Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Protection Profile (PP)

Application Date/ID	2014-01-22 (ITC-4485)
Certification No.	C0431
Sponsor	Japan Agency for Local Authority Information Systems
PP Name	Personal Number Cards Protection Profile
PP Version	1.00
PP Conformance	None
Assurance Package	EAL4 Augmented with AVA_VAN.5, ALC_DVS.2
Developer	Japan Agency for Local Authority Information Systems
Evaluation Facility	Evaluation Center, Electronic Commerce Security Technology Laboratory Inc.

This is to report that the evaluation result for the above PP is certified as follows.
2014-05-15

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

Evaluation Criteria, etc.: This PP is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme."

- 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

"Personal Number Cards Protection Profile" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, 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 describes the content of the certification result in relation to IT Security Evaluation of "Personal Number Cards Protection Profile, Version 1.00" (hereinafter referred to as the "PP [12]") developed by Japan Agency for Local Authority Information Systems, and the evaluation of the PP was finished on April 24, 2014 by Evaluation Center, Electronic Commerce Security Technology Laboratory Inc. (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Japan Agency for Local Authority Information Systems, and provide security information to procurement personnel and consumers who are interested in this PP.

Readers of the Certification Report are advised to read the Protection Profile together with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOEs claiming conformance to PP [12] are described in the PP.

This Certification Report assumes "developers who develop and supply Personal Number Cards conforming to PP [12]" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the PP conforms, and does not guarantee an individual IT product itself.

1.1 Evaluated PP

An overview of the security functionalities and operational conditions required by the PP is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of required by the PP is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. The PPs and STs that claim conformance to this PP shall claim demonstrable conformance.

1.1.2 PP overview

The PP[12] specifies the security requirements for the IC card used as "Personal Number Card" in the Social Security and Tax Number System.
The TOE of the PP[12] is the IC card including an IC chip and contact/contactless interfaces. In the IC chip, programs and data are installed to provide services of Personal Number Card.
The construction of the TOE is shown in Figure 1-1.

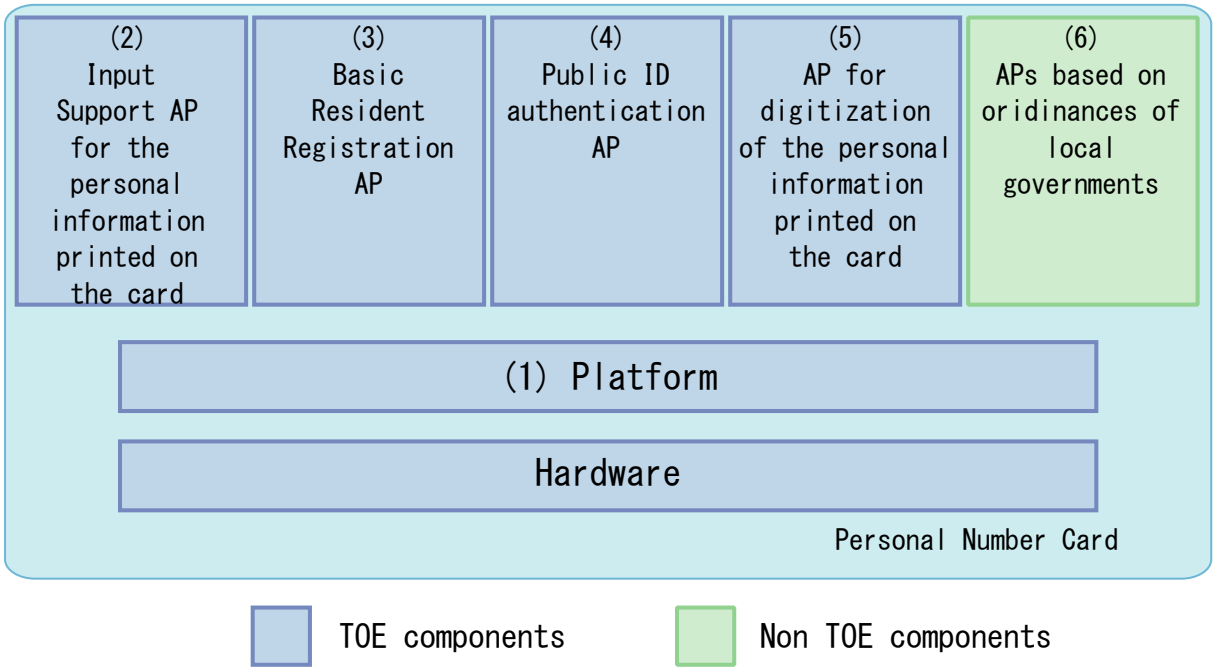

Figure 1-1 Construction of the TOE

Brief descriptions are provided below for components shown in Figure 1-1, (1) Platform, (2) Input Support AP for the personal information printed on the card, (3) Basic Resident Registration Card AP, (4) Public ID authentication AP, (5) AP for digitization of the personal information printed on the card and (6) APs based on ordinances of local governments.

(1) Platform

The platform provides an operational environment for each Application Program (abbreviated as "AP" hereafter). The platform provides the additional functionality to add/delete APs based on ordinances of each local government.

(2) Input Support AP for the personal information printed on the card

This is the application providing the personal number and the four data of the card holder based on "The Social Security and Tax Number System". The four data of the card holder are name, address, date of birth and gender. These data are stored in the TOE in the form of text data and read out by an authenticated user.

(3) Basic Resident Registration AP

This is the card application for Basic Resident Registration Network System. It provides the identical functionality as conventional Basic Resident Registration Card. The card holder's resident registration code is stored. The dedicated terminals installed at each local government are used to read out the code.

(4) Public ID authentication AP

This is the application providing public ID authentication services for individuals. It is used to sign "certificate for digital signature" for electronic application, or "certificate for user certification" for electronic authentication of the card holder. It stores the public key

pair and the certificates in the TOE for each use above. It executes cryptographic operation for generating electronic signature in the card.

(5) AP for digitization of the personal information printed on the card

This is the application which provides digitization of the personal information printed on the card. The printed information includes the four data, the personal number, the photographic portrait and the expiration date. The digitized image data of the whole printed information is stored in a file of the card. Furthermore, digitized image data of the personal number is stored in another file. When the alteration of the printed information was doubted, it is verified by comparing with those stored data displayed on a terminal. The date of the birth, which is stored as text data, is used for age verification of the card holder. The stored data are not confidential, because they are identical with the printed information on the card. However, to prevent the data being read out without recognition of the card holder, the TOE requires a password on readout of the data.

(6) APs based on ordinances of local governments

These are APs installed on Personal Number Cards based on ordinances of local governments.

The following four APs are called as "the basic APs": (2) Input Support AP for the personal information printed on the card, (3) Basic Resident Registration AP, (4) public ID authentication AP, and (5) AP for digitization of the personal information printed on the card.

Each Personal Number Card supplied to J-LIS is issued to the resident (card holder) via the relevant local government. Administrators of the local government or of J-LIS write information specific to the card holder in the card prior to the issue. This procedure is called as personalization of a card. If necessary, APs based on ordinances of each local government may be added to the Personal Number Cards.

The resident to whom the Personal Number Card is issued is referred to the card holder and uses services via the APs installed on the Personal Number Card.

1.1.2.1 Security functions overview

This PP requires two types of security features, one is requested from the services provided by Personal Number Card and the other is requested as general functionalities of IC cards. The major features are as follows.

(1) Protection of communication data

The TOE uses two external interfaces, a contact interface and a contactless interface, to communicate with an external terminal. For the communication which needs protection from eavesdropping or modification, the TOE applies "secure messaging" function in order to protect confidentiality and/or integrity of communication data by means of encryption/decryption and/or generation/verification of MAC (Message Authentication Code).

(2) User authentication and access control

The TOE performs user authentication and enforces access control for each service to provide the service depending on the privileges of the user. "Providing the service" means that the TOE permits a user to use functions of the TOE. Examples are reading out data stored in a file of the TOE (e.g. the personal number), or using of signature generation function of the TOE. The function creating/deleting APs based on ordinances of local governments (optional and out of the TOE) is also the service of the TOE.

A scenario using the TOE is as follows. When a card holder or an administrator of local government uses a service of the TOE, an external terminal will access the TOE before actually using the service. The external terminal is the IT device which directly communicate data with the TOE. For user authentication mechanisms, the TOE employs password system and public key cryptographic system. The authentication of an external IT device by an IC card is referred to as "External Authentication" in the IC card field. In contrast to External Authentication, there is the term called "Internal Authentication". Internal Authentication is the function for external terminals to authenticate the IC card, in order to examine that the TOE is not forged. Internal Authentication is needed for the security of external terminals side. The TOE offers the cryptographic functionality to address Internal Authentication.

(3) Cryptographic processing

The TOE provides cryptographic processing functionality for the services of the platform and each AP. The cryptographic processing functionality is used for secure messaging, user authentication, signing/user certification for the public ID authentication AP and so on.

(4) Counters physical attacks

The security functionality of the TOE also counters physical attacks to the hardware part of the TOE. The attacks assumed are the same as the attacks to general IC cards. There are a variety of attacks using physical measures. Examples of the attacks include physical manipulation for the inside of the IC chip, probing to disclose or modify information, observation and analysis for consumption power or electromagnetic emanation of the TOE to disclose cryptographic keys.

1.1.2.2 Threats and Security Objectives

The TOE conforming to the PP[12] counters each threat by the security functionality described below.

The Personal Number Card supports multiple roles and services available, to provide the services for authorized administrators of local governments and the services for card holders. There is a threat that those who is not authorized to assume the role or to use the services may access the TOE through contact interface and/or contactless interface, to disclose/modify internal data of the TOE or to use processing functions of the TOE illegally. To counter this threat, the TOE identifies and authenticates the user and permits him or her to logically access the inside of the TOE, within the scope of privilege.

As the TOE communicates with an external terminal using the contact interface or contactless interface, there may be a threat masquerading as a legitimate external terminal by monitoring/recording communication data between the TOE and the external

terminal and by replaying the recorded data. Here the TOE is responsible for generating the authentication data. To counter this threat, the External Authentication function is required to use different authentication data each time, without reusing the authentication data.

There is a potential risk that an IC chip installed in an IC card will leak internally processed information through its power consumption or through its electromagnetic emanation, due to the nature of physical embodiment. Also the following attacks must be considered: disclosure of the internal information of the IC chip by physical probing, physical modification of the circuitry of the IC chip or malfunction by exposure to environmental stress. Therefore, it is required to protect TSFs from these physical attacks.

1.1.3 Disclaimers

When modification of personal information printed on a Personal Number Card is doubted, the printed information may be compared and verified with the "card printed data items" which are read out from the TOE to the external terminal by using AP for digitization of the personal information printed on the card. The PP[12] does not request to apply secure messaging for readout of "card printed data items". Therefore, the TOE does not counter the threat that detecting the modification of "card printed data items" at the external terminal side may be disturbed by modifying transmission of those data from the TOE to the terminal.

It depends on the external terminal whether the secure messaging is applied or not for the communication between the external terminal and AP for digitization of the personal information printed on the card or Public ID authentication AP. Therefore, the confidentiality and/or integrity of communication data may not be kept even if the card holder requests these properties.

Concerning with use of Personal Number Card, there are private companies permitted to use services of Personal Number Cards based on Articles 17 and 36 of the Act on Certification Business of Local Governments in Relation to Electronic Signatures (Act No. 153 of 2002). As an example, it is assumed that a card holder requests a copy of his or her certificate of residence at a convenience store by using his/her Personal Number Card. In order to cover such usage, the PP[12] specifies "the system handling certificate data" to use the user certification function of the TOE, as a user of Public ID authentication AP and its privilege. It means that an electronic signature used for user certification of the card holder can be generated by entities other than the card holder. There is a possibility that it cannot be determined whether or not the generated electronic signature was actually generated by the card holder him- or herself. However, such handling of the electronic signature is the matter of a system using Personal Number Cards and therefore outside the scope of the TOE conforming to PP[12].

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on April, 2014, based on functional requirements and assurance requirements of the PP[12] according to the publicised documents "IT Security Evaluation and Certification Scheme"[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

The Certification Body verified the Evaluation Technical Report [13] and the Observation Reports ([15][16][17][18][19]) prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the PP [12] evaluation was conducted in accordance with the prescribed procedure.

The certification oversight reviews were also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the PP evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]).

The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The PP is identified as follows:

Name of PP:	Personal Number Cards Protection Profile
Version of PP:	1.00
Developer:	J-LIS (Japan Agency for Local Authority Information Systems)

3. Security Policy

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

In the PP[12], two types of security functions are required to the TOE. They are functions requested for the services of Personal Number Cards and general functions for IC cards. The main functions required to the TOE are as follows:

- protection of communication data between the TOE and an external terminal,
- user authentication and access control,
- cryptographic processing, and
- countering to physical attacks.

3.1 Security Function Policies

In the PP[12], the security functions are provided to counter the threats shown in 3.1.1.1 and to satisfy the organisational security policies shown in 3.1.2.1.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

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

Table 3-1 Assumed Threats

Identifier	Threat
T.Illegal_Attack	An unauthorized user accesses the TOE via external interfaces to disclose or modify internal data of the TOE, or to use processing function of the TOE. "An unauthorized user" is the entity that does not have the authentication data needed to access the assets of the TOE. [Application note_T.Illegal_Attack] This threat may occur in any operational environments after the production and the shipment of Personal Number Cards, such as under the transportation, under the safekeeping in the organization involved in issue and also after the personalization and the issue to card holders.
T.Replay	An attacker masquerades a legitimate external terminal by monitoring, recording and replaying the authentication procedure between the TOE and the external terminal in order

	to be authenticated by the TOE. The attack causes disclosure or modification of user data of the TOE, or illegal use of processing function of the TOE. [Application note_T.Replay] This threat might be considered as a part of T.Illegal_Attack. However, it is defined here as an independent threat because it identifies a specific attack method.
T.Phys_Attack	An attacker attacks components of the TOE - hardware, firmware or software - with physical means. The attack causes disclosure or modification of user data of the TOE, or unauthorized use of processing function of the TOE. Examples of typical attack measures are as follows: ● Monitoring and analyzing variation of power consumption of the TOE during cryptographic operation to determine the cryptographic key used. ● Probing the inside of the TOE to disclose data. ● Disclosing or modifying data, or using processing function of the TOE illegally by causing errors or malfunction of the TSF operation with glitches or environmental stresses during operation of the TOE. ● Disclosing or modifying data of the TOE or modifying behavior of the TOE by physically manipulating of the inside of TOE.

3.1.1.2 Security Function Policies against Threats

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

(1) Counters to the threats "T.Illegal_Attack" and "T.Replay"

The threat "T.Illegal_Attack" assumes that programs and data inside the TOE are accessed illegally via contact interface or contactless interface of a Personal Number Card. "T.Replay" assumes that the TOE is accessed illegally by reusing authentication procedures intercepted from communications between a Personal Number Card and an external terminal.

To counter these threats, the TOE verifies the authenticity of external terminal communicating with the Personal Number Card, and permits the access to data and cryptographic processing functions only after it has been authorized to do so. For the authentication of external terminals, challenge-response system based on public key cryptosystem using the cryptographic algorithm (RSASSA-PKCS1-v1.5) shown in Table 3-4 is applied. The authentication data shall not be reused and its value shall be different

each time. Thereby, only legitimate external terminals can access programs and data inside the TOE.

(2) Counters to the threat "T.Phys_Attack"

The TOE conforming to the PP[12] is exposed to physical tampering (observation, analyzing or modification), due to the nature of physical embodiment of an IC. The behaviour of the TOE is affected by operating conditions such as voltage, frequency and temperature.

The TOE protects the TSFs from the attacks provided in the mandatory technical document [14] of SOG-IS for IC cards and similar devices.

Examples of the attacks include followings:

- Readout of signals inside of the TOE
- Modification of signals inside of the TOE
- Overcoming sensors to deactivate or to bypass the self-protection features of the TOE
- Fault injection attacks (including DFA)
- Side-channel attacks (including DPA, DEMA)
- Exploitation of test features of IC chip
- Prediction of random number outputs from RNG or decreasing entropy of generated random numbers

3.1.2 Organisational Security Policies and Security Functions

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE conforming to the PP[12] are shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.Secure_messaging	Secure messaging shall be applied to the communication between the TOE and an external terminal indicated, as "applied" in Table 3-3. Applying secure messaging is not mandatory for the communication indicated as "applied or not applied" or "not applied", as shown in the notes of the table.
P.Delivery	On shipment of Personal Number Cards from developers, the functionality to prevent illegal accesses to the TOE shall be activated. "Illegal accesses" refer to logical accesses to the inside of the TOE by unauthorized entities. [Application note_P.Delivery] When the TOE is shipped from developers, a part of the security functionality of the TOE shall be enabled to protect the TOE from illegal accesses. The authentication data, called as "transport key" generally in IC cards, is stored in the TOE. Only the users who know the transport key can access the TOE. Even if an attacker steals the TOE in transport, he/she won't be able to initialize nor use the TOE without the knowledge of the transport key. Transport key is effective not only in transport but also in safekeeping until issuing. "Initial key" and "issuer key" are the authentication data having the similar security property as "transport key". The "transport key" in this PP is the general term for those keys.
P.Cryptography	The TOE provides the environment where cryptographic functions are available to the platform and the basic APs. The cryptographic functions are used for data protection, signature or authentication. Table 3-4 shows cryptographic algorithms, cryptographic operations and purposes of cryptographic functions. Table 3-5 shows cryptographic key sizes, cryptographic key management policies.
P.RND	The TSF generates random numbers to be used for the TSF itself. The quality of random numbers is sufficient to prevent prediction by an attacker. [Application note_P.RND] The quality of random numbers will depend on purposes. The quality should be defined with objective metric. An example of quality metric is a numerical value in the unit of entropy.

Table 3-3 Application of secure messaging

Applied to:	Encryption/decryption	MAC generation/verification
The platform	applied	applied
Input Support AP for the personal information printed on the card	applied or not applied*1	applied or not applied*1
Basic Resident Registration AP	applied (readout of Resident Registration Code)	not applied*2
Public ID authentication AP	applied or not applied*1	applied or not applied*1
AP for digitization of the personal information printed on the card	not applied*2	not applied*2

*1 [applied or not applied] The TOE shall be equipped with the secure messaging function. The function will be used when an external terminal requests it.
*2 [not applied] The TOE does not have to be equipped with the secure messaging function. If equipped, the function may be used depending on the request of an external terminal.

Table 3-4 Cryptographic function policies

Cryptographic algorithm /Standard	Cryptographic operation	Cryptographic keys (see corresponding ID numbers in Table 3-5)	Purpose
AES-CBC mode /FIPS PUB 197, NIST SP 800-38A	Encryption /decryption	K1, K8	Secure messaging, private key decryption (at import)
CMAC with AES /FIPS PUB 197, NIST SP 800-38B	MAC generation /verification	K2	Secure messaging
RSASSA-PKCS1-V1.5 /PKCS#1 v2.2	Signature verification with a public key	K3	External Authentication
	Signature generation with a private key*1	K4, K5, K6	Internal Authentication, signature and user certification for Public ID authentication AP
RSA-OAEP /PKCS#1 v2.2	Decryption with a private key	K7	Session key establishment for secure messaging, Secret key establishment*2 for private key decryption
SHA-256 /FIPS PUB 180-4	Hash operation	-	Used as a supporting technique for RSA cryptographic operation

*1 For "Input Support AP for the personal information printed on the card", "Public ID authentication AP" and "AP for digitization of the personal information printed on the card", meanwhile encoding operation

(including hash) specified in the standard is performed at an external device (external terminal), PKCS padding and signature generation with a private key are performed by the TOE. For "Public ID authentication AP", the TOE also can add "organization code" to the padding. This padding does not conform to the standard.
*2 Applied on the on-line update of a secret key for Public ID authentication AP.

(Note) "ID numbers" in the third column are not included in the PP[12]. To help understanding of the readers, they are introduced for well-organised representation.

Table 3-5 Cryptographic key size and key management

ID number	Name of cryptographic key	Cryptographic key size (bit)	Cryptographic key generation /import	Cryptographic key destruction
K1	Session key (cryptographic key)	128	import	Destruction methods are not provided in the PP[12]
K2	Session key (MAC key)	128		
K3	Public key for external authentication	2048		
K4	Key pair for internal authentication	2048		
K5	Private key for signing	2048		
K6	Private key for user authentication	2048		
K7	Key pair for encryption of session key	2048		
K8	Secret key for decryption of private key	128		

3.1.2.2 Security Functions to Organisational Security Policies

The PP[12] requests the security functions to satisfy the organisational security policies shown in Table 3-2.

(1) Correspondence of the organisational security policy "P.Secure_messaging"

This organisational security policy specifies that the TOE provides the function to encrypt/decrypt communication data or the function to generate/verify MAC for communication data, and that these functions are applied depending on the degree of confidentiality and integrity needed for communication data or the request from the external terminal.

If the TOE provides those functions as specified in Table 3-3, the confidentiality and/or integrity of communication data can be protected to the intended level between individual software inside the TOE and an external terminal.

(2) Correspondence of the organisational security policy "P.Delivery"

This organisational security policy specifies that only legitimate users can access logically to the inside of the TOE that is under the control of a local government, which is the issuer of Personal Number Cards.

In accessing the platform or each of the basic APs, the TOE requires the separate authentication for each. The user is permitted to access to the individual software (either the platform or one of the basic APs), only after the successful authentication for accessing it with a transport key,

(3) Correspondence of the organisational security policy "P.Cryptography"

This organisational security policy specifies the cryptographic algorithms, the keys and the key management policies applied to the TOE (Tables 3-4 and 3-5).

The TOE conforming to the PP[12] provides cryptographic functions and cryptographic key management functions indicated in this organisational security policy.

(4) Correspondence of the organisational security policy "P.RND"

This organisational security policy specifies generating random numbers resistant to attackers' prediction ability.

The TOE conforming to the PP[12] provides a random number generator (RNG) satisfying the quality metric depending on a use of random numbers. The RNG will be either one of the following:

- Physical RNG
- Hybrid RNG that combines a physical RNG and a deterministic RNG.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE conforming to PP[12] as useful information for the assumed readers to determine the use of the TOE conforming to the PP[12].

4.1 Usage Assumptions

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

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

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.PKI	For the effective operation of the TSF, it is assumed that the PKI environment, where the keys for public key cryptosystem (a pair of public and private keys) of the TOE are assured to be effective, is provided.
A.Administrator	The administrator, who creates, changes or deletes data and APs on the TOE, is assumed to be a trusted user and to operate the TOE properly based on the privileges.
A.AP	A person in charge of creating any APs based on ordinances of local governments is assumed to create APs developed by trusted developers with appropriate development methods, on the TOE.

5. Evaluation conducted by Evaluation Facility and Results

5.1 Evaluation Approach

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 were reported in the Evaluation Technical Report.

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

5.2 Overview of Evaluation Activity

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

The evaluation has started on January, 2014 and concluded upon completion of the Evaluation Technical Report dated April, 2014.

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

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer.

Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility.

After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

5.3 Evaluation Results

The evaluator had concluded that the PP[12] satisfies all work units prescribed in the CEM by submitting the Evaluation Technical Report.

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

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

Summary of evaluation results	
APE_INT.1	PP introduction
It was confirmed that the PP[12] provided the security features needed for Personal Number Card below: ● Protection of communication data ● User authentication and access control ● Cryptographic operation ● Counters physical attacks	
APE_CCL.1	Conformance claims
The followings were 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 ● Demonstrable conformance to the PPs/STs is required in claiming conformance to the PP[12]	
APE_SPD.1	Security problem definition
The following was confirmed through the evaluation: ● Threats and organisational security policies were described in terms of CC/CEM.	
APE_OBJ.2	Security objectives
The following was confirmed through the evaluation: ● The security objectives addressing the threats and the organisational security policies in Security problem definitions were described and the rationale was appropriate.	
APE_ECD.1	Extended components definition
The following was confirmed through the evaluation: ● In extended components definition, the security functional component is defined for random number generation of general purpose, which is not included in CC Part2.	
APE_REQ.2	Security requirements
The followings were confirmed through the evaluation: ● Security functional requirements satisfying the security objectives were described ● Rationale for selection of security assurance requirements below: EAL4+ALC_DVS.2+AVA_VAN.5	

5.4 Evaluator Comments/Recommendations

The comments and recommendations by the evaluator are as follows.

Specification and necessary guidance concerning with the usage of TOE and assumed operational environment (including the specification for the terminal deployed at local governments) shall be provided by Japan Agency for Local Authority Information Systems.

The PP[12] requires that any APs based on ordinances of local governments are developed by trusted developers. However, it does not require that these APs will not violate the other APs. Therefore, the TOE has to implement application isolation functionality as needed. If application isolation functionality is implemented, it has to be evaluated.

It is not specified in the PP[12] about which data must be protected. The developer of the TOE is required to specify the data to be protected.

6. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.

2. Contents pointed out in the Observation Reports shall properly be solved.

3. The submitted documentation was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

6.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body 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

It depends on each local government whether an AP based on ordinances of local governments is actually installed. However, Personal Number Cards are still able to load any APs based on ordinances of local governments. There may be attacks which damage the assets of Personal Number Card through the operations such as installing, using or deleting of any APs based on ordinances of local governments. The resistance to these attacks has to be evaluated according to the mandatory technical document [14] of SOG-IS for IC cards and similar devices, through the TOE evaluation.

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

7. Annexes

There is no annex.

8. Glossary

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.

administrator	person who has the right to operate management functions relating to TOE security functions. Note that the person belongs to either Japan Agency for Local Authority Information Systems or local government. The administrators performs setting data, creating APs based on ordinances of local governments in issuing IC cards, and updating data for issued cards
basic AP	general term referring "Input Support AP for the personal information printed on the card", "Basic Resident Registration AP", "Public ID authentication AP", "AP for digitization of the personal information printed on the card"
Basic Resident Registration Network	system that enables nationwide identity verification, by putting the Basic Resident Registration on a network. Here the Basic Resident Registration is to notarize the matter pertaining to the residence of each individual. This is to increase convenience for residents and to rationalize the administration of national and local governments,
card holder	resident to whom the Personal Number Card is issued
External Authentication	authentication of an external terminal by an IC card

Internal Authentication	authentication of an IC card by an external terminal
internal data	data stored in the TOE. This includes user data and TSF data which affects the behaviour of the TOE.
Japan Agency for Local Authority Information Systems	organisation founded on April 1st, 2014 based on the Act on Agency for Local Government Information Systems. This organisation inherits all rights and duties of Local Authorities Systems Development Center (LASDEC). J-LIS is the abbreviation of Japan Agency of Local Authority Information Systems. This organisation is responsible for constructing / improving the Personal Number related systems, such as the numbering system for Personal Numbers. This task is delegated from the national government based on applicable laws and regulations such as "Act on the Use of numbers to Identify a Specific Individual in the Administrative Procedure (Act No.27 of 2013)". This organisation also performs the operation of generating Personal Numbers and of issuing Personal Number Cards on the consignment from local governments.
private key	private key used in an asymmetric key cryptographic algorithm
public key	public key used in an asymmetric key cryptographic algorithm
secret key	cryptographic key used in a symmetric key cryptographic algorithm
Secure messaging	set of means for cryptographically protecting confidentiality and/or integrity of communication data
the four data	name, address, date of birth, and gender
user data	data for the user, that does not affect the operation of the TSF
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CBC	Cipher Block Chaining

CMAC	Cipher-based MAC
DEMA	Differential Electro-Magnetic Analysis
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
FIPS	Federal Information Processing Standard
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RSA	Rivest - Shamir - Adleman algorithm
SHA	Secure Hash Algorithm
SOG-IS	Senior Officials Group Information Systems Security
SP 800	Special Publication 800 series

9. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2012, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2013, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, April 2013, 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] Personal Number Cards Protection Profile, Version 1.00, (April 24, 2014), Japan Agency for Local Authority Information Systems

[13] Evaluation Technical Report, LYX-ETRPP-0002-00, Version 2.0, April 24, 2014, ECSEC Laboratory Inc. Evaluation Center

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

[15] Observation report LYX-EOR-7001-00, (January 24, 2014), ECSEC Laboratory Inc. Evaluation Center

[16] Observation report LYX-EOR-7002-00, (February 5, 2014), ECSEC Laboratory Inc. Evaluation Center

[17] Observation report LYX-EOR-7003-00, (February 12, 2014), ECSEC Laboratory Inc. Evaluation Center

[18] Observation report LYX-EOR-7004-00, (February 24, 2014), ECSEC Laboratory Inc. Evaluation Center

[19] Observation report LYX-EOR-7005-00, (March 3, 2014), ECSEC Laboratory Inc. Evaluation Center