Protection Profile for ePassport IC with Active Authentication

Version 1.00

February 15, 2010

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 (PP) specifies security requirements for IC chip for ePassport conforming to the ePassport Standards "ICAO Doc 9303 Part1, 6th Edition" provided by the International Civil Aviation Organization (ICAO).

This PP applies to IC chips designed for ePassports compatible with the Active Authentication (AA). The Active Authentication makes it possible to verify the identity and authenticity of the IC chip itself and prevent passport forgery using a false IC chip.

The Active Authentication is performed for each IC chip by a pair of its unique public key and private key. The public and private keys are stored in the IC chip. While the public key can be read through the external read access, the private key is kept confidential in the IC chip and only used for internal processing. In the event that the private key is read out from the IC chip, it may be abused to forge an ePassport. IC chips compatible with the Active Authentication shall protect the confidentiality of the private key from a high level of attack capability (e.g. special system or analysis technique).

This PP has been prepared following the rules and formats of Common Criteria (CC) Version 3.1. The developer of ePassport IC conforming to this PP shall prepare a Security Target (ST) that meets any and all requirements defined in this PP.

The ePassport IC should meet the technical specification in general required for the ePassport IC in addition to security functions that meet the requirements of this PP. Technical specification unrelated to the security functions fall outside the requirements of this PP and are separately presented by the procurer.

Part of the requirements of this PP includes reference to standards and materials issued by the ICAO. These standards and materials involve 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 this PP.

This PP has been prepared by the JBMIA under a commission from Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan. All contents of this PP are the copyright of Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan.

[Notation included in this PP]
This PP provides [Note] to prepare the ST conforming to this PP in various parts thereof. [Note] is supporting information to properly understand this PP, and shall not constitute a part of provisions or requirements thereof; provided, however, that since some of the notes serves as information useful for the readers of the ST, the said notes may be reprinted at the discretion of the editor of the ST and, in such cases, make modifications of the descriptions following the context of the ST.

Table of Contents

1. PP Introduction

1.1 PP Reference

Title:	Protection Profile for ePassport IC with Active Authentication
Version number:	1.00
Issue Date:	February 15, 2010
Editor:	JBMIA
Issuer:	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
Registration:	JISEC C0247

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 mounted to the said hardware (hereinafter, the term "IC chip" shall mean the "ePassport IC"). The hardware has a contactless communication antenna externally connected thereto and embedded in the plastic sheet together with the antenna to constitute part of ePassport.

1.2.2 TOE Usage and Main Security Functions

A passport is an identification document, issued by government or public organization, which certifies, for the purpose of international travel, the identity of its holder, generally in a booklet (passport-booklet form). The International Civil Aviation Organization (ICAO) of the United Nations has provided the Passport Booklet Guidelines. For conventional passports, all information necessary as the certificate of identity was printed on a paper booklet, and thereby this could cause these passports to be forged for illicit purposes. In order to prevent 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 passport issuing authority, a high level of forgery prevention effect can be achieved. However, digital signature is not enough to counter forgery by reproducing 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 the plastic sheet and then interfiled in the passport booklet. At immigration, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter referred to as the "terminal"). Information printed on the passport booklet in ordinary characters are encoded

in the same contents, printed in the machine readable zone (MRZ) of the passport booklet, and read by the optical character reader of the terminal. In addition, the information is digitized[1] and stored on the IC chip, i.e., the TOE. These digitalized data are read from 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. TOE operating power supply is generated in the TOE using wireless signal power supplied from the terminal.

The main security functions of the TOE are designed to protect data stored in the TOE from illicit reading or writing. The operation of the security functions applying to contactless communication with the terminal shall comply with the Basic Access Control and Active Authentication Standards defined by the ICAO Doc 9303 Part1[2].

Attacks against protection 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 a physical attack against the TOE. Attacks against the Active Authentication Private Key are assumed to be those performed by an attacker having a high attack potential.

The TOE provides the main security functions, including

- Basic Access Control (Mutual authentication and secure messaging);
- Active authentication support function (Making the terminal authenticate the TOE);
- Write inhibit function (Inhibition of 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 leakage due to physical attacks).

1.2.3 TOE Life Cycle

The TOE life cycle is described to define security requirements for the TOE. The TOE life

[1] Digital signature is added to individual digital data by the passport issuing authority in order to prevent the forgery of digital data. The verification 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.

[2] In this PP, the following two documents are collectively referred to as ICAO Doc 9303 Part1.
- ICAO Doc9303 Machine Readable Travel Documents Part1 Machine Readable Passports Sixth Edition Volume1and 2
- SUPPLEMENT to Doc9303-Part1-Sixth Edition Release7

cycle of general IC chips is often described in terms of seven life cycle phases. For the purposes of this PP, however, it is described in terms of four life cycle phases.

- 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 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 environment

Phase 1

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

Hardware for the IC chip, operating system, or application software for passport may be developed by a different developer, respectively. Where the TOE configuration items are developed across a number of sites, secure development environment is required for all configuration items.

Phase 2

Phase 2 is a manufacturing phase. In phase 2, hardware for the IC chip is manufactured, and operating system and application software for passport are embedded in this hardware. The software is often implemented in ROM format, but may be partially implemented as data in its nonvolatile memory. A file object necessary for an ePassport is created in the TOE and an IC chip identification serial number is written in the file object. The functional tests for the internal circuit of 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 to the operational environment are not considered, but proper development security shall be maintained to protect the confidentiality and integrity of the configuration items of the IC chip.

For the TOE in phase 2, the transport key, readout key, and active authentication information access key are configured and delivered to the passport issuing authorities.

Phase 3

The TOE in phase 3 is put under the control of the passport issuing authorities[3]. Under the control of the passport issuing authorities, no explicit attack against the TOE is assumed but, as the organizational security policy, security functionality that allows only an individual having authority to process the TOE is required for the TOE.

The TOE is interfiled in the e-passport booklet and information necessary for e-passport 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 function. After the completion of personalization of all information, the e-passport is issued to the holder thereof.

Phase 4

Phase 4 is a phase subsequent to the handover of passport booklet to the final user, i.e., 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. Information necessary for immigration procedures is protected against illicit reading by the TOE security function, except in the case where the information is read by the 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 TOE. The information assets in the TOE are protected against external unauthorized access by the TOE security function.

[3] In Japan, the National Printing Bureau and regional passport offices fall under the authorities. The National Printing Bureau 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.

2. Conformance Claim

2.1 CC Conformance Claim

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

- Part 2: Security Functional Components; Revision 3 Final Version [Japanese Version 1.0], July 2009, CCMB-2009-07-002
- Part 3: Security Assurance Components; Revision 3 Final Version [Japanese Version 1.0], July 2009, CCMB-2009-07-003

2.2 PP Claim

This PP claims no conformance to other PP.

2.3 Package Claim

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

2.4 Conformance Rationales

This 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 this 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 assigned an identifier name beginning with the letter "T.", "P.", or "A.", respectively. [Note] is added to individual description, as appropriate. [Note] is described to give way to the understanding of the contents of this PP to avoid misunderstanding thereof when referring to this PP, and not included in the text of the Security Problem Definition.

3.1 Threats

This section describes threats to be countered by the TOE. These threats shall be countered by the TOE or its operational environment independently or in combination with them.

T.Copy

An attacker trying to forge the ePassport may forge the ePassport by reading personal information with digital signature from the TOE and writing the reproduced data in an IC chip having the same functionality as that of the TOE. This attack results in damage to credit for the whole Passport Booklet including the TOE.

[Note 3-1] Where information retrieved from the authorized TOE is reproduced in an illicit IC chip, information stored in the TOE will be reproduced together with the digital signature, forgery protection by means of digital signature verification become disable. Since the original information can be protected against tempering 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 discriminating the facial image.

T.Logical_Attack

In the operational environment after TOE embedded Passport Booklet is issued, an attacker being in a situation to 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] Where an attacker has physical access to the Passport Booklet, the attacker will be able to visually read personal information printed on the Passport Booklet or optically read the printed MRZ data. Since the security functions of the TOE cannot prevent reading such data, the information and data stated above are not included in the threat-related assets to be protected by the TOE. In other words, the purpose of this threat 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 by the use of data that the attacker has read from the MRZ.

T.Physical_Attack

In the operational environment after TOE embedded Passport Booklet is issued, an attacker may try to disclose confidential information (active authentication private key) stored in the TOE by physical means. This physical means includes both of nondestructive attacks made without impairing the TOE functions and destructive attacks made by destructing part of the TOE to have mechanical access to the inside of the TOE.

[Note 3-3] An attack made by an attacker trying to read confidential information (active authentication private key) stored in the TOE through physical access to the TOE. Making such a physical attack will disable the security function operated according to the TOE program to demonstrate the original performance thereof, resulting in potential violation of SFR. The example of nondestructive attacks shows those measurements of leakage electromagnetic wave associated with the TOE operation and inducing malfunctions of security functions by applying environmental stress (e.g. changes in temperature or clock, or application of high-energy electric and magnetic 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 could be used to make the said attacks. The TOE having got attacked may not be reused as a ePassport IC. Even in such case, however, the disclosed private key may be abused to forge the TOE.

3.2 Organizational Security Policies

This section describes organizational security policies that apply to the TOE or operational environment. This PP includes conformance to the standards provided by ICAO and conditions required by the passport issuing authorities in Japan in the organizational security policies.

P.BAC

In the operational environment after TOE embedded Passport Booklet is issued, the TOE allows the terminal to read the given information from the TOE in accordance with the basic access control procedure defined by ICAO Doc 9303 Part 1. This basic access control procedure includes mutual authentication between the TOE and the terminals and secure messaging between the same. TOE files to be read are EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, and EF.SOD under the rules stated above. For any files that are not listed in this PP out of those stated above under the same rules, the handling thereof is not defined. Any users other than the TOE are unable to have access to the basic access key file and the private key file that have stored internal TOE data.

[Note 3-4] To meet global interoperability necessary for ePassport, the basic access control (BAC) procedure should be addressed. The mutual authentication function and the secure messaging function included in the BAC procedure are not intended to counter a high level of attacks, but have certain effect in preventing access to the internal TOE data through illicit devices. Accurately implementing the BAC procedure makes it possible to prevent a

skimming attack (acquisition of part of passport-specific information without opening the ePassport) and eavesdropping attack (acquisition of information contained in data by capturing communication data with terminals). The BAC procedure is regarded as a possible means to counter the reinforced basic attack capability. This PP has been prepared on the assumption of a high level of attack capability on the active authentication private key. However, the skimming attack and the eavesdropping attack countered by the BAC procedure do not fall under the category of such a high level of attack capability.

P.Authority

The TOE under the control of the passport issuing authorities allows only authorized users (persons who succeeded in readout key, transport key, or active authentication information access key verification) to have access to the internal TOE data, as shown in Table 3-1.

Table 3-1 Internal TOE data access management by passport issuing authorities

Authentication status*1	File subject to access control	Operation permitted	Reference: Data subject to operation
Successful verification with readout key	EF.DG13*2	Read	IC chip serial number (entered by manufacturer)
	EF.DG15		Active authentication public key
Successful verification with transport key	Transport key file	Write	Transport key data (update of old data)
	Basic access key file		Basic access control cryptographic key Authenticator generation key
	EF.DG1*3		MRZ data
	EF.DG2*3		Facial image
	EF.DG13*2/*3		Management data (Passport number and Booklet management number)
	EF.COM*3		Common information on basic coding rules
	EF.SOD*3		Security data related to passive authentication defined by ICAO Doc 9303 Part 1, Section IV, NORMATIVE APPENDIX 3
Successful verification with active authentication information access key	EF.DG15*3	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 authorized user. With regard to the file subject to access control included in this table and files storing the read key and active authentication information access key, user access not stated in this table or Notes is inhibited. (Control of access to terminals after issuing to the passport holder, i.e., <Basic access control>, is separately specified.)

*2 EF.DG13 has an IC chip serial number entered by the manufacturer and management data added by the passport issuing authorities.

*3 Read (Permitted/Not permitted) in case of successful key verification is not specified.

[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 (the management of cryptographic key is treated as user data). The TSF data file is not included in files subject to access control stated in Chapter 6, Section "Security Functional Requirements" and 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 invalidate authentication related to each key, thereby inhibiting reading or writing the file based on successful authentication thereof. Table 3-1 shows the relationship between the key used for authentication and its corresponding file in the TOE.

P.Prohibit

Any and all writing to the files in the TOE and reading from the files in the TOE based on successful authentication with readout key are inhibited after issuing to the passport holder. As the means, authentication invalidation through authentication failure with the transport key, readout key, and active authentication information access key (see P.Data_Lock) shall be used.

3.3 Assumptions

This section describes assumptions to be addressed in the operational environment of the TOE. These assumptions are needed for the TOE to validate security functionality.

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 is subjected to secure management and issuing procedures until it is 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 is maintained.

4. Security Objectives

This chapter describes security objectives for the TOE and its environment for the security problems described in Chapter 3. Section 4.1 describes the security objectives to be addressed by the TOE, 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 the security problems.

The security objectives for the TOE and the security objectives for the operational environment are represented by an identifier name beginning with the letter "O." or "OE.", respectively.

4.1 Security Objectives for the TOE

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

O.AA

The TOE shall provide a means to verify the authenticity of the IC chip itself composing the TOE in order to prevent the reproduction 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, address active authentication defined by ICAO Doc 9303 Part 1.

O.Logical_Attack

The TOE shall, under any circumstances, prevent confidential information in the TOE (active authentication private key) from being read outside the TOE through the contactless communication interface of the TOE.

O.Physical_Attack

The TOE shall, by a physical means, avert attacks trying to disclose confidential information in the TOE (active authentication private key) not through the contactless communication interface of the TOE. The physical means shall counter attacks applicable to the TOE out of known attacks against the IC chip taking into account nondestructive attacks and also destructive attacks.

O.BAC

This security objective applies to the operational environment after issuing the Passport Booklet. The basic access control procedure defined by ICAO Doc 9303 Part 1 shall be used to ensure the global interoperability of the ePassport. This procedure includes mutual authentication between the TOE and the terminals and secure messaging between the same.

Communication between the TOE and the terminals performed by the use of the said procedure shall only be permitted. Information the terminal reads from the TOE is stored in the EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, and EF.SOD files out of 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. For any files that are not listed in this PP out of those stated above under the same rules, the handling thereof is not defined. Any users other than the TOE shall not be able to have access to the basic access key file and the private key file that have stored internal TOE data.

According to the provisions of ICAO Doc 9303 Part 1, the common cryptographic key used by the basic access control procedure shall be generated from information printed on the data page of the Passport Booklet, and the contents of the information and the format to describe them shall also comply with the provisions stated above. Thus, the entropy of the said cryptographic key cannot in principle be increased above that specific to the information printed on the data page of the Passport Booklet. For this reason, with regard to the security functionality of the TOE provided by the basic access control procedure, in the case where a brute-force attack is assumed, the entropy specific to the information printed on the data page of the Passport Booklet becomes the upper limit of resistance force to the attack. The TOE shall meet the security requirements by accurately implementing the basic access control procedure.

[Note 4-1] The basic access control procedure uses a cryptographic key generated from the data printed in the MRZ of ePassport to perform mutual authentication and secure messaging. This cryptographic key can be generated from the printed data when the data page of the ePassport is opened, and does not require a high confidentiality level. The entropy of the key generated is also not as large as it can counter a high level of attacks. However, the security functionality of the basic access control procedure will not affect the protection of the active authentication private key. This security objective is not intended to counter a high level of attacks, but intended to accurately implement the basic access control procedure for the protection of the TOE against limited attacks including skimming and eavesdropping.

O.Authority

The TOE shall limit users and operation methods that have access to the internal TOE information, in the environment under the control of the passport issuing authorities according to the organizational security policy P. Authority, table 3-1.

O.Data_Lock

The operation of the internal TOE information shall be limited 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, in the case where the TOE detects an authentication failure with the readout key, transport key, or active authentication information access key, this security objective shall permanently inhibit reading and writing the internal TOE information permitted according to authentication related to each of the said keys. The security objective shall also apply to invalidate the readout key, transport key, or active authentication information access key in the case where the passport issuing authorities causes an intentional authentication failure 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 information are as listed in Table 3-1 of the organizational security policy P.Authority. After the security objective O.Data_Lock is implemented, only the access to TOE stated in the security objective O.BAC is permitted.

4.2 Security Objectives for the Operational Environment

This section describes security objectives that the TOE should address in the operational environment to solve problems with regard to the threats and organizational security policies defined as the security problems. In addition, the security objectives stated herein shall all be derived from the assumptions.

OE.Administrative_Env

The TOE being under the control of the authorities is subjected to secure management and treatment until it 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), the TOE shall be used in a situation in which the interoperability of the PKI environment is maintained in both the passport issuing state or organization and receiving state or organization.

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 4-1 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) parameters of the security problem definition.

Table 4-1 Correspondence between security problem definition and security objectives

Security problem definition \ Security objective	O.AA	O.Physical_Attack	O.Logical_Attack	O.BAC	O.Authority	O.Data_Lock	O.E.Administrative_Env	O.E.PKI
T.Copy	x							
T.Physical_Attack		x						
T.Logical_Attack			x					
P.BAC				x				
P.Authority					x			
P.Data_Lock						x		
P.Prohibit						x		
A.Administrative_Env							x	
A.PKI								x

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 further properly meet the assumptions.

T.Copy

In the case where an attacker uses the reproduction of personal information (with digital signature) read from the TOE with the IC chip having the same functionality as that of the TOE, the forged passport cannot be detected through verification by the digital signature. To prevent this attack, the security objective for the TOE: O.AA addresses embedding of data that can verify the authenticity of the IC chip itself in the TOE. This allows the TOE to detect illicit IC chips and prevent the forgery of passports, thus eliminating the threat T.Copy.

T.Logical_Attack

The security objective for the TOE: O.Logical_Attack makes it possible to inhibit reading confidential information (active authentication private key) in the TOE through the contactless communication interface of the TOE, under any circumstances.
Thus the threat T.Logical_Attack is eliminated.

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 by

physical means not through the contactless communication interface of the TOE. For the physical means, both nondestructive attacks and destructive attacks are considered, and countermeasures by which the TOE can counter known attacks against the IC chip. Thus the threat can be reduced to an adequate extent for the practical use.

P.BAC

The security objective for the TOE: O.BAC allows only the authorized personnel (terminal) to read the internal TOE information through a secure communication path by applying the basic access control procedure defined by ICAO Doc 9303 Part 1. O.BAC covers all contents of P.BAC, thus the organizational security policy P.BAC 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 covers 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 user of the TOE as the implementation means. Actions required for the TOE to address P.Prohibit overlap those for the organizational security policy P.Data_Lock that has assumed an illicit attack against 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

This PP shall define no extended components.

6. Security Requirements

6.1 Security Functional Requirements

The security functional requirements (SFRs) defined by this PP all use components included in CC Part 2. Table 6-1 shows the list of SFRs.

Table 6-1 List of SFRs

Chapter No.	Identifier name	
6.1.1	FCS_CKM.1	Cryptographic key generation
6.1.2	FCS_CKM.4	Cryptographic key destruction
6.1.3	FCS_COP.1a	Cryptographic operation (Active authentication)
6.1.4	FCS_COP.1m	Cryptographic operation (Mutual authentication)
6.1.5	FCS_COP.1s	Cryptographic operation (Secure massaging)
6.1.6	FDP_ACC.1a	Subset access control (Issue processing)
6.1.7	FDP_ACC.1b	Subset access control (Basic access control)
6.1.8	FDP_ACF.1a	Security attribute based access control (Issue processing)
6.1.9	FDP_ACF.1b	Security attribute based access control (Basic access control)
6.1.10	FDP_ITC.1	Import of user data without security attributes
6.1.11	FDP_UCT.1	Basic data exchange confidentiality
6.1.12	FDP_UIT.1	Basic data exchange integrity
6.1.13	FIA_AFL.1a	Authentication failure handling (Active authentication information access key)
6.1.14	FIA_AFL.1b	Authentication failure handling (Transport key)
6.1.15	FIA_AFL.1r	Authentication failure handling (Readout key)
6.1.16	FIA_UAU.2	User authentication before action
6.1.17	FIA_UAU.4	Single-use authentication mechanism
6.1.18	FIA_UAU.5	Multiple authentication mechanism
6.1.19	FIA_UID.2	User identification before action
6.1.20	FMT_MTD.1	Management of TSF data
6.1.21	FMT_SMF.1	Specification of management functions
6.1.22	FMT_SMR.1	Security roles
6.1.23	FPT_PHP.3	Resistance to physical attack
6.1.24	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*, but this PP adds no refinement.

- For the selection of operation, items not subject to selection are shown by strike-through (~~XXX~~).
- This PP has some unspecified operations, which are shown as [assignment: *XXX* (*Italicized and underlined*). The ST author shall complete these unspecified operations.

The following section describes SFRs defined by this PP.

6.1.1 FCS_CKM.1 Cryptographic key generation

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 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic transport key and authenticator generation transport key generation algorithm defined by the following*] and specified cryptographic key sizes [assignment: *16 byte*] that meet [assignment: *Rules for secure messaging included in the Basic Access Control specified by ICAO Doc 9303 Part 1*].

6.1.2 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 deleting cryptographic keys on volatile memory by shutting down power supply and rewriting new cryptographic key data, and [assignment: other cryptographic key destruction method]]*] that meet the following: [assignment: *none*].

6.1.3 FCS_COP.1a Cryptographic operation (Active 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.1.1a The TSF shall perform [assignment: *digital signature for active authentication data*] in accordance with a specified cryptographic

algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *the Digital Signature Standards (complying with ISO/IEC 9796-2:2002 Digital signature scheme 1) used for active authentication defined by ICAO Doc 9303 Part 1*].

[Note 6-1] To perform the operation of the assignment for this requirement, the ST author shall achieve a match with the policies of the passport issuing authorities.

6.1.4 FCS_COP.1m Cryptographic operation (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.1.1m The TSF shall perform [assignment: *authentication data encryption or decryption for mutual authentication and authenticator generation and verification*] in accordance with a specified cryptographic algorithm [assignment: *Triple DES in CBC mode*] and specified cryptographic key sizes [assignment: *16 byte*] that meet the following: [assignment: *Standards for mutual authentication system included in the Basic Access Control defined by ICAO Doc 9303 Part 1*].

6.1.5 FCS_COP.1s Cryptographic operation (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.1.1s The TSF shall perform [assignment: *cryptographic operation shown in Table 6-2*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm shown in Table 6-2*] and cryptographic key sizes [assignment: *cryptographic key sizes shown in Table 6-2*] that meet the following: [assignment: *Standards for secure messaging included in the Basic Access Control defined by ICAO Doc 9303 Part 1*].

Table 6-2 Secure messaging encryption system

Cryptographic algorithm	*Cryptographic key size*	*Cryptographic operation*
Single DES in CBC mode	*8 bytes*	*Authenticator generation and verification (excluding the final block of message)*
Triple DES in CBC mode	*16 bytes*	*Message encryption and decryption, Authenticator generation and verification (final block of message)*

6.1.6 FDP_ACC.1a Subset access control (Issuing process)

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

FDP_ACC.1.1a The TSF shall enforce [assignment: *Issue processing access control SFP*] on [assignment: Subject *[User process], Object [Files shown in Table 3-1 of Organizational security policy P.Authority; except the transport key file] and List of operations among subjects and objects addressed by SFP [Data Input/Output operation to/from object]*].

[Note 6-2] The data "transport key" stored in the "transport key file" out of data files shown in Table 3-1 of P.Authority are TSF data used as user authentication data. This PP defines the management of the transport key with the management requirement FMT_MTD.1 and, therefore, does not include the transport key file in the access control subjects. However, this reflects the discrimination between the user data and the TSF data for CC, but does not mean a difference in mechanisms in terms of implementation.

6.1.7 FDP_ACC.1b Subset access control (Basic access control)

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

FDP_ACC.1.1b The TSF shall enforce [assignment: *Basic access control SFP*] on [assignment: *Subject [Process on behalf of terminal], Object [Files EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM , EF.SOD, Basic access key file, and Private key file] and List of operations among subjects and objects addressed by SFP[Reading data from object]*].

[Note 6-3] ICAO Doc 9303 Part 1 defines the files EF.DG3 to 12, EF.DG14, and EF.DG16 in addition to the files listed above. These files are not used by this TOE, therefore this PP does not define addressing thereof. On the other hand, in the case where a procurer in any country other than Japan uses this PP, the said files may need to be added. Even in the case where this PP or ST author add the files to objects to make a change to SFR of this PP, accurate conformance to this PP will be maintained as far as the SFR of the PP is 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 where the accurate conformance to this PP is maintained.

6.1.8 FDP_ACF.1a Security attribute based access control (Issuing process)

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT.MSA.3 Static attribute initialization

FDP_ACF.1.1a The TSF shall enforce [assignment: *Issue processing access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [User process], object [Files shown in Table 3-1 of the organizational security policy P.Authroity; except the transport key file], and, for each, the SFP-relevant security attribute [Authentication status shown in Table 3-1 of the operational security policy P.Authority]*].

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: *Where the authentication status shown in Table 3-1 of the organizational security policy P.Authority is met, an operation to the file connected to the said authentication status is allowed*].

FDP_ACF.1.3a The TSF shall explicitly authorize 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: *none*].

6.1.9 FDP_ACF.1b Security attribute based access control (Basic access control)

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT.MSA.3 Static attribute initialization

FDP_ACF.1.1b The TSF shall enforce [assignment: *Basic access control SFP*] to objects based on the following: [assignment: *Subject controlled under the indicated SFP [Process on behalf of terminal], object [Files EF.DG1, EF.DG2, EF.DG13, EF.DG15, EF.COM, EF.SOD], and the security attribute [Authentication status of terminal based on mutual authentication]*].

FDP_ACF.1.2b 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 successfully authenticated, subjects are allowed to read data from objects*].

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

FDP_ACF.1.4b The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *Inhibition of access of subjects to the basic access key file and private key file*].

6.1.10 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 initialization

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

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

FDP_ITC.1.3 The TSF shall enforce the following rules when user data importing controlled under the SFP from outside the TOE: [assignment: *Association between file subject to writing and data as specified by "Access to be permitted" in Table 3-1 of the organizational security policy P.Authority*].

6.1.11 FDP_UCT.1 Basic data exchange confidentiality

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

FDP_UCT.1.1 The TSF shall enforce [assignment: *Basic access control SFP*] to be able to [selection: *transmit, receive*] user data in a manner protected from unauthorized disclosure.

6.1.12 FDP_UIT.1 Data exchange integrity

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

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

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

6.1.13 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 6-4] The ST author shall specify a positive integer number in the 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 "No authentication"*)].

6.1.14 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 6-5] 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 "No authentication"*)].

6.1.15 FIA_AFL.1r Authentication failure handling (Read 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 6-6] 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 "No authentication"*)].

6.1.16 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.17 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*].

6.1.18 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 6-3*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms shown in Table 6-3 provide authentication*].

Table 6-3 Multiple authentication mechanisms

Authentication mechanism name	Rule applicable to authentication mechanism
Transport key	Verification with transport keys that have been already stored in the TOE
Readout key	Verification with readout keys that have been already stored in the TOE
Active authentication information access key	Verification with active authentication information access keys that have been already stored in the TOE
Mutual authentication	Rules for authentication of terminals according to the mutual authentication procedure defined by ICAO Doc 9303 Part 1

6.1.19 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf ofthat user.

6.1.20 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT.SMF.1 Specification of management function

FIA_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 6-7] This requirement relates to the configuration of transport key used to transport the TOE from the passport booklet manufacturer to the regional passport

office in phase 3. In this requirement, the authorized personnel who are allowed to manage TSF data are the staff of the National Printing Bureau. 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 National Printing Bureau or the 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 National Printing Bureau 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".

6.1.21 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*].

6.1.22 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 role [assignment: *authorized personnel of the passport issuing authorities*].

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

6.1.23 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 shown in the following list of physical tampering scenarios*] to the [assignment: *hardware of the TOE and firmware and software composing the TSF*] by automatically responding such that the SFRs are always enforced.

[List of physical attack scenarios]

- An attack, which discloses confidential information (active authentication private key) by destructing the outer shell of the TOE and analyzing the behavior of the TOE through physical probing and manipulation to the internal circuit.
- An attack, which discloses confidential information (active authentication private key) by impairing normal TOE operation

through the application of environmental stress (e.g. application of temperature, power supply voltage, or clock outside the normal operating range, or application of electromagnetic pulse, or light irradiation) to the TOE in operation and analyzing the behavior of the TOE at that time.

- An attack, which discloses confidential information (active authentication private key) by analyzing the behavior of the TOE through monitoring of electromagnetic waves leaking from the TOE in operation.

[Note 6-8] Security functional requirements used to counter physical attacks all have been summarized in this requirement. Attacks that monitor leakage of electromagnetic waves associated with the operation of the TOE may not involve interference with or damage to the TSF. As means to counter the said attacks, physical means (e.g. electromagnetic shielding) may be used or logic means (e.g. randomization of power consumption) may be used in combination. However, it is reasonable to include the attacks stated above in the same category as that of other physical attacks in terms of using physical means not through the logical interface of the TOE as tampering means. Therefore, monitoring attacks were made against the physical attack scenarios in this requirement to define requirements to counter such attacks.

6.1.24 FTP_ITC.1 Inter-TSF trusted channel

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

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

FTP_ITC.1.2 The TSF shall permit [selection: ~~*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 6-9] Communication between terminal and TSF shall be performed via the secure messaging channel defined by ICAO Doc 9303 Part 1. After the secure messaging channel is established, only the secure messaging channel is 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 6-4. These components are all included in CC Part 3. Components except ALC_DVS.2 and AVA_VAN.5 are included in the EALA4 assurance

package. ALC_DVS.2 is a high-level component of ALC_DVS.1 and AVA_VAN.5 is that of AVA_VAN.3.

This PP applies no operation to all components shown in Table 6-4.

Table 6-4 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
Test	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 Correspondence between Security Objectives and Security Functional Requirements

Table 4-1 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 6.5 Correspondence between security objectives for the TOE and SFRs

Security objective for the TOE / SFR	FCS_CKM.1	FCS_CKM.4	FCS_COP.1a	FCS_COP.1m	FCS_COP.1s	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_UCT.1	FDP_UIT.1	FDP_ITC.1	FIA_AFL.1a	FIA_AFL.1d	FIA_AFL.1r	FIA_UAU.2	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_PHP.3	FTP_ITC.1
O.Logical_Attack							x		x															
O.Physical_Attack																							x	
O.AA			x			x		x				x												
O.BAC	x	x		x	x		x		x	x	x	x				x	x	x	x					x
O.Authority						x		x				x				x		x	x	x	x	x		
O.Data_Lock													x	x	x									

6.3.1.2 Correspondence Relationship Rationale

This section describes rationales for that the security objectives for the TOE are met by their corresponding SFR 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 ICAO Doc 9303 Part 1. This active authentication is an act for a terminal to authenticate the IC chip of the TOE, and the TOE itself needs not to provide any authentication mechanism. The TOE is authenticated by properly addressing the authentication procedure. To address requirements for the authentication procedure from the terminal, the TOE incorporates the public key and private key pair and performs cryptographic operation using the private key defined by FCS_COP.1a. 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. The security objective O.AA is thoroughly 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. FDP_ACC.1b and FDP_ACF.1b deny reading of data from the private key file by the user process on behalf of the terminal. The security objective O.Logical_Attack is thoroughly achieved by the said SFRs.

O.Physical_Attack

Attack scenarios trying to disclose the active authentication private key that is confidential information by a physical means are stated in the list of physical attack scenarios 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 thoroughly achieved.

O.BAC

FIA_UID.2 and FIA_UAU.2 provides the TOE service for the user (equivalent to a terminal) that has succeeded in identification and authentication. User authentication requires the mutual authentication procedure with the basic access control defined by ICAO, which is defined by FIA_UAU.5. This 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 the basic access control is defined by FDP_UCT.1 and the requirements for the protection of transmitted and received data by FDP_UIT.1 and cryptographic communication channels by FTP_ITC.1. Further, with regard to cryptographic processing required for the basic access control procedure, FCS_COP.1m defines cryptographic operations necessary for the mutual authentication procedure and FCS_COP.1s defines cryptographic operations for secure messaging. With regard to the cryptographic keys used for secure messaging, FDP_ITC.1 defines the import of basic access keys, FCS_CKM.1 defines the generation of session keys, 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.1b and FDP_ACF.1b are defined. The security objective O.BAC is thoroughly achieved by the said SFRs.

O.Authority

For TOE processing by the passport issuing authorities, the identification and authentication requirements FIA_UID.2 and FIA_UAU.2 are applied, in order to grant the processing authority only to the duly authorized user. For user authentication mechanisms, FIA_UAU.5 defines the use of the transport key, readout key, or active authentication information access key. The rules governing access control with FDP_ACC.1a and FDP_ACF.1a are applied to the user that has succeeded in authentication by verification with the said key and access to the internal TOE information defined by O.Authority is granted to that user. The user operation includes writing of the authentication key (transport key), cryptographic keys (active authentication public key and private key pair, and basic access key for secure messaging), and other user data in the TOE. Correspondence between object and security attributes for 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 thoroughly achieved by the said SFRs.

O.Data_Lock

When the active authentication information access key, transport key, or readout key causes a failure in authentication, the security objective of permanently inhibiting authentication corresponding to the relevant key is thoroughly 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 6-6 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 6-6 Dependencies for SFRs

SFR	Dependencies	Support for the Dependencies
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1s and FCS_CKM.4 support to satisfy the dependencies.
FCS_CKM.4	[FDP_ITC.1 or FDP_ ITC.2 or FCS_CKM.1]	FCS_CKM.1 supports to satisfy the dependency.
FCS_COP.1a	[FDP_ITC.1 or FDP_ ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. Since the modification and destruction of cryptographic keys are inhibited, the destruction requirement FCS_CKM.4 does not apply to.
FCS_COP.1m	[FDP_ITC.1 or FDP_ ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 supports. Since the modification and destruction of cryptographic keys are inhibited, the destruction requirement FCS_CKM.4 does not apply to.
FCS_COP.1s	[FDP_ITC.1 or FDP_ ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 and FCS_CKM.4 support to satisfy the dependencies.
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a supports to satisfy the dependency.
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b supports to satisfy the dependency.
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a supports. Objects are generated by default configuration, but not generated in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file generation does not apply to.
FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b supports. Objects are generated by default configuration, but not generated in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file generation does not apply to.
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACF.1a supports. Objects are generated by default configuration, but not generated in the operational environment of the TOE. Therefore, FMT_MSA.3 related to file generation does not apply to.
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1 and FDP_ACC1b support to satisfy the dependencies.
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FTP_ITC.1 and FDP_ACC1b support to satisfy the dependencies.
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.2 supports to satisfy the dependency.
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.2 supports to satisfy the dependency.
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.2 supports to satisfy the dependency.
FIA_UAU.2	FIA_UID.1	FIA_UID.2 supports to satisfy the dependency.
FIA_UAU.4	No dependencies	N/A
FIA_UAU.5	No dependencies	N/A
FIA_UID.2	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.2 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 property of this TOE is focused on the difficulty in forging the TOE (IC chip) by adopting the active authentication function. This security property is achieved through the protection of confidential information (private key) stored in the TOE. Reading confidential information from the IC chip requires an advanced physical attack means. The TOE requires AVA_VAN.5 as the security assurance requirement for the vulnerability assessment on the assumption of an attacker having a high attack potential enabling the said attack. In this connection, ALC_DVS.2 is adopted as the development security assurance requirement to provide stricter protection of development information used for an attack means.

In contrast, to use the IC chip as the TOE, leading-edge technologies are required for SFRs and design methods for realizing the SFRs. However, there are no significant variations in the security functionality of product, and check points 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, is adopted as the development and manufacturing assurance requirements except development security and vulnerability assessment.

Further, ALC_DVS.2 has no dependencies on other components, and dependencies defined for AVA_VAN.5 are the same as those for AVA_VAN.3 (EAL4). As a result, dependencies is same as those for the EAL4 security assurance package, dependencies among the security assurance components shown in Table 6-4 are all satisfied.

7. Glossary

7.1 CC Related

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

7.2 ePassport Related

ICAO	International Civil Aviation Organization
National Printing Bureau	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 personal information of the passport holder to the passport booklet including the TOE and issues the passport. The passport office is set up in various regions and serves as contact 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 encryption 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 delivered 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 put on 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.