. If the Personalisation Terminal want to authenticate itself to the TOE by means of the Terminal Authentication Protocol v.1 (after Chip Authentication v.1) with the Personalisation Agent Keys the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge), FCS_CKM.1/CA (for the derivation of the new session keys after Chip Authentication v.1), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging), FCS_COP.1/SIG_VER (as part of the Terminal Authentication Protocol v.1) and FIA_UAU.6/EAC (for the re-authentication. If the Personalisation Terminal wants to authenticate itself to the TOE by means of the Authentication Mechanism with Personalisation Agent Key the TOE will use TSF according to the FCS_RND.1 (for the generation of the challenge) and FCS_COP.1/CA_ENC (to verify the authentication attempt). The session keys are destroyed according to FCS_CKM.4 after use.

The security objective **OT.Data_Integrity** "Integrity of personal data" requires the TOE to protect the integrity of the logical travel document stored on the travel document's chip against physical manipulation and unauthorized writing. Physical manipulation is addressed by FPT_PHP.3. Logical manipulation of stored user data is addressed by (FDP_ACC.1/TRM, FDP_ACF.1/TRM): only the Personalisation Agent is allowed to write the data in EF.DG1 to EF.DG16 of the logical travel document (FDP_ACF.1.2/TRM, rule 1) and terminals are not allowed to modify any of the data in EF.DG1 to EF.DG16 of the logical travel document (cf. FDP_ACF.1.4/TRM). FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The Personalisation Agent must identify and authenticate themselves according to FIA_UID.1/PACE and FIA_UAU.1/PACE before accessing these data. FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_SMR.1/PACE lists the roles and the SFR FMT_SMF.1 lists the TSF management functions.

Unauthorised modifying of the exchanged data is addressed, in the first line, by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. For PACE secured data exchange, a

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

prerequisite for establishing this trusted channel is a successful PACE Authentication (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. The trusted channel is established using PACE, Chip Authentication v.1, and Terminal Authentication v.1. FDP_RIP.1 requires erasing the values of session keys (here: for K_{MAC}).
The TOE supports the inspection system detect any modification of the transmitted logical travel document data after Chip Authentication v.1. The SFR FIA_UAU.6/EAC and FDP_UIT.1/TRM requires the integrity protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use.

The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards. The SFR FCS_RND.1 represents a general support for cryptographic operations needed.

The security objective **OT.Data_Authenticity** aims ensuring authenticity of the User- and TSF data (after the PACE Authentication) by enabling its verification at the terminal-side and by an active verification by the TOE itself. This objective is mainly achieved by FTP_ITC.1/PACE using FCS_COP.1/PACE_MAC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for KMAC). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used. The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered as trustworthy. The SFR FCS_RND.1 represents a general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Data_Confidentiality** aims that the TOE always ensures confidentiality of the User- and TSF-data stored and, after the PACE Authentication resp.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Chip Authentication, of these data exchanged. This objective for the data stored is mainly achieved by (FDP_ACC.1/TRM, FDP_ACF.1/TRM). FIA_UAU.4/PACE, FIA_UAU.5/PACE and FCS_CKM.4 represent some required specific properties of the protocols used.

This objective for the data exchanged is mainly achieved by FDP_UCT.1/TRM, FDP_UIT.1/TRM and FTP_ITC.1/PACE using FCS_COP.1/PACE_ENC resp. FCS_COP.1/CA_ENC. A prerequisite for establishing this trusted channel is a successful PACE or Chip and Terminal Authentication v.1 (FIA_UID.1/PACE, FIA_UAU.1/PACE) using FCS_CKM.1/DH_PACE resp. FCS_CKM.1/CA and possessing the special properties FIA_UAU.5/PACE, FIA_UAU.6/PACE resp. FIA_UAU.6/EAC. FDP_RIP.1 requires erasing the values of session keys (here: for Kenc). The SFR FMT_MTD.1./KEY_READ restricts the access to the PACE passwords and the Chip Authentication Private Key. FMT_MTD.1/PA requires that SO_D containing signature over the User Data stored on the TOE and used for the Passive Authentication is allowed to be written by the Personalisation Agent only and, hence, is to be considered trustworthy .The SFR FCS_RND.1 represents the general support for cryptographic operations needed. The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Sense_Data_Conf** "Confidentiality of sensitive biometric reference data" is enforced by the Access Control SFP defined in FDP_ACC.1/TRM and FDP_ACF.1/TRM allowing the data of EF.DG3 and EF.DG4 only to be read by successfully authenticated Extended Inspection System being authorized by a valid certificate according FCS_COP.1/SIG_VER.

The SFRs FIA_UID.1/PACE and FIA_UAU.1/PACE require the identification and authentication of the inspection systems. The SFR FIA_UAU.5/PACE requires the successful Chip Authentication (CA) v.1 before any authentication attempt as Extended Inspection System. During the protected communication following the CA v.1 the reuse of authentication data is prevented by FIA_UAU.4/PACE. The SFR FIA_UAU.6/EAC and FDP_UCT.1/TRM requires the confidentiality protection of the transmitted data after Chip Authentication v.1 by means of secure messaging implemented by the cryptographic functions according to FCS_RND.1 (for the generation of the terminal authentication challenge), FCS_CKM.1/CA (for the generation of shared secret and for the derivation of the new session keys), and FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC for the ENC_MAC_Mode secure messaging. The session keys are destroyed according to FCS_CKM.4 after use. The SFR FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ requires that the Chip Authentication Key cannot be written unauthorized or read afterwards.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

To allow a verification of the certificate chain as in FMT_MTD.3 the CVCA's public key and certificate as well as the current date are written or update by authorized identified role as of FMT_MTD.1/CVCA_INI, FMT_MTD.1/CVCA_UPD and FMT_MTD.1/DATE.

The security objective **OT.Chip_Auth_Proof** "Proof of travel document's chip authenticity" is ensured by the Chip Authentication Protocol v.1 provided by FIA_API.1 proving the identity of the TOE. The Chip Authentication Protocol v.1 defined by FCS_CKM.1/CA is performed using a TOE internally stored confidential private key as required by FMT_MTD.1/CAPK and FMT_MTD.1/KEY_READ. The Chip Authentication Protocol v.1 [EAC] requires additional TSF according to FCS_CKM.1/CA (for the derivation of the session keys), FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC (for the ENC_MAC_Mode secure messaging).The SFRs FMT_SMF.1 and FMT_SMR.1/PACE support the functions and roles related.

The security objective **OT.Prot_Abuse-Func** "Protection against Abuse of Functionality" is ensured by the SFR FMT_LIM.1 and FMT_LIM.2 which prevent misuse of test functionality of the TOE or other features which may not be used after TOE Delivery.

The security objective **OT.Prot_Inf_Leak** "Protection against Information Leakage" requires the TOE to protect confidential TSF data stored and/or processed in the travel document's chip against disclosure

- by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines which is addressed by the SFR FPT_EMS.1,
- by forcing a malfunction of the TOE which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or
- by a physical manipulation of the TOE which is addressed by the SFR FPT_PHP.3.

The security objective **OT.Tracing** aims that the TOE prevents gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless interface of the TOE without a priori knowledge of the correct values of shared passwords (CAN, MRZ).This objective is achieved as follows:(i) while establishing PACE communication with CAN or MRZ (non-blocking authorisation data) . by FIA_AFL.1/PACE;(ii) for listening to PACE communication

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

(is of importance for the current PP, since SO_D is card-individual) . FTP_ITC.1/PACE.

The security objective **OT.Prot_Phys-Tamper** "Protection against Physical Tampering" is covered by the SFR FPT_PHP.3.

The security objective **OT.Prot_Malfunction** "Protection against Malfunctions" is covered by (i) the SFR FPT_TST.1 which requires self tests to demonstrate the correct operation and tests of authorized users to verify the integrity of TSF data and TSF code, and (ii) the SFR FPT_FLS.1 which requires a secure state in case of detected failure or operating conditions possibly causing a malfunction.

6.3.2. Dependency Rationale

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained

The following Table shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FCS_CKM.1/CA	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	justification 1 for non-satisfied dependencies Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC, Fulfilled by FCS_CKM.4
FCS_CKM.1/DH_PACE	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction:	Fulfilled by FCS_COP.1/CA_ENC, and FCS_COP.1/CA_MAC, Fulfilled by FCS_CKM.4
FCS_CKM.4	[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]	Fulfilled by FCS_CKM.1/DH_PACE and FCS_CKM.1/CA
FCS_COP.1/CA_ENC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key	Fulfilled by FCS_CKM.1/CA,

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.4
FCS_COP.1/CA_MAC	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA Fulfilled by FCS_CKM.4
FCS_COP.1/PACE_ENC	[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.	fulfilled by FCS_CKM.1/DH_PACE fulfilled by FCS_CKM.4
FCS_COP.1/PACE_MAC	[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.	fulfilled by FCS_CKM.1/DH_PACE fulfilled by FCS_CKM.4
FCS_COP.1/SIG_VER	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/CA, Fulfilled by FCS_CKM.4
FCS_COP.1/HASH	[FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	F Fulfilled by FCS_CKM.4
FCS_RND.1	No dependencies	n.a
FIA_UID.1/PACE	No dependencies	n.a.
FIA_UAU.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FIA_UAU.4/PACE	No dependencies	n.a.
FIA_UAU.5/PACE	No dependencies	n.a.
FIA_UAU.6/EAC	No dependencies	n.a.
FIA_API.1	No dependencies	n.a.
FIA_AFL.1	FIA_UAU.1 Timing of authentication	fulfilled by FIA_UAU.1/PACE
FDP_ACC.1/TRM	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1/TRM
FDP_ACF.1/TRM	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute	Fulfilled by FDP_ACC.1/TRM, justification 2 for non-satisfied

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	initialization	dependencies
FDP_RIP.1	No dependencies	n.a.
FDP_UCT.1/TRM	[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]	Fulfilled by FTP_ITC.1/PACE Fulfilled by FDP_ACC.1/TRM
FDP_UIT.1/TRM	[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]	Fulfilled by FTP ITC.1/PACE Fulfilled by FDP ACC.1/TRM
FTP_ITC.1/PACE	No dependencies	n.a.
FAU_SAS.1	No dependencies	n.a.
FMT_SMR.1/PACE	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.1/PACE
FMT_LIM.1	FMT_LIM.2	Fulfilled by FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	Fulfilled by FMT_LIM.1
FMT_MTD.1/CVCA_INI	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CVCA_UPD	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/DATE	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/CAPK	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/KEY_READ	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_ENA	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/INI_DIS	FMT_SMF.1 Specification of management functions, FMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.1/ PA	FMT_SMF.1 Specification of management functionsFMT_SMR.1 Security roles	Fulfilled by FMT_SMF.1 Fulfilled by FMT_SMR.1/PACE
FMT_MTD.3	FMT_MTD.1	Fulfilled by FMT_MTD.1/CVCA_INI and FMT_MTD.1/CVCA_UPD
FPT_EMS.1	No dependencies	n.a.
FPT_FLS.1	No dependencies	n.a.
FPT_TST.1	No dependencies	n.a.
FPT_PHP.3	No dependencies	n.a.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

FPT_EMS.1	No dependencies	n.a.

Dependencies between the SFR for the TOE

Justification for non-satisfied dependencies between the SFR for TOE:

No.1 : Because a Diffie-Hellman key agreement has no key distribution function, it has not support of dependency in case FCS CKM.2

No. 2: The access control TSF according to FDP_ACF.1/TRM uses security attributes which are defined during the personalisation and are fixed over the whole life time of the TOE. No management of these security attribute (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.

6.3.3. Security Assurance Requirements Rationale

The EAL5 was chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL5 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL5 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the travel document's development and manufacturing especially for the secure handling of the travel document's material.

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the security objectives OT.Sens_Data_Conf and OT.Chip_Auth_Proof.

The component ALC_DVS.2 has no dependencies.

The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Security architecture description

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures

All of these are met or exceeded in the EAL5 assurance package.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

7. TOE Summary Specification.

7.1. TOE security functions by the software

SF	Description
SF_READ_ACC	Data access control
SF_AUTH	Authentication
SF_SM	Data Secure Messaging
SF_WIRTE_MGT	Card Write Management
SF_EAC_TA	Extended Access Control
SF_CRYPTO	Cryptographic operation
SF_PROTECTION	Counter Measure by IC Chip

TOE security function

7.2. TOE security functions by IC Chip

7.2.1. IC chip SFR

SF	Description
SF_DPM	Device phase management
SF_PS	Protection against snooping
SF_PMA	Protection against modifying attacks
SF_PLA	Protection against logical attacks
SF_CS	Cryptographic support (3DES, AES, RSA, EC, SHA-2,TRNG)

Security Function provided by IC Chip

These SF are described in [ICST]

SF_DPM

:Device Phase Management

The life cycle of the IC chip TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from IC chip TOE point of view. These phases are implemented in the IC chip TOE as test mode (phase 3) and user mode (phase 4-7). In addition a chip identification mode exists which is active in all phases. The chip identification data (O.Identification) is stored in a in the not

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

changeable configuration page area and non-volatile memory. In the same area further IC chip TOE configuration data is stored. In addition, user initialization data can be stored in the non-volatile memory during the production phase as well. During this first data programming, the TOE is still in the secure environment and in Test Mode.

SF_PS

:Protection against Snooping

All contents of all memories of the IC chip TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. There is no plain data on the chip. In addition the data transferred over the busses, the SFRs and the peripheral devices (CRC, RNG and Timer) are encrypted as well.

The memory content and bus encryption is done by the MED using a complex key management and by the memories, RAM, CACHE and the bus are entirely encrypted.

Therefore, no data in plain are handled anywhere on the IC chip and thus also the two CPUs compute entirely masked. The symmetric cryptographic co-processor is entirely masked as well.

SF_PMA

: Protection against Modifying Attacks

The IC chip TOE is equipped with an error detection code (EDC) which covers the memory system of RAM, ROM and EEPROM and includes also the MED, MMU and the bus system. Thus introduced failures are detected and in certain errors are also automatically corrected. In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM an EDC value is calculated.

SF_PLA

: Protection against Logical Attacks

The memory access control of the IC chip TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of the privileged levels and gives the software the possibility to define different access rights. The address permissions of the privilege levels are controlled by the MMU. In case of an access violation the MMU will trigger a reset and then a trap service routine can react on the access violation. The policy of setting up the MMU and specifying the memory ranges, to a certain extend, for the privilege levels . with the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

exception of the IFX level - is defined from the user software (OS).

SF_CS

: Cryptographic Support

The IC chip TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations. This security function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function respectively mathematic algorithm itself is not used from the IC chip TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a co-processor supporting the DES and AES algorithms and a combination of a co-processor and software modules to support RSA cryptography, RSA key generation, ECDSA signature generation and verification, ECDH key agreement and EC public key calculation and public key testing.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

8. Glossary and Acronyms

Term	Definition
Accurate Terminal Certificate	A Terminal Certificate is accurate, if the issuing Document Verifier is trusted by the travel document's chip to produce Terminal Certificates with the correct certificate effective date, see [EAC].
Advanced Inspection Procedure (with PACE)	A specific order of authentication steps between a travel document and a terminal as required by [SAC], namely (i) PACE, (ii) Chip Authentication v.1, (iii) Passive Authentication with SO_D and (iv) Terminal Authentication v.1. AIP can generally be used by EIS-AIP-PACE.
Agreement	This term is used in the current PP in order to reflect an appropriate relationship between the parties involved, but not as a legal notion.
Active Authentication	Security mechanism defined in [MRTD] option by which means the travel document's chip proves and the inspection system verifies the identity and authenticity of the travel document's chip as part of a genuine travel document issued by a known State of Organisation.
Application note	Optional informative part of the PP containing sensitive supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.
Audit records	Write-only-once non-volatile memory area of the travel document's chip to store the Initialization Data and Pre-personalisation Data.
Authenticity	Ability to confirm the travel document and its data elements on the travel document's chip were created by the issuing State or Organisation
Basic Access Control (BAC)	Security mechanism defined in [MRTD] by which means the travel document's chip proves and the inspection system protects their communication by means of secure messaging with Document Basic Access Keys (see there).
Basic Inspection System with PACE protocol (BIS-PACE)	A technical system being used by an inspecting authority and operated by a governmental organisation (i.e. an Official Domestic or Foreign Document Verifier) and verifying the travel document presenter as the travel document holder (for ePassport: by comparing the real biometric data (face) of the travel document presenter with the stored biometric data (DG2) of the travel document holder).

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	The Basic Inspection System with PACE is a PACE Terminal additionally supporting/applying the Passive Authentication protocol and is authorised by the travel document Issuer through the Document Verifier of receiving state to read a subset of data stored on the travel document.
Basic Inspection System (BIS)	An inspection system which implements the terminals part of the Basic Access Control Mechanism and authenticates itself to the travel document's chip using the Document Basic Access Keys derived from the printed MRZ data for reading the logical travel document.
(biodata).	The personalised details of the travel document holder of the document appearing as text in the visual and machine readable zones on the biographical data page of a travel document. [MRTD]
Biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) digital portrait and (ii) optional biometric reference data.
Card Access Number (CAN)	Password derived from a short number printed on the front side of the data-page.
Certificate chain	A sequence defining a hierarchy certificates. The Inspection System Certificate is the lowest level, Document Verifier Certificate in between, and Country Verifying Certification Authority Certificates are on the highest level. A certificate of a lower level is signed with the private key corresponding to the public key in the certificate of the next higher level.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means. [MRTD]
Country Signing CA Certificate (C_{CSCA})	Certificate of the Country Signing Certification Authority Public Key (K_{PuCSCA}) issued by Country Signing Certification Authority stored in the inspection system.
Country Signing Certification Authority (CSCA)	An organisation enforcing the policy of the travel document Issuer with respect to confirming correctness of user and TSF data stored in the travel document. The CSCA represents the country specific root of the PKI for the travel documents and creates the Document Signer Certificates within this PKI. The CSCA also issues the self-signed CSCA Certificate (C_{CSCA}) having to be distributed by strictly secure diplomatic means, see. [MRTD], 5.5.1. The Country Signing Certification Authority issuing certificates for

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	Document Signers (cf. [MRTD]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EAC].
Country Verifying Certification Authority (CVCA)	An organisation enforcing the privacy policy of the travel document Issuer with respect to protection of user data stored in the travel document (at a trial of a terminal to get an access to these data). The CVCA represents the country specific root of the PKI for the terminals using it and creates the Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed in form of CVCA Link-Certificates, see [EAC]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a CVCS as a subject; hence, it merely represents an organizational entity within this PP. The Country Signing Certification Authority (CSCA) issuing certificates for Document Signers (cf. [MRTD]) and the domestic CVCA may be integrated into a single entity, e.g. a Country Certification Authority. However, even in this case, separate key pairs must be used for different roles, see [EAC].
Current date	The maximum of the effective dates of valid CVCA, DV and domestic Inspection System certificates known to the TOE. It is used the validate card verifiable certificates.
CV Certificate	Card Verifiable Certificate according to [EAC].
CVCA link Certificate	Certificate of the new public key of the Country Verifying Certification Authority signed with the old public key of the Country Verifying Certification Authority where the certificate effective date for the new key is before the certificate expiration date of the certificate for the old key.
Document Basic Access Key Derivation Algorithm	The [MRTD] describes the Document Basic Access Key Derivation Algorithm on how terminals may derive the Document Basic Access Keys from the second line of the printed MRZ data.
PACE passwords	Passwords used as input for PACE. This may either be the CAN or the SHA-1-value of the concatenation of Serial Number, Date of Birth and Date of Expiry as read from the MRZ, see [SAC],
Document Details Data	Data printed on and electronically stored in the travel document

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	representing the document details like document type, issuing state, document number, date of issue, date of expiry, issuing authority. The document details data are less-sensitive data.
Document Security Object (SO_D)	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hash values of the LDS Data Groups. It is stored in the travel document's chip. It may carry the Document Signer Certificate (C_{DS}). [MRTD]
Document Signer (DS)	An organisation enforcing the policy of the CSCA and signing the Document Security Object stored on the travel document for passive authentication. A Document Signer is authorised by the national CSCA issuing the Document Signer Certificate (C_{DS}), see [EAC]and [MRTD]. This role is usually delegated to a Personalisation Agent.
Document Verifier (DV)	An organisation enforcing the policies of the CVCA and of a Service Provider (here: of a governmental organisation / inspection authority) and managing terminals belonging together (e.g. terminals operated by a State's border police), by – inter alia – issuing Terminal Certificates. A Document Verifier is therefore a Certification Authority, authorised by at least the national CVCA to issue certificates for national terminals, see [EAC]. Since the Standard Inspection Procedure does not imply any certificate-based terminal authentication, the current TOE cannot recognise a DV as a subject; hence, it merely represents an organisational entity within this PP. There can be Domestic and Foreign DV: A domestic DV is acting under the policy of the domestic CVCA being run by the travel document Issuer; a foreign DV is acting under a policy of the respective foreign CVCA (in this case there shall be an appropriate agreement between the travel document Issuer und a foreign CVCA ensuring enforcing the travel document Issuer's privacy policy).
Eavesdropper	A threat agent with high attack potential reading the communication between the travel document's chip and the inspection system to gain the data on the travel document's chip.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity. [MRTD]
Travel document	The contact based or contactless smart card integrated into the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

(electronic)	plastic or paper, optical readable cover and providing the following application: ePassport.
ePassport application	A part of the TOE containing the non-executable, related user data (incl. biometric) as well as the data needed for authentication (incl. MRZ); this application is intended to be used by authorities, amongst other as a machine readable travel document (MRTD). See [EAC].
Extended Access Control	Security mechanism identified in [MRTD] by which means the travel document's chip (i) verifies the authentication of the inspection systems authorized to read the optional biometric reference data, (ii) controls the access to the optional biometric reference data and (iii) protects the confidentiality and integrity of the optional biometric reference data during their transmission to the inspection system by secure messaging.
Extended Inspection	A role of a terminal as part of an inspection system which is in addition
System (EIS)	to Basic Inspection System authorized by the issuing State or Organisation to read the optional biometric reference data and supports the terminals part of the Extended Access Control Authentication Mechanism.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait. [MRTD]
Global Interoperability	The capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine readable data in all travel documents. [MRTD]
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
IC Identification Data	The IC manufacturer writes a unique IC identifier to the chip to control the IC as travel document material during the IC manufacturing and the delivery process to the travel document manufacturer.
Impostor	A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his or her physical appearance to represent himself or herself as another person for the purpose of using that person's document. [MRTD]
Improperly documented person	A person who travels, or attempts to travel with: (a) an expired travel document or an invalid visa; (b) a counterfeit, forged or altered travel document or visa; (c) someone else's travel document or visa; or (d) no travel document or visa, if required. [MRTD]
Initialisation	Process of writing Initialisation Data (see below) to the TOE (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 3).
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 2). These data are for instance used for traceability and for IC identification as travel document's material (IC identification data).
Inspection	The act of a State examining an travel document presented to it by a traveller (the travel document holder) and verifying its authenticity. [MRTD]
Inspection system (IS)	A technical system used by the border control officer of the receiving State (i) examining an travel document presented by the traveller and verifying its authenticity and (ii) verifying the traveller as travel document holder.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. The travel document's chip is an integrated circuit.
Integrity	Ability to confirm the travel document and its data elements on the travel document's chip have not been altered from that created by

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	the issuing State or Organisation
Issuing Organisation	Organisation authorized to issue an official travel document (e.g. the United Nations Organization, issuer of the Laissez-passer). [MRTD]
Issuing State	The Country issuing the travel document. [MRTD]
Logical Data Structure (LDS)	The collection of groupings of Data Elements stored in the optional capacity expansion technology [MRTD]. The capacity expansion technology used is the travel document's chip.
Logical travel document	Data of the travel document holder stored according to the Logical Data Structure [MRTD] as specified by ICAO on the contact based/contactless integrated circuit. It presents contact based/contactless readable data including (but not limited to) 1.personal data of the travel document holder 2.the digital Machine Readable Zone Data (digital MRZ data, EF.DG1), 3.the digitized portraits (EF.DG2), 4.the biometric reference data of finger(s) (EF.DG3) or iris image(s) (EF.DG4) or both and 5.the other data according to LDS (EF.DG5 to EF.DG16). 6.EF.COM and EF.SOD
Machine readable travel document (MRTD)	Official document issued by a State or Organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read. [MRTD]
Machine readable zone (MRZ)	Fixed dimensional area located on the front of the travel document or MRP Data Page or, in the case of the TD1, the back of the travel document, containing mandatory and optional data for machine reading using OCR methods. [MRTD] The MRZ-Password is a restricted-revealable secret that is derived from the machine readable zone and may be used for PACE.
Machine-verifiable biometrics feature	A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine. [MRTD]
Manufacturer	Generic term for the IC Manufacturer producing integrated circuit and the travel document Manufacturer completing the IC to the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	travel document. The Manufacturer is the default user of the TOE during the manufacturing life phase. The TOE itself does not distinguish between the IC Manufacturer and travel document Manufacturer using this role Manufacturer.
Metadata of a CV Certificate	Data within the certificate body (excepting Public Key) as described in [EAC]. The metadata of a CV certificate comprise the following elements: - Certificate Profile Identifier, - Certificate Authority Reference, - Certificate Holder Reference, - Certificate Holder Authorisation Template, - Certificate Effective Date, - Certificate Expiration Date.
ePassport application	Non-executable data defining the functionality of the operating system on the IC as the travel document's chip. It includes •the file structure implementing the LDS [MRTD], •the definition of the User Data, but does not include the User Data itself (i.e. content of EF.DG1 to EF.DG13, EF.DG16, EF.COM and EF.SOD) and •the TSF Data including the definition the authentication data but except the authentication data itself.
Optional biometric reference data	Data stored for biometric authentication of the travel document holder in the travel document's chip as (i) encoded finger image(s) (EF.DG3) or (ii) encoded iris image(s) (EF.DG4) or (iii) both. Note, that the European commission decided to use only fingerprint and not to use iris images as optional biometric reference data.
Passive authentication	(i) verification of the digital signature of the Document Security Object and (ii) comparing the hash values of the read LDS data fields with the hash values contained in the Document Security Object.
Password Authenticated Connection Establishment (PACE)	A communication establishment protocol defined in [SAC],. The PACE Protocol is a password authenticated Diffie-Hellman key agreement protocol providing implicit password-based authentication of the communication partners (e.g. smart card and the terminal connected): i.e. PACE provides a verification, whether the

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	communication partners share the same value of a password π). Based on this authentication, PACE also provides a secure communication, whereby confidentiality and authenticity of data transferred within this communication channel are maintained.
PACE Password	A password needed for PACE authentication, e.g. CAN or MRZ.
Personalisation	The process by which the Personalisation Data are stored in and unambiguously, inseparably associated with the travel document. This may also include the optional biometric data collected during the "Enrolment" (cf. sec. 1.2, TOE life-cycle, Phase 3, Step 6).
Personalisation Agent	An organisation acting on behalf of the travel document Issuer to personalise the travel document for the travel document holder by some or all of the following activities: (i)establishing the identity of the travel document holder for the biographic data in the travel document, (ii)enrolling the biometric reference data of the travel document holder, (iii)writing a subset of these data on the physical travel document (optical personalisation) and storing them in the travel document (electronic personalisation) for the travel document holder as defined in [EAC], (iv)writing the document details data, (v)writing the initial TSF data, (vi)signing the Document Security Object defined in [MRTD] (in the role of DS). Please note that the role 'Personalisation Agent' may be distributed among several institutions according to the operational policy of the travel document Issuer. Generating signature key pair(s) is not in the scope of the tasks of this role.
Personalisation Data	A set of data incl. (i)individual-related data (biographic and biometric data) of the travel document holder, (ii)dedicated document details data and (iii)dedicated initial TSF data (incl. the Document Security Object). Personalisation data are gathered and then written into the non-

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

	volatile memory of the TOE by the Personalisation Agent in the life-cycle phase card issuing
Personalisation Agent Authentication Information	TSF data used for authentication proof and verification of the Personalisation Agent.
Personalisation Agent Key	Cryptographic authentication key used (i) by the Personalisation Agent to prove his identity and to get access to the logical travel document and (ii) by the travel document's chip to verify the authentication attempt of a terminal as Personalisation Agent according to the SFR FIA_UAU.4/PACE, FIA_UAU.5/PACE and FIA_UAU.6/EAC.
Physical part of the travel document	Travel document in form of paper, plastic and chip using secure printing to present data including (but not limited to) 1.biographical data, 2.data of the machine-readable zone, 3.photographic image and 4.other data.
Pre-Personalisation	Process of writing Pre-Personalisation Data (see below) to the TOE including the creation of the travel document Application (cf. sec. 1.2, TOE life-cycle, Phase 2, Step 5)
Pre-personalisation Data	Any data that is injected into the non-volatile memory of the TOE by the travel document Manufacturer (Phase 2) for traceability of non-personalised travel document's and/or to secure shipment within or between life cycle phases 2 and 3. It contains (but is not limited to) the Personalisation Agent Key Pair.
Pre-personalised travel document's chip	travel document's chip equipped with a unique identifier.
Receiving State	The Country to which the traveller is applying for entry. [MRTD]
Reference data	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt.
RF-terminal	A device being able to establish communication with an RF-chip according to ISO/IEC 14443 [ISO14443].
Secondary image	A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means. [MRTD]
Secure messaging in encrypted/combined mode	Secure messaging using encryption and message authentication code according to ISO/IEC 7816-4 [ISO7816]

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Service Provider	An official organisation (inspection authority) providing inspection service which can be used by the travel document holder. Service Provider uses terminals (BIS-PACE) managed by a DV.
Skimming	Imitation of the inspection system to read the logical travel document or parts of it via the contactless communication channel of the TOE without knowledge of the printed MRZ data.
Standard Inspection Procedure	A specific order of authentication steps between an travel document and a terminal as required by [SAC], namely (i) PACE or BAC and (ii) Passive Authentication with SO_D. SIP can generally be used by BIS-PACE and BIS-BAC.
Terminal	A terminal is any technical system communicating with the TOE either through the contact based or contactless interface. A technical system verifying correspondence between the password stored in the travel document and the related value presented to the terminal by the travel document presenter.
In this PP the role 'Terminal' corresponds to any terminal being authenticated by the TOE.	Terminal may implement the terminal's part of the PACE protocol and thus authenticate itself to the travel document using a shared password (CAN or MRZ).
Terminal Authorization	Intersection of the Certificate Holder Authorizations defined by the Inspection System Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
Terminal Authorisation Level	Intersection of the Certificate Holder Authorisations defined by the Terminal Certificate, the Document Verifier Certificate and Country Verifying Certification Authority which shall be all valid for the Current Date.
TOE tracing data	Technical information about the current and previous locations of the travel document gathered by inconspicuous (for the travel document holder) recognising the travel document.
Travel document	Official document issued by a state or organisation which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary, intended for global use, reflecting essential data elements capable of being machine read; see [MRTD] (there "Machine readable travel document").

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Travel Document Holder	The rightful holder of the travel document for whom the issuing State or Organisation personalised the travel document.
Travel document's Chip	A contact based/contactless integrated circuit chip complying with ISO/IEC 14443 [ISO14443] and programmed according to the Logical Data Structure as specified by ICAO, [MRTD], sec III.
Travel document's Chip Embedded Software	Software embedded in a travel document's chip and not being developed by the IC Designer. The travel document's chip Embedded Software is designed in Phase 1 and embedded into the travel document's chip in Phase 2 of the TOE life-cycle.
Traveller	Person presenting the travel document to the inspection system and claiming the identity of the travel document holder.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
Unpersonalised travel document	The travel document that contains the travel document chip holding only Initialization Data and Pre-personalisation Data as delivered to the Personalisation Agent from the Manufacturer.
User data	All data (being not authentication data) (i) stored in the context of the ePassport application of the travel document as defined in [EAC] and (ii) being allowed to be read out solely by an authenticated terminal acting as Basic Inspection System with PACE . CC give the following generic definitions for user data: Data created by and for the user that does not affect the operation of the TSF (CC part 1 [CC]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC]).
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. [MRTD]
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved

Acronyms

Acronyms	Term
BIS	Basic Inspection System
BIS-PACE	Basic Inspection System with PACE
CA	Chip Authentication
CAN	Card Access Number
CC	Common Criteria
EAC	Extended Access Control
EF	Elementary File
ICCSN	Integrated Circuit Card Serial Number.
MF	Master File
MRZ	Machine readable zone
n.a.	Not applicable
OSP	Organisational security policy
PACE	Password Authenticated Connection Establishment
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Chip
PP	Protection Profile
PT	Personalisation Terminal
RF	Radio Frequency
SAR	Security assurance requirements
SFR	Security functional requirement
SIP	Standard Inspection Procedure
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy (defined by the current document)
HAL	Hardware Abstract Layer
AML	Application Middle Layer

Copyright ⓒ 2015 - LG CNS Co., Ltd. All rights reserved