Certification Report

SAITO Yutaka, Commissioner
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

Protection Profile (PP)

Application Date/ID	2024-09-06 (ITC-4903)
Certification No.	JISEC-C0858
Sponsor	Japan Agency for Local Authority Information Systems
PP Name	Personal Number Card Version 2 Protection Profile
PP Version	1.00
PP Conformance	None
Assurance Package	EAL4 Augmented with ALC_DVS.2, AVA_VAN.5
Developer	Japan Agency for Local Authority Information Systems
Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above PP is certified as follows.

2025-12-01

HASHIMOTO Toru, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

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 2022 release 1.
- Common Methodology for Information Technology Security Evaluation 2022 release 1.
- CC:2022 release 1 and CEM:2022 release 1 Errata & Interpretation Version 1.1

Evaluation Result: Pass

"Personal Number Cards Version 2 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 1
1.1 Evaluated PP 1
1.1.1 Assurance Package 1
1.1.2 PP overview 1
1.1.2.1 Security functions overview 4
1.1.2.2 Treats and security objectives 5
1.1.3 Disclaimers 5
1.2 Conduct of Evaluation 6
1.3 Certification 6
2. PP Identification 7
3. Security policy 8
3.1 Security Function Policies 8
3.1.1 Threats and Security Function Policies 8
3.1.1.1 Threats 8
3.1.1.2 Security Function Policies against Threats 9
3.1.2 Organizational Security Policies and Security Functions 10
3.1.2.1 Organizational Security Policies 10
3.1.2.2 Security Functions to Organizational Security Policies 12
4. Assumptions and Clarification of Scope 13
4.1 Usage Assumptions 13
5. Evaluation conducted by Evaluation Facility and Results 15
5.1 Evaluation Facility 15
5.2 Evaluation Approach 15
5.3 Overview of Evaluation Activity 15

5.4 Evaluation Results 16
5.5 Evaluator comments / recommendations 16
6. Certification 17
6.1 Certification Result 17
6.2 Recommendations 17
7. Annexes 17
8. Glossary 18
9. Bibliography 21

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Personal Number Cards Version 2 Protection Profile, Version 1.00" (hereinafter referred to as the "PP[11]") developed by Japan Agency for Local Authority Information Systems, and the evaluation of the PP was finished on September 4, 2025 by ECSEC Laboratory Inc., Evaluation Center. (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[11] are described in the PP.

This Certification Report assumes "developers and procurement entity of products conforming to PP[11]" 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

The following is shown summary the security functions required by PP[11]. For details, refer to Chapter 2 and subsequent chapters.

1.1.1 Assurance Package

The Assurance Package 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[11] specifies the security requirements for the smart card used as "Personal Number Card" in the Social Security and Tax Number System.

The TOE of the PP[11] is the smart card including an IC chip and contact/contactless interfaces. In the IC chip, application programs (hereinafter APs) and data are installed to provide services of personal number card.

The construction of the TOE is shown in Figure 1-1.

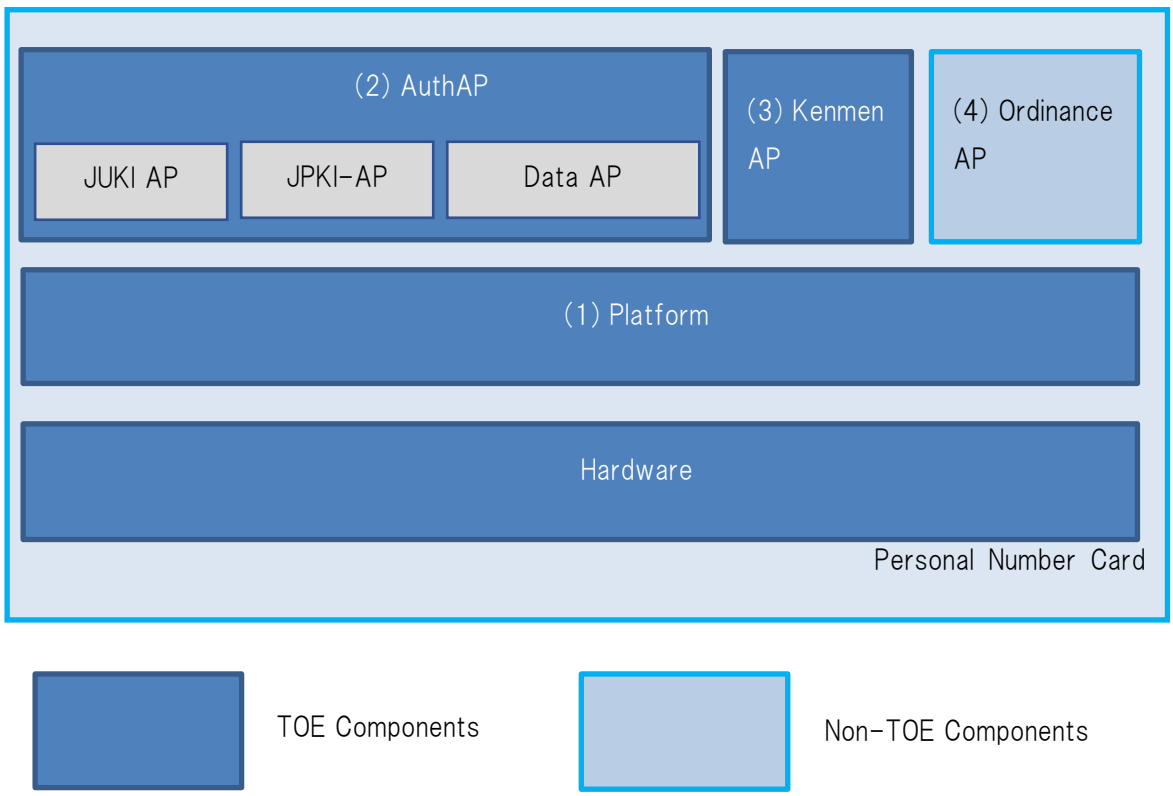

Figure 1-1 Construction of the TOE

In Figure 1-1, the TOE consists of the smart card hardware and the following software: (1) platform, (2) Auth AP, and (3) Kenmen AP. The (4) Ordinance AP, which is software, is outside the scope of the TOE.

TOE hardware provides the operating environment for software while also countering attacks against the hardware. The following describes the software components: (1) Platform, (2) Auth AP, (3) Kenmen AP, and (4) Ordinance AP.

(1) Platform

The platform provides an operational environment for each AP. The platform provides the additional functionality to add/delete APs (Ordinance AP) based on ordinances of each local government.

(2) Auth AP

The Auth AP includes three APs, Basic Resident Registration Network System Card Application (hereinafter JUKI AP), Public Certification Service for Individuals Card Application (hereinafter JPKI AP), and Application for digitization of the personal information

printed on the card (hereinafter Data AP). The Auth AP protects the communication between the Auth AP and the three APs by secure messaging. The Auth AP also provides user authentication (including external authentication), internal authentication, and private letter function. For details on external authentication and internal authentication, refer to Section 1.1.2.1 (2) below.

[JUKI AP]

This is a card application for Basic Resident Registration Network System. This is an AP to use the services provided by the Basic Resident Registration Network System and stores the cardholder's resident registration code. The dedicated terminals installed at each local government are used to read out the code.

[JPKI-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 attestation" for electronic authentication of the cardholder. It stores pairs of the public keys and the private keys and the certificates in the TOE for each use above. It executes cryptographic operation for generating electronic signature in the card.

[Data AP]

This is the application providing the personal number and the four data (name, address, date of birth, gender) of the cardholder. These data are stored in the TOE in the form of text data and read out by an authenticated user.

(3) Kenmen AP

This is the application providing personal information printed on the card. The three data (name, address, date of birth), 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 is suspected, it is verified by comparing printed information (or the personal number) with those stored data displayed on a terminal. Additionally, this AP provides the cardholder with the personal number and the four data in text data format. The stored data are not confidential, because they are identical with the printed information on the card. However, to prevent data from being read without the cardholder's knowledge, this AP requires user authentication (including external authentication) during the read operation. This AP protects communications by secure messaging and provides both internal authentication and external authentication functions.

(4) Ordinance AP

An AP loaded onto the personal number card based on ordinances of local governments.

Hereinafter, (2) Auth AP and (3) Kenmen AP are collectively referred to as "Basic AP".

J-LIS administrators write the data required for the platform and the Basic AP onto the personal number card supplied to J-LIS. Then, each personal number card is issued to the resident (cardholder) via the local governments or other statutory body. Administrators of the J-LIS, local governments or other statutory body write necessary data including information specific to the cardholder in the card prior to the issue (personalization of the card). Additionally, Ordinance APs will be added to the personal number card as necessary.

1.1.2.1 Security functions overview

This PP[11] 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 smart 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 based on secure message attribute of access target. The platform implements secure messaging via SCP 11a, while Auth AP and Kenmen AP implement secure messaging via SCP 11b.

(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 Ordinance APs that are out of scope of the TOE is also the service of the TOE.

First, the user selects a processing object (e.g. a file or a processing function of the TOE). The TOE authenticates the user based on the security attributes of the object. If the user is authenticated successfully, the TOE will permit the user to access the object based on its security attributes. The types of allowable access are also embedded in the security attributes of the object.

There are two types of users for the TOE, human users and external terminals. External terminals refer to the IT devices exchanging data directly with the TOE. For user authentication mechanisms, the TOE provides password system and public key cryptographic system. Authentication of the external terminal by the TOE (the IC card) is referred to as External Authentication in the IC card field. In contrast to External Authentication, there is the term Internal Authentication. Internal Authentication is the function for external terminals to authenticate the IC card (the TOE), to examine that the TOE is not forged (authenticity determination). Internal Authentication is needed for the security of the external terminal side. The TOE offers cryptographic functionality to address Internal Authentication.

(3) Cryptographic operation

The TOE provides cryptographic operation functionality for the services of the platform and each of APs. The cryptographic operation functionality is used for secure messaging, user authentication, signature/user attestation for the Auth AP and so on. Elliptic curve-based signature generation, signature verification, key generation, and shared secret generation use NIST P-384, with a key length of 384 bits.

(4) Countering 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 Treats and security objectives

The TOE conforming to the PP[11] 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 a smart 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

None.

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 September 2025, based on assurance requirements of the PP[11] according to the publicized 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 [12] and the Observation Reports ([14][15]) prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the PP[11] 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][7][8]), CEM ([9]), and Errata and Interpretation ([10]).

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

2. PP Identification

The PP[11] is identified as follows:

Name of PP:	Personal Number Cards Version 2 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[11] adopts to counter threats, and organizational security policies.

In the PP[11], two types of security functions are required to the TOE, as such they are functions requested for the services of personal number cards and general functions for smart cards. The four 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[11], the security functions are provided to counter the threats shown in 3.1.1.1 and to satisfy the organizational security policies shown in 3.1.2.1.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The PP[11] 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	Threats
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 environment 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.Phys_Attack	An attacker attacks components of the TOE 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:

Identifier	Threats
	● Monitoring and analyzing power traces 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[11] counters the threats shown in Table 3-1 by security functions as follows.

(1) Counters to the threat "T.Illegal_Attack"

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.

To counter this threat, the TOE verifies the authenticity of external terminal communicating with the personal number card and permits 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 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[11] is exposed to physical tampering (observation, analyzing or modification), due to the nature of physical embodiment of an IC. The behavior 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 [13] of SOG-IS for smart 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 Organizational Security Policies and Security Functions

3.1.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE conforming to the PP[11] are shown in Table 3-2.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policies
P.Secure_messaging	Secure messaging shall be applied to the communication between the TOE and an external terminal if the access object has been assigned the secure messaging attribute.
P.Delivery	On delivery of personal number cards from developers, the functionality to prevent illegal access 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 access. 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.

Identifier	Organizational Security Policies
P.Cryptography	The TOE provides environment where cryptographic functions are available to the platform and the basic APs. The cryptographic functions are used for data protection, signature, calculation of shared secret or authentication. Table 3-3 shows cryptographic algorithms, cryptographic operations, cryptographic key sizes, and purposes of cryptographic functions. When importing the private key to be used into the TOE, the communication channel is protected, and the private key is decrypted within the TOE using the key encryption key. When importing the public key to be used into TOE, verify the signature within TOE. The TOE imports the temporary public key for private letter, compute the shared secret, and export it. The TOE deletes the cryptographic key after use.
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_PRND] The required quality of random numbers depends on the purposes. The quality should be defined with objective metric.

Table 3-3 Cryptographic function policies

Algorithms	**Cryptographic operation**	**Key size (bits)**	**Purpose**
AES CBC mode (FIPS PUB 197, ISO/IEC 10116)	Encryption /decryption	192	Encryption /decryption for secure messaging
	Decryption		Decryption of keys imported
CMAC with AES (ISO/IEC 9797-1, FIPS PUB 197)	MAC generation / verification		MAC generation / verification for secure messaging Receipt generation of SCP11
ECDSA (FIPS PUB 186-5)	Signature verification with a public key	384 (NIST P-384)	External authenticate
	Signature generation with a private key*1	384 (NIST P-384)	User attestation by the JPKI-AP Signature generation by the JPKI-AP Internal authenticate by the

Algorithms	Cryptographic operation	Key size (bits)	Purpose
			Auth AP
CTR_DRBG, Hash_DRBG, HMAC_DRBG (SP800-90A)	Generation of nonce	—	Use for ECDSA supporting technique
ECDH (BSI-TR03111)	Ephemeral key generation	384 (NIST P-384)	Sharing key material for secure messaging
	Calculate shared secret	384 (NIST P-384)	Calculate shared secret for private letter
KDF with SHA-384 (ANSI X9.63, BSI-TR03111)	Key derivation	192	Key derivation for secure messaging
SHA-384 (FIPS 180-4)	Hash operation	—	Used as a supporting technique for ECDSA
			Session key derivation

3.1.2.2 Security Functions to Organizational Security Policies

The PP[11] requests the security functions to satisfy the organizational security policies shown in 3.1.2.1.

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

This organizational 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.

TOE provides functions to encrypt and decrypt communications between individual software within the TOE and external terminals according to Table 3-3, and/or to generate and verify MACs, thereby achieving the intended level of protection for the confidentiality and/or integrity of communication data.

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

This organizational security policy specifies that only legitimate users can access logically to the inside of the TOE that is under the control of the local governments or other statutory body,

which is the issuer of personal number cards.

In accessing the platform or each of the basic APs, the TOE requires separate authentication for each. The user is permitted to access 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 organizational security policy "P.Cryptography"

This organizational security policy specifies the cryptographic algorithms and the keys that used by the TOE (Table 3-3).

The TOE conforming to the PP[11] provides cryptographic functions and cryptographic key management functions indicated in this organizational security policy.

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

This organizational security policy specifies generating random numbers resistant to attackers' prediction attempts.

The TOE conforming to the PP[11] provides a random number generator (RNG) satisfying the quality metric depending on the use of random numbers. The RNG will be either one of the following:

- Physical RNG
- Deterministic RNG.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE conforming to PP[11] as useful information for the assumed readers to determine the use of the TOE conforming to the PP[11].

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE conforming to PP[11].

The effective performances of the security functions of the TOE conforming to PP[11] are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

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 (pairs of public and private keys) of the TOE are assured to be valid, 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.

Identifier	Assumptions
A.AP	The personnel responsible for loading any APs is assumed to load APs developed by trusted developers with appropriate development methods, on the TOE.
A.Terminal	The person responsible for the management and operation of personal number cards in the organization involved in card issuance shall ensure that the external terminal where data or APs are set up in the TOE is installed in a secure environment that prevents eavesdropping and tampering in the communication path.
A.Card	The person responsible for the management and operation of personal number cards in the organization involved in card issuance shall securely dispose of personal number cards that have been returned by card holders for reasons such as expiration of validity, in a way that does not allow the personal number or encryption key to be restored.

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, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

5.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance requirements 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[11] as well as the content of the evaluation and the verdict of each work unit in the CEM.

5.3 Overview of Evaluation Activity

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

The evaluation started in September 2024 and concluded upon completion of the Evaluation Technical Report dated September 2025. 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 evaluations conducted.

Concerns found in evaluation activities were issued as the Observation Report and 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.

5.4 Evaluation Results

The evaluator had concluded that the PP[11] 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、APE_REQ.2

5.5 Evaluator comments / recommendations

There are no particular evaluator recommendations that should be brought to the attention of the procurer.

6. Certification

The Certification Body performed the certification from the following viewpoints 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 PP[11] 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 evaluation of the PP[11] 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 hardware components of TOE are all part of TSF. Attacks against TSF are subject to vulnerability analysis evaluation, regardless of whether a PP threat description exists.

When communicating with external terminals, secure messaging is applied if the target has been assigned the secure messaging attribute. Whether to assign the secure messaging attribute depends on the separately specified procurement specifications.

7. Annexes

There is no annex.

8. Glossary

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

The abbreviations used in this report are listed below.

basic AP	"Authentication card application" (Auth AP) and "application for the personal information printed on the card" (Kenmen AP) are collectively referred to as basic AP.
card holder	resident to whom the personal number card is issued
external authentication	authentication of an external terminal by a smart card (TOE)
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, the local governments or other statutory body. The administrator performs setting data, creating Ordinance AP in issuing smart cards, and updating data for issued cards
shared key	cryptographic key used in symmetric-key cryptography algorithms.
shared secret	secret information shared between the cardholder and the legitimate sender of the private letter to encrypt and decrypt the contents of the private letter.
public key	public key used in asymmetric cryptography algorithms.

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.
private letter	A function that allows only the card holder to read the contents of the transmission, such as protecting official notices from public organizations or replacing pressure-sealed postcards from private businesses. Public organizations or private businesses encrypt the transmitted information using a key for the private letter and send it to the cardholder. The personal number card generates and outputs a shared secret within the personal number card based on the ephemeral public key sent from the public organization or the private business and the secret key for the private letter function held within the personal number card. The cardholder generates a key for the private letter from the shared secret and decrypts the transmitted information.
secure messaging	set of means for cryptographically protecting confidentiality and/or integrity of communication data
Japan Agency for Local Authority Information Systems	organization founded on April 1st, 2014 based on the Act on Agency for Local Government Information Systems. This organization 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 organization 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 organization also performs the operation of generating personal numbers and of issuing personal number cards on the consignment from local governments.
internal data	data stored in the TOE. This includes user data and TSF data which affects the behavior of the TOE.
internal authentication	authentication of a smart card (TOE) by the external terminal
private key	private key used in an asymmetric key cryptographic algorithm
user data	data for the user, that does not affect the operation of the TSF
four data	name, address, date of birth, and gender
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
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
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
SCP11	Secure Channel Protocol 11. The secure communication specifications defined by GlobalPlatform. These include the definitions for SCP11a, where the smart card and external terminal mutually authenticate each other, and SCP11b, where the external terminal authenticates the smart card.
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 Document, September 2025, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, December 2023, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CC:2022 Revision 1, November 2022, CCMB-2022-11-001(Japanese Version 1.0, September 2023)

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CC:2022 Revision 1, November 2022, CCMB-2022-11-002(Japanese Version 1.0, September 2023)

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CC:2022 Revision 1, November 2022, CCMB-2022-11-003(Japanese Version 1.0, September 2023)

[7] Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities CC:2022 Revision 1, November 2022, CCMB-2022-11-004(Japanese Version 1.0, September 2023)

[8] Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements CC:2022 Revision 1, November 2022, CCMB-2022-11-005(Japanese Version 1.0, September 2023)

[9] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, CEM:2022 Revision 1, November 2022, CCMB-2022-11-006 (Japanese Version 1.0, September 2023)

[10] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 2024, CCMB-2024-07-22 (Japanese Version 1.0, December 2024)

[11] Personal Number Cards Version 2 Protection Profile, Version 1.00, (September 03, 2025), Japan Agency for Local Authority Information Systems

[12] Evaluation Technical Report, LYX23-ETRPP-0001-05B, Version 1.5, September 04, 2025, ECSEC Laboratory Inc. Evaluation Center

[13] Joint Interpretation Library - Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, February 2024

[14] Observation report LYX23-EOR-0001-00, (June 10, 2025), ECSEC Laboratory Inc. Evaluation Center

[15] Observation report LYX23-EOR-0001-01, (July 04, 2025), ECSEC Laboratory Inc. Evaluation Center