Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Protection Profile (PP)

Application Date/ID	2015-11-30 (ITC-5574)
Certification No.	C0499
Sponsor	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
PP Name	Protection Profile for ePassport IC with SAC (PACE) and Active Authentication
PP Version	1.00
PP Conformance	None
Assurance Package	EAL4 Augmented with ALC_DVS.2, AVA_VAN.5
Developer	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan
Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above PP is certified as follows.
2016-03-22

Junichi Kondo, Technical Manager
Information Security Certification Office
IT Security Center
Technology Headquarters

Evaluation Criteria and other standards : The PP is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass

In accordance with the Requirements for IT Security Certification specified by Information-technology Promotion Agency, Japan, "the Protection Profile for ePassport IC with SAC (PACE) and Active Authentication", has been evaluated based on the standards required and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report is to report the sponsor, Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan as the developer of the IT Security Evaluation of "Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, Version 1.00" (hereinafter the "PP" [12]) on certification results, produced through the evaluation of the PP [12] conducted by ECSEC Laboratory Inc. Evaluation Center (hereinafter "Evaluation Facility") with completion date of March 9th, 2016. This report also provides security information to procurement entities and consumers interested in the PP.

Readers of this Certification Report are advised to refer to the PP [12] corresponding to this report. Details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements for the TOE claiming conformance to PP [12] are specifically described in the PP [12].

This Certification Report assumes "developers who develop and supply ePassports conforming to PP [12] and the passport issuing authorities who procure ePassports" to be intended readers. Note that the Certification Report only presents the certification result based on assurance requirements to which the PP conforms, and does not intend to guarantee an individual IT product itself.

Reference should be made to Chapter 8 for the terms used in this Certification Report.

1.1 Evaluated PP

An overview of security functions required in the PP [12] is provided as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package required by the PP is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.
In addition, PP and ST that claims conformance to the PP [12] shall claim strict conformance.

1.1.2 PP Overview

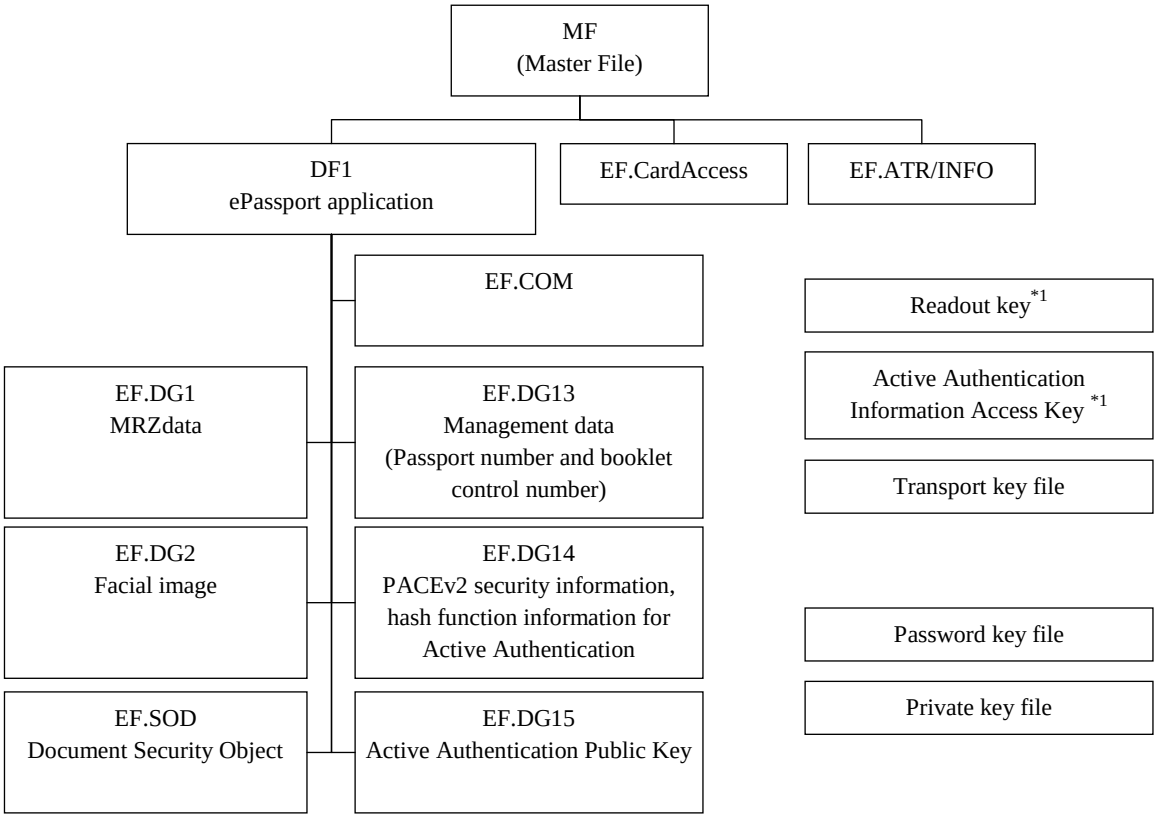
The PP [12] specifies security requirements related to the ePassport IC to be bound in the passport, conforming to ePassport specifications [15] published by the International Civil Aviation Organization (ICAO).

The ePassport IC including necessary software is the TOE for the PP [12]. This ePassport IC is composed of IC chip hardware with a contactless communication interface, basic software (operating system) and an ePassport application program to be installed in the IC. An external antenna used for contactless communication is connected to the IC chip that will be embedded together with the antenna in a plastic sheet to constitute a portion of a passport booklet.

When a passport holder goes through an immigration process, the immigration official inspects the passport booklet using a passport inspection terminal (hereinafter a “terminal"). The whole Information, printed on the passport booklet in ordinary characters, will be encoded and printed in the machine readable zone (MRZ) of the passport booklet,

then read by the optical character reader of the terminal. Note that the information is digitized[1] and stored in the IC chip, the TOE. The digitized data is read out by the terminal via the contactless communication interface of the TOE. The digitized data also includes a facial image.

Figure 1-1 is a recomposed figure of Figure 2 in Part 10 of ePassport specifications [15] to explain the PP overview.



*1 It is not stated as a file in PP [12].

Figure 1-1 File structure of ePassport IC

The PP [12] requires that, prior to reading of the files relating to the ePassport application, the terminal and the TOE to be mutually authenticated and the Secure Messaging to be applied to the communication between them. There are two mechanisms of mutual authentication and Secure Messaging specified in ePassport specifications [15]: Basic Access Control (BAC) and Password Authenticated Connection Establishment v2 (PACE v2). The latter utilises public key cryptography and increases security strength of the session key used in Secure Messaging.

Figure 1-2 shows how BAC and PACE are involved in the procedure for the terminal to access ePassport IC where either BAC or PACE is applied.

[1] In order to prevent the forgery of digital data, digital signature is applied to individual digital data by the passport issuing authorities. The verification process of the digital signature has been standardized by ICAO as Passive Authentication. PKI that provides interoperability for all member States of ICAO is used for the entire process from applying a digital signature through the verification thereof with the terminal, so as to support Passive Authentication. Since Passive Authentication is performed without involvement of the security functions of the TOE, from signing through its verification (including PKI as a background), it is not included in the security requirements for the TOE.

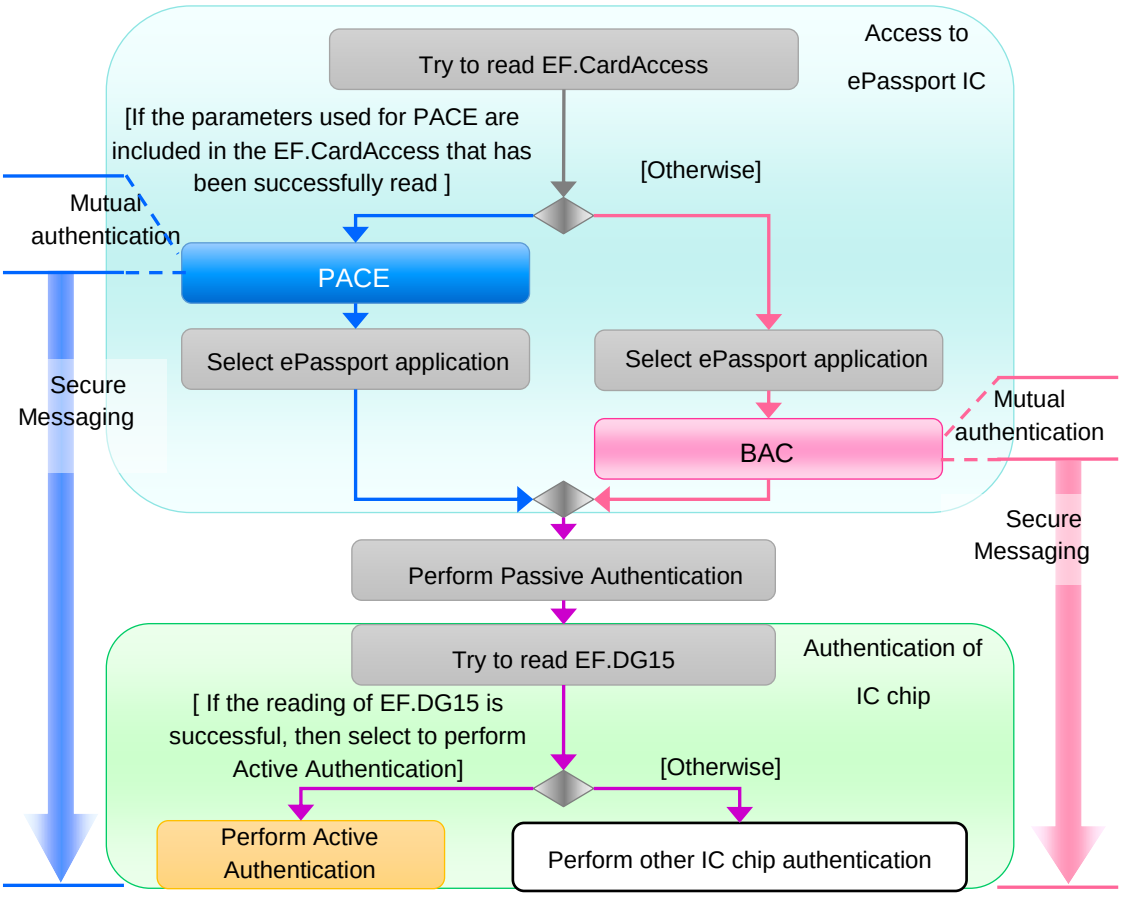


Figure 1-2 Procedure for a terminal to access an ePassport IC

While PACE is considered to be a future standard for mutual authentication and Secure Messaging, Part 11 of ePassport Specifications [15] does not permit to implement only the PACE without BAC in an IC chip until the end of 2017 to ensure its compatibility.

The PP [12] specifies the following IC as a TOE: an IC chip which does not need the BAC function nor the BAC disable function while having the PACE function. On the other hand, the PP [13] specifies that an IC chip requiring the BAC function and the BAC disable function as a TOE.

It is intended to use these two PPs in the following manner: The vulnerability analysis of BAC function will be performed with AVA_VAN.3, and the vulnerability analysis of the rest of security functions will be performed with AVA_VAN.5, by evaluating and certifying a TOE based on PP [12], and the same TOE based on PP [13] simultaneously. Following this approach, even if an ePassport IC implementing BAC is delivered to the passport issuing authorities, it will be possible to issue the ePassport that accepts only PACE for mutual authentication and Secure Messaging but has been practically evaluated with AVA_VAN.5, by using the BAC disable function.

In order to prevent copying of ePassport IC, the PP [12] requires an Active Authentication function proving the authenticity of the IC chip by a challenge-response protocol using public key cryptography. The previously certified PP [21] also required the Active Authentication but the cipher used for the Active Authentication has been changed from RSA to ECDSA in the PP [12].

The TOE life-cycle is divided into four phases, as shown in Figure 1-3.

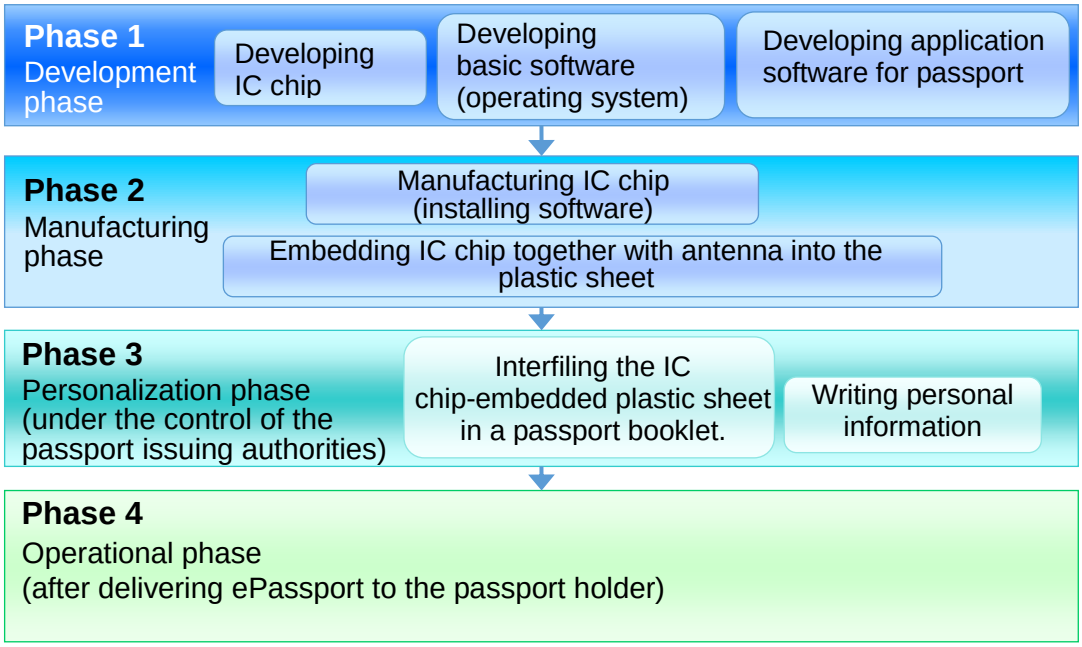


Figure 1-3 Life-cycle of a TOE conforming to the PP [12]

Though threats to the operational environment in Phases 1 and 2 have not been assumed, proper development security must be maintained to protect confidentiality and integrity of development data and the components of IC chips. In Phase 3, a security functionality is required so that only an authorised person will be allowed to process the TOE. Phase 4 requires a security functionality that can counter the attacks made by attackers possessing a High attack potential.

1.1.3 Overview of security functions

The PP [12] requires the TOE to provide the following functions: a function to protect data stored in the TOE from unauthorised reading and writing, PACE function specified in Part 11 of ePassport specifications [15], an Active Authentication, a protection function in transport and tamper-resistance to physical attacks. The overviews of these functions are shown below.

(1) Password Authenticated Connection Establishment (PACE)

The TOE performs mutual authentication with a terminal and applies Secure Messaging to communication with the terminal having succeeded in mutual authentication to permit the terminal to read access-controlled files in the TOE.

Ciphers used in mutual authentication and Secure Messaging for PACE are key establishment scheme using public key cryptography (ECDH[2]), a symmetric key cipher (AES[3]) and a hash function (SHA-1[4] or SHA-256[5])

(2) Active Authentication

[2] Although the option of using DH is also described in ePassport specifications [15], ECDH is selected in the PP [12].
[3] Although the option of using Triple DES is also mentioned in ePassport specifications [15], AES is selected in the PP [12]. In the PP [12], it is required to support both 128-bit AES key and 256-bit AES key.
[4] SHA-1 is used when using 128-bit AES key.
[5] SHA-256 is used when using 256-bit AES key.

In order to prevent copying of ePassport IC, the TOE provides an Active Authentication function to prove the authenticity of the IC chip by a challenge-response using public key cryptography.

Ciphers used in the Active Authentication are a digital signature algorithm (ECDSA[6]) and a hash function (SHA-256 or SHA-384).

(3) Write protection function

A function that prevents any writing to the files in the TOE once a passport has been issued to a passport applicant.

(4) Protection function in transport

The TOE provides a function allowing access to the given files in the TOE only after the authentication is successfully completed using a transport key, in order to protect IC cards from unauthorised use during transport.

(5) Tamper-resistance to physical attacks

The TOE security functionality (TSF) also counters physical attacks against its hardware and software that constitutes the TSF. Assumed attacks for the TOE are the same as for IC cards in general. There exists various attacks using physical means, such as physical manipulation of the IC chip, disclosure and/or modification of information by probing, disclosure of the cryptographic key by monitoring and/or analysing electromagnetic emanation of the TOE.

1.1.3.1 Threats and Security Objectives

The TOE conforming to the PP [12] counters each threat as follows using security functions.
A conventional passport as an ID including all necessary information printed on a paper booklet could have been forged and used by an unauthorised person. . In order to solve this problem, an ePassport IC has a digital signature issued by the official passport issuing authorities applied to digital data stored in the IC chip, and adopts Passive Authentication so as to confirm authenticity of the data read out from the IC chip by using PKI system, in which interoperability between the passport issuing end and receiving end is guaranteed.

Passive Authentication is, however, not enough to counter a forgery made by copying personal information with the official signature and then storing it in another IC chip. Therefore, the PP [12] adopts a challenge-response protocol using public key cryptography called Active Authentication specified in the ePassport specifications [15] so that it can restrict the reading of a private key used for the Active Authentication (hereinafter “Active Authentication Private Key”) from the IC chip to counter the forgery.

The ePassport specifications [15] have adopted the file system specified in ISO/IEC 7816-4. Assuming that the Active Authentication Private Key is also stored in this file system, it might be read out using commands specified in ISO/IEC 7816-4. The PP [12] requires the TOE to reject read access to the key in order to counter such threats.

Data available to be read out from an ePassport IC contains a facial image and information

[6] Although the option of using RSA is also described in the ePassport specifications [15], ECDSA is selected in the PP [12]. Taking it into account, the signature shall be generated using 256-bit or 384-bit private key. SHA-256 is used in case of 256-bit private key, and SHA-384 is used for 384-bit.

for Passive Authentication. It is assumed that there will be some attempts to disclose and/or modify communication data between the ePassport IC and the terminal at the immigration inspection counter. This threat can be countered by applying mutual authentication as well as Secure Messaging between the TOE and the terminal.

Because of the nature of its physical embodiment, an IC chip mounted on an IC card may leak internally processed information through power consumption and electromagnetic emanation. Disclosure of the data in the IC chip by physical probing, physical manipulation of the IC chip circuit, and malfunction due to environmental stress also need to be considered. Thus the TOE is required to provide the functionality to protect TSF against such physical attacks.

1.1.4 Disclaimers in Certification

The PP [12] declares that the PACE is mutual authentication and secure messaging functions. The PACE, as specified in the ePassport specifications, [15] is a mechanism to counter only an attack made by an attacker who does not know MRZ data, in which the attacker interrupts wireless communication to try to eavesdrop and tamper information read out from an ePassport IC to a terminal.

According to the ePassport specifications [15], MRZ data is the information necessary to break into the PACE, and therefore it is possible to read out information for Passive Authentication eventually by masquerading as a legitimate terminal if the attacker can obtain the MRZ data. Thus the authentication cannot counter the threat from the attacker who knows MRZ data trying to break in the PACE to read out data from the ePassport IC. However, even if the attacker can obtain the MRZ data, attackers cannot logically read out an Active Authentication Private Key as long as the TOE conforms to the PP [12].

Although the PP [12] requires the TOE to have Active Authentication support function for protecting the ePassport IC from being copied, the TOE function by itself cannot prevent abuse of the forged passport. In order for the Active Authentication mechanism to properly function as a system, it must have confidentiality of the Active Authentication Private Key as well as integrity and authenticity of the Active Authentication public key. In accordance with assumption A.Administrative_Env discussed later, users authorised by the passport issuing authorities need to securely perform the following:

- Generate an Active Authentication key pair
- Apply the digital signature to the Active Authentication public key
- Store the Active Authentication key pair on the ePassport IC

In addition, users authorised by the passport issuing authorities need to securely manage the key pair(s) to be used to generate a digital signature for data stored on the ePassport IC and maintain the PKI environment appropriately, in accordance with assumption A.PKI described later.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme operated by the Certification Body, the Evaluation Facility has conducted and completed an IT security evaluation in March 2016 based on the functional and assurance requirements related to the PP [12]. The evaluation has been made according to the publicised documents: "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2] and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

Through the verification of the Evaluation Technical Report [14] and the Observation Reports ([18][19][20]) prepared by the Evaluation Facility as well as relevant evaluation documentations, the Certification Body has confirmed that the PP [12] evaluation was conducted in accordance with the prescribed procedure.

Certification oversight reviews have also been prepared for those concerns found in the certification process.

The Certification Body confirmed that all the concerns have been fully resolved and the PP evaluation has been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either [10] or [11]).

The Certification Body has completed the certification activities upon the creation of this Certification Report based on the Evaluation Technical Report.

2. Identification

The PP [12] is identified as follows:

Name of PP:	Protection Profile for ePassport IC with SAC (PACE) and Active Authentication
Version of PP:	1.00
Developer:	Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

3. Security Policy

This chapter describes security function policies adopted by the TOE conforming to the PP [12] to counter threats, and organisational security policies.

The PP [12] requires the TOE to have following seven functions:

- Password Authenticated Connection Establishment (PACE) function (mutual authentication and secure messaging)
- Active Authentication support function (prevention of forgery of an ePassport IC chip)
- Write protection function (protection on writing data after an issuance of a passport)
- Protection function in transport (A TOE protection against attacks during transport before its issuance)
- Tamper resistance (protection against leakage of confidential information caused by physical attacks)

3.1 Security Function Policies

The PP [12] specifies security functions to counter the threats described in 3.1.1.1 and satisfy the organisational security policies described in 3.1.2.1.

3.1.1 Threats and Security Functions

3.1.1.1 Threats

The PP [12] assumes the threats described in Table 3-1 and requests the TOE to provide security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.Copy[7]	An attacker may forge the ePassport 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 the TOE. [Note] If information retrieved from the legitimate TOE is copied into an illicit IC chip, information stored in the TOE will be copied together with the associated digital signature, which makes forgery protection by means of digital signature verification ineffective. Since the

[7] The threat T.Copy points out the limitation of the ePassport IC which only supports the Passive Authentication.

Identifier	Threat
	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 ensure the detection of forged passport just by comparing the facial image.
T.Logical_Attack[8]	In the operational environment after an issuance of a TOE embedded passport booklet, an attacker who can read the MRZ data of the passport booklet may attempt to read confidential information (Active Authentication Private Key) stored in the TOE via the contactless communication interface of the TOE. [Note] If an attacker can physically access 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 accessing the said TOE via the contactless communication interface using data that the attacker has read from the MRZ.
T.Communication_Attack[9]	In the operational environment after an issuance of a TOE embedded passport booklet, an attacker who does not know about MRZ data may interrupt the communication between the TOE and terminal to disclose and/or tamper communication data that should be kept confidential. [Note] As for an attack which interrupts communication

[8] The threat T.Logical_Attack indicates a possibility that the Active Authentication Private Key may be readout using commands defined in the ISO/IEC 7816-4 considering that TOEs adopt the file system defined in the ISO/IEC 7816-4.

[9] The threat T.Communcation_Attack indicates the concerns of attacker's disclosure and tampering of readable data, including facial images. The threats T.Logical_Attack and T.Communication_Attack are stated independently, as the data under attack is distinct.

Identifier	Threat
	between a terminal and a passport booklet, it is considered impossible that the attacker physically accesses the target passport booklet without being noticed by its passport holder and/or an immigration official. An attacker can obtain MRZ data only when the passport booklet is physically accessible. Therefore, an attacker assumed with this threat is assumed not to know the MRZ data.
T.Physical_Attack[10]	In the operational environment after an issuance of a TOE embedded passport booklet, an attacker may attempt to disclose confidential information (Active Authentication Private Key) stored in the TOE, unlock a locked state of a 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] 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. Such a physical attack may disable the security function operated according to the TOE program to provide the original functionality thereof, resulting in potential violation of SFR. The example of nondestructive attacks includes those measurements of leaked electromagnetic wave associated with the TOE operation and induction of malfunctions of security functions by applying environmental stress (e.g. changes in temperature or clock frequency, or application of high-energy electromagnetic fields) to the TOE in operation. The examples of destructive attacks are collecting, analysing, and then disclosing confidential information by probing and manipulating

10 Using a physical means for TOE, the threat T.Physical_Attack is contrasted with the threat T.Logical_Attack, whose available means are limited to the logical means. However, the threat T.Physical_Attack includes attacks combining physical means with logical means (data output via the contactless communication interface), such as the Differential Fault Analysis (DFA).

Identifier	Threat
	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.

3.1.1.2 Security Functions against Threats

The TOE conforming to the PP [12] counters the threats described in Table 3-1 by the following security functions.

(1) Countering the threat T.Copy

The Passive Authentication is an inspection system using PKI system to verify personal information stored in an ePassport IC with a digital signature, which then will be read out through a terminal. The threat T.Copy is assumed to break through an inspection with Passive Authentication, in which an attacker presents a forged ePassport IC having an IC with duplicated personal information, including a digital signature, taken from a different IC.

The ePassport specifications [15] define the following procedure using the Active Authentication to counter this threat.

(a) A terminal sends nonce (8-bytes) to an ePassport IC.

(b) An ePassport IC generates a signature to the received nonce with the Active Authentication Private Key stored in the ePassport IC to send it to the terminal.

(c) The terminal tries to verify a signature using the Active Authentication Public Key read out separately from the ePassport IC and if the signature is successfully verified, the ePassport IC will be confirmed authentic. Note that a digital signature is applied to Active Authentication Public Key, which allows terminals to verify integrity and authenticity of the Active Authentication Public Key using the PKI system.

As for the digital signature algorithms of Active Authentication, the PP [12] defines ECDSA (using a 256-bit or 384-bit private key), which was defined in [16] referred by the ePassport specifications [15].

As for the confidentiality of a related Active Authentication Private Key and integrity of an Active Authentication Public Key and an Active Authentication Private Key, the PP [12] requires a mechanism to issue an ePassport to a passport applicant while preventing the following two actions according to the organisational security policies P.Data_Lock described in 3.1.2.1.

- Reading and/or writing the Active Authentication Private Key
- Writing the Active Authentication Public Key

(2) Countering the threat T.Logical_Attack
The threat T.Logical_Attack assumes a possibility that via a contactless communication interface the Active Authentication Private Key is logically read in an operational environment where a passport booklet with an embedded TOE has been issued.

The TOE counters the above threat by preventing logical reading of the Active Authentication Private Key in the operational environment after the issuance of the passport booklet.

(3) Countering the threat T.Communication_Attack
The threat T.Communication_Attack assumes attacks to disclose and/or tamper readable data including facial images.

This threat can be countered by applying mutual authentication and Secure Messaging between the TOE and terminals.

An applicable mechanism for the mutual authentication and Secure Messaging is PACE defined in the ePassport specifications [15].

Table 3-2 shows cryptographic algorithms used for PACE.

Table 3-2 Cryptographic algorithms used for PACE

Cryptographic algorithm	Cryptographic operation	Cryptographic key sizes (bit)	Usage
SHA-1[*1]	Derivation of a session key for PACE	_[*3]	Mutual authentication and Secure Messaging
SHA-256[*2]	Derivation of a session key for PACE	_[*3]	Mutual authentication and Secure Messaging
ECDH	Key agreement	256 or 384	Mutual authentication and Secure Messaging
CMAC mode AES	Generation and verification of authentication tokens	128 or 256	Mutual authentication
	Generation and verification of authentication codes	128 or 256	Secure Messaging
CBC mode AES	Nonce[*4] encryption	128 or 256	Mutual authentication
	Message encryption and decryption	128 or 256	Secure Messaging

[*1] Used to derive a 128-bit AES session key.

[*2] Used to derive a 256-bit AES session key.

[*3] A hash function does not take a cryptographic key. However, assuming it as a key derivation function, it takes a shared secret established by ECDH concatenated with 32 bits of the counter.

[*4] This nonce, generated by the TOE itself with a random number generator, differs from the nonce seen in Active Authentication.

(4) Countering the threat T. Physical_Attack

A TOE conforming to the PP [12] is exposed to physical tampering (observation, analysis, and modification) due to its nature of an IC as a physical embodiment. Behaviour of a TOE is also affected by operating conditions such as voltage, frequency and temperature.

The TOE conforming to the PP [12] provides protection function for TSF in order to resist the attacks described in the mandatory technical document regarding IC cards and similar devices [17].

Examples of these attacks include:

- Attacks that attempt to extract internal signals of a TOE.
- Attacks that attempt to manipulate internal signals of a TOE.
- Fault Injection Attacks (including DFA)
- Side channel attacks (including DEMA)
- Exploitation of the test features of IC chips.
- Reactivation of disabled access control mechanisms
- Attacks that predict random numbers generated by a random number generator and/or decrease the entropy of output random numbers.

3.1.2 Organisational Security Policies and Security Functions

3.1.2.1 Organisational Security Policies

Table 3-3 shows organisational security policies required for the use of the TOE conforming to the PP [12].

Table 3-3 Organisational Security Policies

Identifier	Organisational Security Policy
P.PACE	In the operational environment after an issuance of a TOE embedded passport booklet, the TOE shall allow a terminal to read certain information from the TOE in accordance with the PACE protocol defined in Part 11 of ePassport specifications [15]. PACE 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 described in the above specifications. 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 [12] is not defined.
P.Authority[11]	The TOE under the control of the passport issuing authorities allows only authorised users (persons who succeeded in verification of readout key, transport key, or Active Authentication Information Access Key) to have access to the

[11] Corresponding to protection function in transport

Identifier	Organisational Security Policy
	internal data of the TOE, as shown in Table 3-4.
P.Data_Lock[12]	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 preventing reading or writing the files based on successful authentication thereof. Table 3-4 shows the relationship between the keys used for authentication and the corresponding files in the TOE.
P.Prohibit[13]	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 prevented after an issuance of an ePassport to the passport applicant. This policy makes use of blocking authentication caused by an authentication failure with a transport key, a readout key and an Active Authentication Information Access Key (see P.Data_Lock).

Table 3-4 Access control of internal data of the TOE by passport issuing authorities

Authentication status	File subject to access control	Permitted operation	Reference: Data subject to operation
Successful verification with readout key*1	EF.DG13*2	Read	IC chip serial number (entered by manufacturer)
Successful verification with transport key*1	Transport key file	Write	Transport key data (update of the previous 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		PACEv2 security information Hash function information for Active Authentication
	EF.COM*3		Common data

12 Corresponding to write protection function
13 Corresponding to write protection function

Authentication status	File subject to access control	Permitted operation	Reference: Data subject to operation
	EF.SOD		Security data related to Passive Authentication defined in Part 10 of ePassport specifications [15]
	EF.CardAccess	Write	PACEv2 security information
	EF.DG15	Read	Active Authentication Public key
Successful verification with Active Authentication Information Access Key*1	EF.DG15	Write	Active Authentication Public Key
	Private key file		Active Authentication Private Key

*1 A readout key, a transport key and an Active Authentication Information Access Key are configured by the manufacturer. A transport key can be modified (updated) by a user. User accesses not stated in this table or note is denied: access to files subject to access control specified in this table, access to files storing a readout key which may change authentication status or files storing an Active Authentication Information Access Key. (Access to information in the TOE through a terminal after the issuance of a TOE embedded passport booklet is controlled by PACE, which will be separately specified.)

*2 An IC chip serial number has already been recorded in EF.DG13 by the manufacturer and its management data will be appended to the file by the passport issuing authorities.

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

Table 3-5 shows the relationship between organisational security policies shown in Table 3-3 and applicable phases.

Table 3-5 Organisational security policies and applicable phases

Organisational security policies	Phase			
	Phase 1	Phase 2	Phase 3	Phase 4
P.PACE				X
P.Authority			X	
P.Data_Lock			X	
P.Prohibit			X	X

[Note] "X" indicates that organisational security policies shall be applied.

3.1.2.2 Security Functions for Organisational Security Policies

The PP [12] requires TOEs to provide functions that satisfy the organisational security policies shown in Table 3-3.

(1) Supporting the organisational security policy P.PACE (Password Authenticated Connection Establishment (PACE))

In the operational environment after an issuance of a TOE embedded passport booklet, the organisational security policy defines that a terminal reads the given information from the TOE in accordance with the PACE protocol defined in the ePassport specifications [15].

The TOE provides the function supporting the PACE protocol defined by Part 11 of ePassport specifications [15], which enables that the given information be securely read out from TOE at the intended level of the PACE protocol.

(2) Supporting the organisational security policy P.Authority (protection function in transport)

The organisational security policy defines that access to files in the TOE under the control of the passport issuing authorities to be controlled in accordance with Table 3-4.

In order to access files in the TOE, the TOE requires a user authentication with a transport key, a readout key, or an Active Authentication Information Access Key, and only when the authentication is successful, the access to files in the TOE shall be allowed based on the authentication status for each key.

(3) Supporting the organisational security policy P.Data_Lock (write protection function)

The organisational security policy defines that if the TOE detects a failure in authentication with a transport key, a readout key or an Active Authentication Information Access Key, the TOE permanently disables authentication related to the said key and thereby prevents reading or writing files that require successful authentication shown in Table 3-4.

When detecting a failure in authentication with a readout key, a transport key, or an Active Authentication Information Access Key, the TOE disables authentication mechanism that uses the said key, which prevents access to the files with these keys.

(4) Supporting the organisational security policy P.Prohibit (write protection function)

The organisational security policy defines that any writing to files in the TOE and/or reading those files after successful authentication of a readout key must be prevented once a passport has been issued to a passport applicant.

By causing authentication failures with a transport key, a readout key, or an Active Authentication Information Access Key before the issuance of a passport to a passport applicant, writing to files in the TOE and reading those files after authentication of a readout key is prevented by using the function provided by the TOE described above (4).

4. Assumptions and Clarification of Scope

This chapter describes assumptions and an operational environment for the operation of the TOE conforming to the Protection Profile (PP) [12].

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE conforming to the PP [12].

Effective performances of the security functions of the TOE conforming to the PP [12] are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.Administrative_Env	The TOE delivered from a TOE manufacturer to the passport issuing authorities will be securely controlled by the authorities and undergo an issuing process before its issuance to a passport applicant.
A.PKI	In order for the passport inspection authorities of the receiving country to verify authenticity of information that has been digitally signed by the passport issuer and stored in the TOE (including an Active Authentication Public Key), interoperability of the PKI environments between the issuing and receiving countries will be maintained by the passport issuing authorities.

5. Evaluation conducted by Evaluation Facility and Results

5.1 Evaluation Facility

ECSEC Laboratory Inc. Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body as a member of the Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). The evaluation facility is periodically checked and confirmed that it meets the requirements on appropriateness of the management and the evaluators necessary for maintaining the quality of evaluation.

5.2 Evaluation Approach

The evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3.

Details for evaluation activities have been reported in the Evaluation Technical Report.

The Evaluation Technical Report explains the summary of the PP [12] as well as the evaluation details and the verdict for each work unit in the CEM.

5.3 Overview of Evaluation Activity

The history of the evaluation activities is described in the Evaluation Technical Report as follows.

The evaluation started on November 2015 has concluded upon completion of the Evaluation Technical Report dated March 2016.

The Evaluation Facility has received a full set of evaluation deliverables necessary for the evaluation provided by the developer, and examined the evidence in relation to a series of evaluation activities.

Any concern found in the evaluation activities for each work unit has been included in the Observation Reports, which have been issued and reported to the developer.

All the concerns have been solved after being reviewed by the developer.

Concerns that the Certification Body found in the evaluation process have been described in certification oversight reviews sent to the Evaluation Facility.

All the above concerns, examined by the Evaluation Facility and the developer, have been reflected in the Evaluation Technical Report.

5.4 Evaluation Results

The evaluator has concluded that, upon provision of the Evaluation Technical Report, the PP [12] satisfies all work units prescribed in the CEM.

As a result of the evaluation, the verdict "PASS" has been confirmed for the following assurance components:

APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, APE_REQ.2

Table 5-1 Overview of the evaluation results

Summary of evaluation results	
APE_INT.1	PP introduction
It has been confirmed that the PP [12] provided the security features needed for ePassport below: - PACE function - Active Authentication support function - Write protection function - Protection function in transport - Tamper resistance	
APE_CCL.1	Conformance claims
The following have been confirmed through the evaluation: - Conformance to Common Criteria Version 3.1 Release 4 - Security functional requirements: Common Criteria Part2 Extended - Security assurance requirements: Common Criteria Part3 Conformant - Not claiming conformance to other PPs - Strict conformance to the PPs/STs is required in claiming conformance to the PP [12]	
APE_SPD.1	Security problem definition
The following has been confirmed through the evaluation: - Threats and organisational security policies are described in terms of CC/CEM.	
APE_OBJ.2	Security objectives
The following has been confirmed through the evaluation: - Security objectives addressing the threats and the organisational security policies in the Security problem definitions are described and its rationale is appropriate.	
APE_ECD.1	Extended components definition
The following has been confirmed through the evaluation: - In the extended components definition, a security functional component not described in CC Part 2 is defined for random number generation for general purposes.	
APE_REQ.2	Security requirements
The following have been confirmed through the evaluation: - Security functional requirements satisfying the security objectives are described - Rationale for selection of security assurance requirements EAL4+ALC_DVS.2+AVA_VAN.5	

5.5 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurers.

6. Certification

Based on the materials submitted by the Evaluation Facility during the evaluation process, the Certification Body has conducted certification including the following confirmations:

1. Whether the concerns pointed out in the Observation Reports are appropriate.

2. Whether the concerns pointed out in the Observation Reports have been properly resolved.

3. Through checking of the submitted documentation, whether the relevant work units have been evaluated as presented in the Evaluation Technical Report.

4. Whether the rationale for the evaluation verdict made by the evaluator presented in the Evaluation Technical Report is appropriate.

5. Whether the evaluator's evaluation methodology presented in the Evaluation Technical Report is complying with the CEM.

Concerns found in the certification process are documented in the certification oversight reviews, which have been sent to the Evaluation Facility.

The Certification Body has issued this Certification Report upon confirmation that in the PP [12] and the Evaluation Technical Report such concerns described in the certification oversight reviews have been fully solved.

6.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body has determined that the PP [12] satisfies assurance requirements APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, and APE_REQ.2 in the CC Part 3.

6.2 Recommendations

The Protection Profile (PP) [12] does not specify standards regarding random number generation and the quality of random numbers. In specifying these, aspects should be considered such as applications of random numbers, and the security properties required for the random number generator. The developer of the TOE shall specify these aspects through the Security Target (ST).

If the TOE claims conformance to PP [12], the developer of TOE should seek that the TOE is separately evaluated and certified based on PP [13]. This is what is intended by the applicant. Following this approach, vulnerability assessment is performed with AVA_VAN.5 for security functions other than Basic Access Control (BAC). Vulnerabilities in measures to cope with attacks that reactivate disabled BAC function will be assessed in AVA_VAN.5 through the evaluation conforming to the PP [12].

While the PP [12] is written considering global interoperability of ePassports, it does not necessarily cover all the files and functions defined in the ePassport specifications [15]. When using the PP [12] for procurement outside Japan, some additional files or functions may be needed.

The validity of cryptographic algorithms is not assured at the time of the TOE evaluation conforming to the PP. Therefore, it is necessary to confirm that each cryptographic algorithm specified in the PP [12] is still valid and not compromised yet.

7. Annexes

There is no annex.

8. Terms

8.1 Abbreviations related to CC

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

8.2 Terms and abbreviations used in this certification report

The definitions of terms and abbreviations used in this report are listed below.

Active Authentication	A security mechanism in which a public key and private key pair using the public key cryptography system is stored to keep the private key secret in the IC chip constituting a part of the TOE. The public key is transmitted to an external device trying to authenticate the TOE and after that the TOE will be authenticated through cryptographic calculation by the challenge-response protocol using the private key, which has been kept secret in the TOE. The Active Authentication protocol has been standardized by ICAO.
Active Authentication Information	Authentication data for writing Active Authentication key pairs
Access Key	
Basic Access Control	A mechanism for the mutual authentication and Secure Messaging specified in the ePassport specifications [15], which is referred to as BAC.
Issuance	To make a passport legally valid. To create a passport itself to render it effective as a passport.

Passive Authentication	A security mechanism in which the digital signature of the passport issuing authority is put on personal data to be stored in the TOE and if the PKI system with assured interoperability is used by both the passport issuing and receiving ends, authenticity of the data read from the TOE will be verified. The Passive Authentication procedure has been standardized by ICAO.
Passport	An identification document issued by a national government or an equivalent public institution to an overseas traveler. In general, a passport is issued as a booklet (passport booklet).
Passport issuing authorities	The Ministry of Foreign Affairs, passport manufacturers and regional passport offices under the direction of the said Ministry. The passport manufacturers file plastic sheets with TOEs into passport booklets in which necessary information other than personal information (birthdate, facial image data, security-related data regarding the aforementioned data, etc.) are written. Personal information are to be written in the passports by passport officers.
Passport manufacturer	A manufacturer manufacturing passport booklets with TOEs in which basic data (management data such as a passport number, an active authentication public key and a private key pair, etc.) will be written.
Passport office	A passport issuing organisation at which personal information of a passport holder is written in a passport booklet including the TOE. Passport offices, located in various regions, serve as a point of contact for a passport applicant to which a passport will be delivered.
Password Authenticated Connection Establishment	A mechanism for the mutual authentication and Secure Messaging specified in the ePassport specifications [15], which is referred to as PACEv2.
Password key file	A file containing keys derived from MRZ data and used for the nonce encryption in the PACEv2 protocol

Readout key	Authentication data for reading IC chip serial numbers
Secure Messaging	A set of means for cryptographic protection of [parts of] command-response pairs (See 3.5 of ISO/IEC 7816-8:2004.)
Transport key	Authentication data for protecting an integrated circuit (IC) card against unauthorised use during its transportation
AES	Advanced Encryption Standard
ATR	Answer-to-Reset
BAC	Basic Access Control
CBC	Cipher Block Chaining
CMAC	Cipher-based MAC
DEMA	Differential Electro-Magnetic Analysis
DES	Data Encryption Standard
DF	Dedicated file. Structure containing file control information and, optionally, memory available for allocation. (See the definition 3.19 in ISO/IEC 7816-4:2013.)
DFA	Differential Fault Analysis
DG	Data Group
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary file. Set of data units or records or data objects sharing the same file identifier. (See 3.23 of ISO/IEC 7816-4:2013.)
EF.ATR/INFO	Answer-to-Reset file or Information file (See Clause 4 of ISO/IEC 7816-4:2013.)
EF.CardAccess	EF deployed directly under MF and contains PACEv2 security information

EF.COM	EF that provides the list of DGs located under the DF containing the version information for the Logical Data Structure (LDS), which specifies the types of formats to be used for data storage in ICs for passport booklets, and an ePassport application
EF.DG1	EF containing the MRZ data
EF.DG2	EF containing a facial image
EF.DG13	EF containing management data (a passport number and booklet management number)
EF.DG14	EF containing PACEv2 security information and information on hash functions for Active Authentication
EF.DG15	EF containing an Active Authentication public key
EF.SOD	EF containing hash values of other data groups and the digital signature for Passive Authentication
ICAO	International Civil Aviation Organization
MAC	Message Authentication Code
MF	Master file. A unique DF representing the root in a card using a hierarchy of DFs. (See 3.33 of ISO/IEC 7816-4:2013.)
MRZ	Machine Readable Zone. A machine readable zone that consists of a digitized facial image printed on the personal data page of ePassports, and the area for 88 letters provided at the bottom of the personal data page, in which personal data such as a name, nationality, sex, date of birth, passport number and date of expiry are printed.
MRZ data	Information printed on the data page of ePassports, which can be read by a terminal
PACE	Password Authenticated Connection Establishment
PACEv2	Password Authenticated Connection Establishment v2

PACEv2 security information	Information such as cryptographic algorithms and domain parameters used in PACEv2
PKI	Public Key Infrastructure
SAC	Supplemental Access Control Subsection 1.1.3 titled "Supplemental Access Control" of the bibliography [22] gives the following explanations. "This Technical Report specifies PACE v2 as an access control mechanism that is supplemental to BAC. PACE MAY be implemented in addition to BAC, i.e. — States MUST NOT implement PACE without implementing BAC if global interoperability is required. — Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip."
SHA	Secure Hash Algorithm
SOD	Document Security Object

9. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1:

Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] 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

[13] Protection Profile for ePassport IC with SAC (BAC + PACE) and Active Authentication, Version 1.00, (March 8, 2016), Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan

[14] Evaluation Technical Report QXE02-ETRPP-0002-00, Version 2.0, March 9, 2016, ECSEC Laboratory Inc. Evaluation Center

[15] ICAO Doc9303 Machine Readable Travel Documents Seventh Edition, 2015

[16] Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012, Bundesamt für Sicherheit in der Informationstechnik

[17] Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 2.9, January 2013

[18] Observation report QXE-EOR-7001-00, (December 7, 2015), ECSEC Laboratory Inc. Evaluation Center

[19] Observation report QXE-EOR-7002-00, (December 21, 2015), ECSEC Laboratory Inc. Evaluation Center

[20] Observation report QXE-EOR-7003-00, (December 25, 2015), ECSEC Laboratory Inc. Evaluation Center

[21] 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

[22] International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014