Protection Profile for ePassport IC with SAC (PACE) and Active Authentication

Version 1.00

March 8, 2016

Passport Division, Consular Affairs Bureau,
Ministry of Foreign Affairs of Japan

JBMIA

This document is a translation of the evaluated and certified protection profile written in Japanese.

Foreword

This Protection Profile (hereinafter “the PP”) specifies security requirements for ePassport IC chips conforming to the ePassport Standards Doc 9303 provided by the International Civil Aviation Organization (ICAO).

IC chip assumed in the PP applies to ePassports for supporting the Supplemental Access Control (SAC) and Active Authentication (AA).

IC chips supporting the SAC are required to support both Basic Access Control (BAC) and Password Authenticated Connection Establishment v2 (PACE v2).

Both BAC and PACE are the means of mutual authentication and Secure Messaging, and the latter has increased security strength of the session key. In the future, PACE will become a standard for mutual authentication and Secure Messaging. Until the end of 2017, however, in terms of ensuring compatibility, implementing only PACE without BAC in an IC chip is not allowed. Note that an IC chip is required to conform to the PP and “Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication” (hereinafter “the BAC+PACE PP”) when the chip, as a TOE, is capable of BAC function and of disabling BAC function. In this case, BAC function and its disabling function are evaluated based on the BAC+PACE PP, and the other security functions are evaluated based on the ST that conforms to the PP. On the other hand, when an IC chip without such functions is defined as a TOE, it is required to conform to only the PP.

The Active Authentication is to prevent passport forgery that uses a faked IC chip by verifying the authenticity of the unique private key stored in the IC chip.

The PP has been prepared based on the rules and formats of Common Criteria (CC) Version 3.1. The developer of ePassport ICs that conform to the PP shall prepare a Security Target (ST) that meets any and all requirements defined in the PP.

ePassport ICs should meet overall technical specifications required for ePassport ICs in addition to fulfilling the security functions that meet the PP’s requirements. Technical specifications not involved in the security functions are not defined in the PP, and are separately provided by the procurer.

Some requirements of the PP include references to standards and materials issued by ICAO. These standards and materials are related to cryptographic algorithms and authentication procedure, and are not included in the CC. The standards and materials are required for the development of the Target of Evaluation (TOE) that meets the PP.

The PP has been prepared by the JBMIA under a commission from Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan.

[Notes in the PP]

The PP provides various Notes to support preparation of the STs conforming to the PP. Each Note is supplemental information for readers to properly understand the PP, and is not intended to constitute provisions or requirements of the PP. However, some Notes are useful for the readers of the ST, and therefore, the said Notes may be copied to the ST at the discretion of the ST author. In such cases, the descriptions may be rewritten according to the context of the ST.

Table of contents

1. PP Introduction

1.1 PP Reference

Title:	Protection Profile for ePassport IC with SAC (PACE) and Active Authentication
Version number:	1.00
Issue Date:	March 8, 2016
Editor:	JBMIA
Issuer:	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
Registration:	JISEC C0499

1.2 TOE Overview

1.2.1 TOE Types

The TOE is ePassport IC (including necessary software). This ePassport IC is composed of IC chip hardware with the contactless communication interface, and basic software (operating system) and ePassport application program that are installed in the said hardware (hereinafter, the term an "IC chip" shall mean an “ePassport IC"). An external antenna is connected to the IC chip for contactless communication purpose, and the IC chip is embedded in the plastic sheet together with the antenna to constitute a portion of a passport booklet.

1.2.2 TOE Usage and Main Security Functions

A passport is an identification document issued by each country’s government or equivalent public organization, which certifies, for the purpose of international travel, the identity of its holder, generally in a booklet form (passport booklet). The International Civil Aviation Organization (ICAO) of the United Nations has provided the passport booklet guidelines. As for conventional passports, all information necessary as the identification was printed on a paper booklet, and thereby this could cause these passports to be forged for illicit purposes. In order to prevent such forgery, an IC chip containing personal information with digital signature has been incorporated in a passport booklet. Since valid digital signature can be granted only by the official passport issuing authorities, a high level of forgery prevention can be achieved. However, digital signature is not enough to counter forgery of copying personal information with authorized signature to store such information on a different IC chip.

This type of forgery attack can be countered by adding the Active Authentication function to the IC chip and verifying the authenticity of the IC chip with the use of the said function.

The TOE is embedded in a plastic sheet and then interfiled in a passport booklet. At immigration, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter a "terminal"). Aside from the information printed on the passport booklet in ordinary characters, the same information is encoded, printed on the machine readable zone (MRZ) of the passport booklet, and read by the optical character reader of the terminal. The information is digitized[1] and is stored in the IC chip, i.e., the TOE. These digitalized data are read by the terminal through the contactless communication interface of the TOE. The digitalized data include facial images.

The antenna used for the TOE to perform contactless communication with the terminal is connected to the TOE in the plastic sheet. The TOE operates using wireless signal power supplied from the terminal.

The main security functions of the TOE are to protect data stored in the TOE from illicit reading or writing. The operation of the security functions applied to contactless communication with the terminal shall comply with the PACE, and Active Authentication specifications defined by Part 11 of Doc 9303.

Attacks on protected data in the TOE include those through the contactless communication interface of the TOE and those attempting to disclose internal confidential information (Active Authentication Private Key) through physical attacks on the TOE.

The TOE provides the main security functions, including:

- PACE function (mutual authentication and Secure Messaging);
- Active Authentication support function (prevention of copying the IC chip);
- Write protection function (protection on writing data after issuing a passport);
- Protection function in transport (protection against attacks during transport before issuing the TOE); and
- Tamper resistance (protection against confidential information leak due to physical attacks).

1.2.3 TOE Life Cycle

The TOE life cycle is described below to clarify the security requirements for the TOE. The TOE life cycle of general IC chips is often described in terms of seven phases in the life cycle. As for the ePassport IC, however, the life cycle is divided into four phases instead of seven.

- Phase 1 (Development): Development of IC chip hardware, basic software (operating system), and application software
- Phase 2 (Manufacturing): Manufacturing of the IC chip (with software installed) and embedding it together with antenna in the plastic sheet
- Phase 3 (Personalization) Production of a passport booklet and writing of personal data
- Phase 4 (Operational Use): Use of the TOE by the passport holder in operational

[1] Digital signature is added to individual digital data by the passport issuing authorities in order to prevent the forgery of digital data. The verification process of the digital signature has been standardized as the Passive Authentication by ICAO. PKI that provides interoperability for all member states of ICAO is implemented from the grant of digital signature through the verification thereof with the terminal for the purpose of supporting Passive Authentication. Since the Passive Authentication is performed through verification of digital signature (including background PKI) without involvement of the security functions of the TOE, it is not included in the security requirements for the TOE.

environment

Phase 1

Phase 1 is a development phase. In phase 1, threats in the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of development data. Security related to the TOE in the development phase is evaluated as the development security in assurance requirements. The TOE security functions are still not validly operational in the development phase.

In Phase 1, the development of the hardware for the IC chip, of operating system, and of application software for passport may be conducted by separate developers. If the development of each component to constitute a TOE is conducted at multiple sites, secure development environment is required for all of the components.

Phase 2

Phase 2 is a manufacturing phase. In Phase 2, the hardware for the IC chip is manufactured, and operating system and application software for passport are installed in this hardware. A file object necessary for an ePassport is created in the TOE and an IC chip identification serial number is written into the file object. The functional tests of the internal circuit of the IC chip are conducted before the IC chip is sealed. After that, only the contactless communication interface becomes available as an external interface. The manufactured IC chip is embedded in the plastic sheet together with the contactless communication antenna. In this phase, threats from the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of the components of the IC chip.

The TOE in Phase 2 is configured with the transport key, readout key, and Active Authentication Information Access Key, and delivered to the passport issuing authorities[2].

Phase 3

The TOE in Phase 3 is put under the control of the passport issuing authorities. Although no explicit attack against the TOE is assumed under the control of the passport issuing authorities, the TOE is required to have security functionality that allows only authorized individuals to process the TOE, as the organizational security policy.

The TOE is interfiled in the ePassport booklet and information necessary for ePassport is written therein. This information includes the personal information of the passport holder (e.g. name, information on birth and so on) and cryptographic key used by the security functions.

After the completion of personalization of all information, the ePassport is issued to the holder thereof.

Phase 4

Phase 4 is a phase subsequent to the handover of the passport booklet to the end user, i.e.,

2 In Japan, the Ministry of Foreign Affairs of Japan and the passport manufacturer and regional passport offices under its direction fall under the authorities. The passport manufacturer interfiles a TOE embedded plastic sheet in a passport booklet and configures necessary data other than personal information (e.g. date of birth, facial image data, and data for security related to the said data). Regional passport offices configure passport data related to personal information.

the holder thereof. The passport booklet is carried along with the holder thereof and used as a means to certify the identity of the holder in various situations, including immigration procedures.

In Phase 4, no information stored in the TOE is altered or deleted. The TOE security function protects the information necessary for immigration procedures against illicit reading, unless the information is read by an authorized terminal. The private key for Active Authentication is only used for the internal processing of the TOE and will never be readout to anywhere other than the TOE. The TOE security functions protect the information assets in the TOE against external unauthorized access.

2. Conformance Claim

2.1 CC Conformance Claim

CC, to which the PP conforms, are identified. The PP conforms to the following CC V3.1 (in Japanese version released by JISEC):

- Part 1: Overview and the General Model; September 2012, Version 3.1 Revision 4 [Japanese Version 1.0], CCMB-2012-09-001
- Part 2: Security Functional Components; September 2012, Version 3.1 Revision 4 [Japanese Version 1.0], CCMB-2012-09-002
- Part 3: Security Assurance Components; September 2012, Version 3.1 Revision 4 [Japanese Version 1.0], CCMB-2012-09-003
- Conformance to CC Part 2: CC part 2 extended
- Conformance to CC Part 3: CC part 3 conformant

2.2 PP Claim

The PP claims no conformance to other PP.

2.3 Package Claim

- In the PP, the assurance requirement package applicable to the TOE is EAL4 augmented.
- Assurance components augmented are ALC_DVS.2 and AVA_VAN.5.

2.4 Conformance Rationales

The PP claims no conformance to other PP and thereby provides no description of conformance rationales.

2.5 Conformance Statement

Any and all protection profiles and security targets that claim conformance to the PP shall claim strict conformance.

3. Security Problem Definition

This chapter defines security problems related to the TOE. The security problems are defined from the three aspects: Threats (to be countered by the TOE and/or environment), Organizational security policies (to be handled by the TOE and/or environment), and Assumptions (to be met by the environment). The TOE and environment shall address these security problems in a proper way.

The threats, organizational security policies, and assumptions are named using an identifier with the prefix “T.,” “P.,” or “A.,” respectively. [Note] is added to individual description as required.
[Note] is provided for precise understanding of the contents of the PP when referring to it, and shall not be included in the body of the security problem definition.

3.1 Threats

This section describes threats that a TOE shall counter. These threats shall be countered by the TOE, its operational environment or combination of these two.

T.Copy

An attacker trying to forge an ePassport may do so by reading personal information along with digital signature from the TOE and writing the copied data in an IC chip having the same functionality as that of the TOE. This attack damages the credibility of the entire passport booklet system including TOEs.

[Note 3-1] If information retrieved from the legitimate TOE is copied into an illicit IC chip, as information stored in the TOE will be copied together with the associated digital signature, forgery protection by means of digital signature verification becomes ineffective. Since the original information can be protected against tampering by means of digital signature, passport forgery may be detected by means of comparative verification of the facial image. However, it is difficult to surely detect forged passport just by comparing the facial image.

T.Logical_Attack

In the operational environment after issuing a TOE embedded passport booklet, an attacker who can read the MRZ data of the passport booklet may try to read confidential information (Active Authentication Private Key) stored in the TOE through the contactless communication interface of the TOE.

[Note 3-2] If an attacker has physical access to a passport booklet, the attacker can visually read personal information printed on the passport booklet and optically read the printed MRZ data. Since the security functions of the TOE cannot prevent such sort of readings, the information and data stated above is not included in the threat-related assets to be protected by the TOE. In other words, the intended meaning of the threat here is an attack aimed to read confidential information (Active Authentication Private Key) stored in the TOE by having access to the said TOE through the contactless communication interface using data that the

attacker has read from the MRZ.

T.Communication_Attack

In the operational environment after issuing a TOE embedded passport booklet, an attacker who does not know about MRZ data may interfere with the communication between the TOE and a terminal to disclose and/or alter communication data that should be concealed.

[Note 3-3] As for an attack which interferes with communication between a terminal and a passport booklet, it is considered impossible that the attacker physically accesses the target passport booklet without being noticed by the passport holder and/or an immigration official. An attacker can obtain MRZ data only when the passport booklet is physically accessible. Therefore, the attacker mentioned here is assumed to be unaware of the MRZ data.

T.Physical_Attack

In the operational environment after issuing a TOE embedded passport booklet, an attacker may attempt to disclose confidential information (Active Authentication Private Key) stored in the TOE, unlock the state of the locked key, or reactivate a deactivated access control function by physical means. This physical means include both of nondestructive attacks made without impairing the TOE functions and destructive attacks made by destroying part of the TOE to have mechanical access to the inside of the TOE.

[Note 3-4] An attacker may attempt to read confidential information (Active Authentication Private Key) or rewrite information stored in the TOE through physical access to the TOE. Making such a physical attack may impair the security function operated by the TOE program to provide the original functionality thereof, resulting in potential violation of SFR. The example of nondestructive attacks includes measurements on leaked electromagnetic wave associated with the TOE operation and induction of malfunctions in security functions by applying environmental stress (e.g. changes in temperature or clock, or application of high-energy electromagnetic fields) to the TOE in operation. The example of destructive attacks shows those collecting, analyzing, and then disclosing confidential information by probing and manipulating the internal circuit. Test pins and power supply pins left in the TOE may be used to make the said attacks. The TOE that has been subject to a destructive attack may not be reused as an ePassport IC. Even in such case, however, the disclosed private key may be abused to forge TOEs.

3.2 Organizational Security Policies

This section describes organizational security policies that apply to TOEs and operational environment. In the PP, the organizational security policies include conformance to the standards provided by ICAO and conditions required by the passport issuing authorities in Japan.

P.PACE

In the operational environment after issuing a TOE embedded passport booklet, the TOE shall allow a terminal to read a certain information from the TOE in accordance with the PACE

procedure defined by Part 11 of Doc 9303. This procedure includes mutual authentication and Secure Messaging between the TOE and terminal devices. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD under the rules stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the PP is not defined.

P.Authority

The TOE under the control of the passport issuing authorities shall allow only authorized users (persons who succeeded in verification of readout key, transport key, or Active Authentication Information Access Key) to have access to the internal data of the TOE, as shown in Table 1.

Table 1 Internal data of the TOE access control by passport issuing authorities

Authentication status*1	File subject to access control	Operation permitted	Reference: Data to be operated
Successful verification with readout key	EF.DG13*2	Read	IC chip serial number (entered by manufacturer)
Successful verification with transport key	Transport key file	Write	Transport key data (update of old data)
	Password key file		Password key
	EF.DG1	Read or Write	MRZ data
	EF.DG2		Facial image
	EF.DG13*2		Management data (Passport number and Booklet management number)
	EF.DG14		PACE v2 Security information Active Authentication hash function information
	EF.COM*3		Common data
	EF.SOD		Security data related to Passive Authentication defined by Part 10 of [DOC9303].
	EF.CardAccess	Write	PACE v2 Security information
	EF.DG15	Read	Active Authentication Public Key
Successful verification with Active Authentication Information Access Key	EF.DG15	Write	Active Authentication Public Key
	Private key file		Active Authentication Private Key

*1 The readout key, transport key, and Active Authentication Information Access Key are configured by the manufacturer. The transport key can be changed (updated) by an authorized user. With regard to the files subject to access control included in this table and files storing the read key and Active Authentication Information Access Key which may vary the authentication status, user access that is not stated in this table or Notes is prohibited. (The access controls to information in the TOE from terminals after issuing a TOE embedded passport booklet to the passport holder, i.e., PACE are separately specified.)

*2 In EF.DG13, an IC chip serial number has been recorded by the manufacturer, and the management data is appended to the file by the passport issuing authorities.

*3 EF.COM file may not be created according to the passport issuing authorities' instructions.

[Note 3-5]
All files stated in the table above store user data or TSF data. The transport key file stores TSF data, and all other files store user data (cryptographic keys are managed as user data). The TSF data file is not included in files subject to access control stated in Chapter 6, Section "Security Functional Requirements," but treated in FMT_MTD.1.

P.Data_Lock

When the TOE detects a failure in authentication with the transport key, readout key or Active Authentication Information Access Key, it will permanently disable authentication related to each key, thereby prohibiting reading or writing the file based on successful authentication thereof. Table 1 shows the relationship between the key used for authentication and its corresponding file in the TOE.

P.Prohibit

Any and all writings to the files in the TOE and readings from the files in the TOE based on successful authentication with readout key are prohibited after issuing an ePassport to the passport holder. Disabling authentication through authentication failure with the transport key, readout key, and Active Authentication Information Access Key (see P.Data_Lock) shall be used as the means for that purpose.

3.3 Assumptions

This section describes assumptions to be addressed in the operational environment of TOEs. These assumptions need to be true for TOEs' security functionality becomes effective.

A.Administrative_Env

The TOE that was delivered from the TOE manufacturer to the passport issuing authorities and is under the control of the authorities shall be securely controlled and go through an issuing process until it is finally issued to the passport holder.

A.PKI

In order for the passport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuer and stored in the TOE (including the Active Authentication Public Key), the interoperability of the PKI environment both of the issuing and receiving states or organizations of the passport shall be maintained by passport issuing authorities.

4. Security Objectives

This chapter describes security objectives for TOEs and its environment for the security problems described in Chapter 3. Section 4.1 describes the security objectives to be addressed by the TOEs, while Section 4.2 describes those to be addressed by its environment. In addition, Section 4.3 describes rationales for the appropriateness of the security objectives for solving the security problems.

The security objectives for the TOEs and the security objectives for the operational environment are represented by an identifier with the prefix “O.” or “OE.” respectively.

4.1 Security Objectives for the TOE

This section describes security objectives that TOEs should address to solve problems with regard to the threats and organizational security policies that are defined as the security problems.

O.AA

TOEs shall provide a means to verify the authenticity of the IC chip itself that composes the TOE in order to prevent the copy of personal information including the digital signature on an illicit IC chip and the forgery of the passport. This means shall be standardized so as to ensure the global interoperability of ePassport and, for this purpose, shall support the Active Authentication defined by Part 11 of [DOC9303].

O.Logical_Attack

TOEs shall, under any circumstances, prevent confidential information in them (Active Authentication Private Key) from being externally read through the contactless communication interface of the TOE.

O.Physical_Attack

TOEs shall prevent the confidential information (Active Authentication Private Key) within the TOEs from being disclosed or the information relating to the security from being tampered with by the attackers using physical means. TOEs shall counter attacks applicable to TOEs themselves out of known attacks against IC chips, considering physical means including both nondestructive attacks and destructive attacks.

O.PACE

This security objective applies to the operational environment after issuing the passport booklet. PACE procedure defined by Part 11 of [DOC9303], if the terminals require, shall be used to ensure the global interoperability of the ePassport. This procedure shall be used in the mutual authentication and Secure Messaging between the TOE and terminals.
Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, and EF.SOD files among the files contained in the rules stated above. The TOE shall permit only the terminal that has succeeded in mutual authentication to

read the files stated above. As for any files under the same rules except the files stated above, the handling of such files which are not listed in the PP is not defined.

O.Authority

The TOE shall limit users who can access the internal TOE data and their operations, in the environment under the control of the passport issuing authorities according to Table 1 described in the organizational security policy P. Authority.

O.Data_Lock

The operation of the internal TOE data shall be available only to the authorized user (i.e., authorized personnel under the control of the passport issuing authorities or the terminal after issuing the passport) to prevent illicit reading and writing by any users other than those stated above. As a means for this purpose, if the TOE detects an authentication failure with the readout key, transport key, or Active Authentication Information Access Key, it shall be permanently prohibited to read or to write the internal TOE data permitted according to authentication related to each of the said keys. This security objective shall also apply in the event that the passport issuing authorities disable readout key, transport key, or Active Authentication Information Access Key by causing an authentication failure intentionally before the TOE is issued to the passport holder. The relationship between the readout key, transport key, and Active Authentication Information Access Key and their corresponding internal TOE data is as listed in Table 1 of the organizational security policy P.Authority. After the security objective O.Data_Lock is achieved, only the access to TOE stated in the security objective O.PACE is permitted.

4.2 Security Objectives for the Operational Environment

This section describes security objectives that TOEs should address in the operational environment to solve problems with regard to the threats and organizational security policies and assumptions defined as the security problems.

OE.Administrative_Env

The TOEs under the control of the passport issuing authorities are subjected to secure management and treatment until each of these TOEs is delivered to the passport holder through the issuing procedures.

OE.PKI

In order for the ePassport inspection authorities of the receiving state or organization to verify the authenticity of information that has been digitally signed by the passport issuing state or organization and stored in the TOE (i.e., information on the passport holder and the Active Authentication Public Key), passport issuing authorities shall maintain the interoperability of the PKI environment in both the passport issuing state and receiving state.

4.3 Security Objectives Rationales

This chapter describes rationales for the effectiveness of the security objectives stated above for individual parameters of the security problem definition. Section 4.3.1 describes that each of the security objective can be traced back to any of the security problems, while Section 4.3.2 describes that any of the security problems is effectively addressed by the corresponding security objective.

4.3.1 Correspondence between Security Problem Definition and Security Objectives

Table 2 shows the correspondence between the security problem definition and the security objectives. As shown in the table, all security objectives can be traced back to one (or more) item(s) in the security problem definition.

Table 2 Correspondence between security problem definition and security objectives

Security problem definition \ Security objective	O.AA	O.Logical_Attack	O.Physical_Attack	O.PACE	O.Authority	O.Data_Lock	OE.Administrative_Env	OE.PKI
T.Copy	×							
T.Logical_Attack		×						
T.Communication_Attack				×				
T.Physical_Attack			×					
P.PACE				×				
P.Authority					×			
P.Data_Lock						×		
P.Prohibit						×		
A.Administrative_Env							×	
A.PKI								×

4.3.2 Security Objectives Rationale

This section describes rationales for the security objectives for the TOE and the operational environment to thoroughly counter all identified threats, implement organizational security policies, and also properly meet the assumptions.

T.Copy

If an attacker copies the personal information (with digital signature) read from the TOE to the IC chip having the same functionality as that of the TOE, the forged passport cannot be detected through the verification of digital signature. To prevent this attack, the security objective for the TOE: O.AA addresses embedding of data that enable verifying the authenticity of the IC chip itself in the TOE. This enables the TOE to detect illicit IC chips and prevent the forgery of passports, thus removing the threat of T.Copy.

T.Logical_Attack

The security objective for the TOE: O.Logical_Attack makes it possible to prohibit reading confidential information (Active Authentication Private Key) in the TOE through the contactless communication interface of the TOE, under any circumstances.
Thus the threat of T.Logical_Attack is removed.

T.Communication_Attack

The security objectives for the TOE: O.PACE makes it possible to use a secure communication path for the communication between the terminals and the TOE. Thus the threat of disclosure and alteration of the communication data of T.Communication_Attack can be diminished to an adequate level for the practical use.

T.Physical_Attack

The security objective for the TOE: O.Physical_Attack makes it possible to counter an attack to disclose confidential information (Active Authentication Private Key) in the TOE or tamper security-related information not via the contactless communication interface of the TOE but physical means. Regarding the physical means, both nondestructive attacks and destructive attacks are considered, and countermeasures shall be implemented so that the TOE can counter known attacks against the IC chip. Thus the threat can be diminished to an adequate level for the practical use.

P.PACE

The security objective for the TOE: O.PACE allows only the authorized personnel (terminal) to read the internal TOE data through a secure communication path by applying PACE procedure defined by Part 11 of [DOC9303]. O.PACE includes all contents of P.PACE, thus the organizational security policy P.PACE is properly implemented.

P.Authority

The security objective for the TOE: O.Authority provides the contents to directly implement the organizational security policy P.Authority.

P.Data_Lock

The security objective for the TOE: O.Data_Lock includes the contents required by the organizational security policy P.Data_Lock and properly implements P.Data_Lock.

P.Prohibit

The organizational security policy P.Prohibit requires the implementation of an intentional authentication failure by the authorized TOE user as the implementation means. Actions required for the TOE to address P.Prohibit are the same as those for the organizational security policy P.Data_Lock that has assumed an illicit attack on the TOE. Therefore, the security objective for the TOE: O.Data_Lock will also implement the contents of P.Prohibit.

A.Administrative_Env

The security objective for the operational environment: OE.Administrative_Env directly corresponds to the assumption A.Administrative_Env, thus this assumption is met.

A.PKI

The security objective for the operational environment: OE.PKI directly corresponds to the assumption A.PKI, thus this assumption is met.

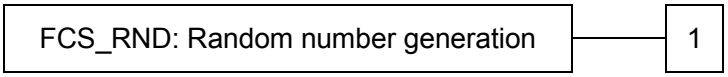
5. Extended Components Definition

The PP defines the following extended components.

5.1 FCS_RND: Random number generation

Family Behaviour
This family defines quality requirements for the generation of random numbers to be used for cryptographic purposes.

Component levelling



FCS_RND.1 Random number generation requires the random numbers to meet defined quality standards.

Management: FCS_RND.1
There is no management activity foreseen.

Audit: RCS_RND.1
There is no auditable event foreseen.

FCS_RND.1 Quality standards for random numbers

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a random number generation mechanism that meet [assignment: *defined quality standard*].

6. Security Requirements

6.1 Security Functional Requirements

Table 3 shows the list of the security functional requirements (SFRs) defined by the PP.

Table 3 List of SFRs

Chapter No.	Identifier name	
6.1.1	FCS_CKM.1p	Cryptographic key generation (PACE, session keys)
6.1.2	FCS_CKM.1e	Cryptographic key generation (PACE, ephemeral key pairs)
6.1.3	FCS_CKM.4	Cryptographic key destruction
6.1.4	FCS_COP.1a	Cryptographic operation (Active Authentication, signature generation)
6.1.5	FCS_COP.1h	Cryptographic operation (Active Authentication, hash functions)
6.1.6	FCS_COP.1n	Cryptographic operation (Nonce encryption)
6.1.7	FCS_COP.1e	Cryptographic operation (Key agreement)
6.1.8	FCS_COP.1hp	Cryptographic operation (PACE, hash functions)
6.1.9	FCS_COP.1mp	Cryptographic operation (PACE, mutual authentication)
6.1.10	FCS_COP.1sp	Cryptographic operation (PACE, Secure Messaging)
6.1.11	FCS_RND.1	Quality standards for random numbers
6.1.12	FDP_ACC.1a	Subset access control (Issuance procedure)
6.1.13	FDP_ACC.1p	Subset access control (PACE)
6.1.14	FDP_ACF.1a	Security attribute based access control (Issuance procedure)
6.1.15	FDP_ACF.1p	Security attribute based access control (PACE)
6.1.16	FDP_ITC.1	Import of user data without security attributes
6.1.17	FDP_UCT.1p	Basic data exchange confidentiality (PACE)
6.1.18	FDP_UIT.1p	Data exchange integrity (PACE)
6.1.19	FIA_AFL.1a	Authentication failure handling (Active Authentication Information Access Key)
6.1.20	FIA_AFL.1d	Authentication failure handling (Transport key)
6.1.21	FIA_AFL.1r	Authentication failure handling (Readout key)
6.1.22	FIA_UAU.1	Timing of authentication
6.1.23	FIA_UAU.4	Single-use authentication mechanism
6.1.24	FIA_UAU.5	Multiple authentication mechanisms
6.1.25	FIA_UID.1	Timing of identification
6.1.26	FMT_MTD.1	Management of TSF data
6.1.27	FMT_SMF.1	Specification of management functions
6.1.28	FMT_SMR.1	Security roles
6.1.29	FPT_PHP.3	Resistance to physical attack
6.1.30	FTP_ITC.1	Inter-TSF trusted channel

SFR is defined by performing as-needed operation on the security functional component defined by CC Part 2. The operation is denoted for each SFR by the following method:

- SFR subject to iteration operation is identified by adding a low-case alphabetic character such as “a” and a parenthesized brief description showing the purpose of SFR (e.g. “Active

Authentication") after the corresponding component identifier.

- The point of assignment or selection operation is shown as [assignment: *XXX* (italicized)] or [selection: *XXX* (italicized)]. Refinement is also italicized.
- For the selection operation, items not subject to selection are shown by strike-through (~~Strikethrough~~).
- The PP has some uncompleted operations, which are shown as [assignment: *XXX* (*Italicized and underlined*). The ST author shall complete these uncompleted operations.

The following section describes SFRs defined by the PP.

6.1.1 FCS_ CKM.1p Cryptographic key generation (PACE, 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.1.1p The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *session key generation algorithm in PACE specified by Part 11 of [DOC9303] and [TR-03111]*] and specified cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for session key generation in PACE specified by Part 11 of [DOC9303] and [TR-03111]*].

6.1.2 FCS_CKM.1e Cryptographic key generation (PACE, ephemeral key pairs)

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.1.1e The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *Elliptic Curve Key Pair Generation*] and specified cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: *Standards for the key pair generation specified by [TR-03111]*].

6.1.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *[selection: method for erasing cryptographic keys on volatile memory by shutting down power supply, overwriting new cryptographic key data, and [assignment: other cryptographic key destruction method]*]] that meets the following: [assignment: *none*].

[Note 6-1]: To meet requirements of 9.8.3 Session Termination in Part 11 of [DOC9303], the ST author shall repeatedly define this requirement as necessary.

6.1.4 FCS_COP.1a Cryptographic operation (Active Authentication, signature generation)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1a The TSF shall perform [assignment: *generation of digital signature for Active Authentication data*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA*] and cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: the *Digital Signature Standards specified by [TR-03111]*].

[Note 6-2]: Only the combination of 256 bits and SHA-256 or that of 384 bits and SHA-384 is permitted as the key sizes for this requirement and the hash algorithm of FCS_COP.1h.

6.1.5 FCS_COP.1h Cryptographic operation (Active Authentication, hash functions)

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.1.1h The TSF shall perform [assignment: *generation of data for Active Authentication*] in accordance with a specified cryptographic algorithm [assignment: S*HA-256 and SHA-384*] and cryptographic key sizes [assignment: *non*e] that meet the following: [assignment: the *Digital Signature Standards specified by [TR-03111]*].

6.1.6 FCS_COP.1n Cryptographic operation (Nonce encryption)

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.1.1n The TSF shall perform [assignment: *nonce encryption*] in accordance with a specified cryptographic algorithm [assignment: *AES-CBC*] and cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for the PACE procedure specified by Part 11 of [DOC9303]*].

6.1.7 FCS_COP.1e Cryptographic operation (Key agreement)

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.1.1e The TSF shall perform [assignment: *key agreement*] in accordance with a specified cryptographic algorithm [assignment: *ECDH*] and cryptographic key sizes [assignment: *256 bits and 384 bits*] that meet the following: [assignment: *Standards for the PACE procedure specified by Part 11 of [DOC9303]*].

6.1.8 FCS_COP.1hp Cryptographic operation (PACE, hash functions)

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.1.1hp The TSF shall perform [assignment: *generation of session keys for PACE*] in accordance with a specified cryptographic algorithm [assignment: *SHA-1 and SHA-256*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *Standards for session key generation in PACE specified by Part 11 of [DOC9303]*].

6.1.9 FCS_COP.1mp Cryptographic operation (PACE, mutual authentication)

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.1.1mp The TSF shall perform [assignment: authentication token generation and verification] in accordance with a specified cryptographic algorithm [assignment: *AES-CMAC*] and cryptographic key sizes [assignment: *128 bits and 256 bits*] that meet the following: [assignment: *Standards for mutual authentication included in PACE specified by Part 11 of [DOC9303]*].

6.1.10 FCS_COP.1sp Cryptographic operation (PACE, Secure Messaging)

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.1.1sp The TSF shall perform [assignment: *cryptographic operation shown in Table 4*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm shown in Table 4*] and cryptographic key sizes [assignment: *cryptographic key sizes shown in Table 4*] that meet the following: [assignment: *Standards for Secure Messaging included in PACE specified by [DOC9303]*].

Table 4 Cryptographic mechanisms in Secure Messaging (PACE)

Cryptographic algorithm	*Cryptographic key sizes*	*Cryptographic operation*
AES in CBC mode	*128 bits and 256 bits*	*Message encryption and decryption*
AES-CMAC	*128 bits and 256 bits*	*Generation and verification of Message Authentication Code*

[Note 6-3]: Whether the Secure Messaging is applied or not depends on the type of commands. Therefore, data encryption and message authentication codes are not necessarily applied to all commands and responses.

6.1.11 FCS_RND.1 Quality standards for random numbers

Hierarchical to: No other components.
Dependencies: No dependencies

FCS_RND.1.1 The TSF shall provide a random number generation mechanism that meets the following: [assignment: *defined quality standard*].

[Note 6-4]: See documents such as BSI AIS20, BSI AIS31, NIST SP800-90, ISO/IEC 18031 for information on quality standards for random numbers.

[Note 6-5]: When implementing ECDSA calculation defined by FCS_COP.1a with high-level software, the ST author shall iterate this requirement for the quality of random numbers generated in the calculation process.

6.1.12 FDP_ACC.1a Subset access control (Issuance procedure)

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1a The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] on [assignment: *Subject [User process], Objects [Files shown in Table 1 of Organizational security policy P.Authority] and List of operations among subjects and objects addressed by SFP [Data Input/Output operation to/from object]*].

6.1.13 FDP_ACC.1p Subset access control (PACE)

Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1p The TSF shall enforce the [assignment: *PACE SFP*] on [assignment: *Subject [Process on behalf of terminal], Objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM , EF.SOD, password key file, transport key file, and private key file] and list of operations among subjects and objects addressed by SFP [Reading data from object]*].

[Note 6-6] Files other than those listed above are also defined by [DOC9303]. When a procurer in any country other than Japan uses the PP, the said files may need to be added. Even when the PP or ST author adds the files to objects to make a change to SFR of the PP, strict conformance to the PP will be maintained as far as the SFRs of the PP are met. However, to add any object and its operation for ST preparation, the need for the agreement of the Procurer of TOE should be considered even if the strict conformance to the PP is maintained.

[Note 6-7] PACE SFP is the access control policy applied after succeeding in mutual authentication based on PACE.

6.1.14 FDP_ACF.1a Security attribute based access control (Issuance procedure)

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1a The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [User process], objects [Files shown in Table 1 of the organizational security policy P.Authroity], and, the SFP-relevant security attributes [Authentication status shown in Table 1 of the organizational security policy P.Authority]* according to each].

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *When the authentication status shown in Table 1 of the organizational security policy P.Authority is met, an operation to the file associated with the said authentication status is allowed*].

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

FDP_ACF.1.4a The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *Access to files that are not listed in Table 1 of the organizational security policy P.Authroity is prohibited.*].

6.1.15 FDP_ACF.1p Security attribute based access control (PACE)

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1p The TSF shall enforce the [assignment: *PACE SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [Process on behalf of terminal], objects [Files EF.DG1, EF.DG2, EF.DG13, EF.DG14, EF.DG15, EF.COM, EF.SOD password key file, transport key file, and private key file], and the SFP-related security attributes [Authentication status of terminal based on mutual authentication]*].

FDP_ACF.1.2p The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Where the authentication status of terminal has been successful, subjects are allowed to read data from objects*].

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

FDP_ACF.1.4p The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *Subjects are prohibited to write data to or read data from the transport key file, password key file, and private key file*].

6.1.16 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the [assignment: *Issuance procedure access control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].

6.1.17 FDP_UCT.1p Basic data exchange confidentiality (PACE)

Hierarchical to: No other components.
Dependencies: [FTP_ITC.1 Inter-TSF trusted channel or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1p The TSF shall enforce of [assignment: *PACE SFP*] to [selection: *transmit,*

receive] user data in a manner protected from unauthorised disclosure.

6.1.18 FDP_UIT.1p Data exchange integrity (PACE)

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1p The TSF shall enforce the [assignment: *PACE SFP*] to [selection: *transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2p The TSF shall be able to determine, on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred.

6.1.19 FIA_AFL.1a Authentication failure handling (Active Authentication Information Access Key)

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1a The TSF shall detect when [selection: *[assignment: positive integer number]*, ~~*an administrator configurable positive integer within [assignment: range of acceptable values]*~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the Active Authentication Information Access Key*].

[Note 6-8] The ST author shall specify a positive integer number in a range of 1 to 15.

FIA_AFL.1.2a When the defined number of unsuccessful authentication attempts has been [selection: *met*~~*, surpassed*~~], the TSF shall [assignment: *permanently stop authentication with the Active Authentication Information Access Key (fix the authentication status with the Active Authentication Information Access Key to "Not authenticated yet")*].

6.1.20 FIA_AFL.1d Authentication failure handling (Transport key)

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1d The TSF shall detect when [selection: *[assignment: positive integer number]*, ~~*an administrator configurable positive integer within [assignment: range of acceptable values]*~~] unsuccessful authentication attempts occur related to [assignment:

authentication with the transport key].

[Note 6-9] The ST author shall specify a positive integer number in the range of 1 to 15.

FIA_AFL.1.2d When the defined number of unsuccessful authentication attempts has been [selection: *met, ~~surpassed~~*], the TSF shall [assignment: *permanently stop authentication with the transport key (fix the authentication status with the transport key to "Not authenticated yet")*].

6.1.21 FIA_AFL.1r Authentication failure handling (Readout key)

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1r The TSF shall detect when [selection: *[assignment: positive integer number]*, *~~an administrator configurable positive integer within [assignment: range of acceptable values]~~*] unsuccessful authentication attempts occur related to [assignment: *authentication with the readout key*].

[Note 6-10] The ST author shall specify a positive integer number in the range of 1 to 15.

FIA_AFL.1.2r When the defined number of unsuccessful authentication attempts has been [selection: *met, ~~surpassed~~*] , the TSF shall [assignment: *permanently stop authentication with the readout key (fix the authentication status with the readout key to "Not authenticated yet")*].

6.1.22 FIA_UAU.1 Timing of authentication

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

FIA_UAU.1.1 The TSF shall allow [assignment: *readout of EF.CardAccess and EF.ATR/INFO*], on behalf of the user to be performed before the user is authenticated.

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

6.1.23 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *mutual authentication mechanism with the PACE procedure*].

6.1.24 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [assignment: *multiple authentication mechanisms shown in Table 5*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identify according to the [assignment: *rules describing how the multiple authentication mechanisms shown in Table 5 provide authentication*].

Table 5 Multiple authentication mechanisms

Authentication mechanism name	*Rule applicable to authentication mechanism*
Transport key	*Rule of authenticating the authorized personnel of the passport issuing authorities by verifying transport key that have been already stored in the TOE*
Readout key	*Rule of authenticating the authorized personnel of the passport issuing authorities by verification with readout key that have been already stored in the TOE*
Active Authentication Information Access Key	*Rule of authenticating the authorized personnel of the passport issuing authorities by verification with Active Authentication Information Access Key that have been already stored in the TOE*
Mutual authentication	*Rule of authenticating terminals according to the mutual authentication procedure in PACE defined by [DOC9303]*

6.1.25 FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *readout of EF.CardAccess and EF.ATR/INFO*], on behalf of the user to be performed before the user is identified.

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

6.1.26 FMT_MTD.1 Management of TSF data

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

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: ~~*change_default, query,*~~ *modify,* ~~*delete, clear, [assignment: other operations]*~~] the [assignment: *transport key*] to [assignment: *the authorized personnel of the passport issuing authorities*].

[Note 6-11] This requirement has to do with the configuration of transport key used to transport the TOE from the passport booklet manufacturer to a regional passport office in Phase 3. In this requirement, the authorized personnel who are allowed to manage TSF data are the staff of the

passport manufacturer. The staff has no chance to rewrite the transport key after the TOE has been transported to the regional passport office.

On the other hand, when the TOE is located in either the passport manufacturer or a regional passport office, there is also no threat that an attacker illicitly rewrites the transport key. Therefore, there is no necessity to distinguish between the staff of the passport manufacturer and that of the regional passport office. For this reason, this requirement makes no particular distinction between them and refers the authorized administrator as the “authorized personnel of the passport issuing authorities.”

6.1.27 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *modification of transport key*].

6.1.28 FMT_SMR.1 Security roles

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

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *authorized personnel of the passport issuing authorities*].

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

6.1.29 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist [assignment: *attacks defined by the CC Supporting Documents related to Smartcards*] to the [assignment: *hardware of the TOE and software composing the TSF*] by responding automatically such that the SFRs are always enforced.

[Note 6-12] The supporting documents that are the latest version at the time of the evaluation for the TOE are applied. The document at the time of PP issuance is the “Application of Attack Potential to Smartcards, Version 2.9, May 2013.”

6.1.30 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 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 channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: ~~*the TSF,*~~ *another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *reading data from the TOE*].

[Note 6-13] Communication between terminal and TSF shall be performed via the Secure Messaging channel defined by [DOC9303]. After the Secure Messaging channel is established, only the Secure Messaging channel is to be available for the communication path between terminal and TOE.

6.2 Security Assurance Requirements

Security assurance requirements applicable to this TOE are defined by assurance components shown in Table 6. These components are all included in CC Part 3. Components except ALC_DVS.2 and AVA_VAN.5 are included in the EAL4 assurance package. ALC_DVS.2 is a high-level component of ALC_DVS.1 and AVA_VAN.5 is a high-level component of AVA_VAN.3.

The PP applies no operation to all components shown in Table 6.

Table 6 Assurance components

Assurance class	Assurance component
Security target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life- cycle support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
Tests	ATE_COV.2

	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

This chapter describes rationales for that the defined SFRs properly achieve the security objectives for the TOE.
Section 6.3.1.1 describes that each of the SFRs can be traced back to any of the security objectives for the TOE, while Section 6.3.1.2 describes that each of the security objectives for the TOE is properly met by the corresponding effective SFR.

6.3.1.1 Tracing between Security Objectives and Security Functional Requirements

Table 7 shows the SFRs corresponding to the security objectives for the TOE. This table provides the rationales for the traceability of all SFRs to at least one security objective for the TOE.

Table 7 Tracing between security objectives for the TOE and SFRs

SFR \ Security objective for the TOE	O.Logical_Attack	O.Physical_Attack	O.AA	O.PACE	O.Authority	O.Data_Lock
FCS_CKM.1p				×		
FCS_CKM.1e				×		
FCS_CKM.4			×	×		
FCS_COP.1a			×			
FCS_COP.1h			×			
FCS_COP.1n				×		
FCS_COP.1e				×		
FCS_COP.1hp				×		
FCS_COP.1mp				×		
FCS_COP.1sp				×		
FCS_RND.1				×		
FDP_ACC.1a			×		×	
FDP_ACC.1p	×			×		
FDP_ACF.1a			×		×	
FDP_ACF.1p	×			×		
FDP_ITC.1			×	×	×	
FDP_UCT.1p				×		
FDP_UIT.1p				×		
FIA_AFL.1a						×
FIA_AFL.1d						×
FIA_AFL.1r						×

FIA_UAU.1				×	×	
FIA_UAU.4				×		
FIA_UAU.5				×	×	
FIA_UID.1				×	×	
FMT_MTD.1					×	
FMT_SMF.1					×	
FMT_SMR.1					×	
FPT_PHP.3		×				
FTP_ITC.1				×		

6.3.1.2 Justification for the tracing

This section describes rationales for that the security objectives for the TOE are met by their corresponding SFRs and, at the same time, indicates that individual SFRs have effectiveness in meeting the security objectives for the TOE.

O.AA

To achieve the security objective O.AA, it shall address the Active Authentication procedure defined by Part 11 of [DOC9303]. This Active Authentication is a process for a terminal to authenticate the IC chip of the TOE, and the TOE itself is not required to provide any authentication mechanism. The TOE is authenticated by properly responding the authentication procedure. To meet requirements for the authentication procedure from the terminal, the TOE incorporates the public key and private key pair, performs cryptographic operation using the private key defined by FCS_COP.1a, and hashing operation defined by FCS_COP.1h. The public key and private key pair is imported to the TOE by FDP_ITC.1. Access control associated with FDP_ITC.1 is defined by FDP_ACC.1a and FDP_ACF.1a. Destruction of the private key on RAM is defined by FCS_CKM.4. The security objective O.AA is sufficiently achieved by the said SFRs.

O.Logical_Attack

Confidential information (Active Authentication Private Key) subject to protection is stored in the private key file of the TOE. It is denied for the user process on behalf of the terminal to read data from the private key file, by FDP_ACC.1P and FDP_ACF.1p applied to the TOE after issuing the TOE embedded passport. The security objective O.Logical_Attack is sufficiently achieved by the said SFRs.

O.Physical_Attack

Attack scenarios trying to disclose the Active Authentication Private Key that is confidential information, and to tamper security related information within the TOE, by physical means are stated in the list of physical attacks shown in the FPT_PHP.3 section. The TSF automatically resists the attacks according to FPT_PHP.3 to protect against the disclosure of the confidential information. With that, the security objective O.Physical_Attack is sufficiently achieved.

O.PACE

FIA_UID.1 and FIA_UAU.1 provide the TOE service for the user who has succeeded in identification and authentication. User authentication requires the mutual authentication procedure with PACE defined by ICAO, which is defined by FIA_UAU.5. The mutual authentication procedure requires new authentication data based on random numbers for each authentication, which is defined by FIA_UAU.4. Likewise, Secure Messaging required by PACE is defined by the requirements for the protection of transmitted and received data by FDP_UCT.1p and FDP_UIT.1p, and the requirement of cryptographic communication channels by FTP_ITC.1. Furthermore, with regard to cryptographic processing required for the PACE procedure, FCS_COP.1mp defines cryptographic operations necessary for the mutual authentication procedure and FCS_COP.1sp defines cryptographic operations for Secure Messaging. With regard to the cryptographic keys used for Secure Messaging, FDP_ITC.1 defines the import of password key, FCS_CKM.1e defines the generation of ephemeral key pairs, FCS_COP.1e defines the key agreement, FCS_CKM.1p and FCS_COP.1hp define the generation of session keys, FCS_RND.1 defines the generation of random numbers such as random Nonce, FCS_COP.1n defines the encryption of Nonce, and FCS_CKM.4 defines the destruction of these keys. In order for only permitted personnel to read given information from the TOE, rules governing access control with FDP_ACC.1p and FDP_ACF.1p are defined. O.PACE is sufficiently achieved by the said SFRs.

O.Authority

During the TOE process done by the passport issuing authorities, the identification and authentication requirements FIA_UID.1 and FIA_UAU.1 are applied in order to grant the processing authority only to the duly authorized user. As for the user authentication mechanisms, FIA_UAU.5 defines the use of the transport key, readout key, or Active Authentication Information Access Key. If a user is successfully authenticated by the verification with the key, the user is permitted to access to the internal data of the TOE defined by O.Authority, applying the access control rule FDP_ACC.1a and FDP_ACF.1a. The user operation includes writing of the authentication key (transport key), cryptographic keys (Active Authentication Public Key and private key pair, and password key for Secure Messaging), and other user data in the TOE. The association between objects and security attributes when writing is defined by FDP_ITC.1. O.Authority includes updating (rewriting) of the transport keys by the authorized personnel of the passport issuing authorities and is defined by FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. The security objective O.Authority is sufficiently achieved by the said SFRs.

O.Data_Lock

In the event of an authentication failure with the transport key, readout key or Active Authentication Information Access Key, authentication corresponding to the relevant key is permanently prohibited, and as the result, the security objective of permanently prohibiting readout and write of the internal data of the TOE is sufficiently achieved by the three SFRs: FIA_AFL.1a, FIA_AFL.1d, and FIA_AFL.1r.

6.3.1.3 Dependencies for Security Functional Requirements

Table 8 shows dependencies and support for the dependencies defined for SFRs.

In the table, the Dependencies column describes dependencies defined for SFRs, and the Support for the Dependencies column describes by what SFRs the defined dependencies are satisfied or rationales indicating the justification for non-satisfied dependencies.

Table 8 Dependencies for SFRs

SFR	Dependencies	Support for the Dependencies
FCS_CKM.1p	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1sp, FCS_COP.1mp, and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.1e	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1e and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1, FCS_CKM.1p and FCS_CKM.1e support to satisfy the dependency. FDP_ITC.1 supports keys only on volatile memory.
FCS_COP.1a	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. FCS_CKM.4 supports keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to.
FCS_COP.1h	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Since keys do not exist, any requirements do not apply to.
FCS_COP.1n	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. FCS.CKM.4 supports on keys on volatile memory. Since the modification and destruction of keys on nonvolatile memory are prohibited, FCS_CKM.4 does not apply to.
FCS_COP.1e	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1e and FCS_CKM.4 support to satisfy the dependencies.
FCS_COP.1hp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Since keys do not exist, any requirements do not apply to.
FCS_COP.1mp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.
FCS_COP.1sp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p and FCS_CKM.4 support to satisfy the dependencies.
FCS_RND.1	No dependencies	N/A
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a supports to satisfy the dependency.
FDP_ACC.1p	FDP_ACF.1	FDP_ACF.1p supports to satisfy the dependency.
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_ACF.1p	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1p supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1a supports. Objects are created at initial configuration, but not created in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file creation does not apply to.

FDP_UCT.1p	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.
FDP_UIT.1p	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FTP_ITC.1 and FDP_ACC.1p support to satisfy the dependencies.
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.1 supports to satisfy the dependency.
FIA_UAU.1	FIA_UID.1	FIA_UID.1 supports to satisfy the dependency.
FIA_UAU.4	No dependencies	N/A
FIA_UAU.5	No dependencies	N/A
FIA_UID.1	No dependencies	N/A
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1 support to satisfy the dependencies.
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1 supports to satisfy the dependency.
FPT_PHP.3	No dependencies	N/A
FTP_ITC.1	No dependencies	N/A

6.3.2 Security Assurance Requirements Rationale

The security functionality of the TOE is featured by difficulty of TOE (IC chip) forgeries realized by adoption of the Active Authentication function and strengthening Secure Messaging with PACE. The security characteristics of the Active Authentication function are achieved by protecting the internal confidential information (private key) in the TOE. And, the security characteristics of the strengthened Secure Messaging functionality are achieved by the use of the session key which possesses sufficient entropy.

Reading out the information kept secret in an IC chip requires advanced means of physical attacks, and it costs a certain amount of facilities and takes some time to decipher the strengthened Secure Messaging.

Assuming attackers possessing a high attack potential who are capable of such attacks, AVA_VAN.5 is required as the security assurance requirement for the vulnerability assessment. In addition, ALC_DVS.2 is adopted as the development security assurance requirement to provide stricter protection of development information used for an attack means.

When using the IC chip as the TOE, state of the art technologies are required for SFRs and design methods to realize such SFRs. However, there are no significant variations in the security functionality of product, and points to be checked for the vulnerability assessment are also well-defined. Consequently, EAL4, which is the top level for commercial product but does not require stringency as high as that for EAL5 whose target application is military use, is adopted as the development and manufacturing assurance requirements except development security and vulnerability assessment.

Note that ALC_DVS.2 does not have dependencies on other components, and the dependencies defined in AVA_VAN.5 are identical to those in AVA_VAN.3 (EAL4). Therefore, being identical to the EAL4 assurance package in terms of dependencies, dependencies among the security assurance components shown in Table 6 are all satisfied.

7. Glossary

7.1 CC Related

PP	Protection Profile
CC	Common Criteria; The same contents of the CC are also established as ISO/IEC 15408 Standards.
ST	Security Target
TOE	Target of Evaluation

7.2 ePassport Related

ICAO	International Civil Aviation Organization
SAC	Supplemental Access Control: This is written in 1.1.3 Supplemental Access Control of [TR_SAC] as follows. This Technical Report specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control. PACE MAY be implemented in addition to Basic Access Control, i.e. • States MUST NOT implement PACE without implementing Basic Access Control if global interoperability is required. • Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.
Passport manufacturer	An organization, which manufactures passport booklets and configures basic data (e.g. management data such as passport number, and Active Authentication Public Key and private key pair) to the TOE.
Passport office	An organization, which configures the passport booklet including the TOE with the personal information of the passport holder, and issues the passport. The passport offices are set up in various regions and serve as a counter to deliver the passport to the passport holder.
Active Authentication	Security mechanism, by which means the public key and private key pair based on the public key cryptography system is stored and the private key is kept secret in the IC chip that is a part of the TOE. The public key is transmitted to an external device trying to authenticate the TOE and the TOE is authenticated through cryptographic calculation by the challenge response system using the private key, which has been kept a secret in the TOE. The Active Authentication procedure has been standardized by ICAO.
Passive Authentication	Security mechanism, by which the digital signature of the passport issuing authority is applied to personal information data stored in the TOE, and the authenticity of data read from the TOE is verified by using the PKI system with assured interoperability both on the passport issuing and receiving sides. The Passive Authentication procedure has been standardized by ICAO.
Readout key	A key which is used at issuing a passport, and is embedded in the

	TOE at the manufacturing stage. Refer to Table 1 for operations which are permitted by successful verification.
Transport key	Same as above.
Active Authentication Information Access Key	Same as above.
MRZ data	Data which are printed on a surface of ePassport and readable with terminals.
Password key file	A file storing the key, which is derived from MRZ data, used for encryption of Nonce at the PACE procedure.
PACE v2 security information	Information used for PACE v2 such as cryptographic algorithms and domain parameters.

8. Reference

[DOC9303]	ICAO Doc 9303 Machine Readable Travel Documents Seventh Edition, 2015
[TR-03111]	BSI: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 2012
[TR_SAC]	Technical Report Supplemental Access Control for Machine Readable Travel Documents Version 1.1, 15 April 2014