Personal Number Cards Version 2

Protection Profile

Version 1.00

3-September-2025

Japan Agency for Local Authority Information Systems

ECSEC Laboratory Inc. Technical Center

JISEC-C0858

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

Glossary and acronyms

General CC terms

CC	Common Criteria: Criteria of security evaluation for IT products. ISO/IEC 15408 is the counterpart of CC in ISO/IEC standards
CCRA	The Common Criteria Recognition Arrangement. It is the arrangement that the results of evaluation and certification under the schemes of the other countries are mutually recognized and accepted among CC evaluation and certification schemes acceding to CCRA.
CEM	Common Evaluation Methodology. A document describing the minimum activities to be taken by the evaluation body to carry out the evaluation.
PP	Protection Profile. Implementation-independent statement of security needs for a TOE type.
SFR	Security Functional Requirement. Security objectives of the TOE rewritten in standardized language.
ST	Security Target. Implementation-dependent statement of security needs for a specific identified TOE.
TOE	Target of Evaluation. A set of software, firmware and/or hardware, with guidance.
TSF	TOE security functionality. Combined functionality of all hardware, software, and firmware of a TOE that be relied upon for the correct enforcement of the SFRs.

Terms related to the TOE

AES	Advanced Encryption Standard. One of symmetric key cryptographic algorithms.
AP	Application Program. Software developed and used for a specific purpose.
APDU	Application Protocol Data Unit. Data block sent and received as a command response to the smart card.
CBC	Cipher Block Chaining. One of block cipher modes of operation.
CMAC	Cipher-based MAC. Message authentication code algorithm using block ciphers.
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman. A Key agreement algorithm using elliptic curve cryptography.
ECDSA	Elliptic Curve Digital Signature Algorithm. A digital signature algorithm using elliptic curve cryptography.
IC	Integrated Circuit.
ISD	Issuer Security Domain.
MAC	Message Authentication Code. Short information to authenticate a message.
NIST	National Institute of Standards and Technology.
PIN	Personal Identification Number.
PUK	PIN Unlock Key. Information for resetting the PIN.
receipt key	Key to calculating the receipt generated by the SD in the SCP11.
SCP11	Secure Channel Protocol 11. Specification of secure communication as defined by the GlobalPlatform (Industry standardization organization for smart card management systems). SCP11a, which provides mutual authentication between

	the TOE and an external terminal, and SCP11b, which provides authentication of the TOE, are used. See [GPC093] Section 4.1.
SD	Security Domain.
SSD	Supplementary Security Domain. Area where authorized entities can install and manage APs according to their own lifecycle.
SHA	Secure Hash Algorithm. Standardized cryptographic hash function.
S-DEK	Session Data Encryption Key. Key to encrypt/decrypt confidential data.
S-ENC	Secure Channel Session Encryption Key. Key to encrypt/decrypt Secure Messaging command responses.
S-MAC	Secure Channel Session Message Authentication Code Key for Command.
S-RMAC	Secure Channel Session Message Authentication Code Key for Response.
Personal Number Card	Official versatile smart card which includes functions and the services of Basic Resident Registration card used for Basic Resident Registration Network System and adds several new APs. Scope of users is expanded to the whole nation, not only applicants. As basic functions of every smart card, the two APs are included: the authentication AP [Auth AP] and the AP for digitization of the personal information printed on the card [Kenmen AP]. Furthermore, each local government issuing the card may create any APs based on ordinances of the municipalities.
Composite evaluation	A smart card is an IT product composed of software and hardware, which consists of several parts such as an IC chip and an antenna for contactless communication. Smart card products created by integrating one hardware and various software can be evaluated; evaluate the hardware part first, and then the rest equipped with the software. This will allow sharing of the hardware evaluation that often takes a long time and thus reduce total cost of evaluation. This system, the platform part is evaluated first and the whole of the IT product including additional parts is evaluated next, is called “composite evaluation”. In the case of the smart card mentioned above, the target of the composite evaluation will be the software part added on the hardware part and the combination part of the software and the hardware. For the hardware part evaluated already, the former evaluation result of the ST and the evaluation technical report (ETR) can be reused. However, since the ETR is not a public document, the authorization from both the evaluation facility and the certification body concerning the ETR is necessary to reuse it. Especially, in case that the platform part evaluation and the composite evaluation are performed in the different schemes, the sufficient prior coordination among all interested parties will be required.
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. Personal number cards generate and outputs a shared secret within personal number cards based on the ephemeral public key sent from the public organization or the private businesses and the secret key for the private letter function held within personal number cards. The cardholder generates a key for the private letter from the shared secret and decrypts the transmitted information.

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.

Preliminary notice

The background of this protection profile is explained here. Development of the card conforming to this PP is also mentioned.

The current personal number card has been in issue for some time since January 2016. Personal Number Cards Version 2 Protection Profile is developed in response to the next Personal Number Card Task Force, which studied and prepared a final summary of the next Personal Number Card in accordance with the Priority Plan for the Realisation of the Digital Society (Cabinet Decision, June 2023).

As a passport to a digital society that can be used for both face-to-face and non-face-to-face identification, personal number cards are the foundation for online digitisation in the public and private businesses and is expected to help create a secure and convenient digital society based on personal number cards. In the next phase of personal number cards, the security of the encryption algorithm has been strengthened to ensure security in response to technological developments, and the structure has been changed to become two basic APs so that the public will find it more convenient.

Security requirements for personal number cards

This PP provides the security requirements for personal number cards. Personal number cards shall be evaluated with Common Criteria, the international standards for IT security, to demonstrate that adequate security counter measures have been taken. Personal number cards shall satisfy every requirement shown in this PP.

The scope of the security evaluation

Personal number cards are the smart card equipped with both an IC module interface and a contactless interface. The entire smart card, including hardware and software, is subject to CC evaluation.

Composite evaluation is applicable. When the hardware part of the smart card has been evaluated, the redundant evaluation may be omitted in the composite evaluation. Meanwhile, additional evaluation for the security functionality implemented by software or combination of software and hardware shall be performed.

When composite evaluation is not applied, the entire smart card shall be evaluated.

Development of the ST

The developer develops the ST conforming to this PP for CC evaluation. The TOE shall be the entire smart card, whether composite evaluation is applied or not.

This PP requires demonstrable conformance for the ST claiming conformance to. The ST shall offer solution to the generic security problems described in this PP. Namely, the author of the ST shall adopt the solution being equivalent or more restrictive to that described in the PP.

Composite evaluation

On the evaluation of personal number cards composed of software and hardware, if the hardware part of the TOE was evaluated in advance, duplication of evaluation can be avoided by composite evaluation. Composite evaluation is governed by CC Part 1.

Security requirements for the smart card are satisfied by;

(a) The security functionalities by hardware

(b) The security functionalities by software

(c) The security functionalities by combination of hardware and software

The security functionalities (a) have been evaluated in the IC chip TOE. Therefore, the evaluation of the whole smart card will be achieved with additional evaluation of (b) and (c). That is to say, the subject of composite evaluation is all security functionalities of this PP except those implemented solely by the hardware.

(c) is the case where security functionalities of the hardware are supplemented by the software. For example, to counter the attack exposing a cryptographic key by DPA (Differential Power Analysis), the cryptographic operation program is devised so that it becomes difficult to estimate cryptographic keys by analysing power consumption during cryptographic operation.

Contents

1 PP introduction

1.1 PP reference

Title:	Personal Number Card Version 2 Protection Profile
Version:	1.00
Publication date:	3-September-2025
Sponsor:	J-LIS (Japan Agency for Local Authority Information Systems)
Editor:	ECSEC Laboratory Inc. Technical Center
Certification ID:	JISEC-C0858

1.2 TOE overview

1.2.1 TOE type

The TOE is the IC card. It is the dedicated product for the Social Security and Tax Number System.

1.2.2 TOE usage

The TOE is the smart card used as “personal number cards” for the Social Security and Tax Number System, based on relevant laws and regulations.

(1) Construction of the TOE

The TOE consists of hardware and software.

The hardware embodiment of the TOE is the plastic card in which an IC chip containing firmware and components for physical external interfaces are embedded. The physical external interfaces are both contact and contactless. Information of the card holder, such as name and photographic portrait, is printed on the surface of the card.

The software of the TOE consists of programs providing services of personal number cards and data for the programs. The programs consist of “the platform” and APs (Application Programs). The platform provides an operational environment for APs. The operational environment is partitioned in multiple logical domains for management, which are called security domains (SDs). The TOE can configure multiple SDs on the platform, and each AP runs only inside the SD to which it belongs. An SD may include other SDs in it. There is the root SD called the issuer SD (ISD), which covers the whole of the platform. The ISD is pre-created in a development environment. An SD except for ISD is called as a supplementary SD (SSD). SSDs are created within ISD. Creation and deletion of SSDs can be done in operational environment.

Two kinds of APs run on the platform according to a use. Those two APs are “authentication card application” (hereinafter Auth AP) and “application for the personal information printed on the card” (hereinafter Kenmen AP). They are called “the basic APs” in this PP. The basic APs are located on ISD directly in a development environment and never belong to any SSDs.

Any municipalities issuing personal number cards may add APs based on ordinances of the municipalities (hereinafter Ordinance AP). Any Ordinance APs are added in SSD(s) and distinguished from the basic APs. Detailed explanation is provided in the next section (2).

The construction of the TOE is explained as follows. An example of the internal construction of the TOE is shown in Figure 1-1. The purpose of this figure is to present the major components of the TOE for

understanding the behaviour of the TOE. It does not intend to specify nor limit the implementation of the TOE.

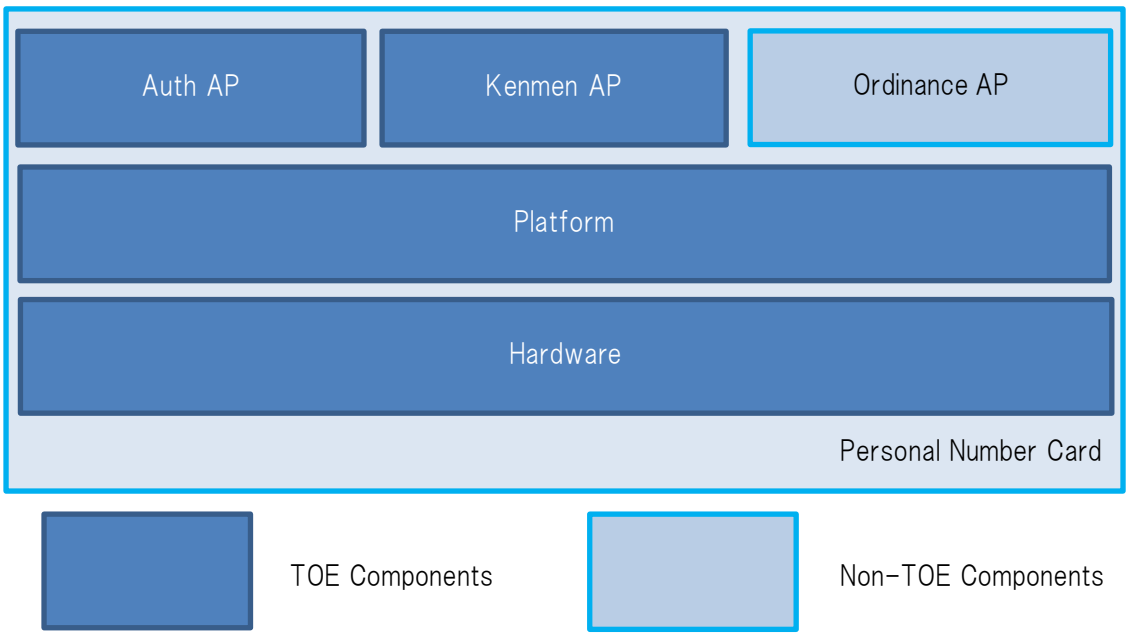

Figure 1-1 Construction of the TOE

The software of the TOE consists of the platform and the two basic APs. They provide their own services to users. “Providing a service” means that the TOE allows a user to use the functionality of the TOE within the privileges of the user. The services are not limited to read out the data from the TOE. Any interactions between users and the TOE are called as services of the TOE, such as functions storing or modifying data, or processing functions. Any Ordinance APs are optional by municipalities and not included in the components of the TOE.

(2) Services provided by the basic APs

Personal number cards are issued to residents via municipalities and other statutory bodies. The two basic APs provide services described below. Some of the services are available for municipal operations as well as for private businesses operations. In principle, user authentication is required before using any services. However, some specific data can be read out without user authentication.

[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.

[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.

[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 was doubted, 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 external authentication during the read operation. This AP protects communications by secure messaging and provides both internal authentication and external authentication functions.

1.2.3 Major security features

The TOE provides security features to protect the information assets. The software part of the TOE (the platform and the basic APs) controls logical accesses via external interfaces. It identifies and authenticates a user and permits him/her to access information or resources of the TOE depending on his/her privileges. As the platform and the two basic APs are mutually independent software, the users and service features for them are specified separately. Therefore, the security functional requirements (SFRs) are also specified for each of the software types above.

This chapter describes the security features of the entire TOE. The different security features for each of software types will be described in the chapter 3 or later. On the other hand, the hardware part of the TOE is utilized as a common resource for the software. The hardware provides operational environment for the software and counters the attacks to the hardware itself as well.

The major security features of the TOE are described below.

(1) Protection of communication data

The TOE provides two interfaces, contact and contactless interfaces, to communicate with an external terminal. Based on the secure messaging attributes of the access target, for the communication which needs protection from eavesdropping or modification, the TOE applies "secure messaging" function to protect confidentiality and integrity of communication data by means of encryption/decryption and generation/verification of MAC (Message Authentication Code). The platform uses secure messaging based on the SCP11a, while the Auth AP and the Kenmen AP use secure messaging based on the SCP11b.

(2) User authentication and access control

The TOE performs user authentication and access control for each service and provides the service depending on the privileges of the user. “Providing the service” means that the TOE permits the user to use functions of the TOE. For example, reading out data stored in a file of the TOE (e.g. a personal number) or using the signature function of the TOE. The function creating/deleting APs based on ordinances of municipalities is also the service of the TOE

In case of security mechanisms of typical IC cards, a user first selects a processing object (e.g. a file or an 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 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[1] 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, which is 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.

All hardware parts of the TOE belong to the TSF. Any attacks to the TSF should be considered in terms of evaluation of vulnerability analysis, regardless of the threats described in this PP.

1.2.4 Available non-TOE hardware/software/firmware

The TOE is the IC card which consists of embedded software for personal number cards and hardware to run the embedded software. Operation of the TOE does not rely on other IT environment, except for power supply from the external terminal.

The usages of the TOE components, the platform and the two basic APs, are different each other. Users of the TOE (municipalities, government agencies, private businesses, personals and so on) are required to prepare terminal devices depending on their purposes.

[1] Meaning of the narrow sense of “External Authentication” is that an IC card (the TOE) authenticates a particular external terminal based on a cryptographic algorithm. This narrow sense is applied for a specific authentication mechanism in chapter 3 and chapter 4.

1.2.5 Life cycle of the TOE

The lifecycle of the TOE is described. This is the information to help understanding the TOE and does not intend to provide specific development methods nor development environments. The authors of PPs/STs conforming to this PP can describe the lifecycle based on the real environment regardless of the description here.

(1) Development of the IC chip (hardware)

The developer develops the IC chip to be embedded in personal number cards. This process includes development of the photomasks for the IC chip production and the dedicated firmware for the IC chip.

The software is embedded into the IC chip at this phase or the phase (3). The development of the software is done at the phase (2).

On this phase of hardware development, the development is often distributed across multiple sites. Various processes might be performed at different development sites, such as design of the circuits, design and production of the photomasks for the IC chip, production of the IC chip.

(2) Development of the platform and the basic APs

The software (the platform and the basic APs) are developed. The development of the software can be performed independently from the development of the hardware (1).

(3) Production of personal number cards

Personal number cards are manufactured through the processes embedding the software corresponding to the TOE of this PP into the IC chip (or it may be done at a part of the hardware production phase) and embedding the IC chip in the plastic card together with an antenna for contactless communication. The development phase of the lifecycle includes these phases from (1) to (3). Personal number cards manufactured are supplied to J-LIS

(4) Issue of personal number cards

J-LIS administrators write the data required for the platform and the two basic AP onto personal number cards supplied to J-LIS. Then, each personal number card is issued to the resident (cardholder) via the municipality or other statutory body. Administrators of the J-LIS, municipality or other statutory body write necessary data including information specific to the cardholder in the card prior to the issue. This procedure is called as personalization of a card. This phase and the subsequent correspond to operational phase.

(5) Creation of Any APs based on ordinances of municipality

The municipalities issuing personal number cards may add own APs based on ordinances of the municipalities. They are optional by the municipalities and not necessarily created.

(6) Use of personal number cards by the card holder

The resident to whom personal number cards are issued are referred to the card holder and use the services of the card. Various organizations relating to services of personal number cards other than the card holder are also able to use services of personal number cards. Examples of the organizations are municipalities, government agencies or private businesses admitted by laws.

2 Conformance claim

2.1 CC conformance claim

This PP claims CC:2022 Release 1 *(The original Japanese version PP conforms to "CC: 2022 Release 1 translation version 1.0" by IPA).* Errata and Interpretation [ERT] applies to this PP.

This PP claims [CC] part 2 conformant and [CC] part 3 conformant.

2.2 PP claim

This PP does not claim conformance to other PPs.

2.3 Package claim

This PP claims package conformance to EAL4 augmented.

The augmented SARs are ALC_DVS.2 and AVA_VAN.5.

2.4 Conformance rationale

There is no conformance rationale because this PP claims no conformance to other PPs.

2.5 Conformance statement

This PP requires demonstrable conformance to the PPs/STs claiming conformance to this PP.

3 Security problem definition

Security problems concerning the TOE are defined in this chapter. Security problems are described on three aspects: threats - countered by the TOE and/or its environment, organizational security policies - enforced by the TOE and/or its environment, and assumptions – met by the operational environment. These problems are concerned with the operational phase of the life cycle of the TOE (see 1.2.4). The TOE and the environment should address properly these problems.

Threats, organizational security policies, and assumptions are identified with initial letters “T.”, “P.”, and “A.” respectively. “Application note” is appended as necessary. It is reference information to help understanding the PP. As they are not portions of the security problem definitions, it is not required to refer them in STs/PPs conformant to this PP.

3.1 Users

Users involved with this TOE are described. Users of the TOE are divided into four categories as follows. These categories are based on roles of users. Users corresponding to each role are explained in terms of usage of the TOE below.

Cardholder	A person to whom the personal number card (TOE) is issued by the municipality or other statutory body. The cardholder uses service functions of the basic APs or any optional APs that are out of scope of the TOE. The external terminal at the municipality or the PC owned by the cardholder is applied depending on service contents.
Administrator	A person who administers the TOE in operational environment. Administration is the work needed for proper operation of the TOE, such as creating/deleting non-TOE AP, data setting/modification for the platform/basic APs or releasing of blocked password. There are platform administrators, Auth AP administrators, JUKI AP administrators, JPKI-AP administrators, Data AP administrators, and Kenmen AP administrators. The administrators of free space are the J-LIS or the person authorized by the J-LIS to manage free space and mounts the Ordinance AP, etc. in the free space.
Organizations	Various organizations relating to the services of the TOE use the TOE. Examples of organizations are the municipalities, government agencies or private businesses which are admitted using the services of the TOE by laws. Organizations are shown as “the system handling xx” in this PP.
External terminal	IT equipment located outside the TOE that exchanges data with the TOE in the operational environment of the TOE. It is also referred to as the external device.

3.2 Assets

The information assets protected by the TOE security functionality (TSF) are the user data stored in the TOE and the processing functions of the TOE for users. The user data is the data used for cardholders and is valuable for the cardholders. An example of user data is cardholder’s personal number based on “The Social Security and Tax Number System”. An example of a processing function is electronic signature

generation function for the cardholder applied to public ID authentication, which is based on public key cryptographic system.

User data of the TOE and processing functions for users are objects protected by the TSF and referred to primary assets. Primary assets are described explicitly as the assets in the “Threats” of PP/ST. User data other than that protected by the TSF is not a protected asset. The TOE can be added additional APs in the free space outside the TOE. They are not provided in this PP and the user data for them are not included in the assets of the TOE.

The TOE assets used to protect primary assets are referred to secondary assets. The TOE security functionality (TSF) and data used for the TSF are considered as the secondary assets. If the TSF itself is tampered, or TSF data is disclosed or modified, the TSF will not operate correctly and no longer be able to protect the primary assets. Therefore, the TSF and the TSF data shall be protected by the TSF itself.

Generally, only primary assets should be defined in threats and organizational security policies of PPs/STs. Secondary assets have no need to be identified and included at early stage, because they depend on the protection mechanism for the primary assets. However, this PP includes physical attacks against IC card (attacks to the hardware that is a part of the TSF) into the threats. Physical attacks against hardware include independent attacks from logical attacks to the primary assets. The TOE shall counter them. Physical attacks include attacks that exploit APs outside the TOE.

The scope of physical attacks to be countered is shown specifically in [JILAP]. Evaluation of the TOE for physical attacks should be carried out according to the newest supporting documents at the point of the evaluation.

3.3 Threats

The threats that the TOE should counter are as follows. They shall be countered by the TOE, its operational environment or a combination of the two.

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 protected 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 the issue and also after the personalization and the issue to card holders.

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 analysing 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 behaviour of the TOE by physically manipulating the inside of TOE.

3.4 Organizational security policies

Organizational security policies applied to the TOE and/or the operational environment of the TOE are described. “The organizations” refer to J-LIS and municipality or other statutory body.

P.Secure_Messaging

The TOE applies secure messaging in communications with external terminals when a secure messaging attribute is assigned to an access target.

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 APs. The cryptographic functions are used for data protection, signature generation, calculating shared secret or authentication. Table 4-1 shows the cryptographic algorithms, cryptographic operations, cryptographic key lengths, and cryptographic function usages required for TOE. When importing the private key into the TOE, the communication channel is protected, and the private key is decrypted using the key encryption key within the TOE. When importing a public key, the signature is verified within the TOE. The TOE imports an ephemeral public key for the private letter[2], performs a shared secret calculation, and then exports it. The TOE deletes the encryption 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: P.RND] The quality of random numbers will depend on purposes. The quality should be defined with objective metric.

[2] TOE does not verify signature when importing the ephemeral public key for private letter.

3.5 Assumptions

Assumptions are applied to the operational environment of the TOE. They are necessary for the TOE to provide its security functionality.

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

The person in charge of creating any APs is assumed to create 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.

4 Security objectives

To address the SPD shown in the chapter 3, the security objectives for the TOE and the environment of the TOE are described. Security objectives for the TOE is shown in 4.1 and security objectives for the environment of the TOE are shown in 4.2 respectively. Rationale demonstrating adequacy of the objectives for the SPDs is shown in 4.3.

Security objectives for the TOE and for the environment of the TOE are identified with the initial letters “O.” or “OE.” respectively.

4.1 Security objectives of the TOE

O.I&A

The TOE shall identify/authenticate a user of the TOE and authorize the user who has been authenticated successfully to perform the actions corresponding to the role of the user. For user authentication, authentication mechanisms are used based on either collation of secret information (e.g. password (PW) and transport key), or public key cryptosystem.

> [Application note: O.I&A] Specification of authentication mechanisms and user privileges will be provided by the procurement authority, separately from this PP.

O.Access_Control

The TOE shall permit the subjects controlled under the TOE to access the objects controlled under the TOE based on privileges of each subject. The other accesses shall be prohibited. A subject is an active process in the TOE and executes operations to objects. A subject is associated with a user and operates objects on behalf of the authenticated user. Objects are passive entities which are operated by subjects, in the TOE. Examples of objects are user data files, any APs that are out of scope of the TOE (hereinafter non-TOE AP), SSDs or processing functions in the TOE. Operations include input and output of user data, execution of processing functions or creation/deletion of objects.

O.Secure_Messaging

The TOE shall apply secure messaging in communications with the external terminal when the secure messaging attribute is assigned to a access target. In the secure messaging, communication data shall be protected from disclosure and modification with encryption/decryption and generation/verification of MAC (Message Authentication Code) by applying the secret key cryptographic algorithm.

O.Delivery

Personal number cards shipped from the developer shall store secret authentication data inside the cards to prohibit persons who do not know the data from accessing the inside of the card. This countermeasure is performed by the platform and each AP of the two basic APs individually.

O.Cryptography

The TOE shall provide cryptographic operational function and cryptographic key management function for the platform and the APs. The cryptographic function applied to the platform and the APs shall comply with the policies shown in Table 4-1. When importing private keys into a TOE, the communication channel

shall be protected. Furthermore, private keys shall be decrypted using a key encryption key within the TOE. When the TOE imports public keys for external authentication into the TOE, the signature shall be verified within the TOE. The TOE shall import the ephemeral public key for the private letter, calculate the shared secret, and then export it. TOE shall delete the encryption key after use.

Table 4-1 Cryptographic function policies

Algorithms	Cryptographic operation	Key size	Purpose
AES-CBC mode [FIPS197], [ISOIEC10116]	Encryption /decryption	192 bits	Encryption /decryption for secure messaging
	Decryption		Decryption of keys imported
CMAC with AES [ISOIEC9797_1], [FIPS197]	MAC generation / verification		MAC generation / verification for secure messaging Receipt generation of SCP11
ECDSA [FIPS186_5]	Signature verification with a public key	384 bits (NIST P-384)	External authenticate
	Signature generation with a private key		User attestation by the JPKI-AP Signature generation by the JPKI-AP Internal authenticate by the Auth AP
CTR_DRBG, Hash_DRBG, HMAC_DRBG [SP800_90A]	Generation of nonce	-	Use for ECDSA supporting technique
ECDH [TR03111]	Ephemeral key generation	384 bits (NIST P-384)	Sharing key material for secure messaging
	Calculate shared secret		Calculate shared secret for private letter
KDF with SHA-384 [X9.63], [TR03111]	Key derivation	192 bits	Key derivation for secure messaging
SHA-384 [FIPS180_4]	Hash operation	-	Used as a supporting technique for ECDSA
			Session key derivation

O.Phys_Attack

The TSF shall protect data inside of the TOE from disclosure and modification, or functions of the TOE from unauthorized use, with physical attacks to the elements of the TOE (hardware/software). The physical attacks to be countered by the TSF are shown in [JILAP].

> [Application note: O.Phys_Attack] Attacks shown in the documents above correspond to overall attacks for smart cards. They are not restricted only to physical attacks. However, O.Phys_Attack covers physical attacks that are not countered by the software of the TOE alone. Please beware that the scope of O.Phys_Attack is not the same as that of the documents.

O.RND

The TSF shall generate random numbers meeting the quality metric depending on purposes. Furthermore, the TSF shall prevent itself from leaking information so that an attacker cannot guess the random number generated.

4.2 Security objectives of the environment

For the threats, the organizational security policies or the assumptions, which are defined as the security problems, the security objectives to be addressed by the operational environment of the TOE to solve those problems are described. Every security objective described here is derived from the assumptions.

OE.PKI

The person responsible for the administration and operation of personal number cards issuing organization provide the PKI system that assures validity of keys of the public key cryptosystem (pairs of public keys and private keys) of the TOE in the operational environment of the TOE.

OE.Administrator

The person responsible for the administration and operation of personal number cards issuing organization appoint administrators who create, modify or delete data or APs within the TOE. The administrators should be appointed on the condition that; they are able to correctly operate the specific IT devices and will not attempt any malicious act on the assets of the TOE, and that the responsible person grant them the right to perform said duties.

OE.AP

The person in charge of administration and operation of personal number cards or administrators of the TOE in municipality confirm that non-TOE AP have been developed by trusted developers with proper development methods so that unreliable APs are not introduced.

OE.Terminal

To prevent eavesdropping and tampering in the communication path, the person responsible for the management and operation of personal number cards in the organization involved in card issuance confirms that the external terminal where data or APs are set up in the TOE before card issuance is installed in physically protected environment.

OE.Card

The person responsible for the management and operation of personal number cards in the organization involved in card issuance securely disposes of personal number cards that has been returned by the cardholder for reasons such as expiration of validity to prevents the restoration of the personal number and encryption keys.

4.3 Security objectives rationale

In this chapter, the rationale for each security objective described above being effective for the items of the security problem definitions is described. In 4.3.1, it is demonstrated that the security objectives for the TOE and the environment for the TOE can be traced back to one or more security problem definitions.

In 4.3.2, it is demonstrated that each security problem is addressed effectively by the corresponding security objectives.

4.3.1 Tracing between security problem definitions and security objectives

The tracing between the security problem definitions and the security objectives is shown in Table 4-2. It shows that all security objectives trace back to one (or more) security problem definitions.

Table 4-2 Tracing between security problem definitions and security objectives

Security objectives / Security problem definitions	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND	OE.PKI	OE.Administrator	OE.AP	OE.Terminal	OE.Card
T.Illegal_Attack	X	X										
T.Phys_Attack			X									
P.Secure_Messaging				X		X						
P.Delivery	X				X							
P.Cryptography						X						
P.RND							X					
A.PKI								X				
A.Administrator									X			
A.AP										X		
A.Terminal											X	
A.Card												X

4.3.2 Justification for security objectives

It is justified that the security objectives for the TOE and the environment of the TOE counter all threats, enforce all organizational security policies and uphold all assumptions.

T.Illegal_Attack

O.I&A provides that the TOE identifies and authenticates the user of the TOE and grants only the user, who has been authenticated successfully, the privilege corresponding to the role assigned to the user. O.Access_Control limits the extent of accessing to objects to what is limited by the privileges associated with the identification information. These security objectives prevent users from disclosing or modifying data beyond their privileges or using the service functions illegally. These security objectives diminish sufficiently the threat T.Illegal_Attack.

T.Phys_Attack

Security violation of the assets by physical attacks to the TOE will be prevented by O.Phys_Attack. O.Phys_Attack covers whole of the threat T.Phys_Attack by claiming compliance with CC supporting documents, therefore the threat T.Phys_Attack is diminished sufficiently.

P.Secure_Messaging

O.Secure_Messaging protects communication data between the TOE and the external terminal from disclosure and modification. The levels of confidentiality and integrity requested for each data, and the operational environments are different between the platform and the two basic APs. Therefore, The TOE applies secure messaging when the target of access has the secure messaging attribute. Cryptographic algorithms for secure messaging are provided according to the rules shown in O.Cryptography. These objectives enforce P.Secure_Messaging.

P.Delivery

P.Delivery includes protection requirements for the TOE not only for operational environment but for transport of the TOE. Therefore, O.I&A which is applied only to the TOE in the operational environment is not sufficient. O.Delivery complements the security counter measures.

O.Delivery addresses P.Delivery and provides policies for countermeasures to protect the TOE from attacks in transport and safekeeping. The TOE of this stage cannot provide sufficient security functionality, because secure setting for the TOE has not been completed yet. However, it is possible to activate authentication function relating to accesses to the inside of the TOE and it addresses P.Delivery. The authentication data for this authentication function is a secret data called as “transport key” for IC card. O.Delivery addresses P.Delivery by requiring authentication mechanism using the transport key. The authentication mechanism of O.Delivery is a part of the security functionality of the TOE. It overlaps with a part of the security mechanisms provided by O.I&A. These security objectives prevent illegal accesses to the TOE in transport and in safekeeping by the card issuing organization. Thereby, P.Delivery is enforced.

P.Cryptography

O.Cryptography refers Table 4-1 presenting the cryptographic function policies (policies for cryptographic operation and cryptographic key management) provided by P.Cryptography and states that the policies are enforced. O.Cryptography also states that it supports key importing, the private letter, and key deletion. O.Cryptography enforces P.Cryptography properly, because O.Cryptography directly enforces P.Cryptography.

P.RND

If O.RND is enforced, random numbers with a quality sufficient for the TSF will be generated, and also it will prevent an attacker from retrieving information helpful to guess random numbers. O.RND prevents an attacker from guessing random numbers generated. P.RND is enforced properly.

A.PKI

OE.PKI is suitable as it directly upholds A.PKI.

A.Administrator

OE.Administrator indicates that administrators in charge of creating, modifying or deleting of data or APs within TOE should be appointed on the condition that; they are able to correctly operate the specific IT devices and will not attempt any malicious act on the assets of the TOE, and that necessary rights for the administration are granted to them. This objective is suitable to uphold A.Administrator.

A.AP

OE.AP requires confirmation that any APs based on ordinances of local governments have been developed by trusted developers, with appropriate development methods. This security objective upholds A.AP directly.

A.Terminal

OE.Terminal requires confirmation that any external terminal implementing data or AP configuration within the TOE is located in physically protected and secure environment. This security objective upholds A.Terminal directly.

A.Card

OE.Card directly corresponds to the contents of A.Card and appropriately upholds A.Card.

5 Extended components definition

This protection profile does not use any extended components.

6 Security requirements

6.1 Security functional requirements

SFRs in this PP are defined using the components from CC part2. SFRs are provided by the security functional components tailored through operations as needed.

The notation for operations used in this PP is as follows:

- Assignment or selection are expressed with italic: [assignment: *xxx (italic)*], [selection: *xxx (italic)*].
- Non-selected items in selection operation are expressed with strike-through: ~~strikethrough.~~
- Refinements are expressed with ***italic and bold*** in the SFR. The SFR descriptions that are replaced by the refinements are shown with a strike-through: ~~strikethrough~~.
- Iterated operation is expressed with information for distinction in parenthesis behind the SFR name, and with the short name attached.

Uncompleted operations are expressed with under-line: [assignment: *xxx (italic/underline)*]. ST authors shall complete those uncompleted operations. SFRs provided in this PP are shown below.

6.1.1 Class FCS: Cryptographic support

6.1.1.1 FCS_CKM.1 Cryptographic key generation (ephemeral key pair for key exchange)

Component relationships

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_CKM.5 Cryptographic key derivation, or
FCS_COP.1 Cryptographic operation]
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate ***key pairs for key exchange*** ~~cryptographic keys~~ in accordance with a specified cryptographic key generation algorithm [assignment: *Elliptic curve key pair generation*] and specified cryptographic key sizes [assignment: *384 bits (P-384)*] that meet the following: [assignment: *[FIPS186_5] A.2*].

6.1.1.2 FCS_CKM.2 Cryptographic key distribution (elliptic curve Diffie-Hellman key establishment)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *key distribution method compliant with SCP11a and SCP11b*] that meets the following: [assignment: *[GPC093] Section 4.1*].

6.1.1.3 FCS_CKM.5 Cryptographic key derivation (elliptic curve Diffie-Hellman key exchange)

Component relationships

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.5.1

The TSF shall derive cryptographic keys [assignment: *session keys (Receipt key, S-DEK, S-ENC, S-MAC, S-RMAC)*] from [assignment: *secrets shown below*] in accordance with a specified key derivation algorithm [assignment: *KDF with SHA-384*] and specified cryptographic key sizes [assignment: *192 bits*] that meet the following: [assignment: *[TR03111] Section 4.3.3, [X9.63] Section 5.6.3*].

SCP11a: A secret generated from an ephemeral public key received from the external terminal and an ephemeral private key generated by the TOE, and a secret generated from a public key extracted from a certificate received from the external terminal and a private key for key agreement corresponding to a certificate for key agreement to be sent to an external terminal

SCP11b (internal authenticate of Auth AP and Kemen AP): A secret generated from an ephemeral public key received from the external terminal and an ephemeral private key generated by the TOE, and the ephemeral public key received from the external terminal and a private key for key agreement corresponding to a public key certificate for key agreement to be sent to an external terminal

6.1.1.4 FCS_CKM.6 Timing and event of cryptographic key destruction

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.6.1

The TSF shall destroy [assignment: *list of cryptographic keys shown below*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction]*].

SCP11a: a secret generated from a public key extracted from a certificate received from the external terminal and a private key for key agreement corresponding to a public key certificate for key agreement to be sent to an external terminal

SCP11b: A secret generated from an ephemeral public key received from the external terminal and a private key for key agreement corresponding to a public key certificate for key agreement to be sent to an external terminal

SCP11 common: *an ephemeral private key for key agreement, a secret generated from an ephemeral public key received from the external terminal and an ephemeral private key generated by the TOE, Receipt key, S-DEK, S-ENC, S-MAC, S-RMAC*

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

[Application note: FCS_CKM.6] For volatile memory, the power supply cut-off to volatile memory may be included in the cryptographic destruction method.

6.1.1.5 FCS_COP.1/ED Cryptographic operation (AES encryption / decryption)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ED

The TSF shall perform [assignment: *encryption/decryption of APDU* for secure messaging, decryption of confidential data using S-DEK*] in accordance with a specified cryptographic algorithm [assignment: *AES CBC mode*] and cryptographic key sizes [assignment: *cryptographic 192 bits*] that meet the following: [assignment: *[FIPS197] (AES), [ISOIEC10116] (CBC)*].

6.1.1.6 FCS_COP.1/MAC Cryptographic operation (MAC)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/MAC

The TSF shall perform [assignment: *MAC generation/verification of APDU for secure messaging*] in accordance with a specified cryptographic algorithm [assignment: *CMAC with AES*] and cryptographic key sizes [assignment: *192 bits*] that meet the following: [assignment: *[ISOIEC9797_1], Section 7.6*].

6.1.1.7 FCS_COP.1/KeyDec Cryptographic operation (decryption of keys)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/KeyDec

The TSF shall perform [assignment: *decryption of a private key for key agreement, a private key for signature generation, a private key for user authentication and a private key for internal authenticate that are imported*] in accordance with a specified cryptographic algorithm [assignment: *AES CBC mode*] and cryptographic key sizes [assignment: *cryptographic 192 bits*] that meet the following: [assignment: *[FIPS197] (AES), [ISOIEC10116] (CBC)*].

6.1.1.8 FCS_COP.1/Receipt Cryptographic operation (receipt generation)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/Receipt

The TSF shall perform [assignment: *generation of receipt for SCP11*] in accordance with a specified cryptographic algorithm [assignment: *CMAC with AES*] and cryptographic key sizes [assignment: *192 bits*] that meet the following: [assignment: *[ISOIEC9797_1], Section 7.6*].

6.1.1.9 FCS_COP.1/SigGen Cryptographic operation (signature generation)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/SigGen

The TSF shall perform [assignment: *signature generation*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA using SHA-384*] and cryptographic key sizes [assignment: *384 bits (P-384)*] that meet the following: [assignment: *[FIPS186_5], Section 6*].

6.1.1.10 FCS_COP.1/PersoAuth Cryptographic operation (signature generation for user attestation)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/PersoAuth

The TSF shall perform [assignment: *signature generation for user attestation*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA using SHA-384*] and cryptographic key sizes [assignment: *384 bits (P-384)*] that meet the following: [assignment: *[FIPS186_5], Section 6*].

6.1.1.11 FCS_COP.1/TOEAuth Cryptographic operation (signature generation for internal authentication of the TOE)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/TOEAuth

The TSF shall perform [assignment: *signature generation for internal authentication of the TOE*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA using SHA-384*] and cryptographic key sizes [assignment: *384 bits (P-384)*] that meet the following: [assignment: *[FIPS186_5], Section 6*].

6.1.1.12 FCS_COP.1/ExtAuth Cryptographic operation (signature verification for external authentication)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ExtAuth

The TSF shall perform [assignment: *signature verification*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA using SHA-384*] and cryptographic key sizes [assignment: *384 bits (P-384)*] that meet the following: [assignment: *[FIPS186_5], Section 6*].

6.1.1.13 FCS_COP.1/Hash Cryptographic operation (hashing)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or

FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/Hash

The TSF shall perform [assignment: *ECDSA signature generation, message digest computation related to ECDSA signature verification, key derivation related to ECDH, [assignment: list of hash calculation]]* in accordance with a specified cryptographic algorithm [assignment: *none*] and cryptographic key sizes [assignment: *SHA-384*] that meet the following: [assignment: *[FIPS180_4]*].

6.1.1.14 FCS_COP.1/ShSes Cryptographic operation (calculate shared secret for the private letter)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ShSes

The TSF shall perform [assignment: *calculate shared secret for the private letter]* in accordance with a specified cryptographic algorithm [assignment: *ElGamal key establishment*] and cryptographic key sizes [assignment: *384 bits (P-384)*] that meet the following: [assignment: *[TR03111] Section 4.3.2.2*].

6.1.1.15 FCS_RNG.1/ES Random number generation (entropy source)

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1/ES

The TSF shall provide a [selection: *physical~~, non-physical true, deterministic, hybrid physical, hybrid deterministic~~*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2/ES

The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].

[Application note: FCS_RNG.1/ES] The assumed random number generator is the PTG.2 class in [KS2011]. This security functional requirement is the entropy source for the DRBG[3] required by [FIPS186_5].

6.1.1.16 FCS_RNG.1/DRBG Random number generation (DRBG)

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1/DRBG

[3] Except for HMAC_DRBG used in the deterministic ECDSA in [FIPS186_5] A.3.3.

The TSF shall provide a [selection: ~~*physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*~~] random number generator that implements: [assignment: *applied DRBG in Table 6-1*].

FCS_RNG.1.2/DRBG

The TSF shall provide [selection: *bits~~, octets of bits, numbers [assignment: format of the numbers]~~*] that meet [assignment: *generation length in Table 6-1*].

Table 6-1 Used DRBG

Object of generation	***Generation method in [FIPS186_5]***	***Applied DRBG***	***Standard***	***Generation length***
Ephemeral key	*[selection: A.2.1, A.2.2]*	*[selection: CTR_DRBG, Hash_DRBG, HMAC_DRBG]*	*[SP800_90A]*	*[assignment: generation length]*
[selection: nonce, none]	*[selection: A.3.1, A.3.2, A.3.3, none]*	*[selection: CTR_DRBG, Hash_DRBG, HMAC_DRBG, none]*	*[selection: [SP800_90A], none]*	*[selection: [assignment: generation length], none]*

[Application note: FCS_RNG.1/DRBG] This security functional requirement is the DRBG used for [FIPS186_5] A.2 ephemeral key generation and A.3 per-message secret (nonce). The ST author shall select [FIPS186_5] A.2.1 or A.2.2 for ephemeral key generation and assign the DRBG in use. The ST author shall also select either [FIPS186_5] A.3.1, A.3.2, or A.3.3 for nonce generation and select the DRBG being used. The ST author shall also select either [FIPS186_5] A.3.1, A.3.2, or A.3.3 for nonce generation and select the DRBG in use. Generation length is 384 - 511. If the TOE uses A.3.3 and does not use HMAC_DRBG, select “None” for all.

6.1.2 Class FDP: User data protection

6.1.2.1 FDP_ACC.1 Subset access control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1

FDP_ACC.1.1 The TSF shall enforce the [assignment: *Personal Number Cards access control SFP*] on [assignment: *Subject:< processes shown at the subject column of Table 6-2>, Object:<entities shown at the object column of Table 6-2>, Operations among subjects and objects covered by the SFP:<operations shown at the operation column of Table 6-2>*].

Table 6-2 Subjects/objects/operations

[Note] EA: External Authentication, TV: Transport key Verification, PV: PIN Verification, PWV: Verification of password for signature generation

Subject	***Object***	***Authentication required***	***Operation***
Platform			
Process on behalf of the administrator of the platform	*[assignment: list of files containing user data*]*	*[selection: EA, TV, [assignment: list of authentications]]*	*[selection: rewrite, read]*
	SSD	*EA*	*create/delete*
Process on behalf of the administrator of free space	*non-TOE AP*	*EA*	*create/delete*
Process on behalf of the external terminal	*a file of public key certificate for key agreement of SCP11a*	*none*	*read*
Auth AP			
Process on behalf of the administrator of the Auth AP	*[assignment: list of files containing user data*]*	*[selection: EA, TV, [assignment: list of authentications]]*	*[selection: rewrite, read]*
Process on behalf of the external terminal	*a file of public key certificate for key agreement of SCP11b*	*none*	*read*
Process on behalf of the external terminal	*a file of public key certificate for internal authenticate*	*none*	*read*
Process on behalf of the cardholder	*a file of public key certificate for the private letter*	*PV*	*read*
JUKI AP			
Process on behalf of the administrator of the JUKI AP	*[assignment: list of files containing user data*]*	*[selection: EA, TV, [assignment: list of authentications]]*	*[selection: write, rewrite, read]*
Process on behalf of the administrator of the JUKI AP	*Resident registration code file*	*TV*	*write*
		EV	*rewrite*
		EV	*read*
Process on behalf of the cardholder and the system handling the Basic Resident Registration data[4]	*Resident registration code file*	*EV and PV*	*read*
JPKI-AP			
Process on behalf of the administrator of the JPKI-AP	*[assignment: list of files containing user data*]*	*[selection: EA, TV, [assignment: list of authentications]]*	*[selection: rewrite, read]*
Process on behalf of the cardholder	*The signing function with the signature private key*	*PWV*	*sign*
	The signing function with the user attestation *private key*	*PV*	*sign*

[4] The reading of the resident code file requires both successful authentication of the cardholder and successful authentication of the system handling the resident code data.

Subject	***Object***	***Authentication required***	***Operation***
	A file of certificate for user attestation	*None*	*read*
Process on behalf of the system handling certificate data	*The signing function with the user attestation private key*	*[assignment: list of authentications]*	*sign*
	A file of certificate for user attestation	*None*	*read*
Data AP			
Process on behalf of the administrator of the Data AP	*[assignment: list of files containing user data*]*	*[selection: EA, TV, [assignment: list of authentications]]*	*[selection: rewrite, read]*
Process on behalf of the administrator of the Data AP	*Personal number (text) file* *four data (text) file* *Signature of the personal number and the four data file*	*TV or EA*	*rewrite*
Process on behalf of the cardholder		*PV or PWV*	*read*
Process on behalf of the system handling the personal number and the four data		*EA*	*read*
Kenmen AP			
Process on behalf of the administrator of the Kenmen AP	*[assignment: list of files containing user data*]*	*[selection: EA, TV, [assignment: list of authentications]]*	*[selection: rewrite, read]*
Process on behalf of the administrator of the Kenmen AP	*file of the digitized image data of the whole printed information* *file of the date of birth (image)* *file of the personal number (image)* *Personal number (text) file* *four data (text) file* *Signature of the personal number and the four data file*	*TV or EA*	*rewrite*
Process on behalf of the external terminal	*a file for public key certificate for key agreement of SCP11b*	*none*	*read*
Process on behalf of the system handling the digitized image data of the whole printed information	*file of the digitized image data of the whole printed information*	*EA*	*read*
Process on behalf of the system handling the date of birth	*file of the date of birth (image)*		
Process on behalf of the system handling the personal number	*file of the personal number (image)*		
Process on behalf of the system handling the personal number and the four data	*Personal number (text) file* *four data (text) file* *Signature of the personal number and the four data file*		

** Objects "files containing user data" and operations for the objects are not specified in this PP. An ST author shall complete these operations in accordance with the specification provided by the procurement authority. "Selection" operation should be repeated for each object (a user data file).*

6.1.2.2 FDP_ACF.1 Security attribute based access control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Security attribute-based access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1

The TSF shall enforce the [assignment: *Personal Number Cards access control SFP*] to objects based on the following: [assignment: *Subjects:< processes shown at the subject Table 6-2>, Objects:<entities shown at the object column of Table 6-2>, SFP relevant security attributes for each subject:<authentication result of the user associated with the subject shown in Table 6-2>*].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *If authentication result of the user associated with the subject is "authenticated successfully", the subject will be able to perform operations allowed to the object*].

FDP_ACF.1.3

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

FDP_ACF.1.4

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

6.1.2.3 FDP_ETC.1 Export of user data without security attributes

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1

The TSF shall enforce the [assignment: *private letter information flow control SFP*] when exporting user ***(shared secret for the private letter)*** data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

6.1.2.4 FDP_IFC.1/PubKey Subset information flow control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/PubKey

The TSF shall enforce the [assignment: *cryptographic key import information flow control SFP*] on [assignment: *Subjects:<the process of the TOE importing a public key for External Authentication and a public key for key agreement from an external terminal>, Information:<a public key for External Authentication and a public key for key agreement>, and Operations:<import>*].

6.1.2.5 FDP_IFC.1/Pri Subset information flow control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Pri

The TSF shall enforce the [assignment: *private letter information flow control SFP*] on [assignment: *Subjects:<the process of the TOE importing an ephemeral public key for the private letter from an external terminal and exporting a shared secret for the private letter to the external terminal>, Information:<an ephemeral public key for the private letter, a shared secret for the private letter>, and Operations:<import of the ephemeral public key for the private letter, export of the shared secret for the private letter>*].

6.1.2.6 FDP_IFF.1/PubKey Simple security attributes

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/PubKey

The TSF shall enforce the [assignment: *cryptographic key import information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *Subjects:< the process of the TOE importing a public key for External Authentication and a public key for key agreement from the external terminal>, Information:<a public key for External Authentication and a public key for key agreement)>, The security attributes for subjects:<the reference data for information verification> and The security attributes for information:<the verification data attached to information>*].

FDP_IFF.1.2/PubKey

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *If the TSF succeeds in verifying the information with the reference data for information verification and the verification data attached to the information, the information flow to the subject will be permitted. The method for determining whether verification has been successful is as follows:*

Case of a public key for External Authentication and a public key for key agreement: The TOE verifies the signature of the certificate (including the public key) sent from the external terminal, by the signatory's public key stored in the TOE (here the reference data for information verification is the signatory's public key)].

FDP_IFF.1.3/PubKey

The TSF shall enforce the [assignment: *none*].

FDP_IFF.1.4/PubKey

The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *none*].

FDP_IFF.1.5/PubKey

The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].

6.1.2.7 FDP_IFF.1/Pri Simple security attributes

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/Pri

The TSF shall enforce the [assignment: *private letter information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *Subjects:< the process of the TOE importing the ephemeral public key for private letter from the external terminal and exporting a shared secret for the private letter to the external terminal>, Information:<the ephemeral public key for the private letter and shared secret for the private letter >, The security attributes for subjects: <performing the secure messaging and PIN verification succeed >*].

FDP_IFF.1.2/Pri

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *If the process of the TOE importing the ephemeral public key for the private letter from the external terminal succeeds in verifying PIN and performing secure messaging, importing the ephemeral public key for the private letter to the subject and exporting the shared secret for the private key from the subject will be permitted*].

FDP_IFF.1.3/Pri

The TSF shall enforce the [assignment: *none*].

FDP_IFF.1.4/Pri

The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *none*].

FDP_IFF.1.5/Pri

The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].

6.1.2.8 FDP_ITC.1/PubKey Import of user data without security attributes (a public key for External Authentication and a public key for key agreement)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/PubKey

The TSF shall enforce the [assignment: *cryptographic key import information flow control SFP*] when importing user data ***(a public key for External Authentication and a public key for key agreement)***, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/PubKey

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

FDP_ITC.1.3/PubKey

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

6.1.2.9 FDP_ITC.1/Pri Import of user data without security attributes (a public key for private letter)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/Pri

The TSF shall enforce the [assignment: *private letter information flow control SFP*] when importing user data ***(a public key for the private letter)***, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Pri

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

FDP_ITC.1.3/Pri

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

6.1.2.10 FDP_ITC.1/UData Import of user data without security attributes (except the public key for External Authentication, the public key for key agreement and the public key for private letter)

Component relationships

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1/UData

The TSF shall enforce the [assignment: *cryptographic key import information flow control SFP*] when importing user data ***(except the public key for External Authentication, the public key for key agreement and the public key for the private letter)***, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/UData

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

FDP_ITC.1.3/UData

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

6.1.3 Class FIA: Identification and authentication

6.1.3.1 FIA_AFL.1 Authentication failures

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when [assignment: *positive integer number in Table 6-3*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events in Table 6-3*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [selection *met*], the TSF shall [assignment: *list of actions in Table 6-3*].

Table 6-3 Action when authentication failures

List of authentication failures	Number	List of actions
Password verification for signing[5]	*5*	*Lock of the password for signing* *Unlock of the password for signing by successful external authentication of the Auth AP*
PIN verification	*3*	*Lock of the PIN* *Unlock of the PIN by successful PUK verification or external authentication of the Auth AP*
PUK verification	*10*	*Lock of the PUK* *Unlock of the PUK by successful password for signing verification or external authentication of the Auth AP*
Transport key verification	*3*	*Lock of the Transport key*
[assignment：list of authentication events]	*[assignment：positive integer number]*	*[assignment：list of actions]*

6.1.3.2 FIA_API.1 Authentication proof of identity

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1

The TSF shall provide an [assignment: *mutual authentication protocol based on SCP11a by the platform, internal authentication protocol based on SCP11b by the Auth PP and the Kenmen AP*] to prove the identity of [assignment: *the platform, the Auth AP, the Kenmen AP*] by including the following properties [assignment: *the public key certificate for key agreement of SCP11a in the platform, the public key certificate for key agreement of SCP11b in the Auth AP, the public key certificate for key agreement of SCP11b in the Kenmen AP*] to an external entity.

6.1.3.3 FIA_SOS.2 TSF Generation of secrets

Component relationships

Hierarchical to: No other components.

[5] The password for signing consists of alphabetic and numerical characters, and the PIN and PUK consist of numerical characters only.

Dependencies: No dependencies.

FIA_SOS.2.1

The TSF shall provide a mechanism to generate ***nonce*** ~~secrets~~ that meet [assignment: *[FIPS186_5] [selection: A.3.1, A.3.2, A.3.3]*].

FIA_SOS.2.2

The TSF shall be able to enforce the use of TSF generated ***nonce*** ~~secrets~~ for [assignment: *signature generation*].

[Application note: FIA_SOS.2] TOE generates nonce according to the per-message secret described in [FIPS186_5] A.3. The ST author shall describe the generation method used in FCS_RNG.1/DRBG. However, if the TOE selects [FIPS186_5] A.3.3 and does not use HMAC_DRBG but uses the generation algorithm described in A.3.3, the ST author shall fill in "Nonce required in relation to ECDSA signature generation" in the assignment of FCS_COP.1/Hash.

6.1.3.4 FIA_UAU.1 Timing of authentication

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1

The TSF shall allow [assignment: *list of TSF mediated actions shown in Table 6-4*] on behalf of the user to be performed before the user is authenticated.

Table 6-4 List of TSF mediated actions

AP	Authentication mechanism
All of APs	*Select the ISD, SSDs, APs*
Platform	*Read the file of the public key certificate for key agreement of SCP11a*
	Verify the public key certificate which inputted by the external terminal by the public key of the signatory which stored in the TOE
	[assignment: list of TSF mediated actions that do not conflict the Personal Number Cards access control SFP and the cryptographic key import information flow control SFP, and that do not access to TSF data.]
Auth AP	*Read the file of the public key certificate for key agreement of SCP11b*
	Read the file of the public key certificate for internal authenticate
	Begin SCP11b
	Transmit a challenge
	[assignment: list of TSF mediated actions that do not conflict the Personal Number Cards access control SFP, private letter information flow control SFP and the cryptographic key import information flow control SFP, and that do not access to TSF data.]
JPKI-AP	*Read the file of certificate for user attestation*
	[assignment: list of TSF mediated actions that do not conflict the Personal Number Cards access control SFP and that do not access to TSF data.]
Kenmen AP	*Read the file of the public key certificate for key agreement of SCP11b*

AP	Authentication mechanism
	Begin SCP11b
	Transmit a challenge
	[assignment: list of TSF mediated actions that do not conflict the Personal Number Cards access control SFP and the cryptographic key import information flow control SFP, and that do not access to TSF data.]
[assignment: list of AP]	*[assignment: list of TSF mediated actions that do not conflict the Personal Number Cards access control SFP and the cryptographic key import information flow control SFP, and that do not access to TSF data.]*

FIA_UAU.1.2

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

6.1.3.5 FIA_UAU.4 Single-use authentication mechanisms

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to [assignment: *the authentication mechanism shown in Table 6-5*].

Table 6-5 Authentication mechanism to prevent reuse of authentication data

Entity	Authentication mechanism	Authentication data
Platform, Auth AP, JUKI AP, JPKI-AP, Data AP, Kenmen AP	*External authentication*	*Challenge in external authentication*

6.1.3.6 FIA_UAU.5 Multiple authentication mechanisms

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1

The TSF shall provide [assignment: *list of multiple authentication mechanisms shown in Table 6-6*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [assignment: *methods providing authentication shown in Table 6-6*].

Table 6-6 Multiple authentication mechanism

Authentication mechanism	APs that require authentication	Methods of authentication
Password verification for signing	*Auth AP* *JPKI-AP* *Data AP*	*Authentication is successful when a password entered by the cardholder matches the password for signing stored in the Auth AP.*
PIN verification	*Auth AP* *JPKI-AP* *JUKI AP* *Data AP*	*Authentication is successful when a PIN entered by the cardholder matches the PIN stored in the Auth AP.*
PUK verification	*Auth AP*	*Authentication is successful when a PUK entered by the cardholder matches the PUK stored in the Auth AP.*
Transport key verification	*Platform*	*Authentication is successful when a key entered by the platform administrator matches the transport key stored in the platform.*
	Auth AP *JPKI-AP* *JUKI AP* *Data AP*	*Authentication is successful when a key entered by administrators of APs shown left column matches the transport key stored in the Auth AP.*
	Kenmen AP	*Authentication is successful when a key entered by the Kenmen AP administrator matches the transport key stored in the Kenmen AP.*
External authentication	*Platform*	*Authentication is successful when the public key certificate input by the external device* is verified using the public key stored in the platform and the verification is successful.*
	Auth AP *JPKI-AP* *JUKI AP* *Data AP* *Kenmen AP*	*When the public key certificate input by the external device is verified using the public key stored in each of the APs listed on the left and the verification is successful, the public key contained in the certificate is temporarily saved.* *The TOE sends a challenge to the external device in response to the external device's challenge request. The external device signs the challenge with the private key corresponding to the temporary public key.* *When the external device sends a signature to the TOE, the TOE verifies the signature with the temporary public key, and if it is successful, authentication is successful.*
[assignment: list of authentication mechanism]	*[assignment: list of APs that authenticate]*	*[assignment: list of methods of authenticate]*

* The external device corresponds to the process that acts on the subject in Table 6-2.

6.1.3.7 FIA_UID.1 Timing of identification

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1

The TSF shall allow [assignment: *list of TSF-mediated actions shown in Table 6-4*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

6.1.4 Class FMT: Security management

6.1.4.1 FMT_LIM.1 Limited capabilities

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1

The TSF shall limit its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: *After locking[6] the transport key during personalisation and subsequently prohibiting the successful unlocking of the transport key and authentication of the transport key.*]

[Application note: FMT_LIM.1] Together with FMT_LIM.2, it prevents exposure and modification of TSF data by prohibiting successful transport key authentication.

6.1.4.2 FMT_LIM.2 Limited availability

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1

The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Locking the transport key during personalisation and subsequently prohibiting the successful unlocking of the transport key and authentication of the transport key.*]

6.1.4.3 FMT_MSA.3 Static attribute initialisation

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [assignment: *Personal Number Cards access control SFP*] to provide [selection, choose one of: *restrictive~~, permissive, [assignment: other property]~~*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

[6] There are two ways to block: locking the transport key and stopping the transport key authentication command APDU.

The TSF shall allow the [assignment: *administrator of objects (administrator of platform, administrator of free space)*] to specify alternative initial values to override the default values when ***objects (non-TOE AP, SSD)*** ~~an object *or information*~~ *is* created.

[Application note: FMT_MSA.3] The default property of security attributes on creation of objects (non-TOE AP, SSDs) is provided by FMT_MSA.3.1. Because the platform and the basic APs are created in the development environment, they are not the subjects of this SFR.

The security attributes of those objects will not be changed after creation (however, deletion or re-creation of those objects may be possible). Therefore, FMT_MSA.1, that is the management requirement for security attribute in operational environment, is not applied.

The administrators of those objects have the privilege to initialize the security attributes, and the mechanism to realize the requirement (for the element FMT_MSA.3.2) depends on an implementation method. For example, if an AP is re-created after deletion, being accompanied by a collective change of the security attributes, this requirement will be satisfied.

6.1.4.4 FMT_MTD.1 Management of TSF data

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: ~~*change_default, query,* modify~~*,* ~~*delete, clear, [assignment: other operations]*~~] the [assignment: *list of TSF data shown in Table 6-7*] to [assignment: *the administrators shown in Table 6-7*].

Table 6-7 TSF data to be managed

Applied to:	TSF data	Administrator of TSF data
Auth AP	*PIN*	*the cardholder* *administrator of the Auth AP* *the system handling data of the Auth AP*[7]
	password for signing	
	PUK	
Kenmen AP	*[assignment: list of TSF data]*	*administrator of the Kenmen AP* *The system handling the digitized image data of the whole printed information*

6.1.4.5 FMT_SMF.1 Specification of Management Functions

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [assignment: *management functions shown in Table 6-8]*.

[7] Systems handling authentication information have the authority to change PINs. The changed PIN is notified to the cardholder.

Table 6-8 Management functions

Applied to:	Management function
Auth AP	*Unlock and modify the password for signing, unlock and modify the PIN, unlock and modify the PUK*
Kenmen AP	*[assignment: list of management functions]*

6.1.4.6 FMT_SMR.1 Security roles

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [assignment: *the roles shown in Table 6-9 for the platform and the APs each*].

Table 6-9 Security roles

Applied to:	Role
The platform	*Administrator of the platform, Administrator of free space*
Auth AP	*Cardholder, Administrator of the Auth AP*、*The system handling data of the Auth AP*
Kenmen AP	*Administrator of the Data AP*、*The system handling the digitized image data of the whole printed information*

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 FPT_PHP.3 Resistance to physical attack

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1

The TSF shall resist [assignment: *attacks with physical means and included in the IC evaluation method provided by the latest [JILAP]*] to the [assignment: *all hardware components that implement the TSF*] by responding automatically such that the SFRs are always enforced.

[**Application note: FPT_PHP.3]** The latest [JILAP] at the time of evaluation shall be applied.

6.1.6 Class FTP: Trusted path/channels

6.1.6.1 FTP_ITC.1 Inter-TSF trusted channel

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

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

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [assignment: *data transfer that encryption/decryption and MAC generation/verification are applied to, as shown in Table 6-10]*.

Table 6-10 Application methods of secure messaging

Applied to:	Encryption/decryption	MAC generation/verification
The platform	*applicable*	*applicable*
Auth AP *JUKI AP* *JPKI-AP* *Data AP* *Kenmen AP*	*applicable when the secure messaging attribute is assigned to the access target.*	*applicable when the secure messaging attribute is assigned to the access target.*

6.2 Security assurance requirements

The security assurance requirements applicable to the TOE are ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2 +, ALC_LCD.1, ALC_TAT.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.5.

6.3 Security requirements rationale

6.3.1 Security functional requirements rational

The tracing between the security objectives and the SFRs is shown in Table 6-11.

Table 6-11 Tracing between the security objectives and the SFRs

Security objectives / SFR	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND
FCS_CKM.1				X		X	
FCS_CKM.2				X		X	
FCS_CKM.5				X		X	

Security objectives / SFR	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND
FCS_CKM.6				X		X	
FCS_COP.1/ED				X		X	
FCS_COP.1/MAC				X		X	
FCS_COP.1/KeyDec						X	
FCS_COP.1/Receipt						X	
FCS_COP.1/SigGen						X	
FCS_COP.1/PersoAuth						X	
FCS_COP.1/TOEAuth						X	
FCS_COP.1/ExtAuth	X					X	
FCS_COP.1/Hash	X					X	
FCS_COP.1/Shses						X	
FCS_RNG.1/ES				X			X
FCS_RNG.1/DRBG				X		X	
FDP_ACC.1		X		X		X	
FDP_ACF.1		X		X		X	
FDP_ETC.1						X	
FDP_IFC.1/PubKey	X			X		X	
FDP_IFC.1/Pri						X	
FDP_IFF.1/PubKey	X			X		X	
FDP_IFF.1/Pri						X	
FDP_ITC.1/PubKey	X			X		X	
FDP_ITC.1/Pri						X	
FDP_ITC.1/UData		X		X		X	
FIA_AFL.1	X						
FIA_API.1				X			
FIA_SOS.2						X	
FIA_UAU.1	X				X		
FIA_UAU.4	X						
FIA_UAU.5	X				X		
FIA_UID.1	X				X		
FMT_LIM.1					X		
FMT_LIM.2					X		
FMT_MSA.3		X					

Security objectives / SFR	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND
FMT_MTD.1	X						
FMT_SMF.1	X						
FMT_SMR.1	X	X					
FPT_PHP.3			X				X
FTP_ITC.1				X		X	

The rationale is shown for each security objective for the TOE being met by its associated SFRs. It is also demonstrated that every SFR is effective to satisfy the security objectives of the TOE.

O.I&A

FIA_UAU.1 and FIA_UID.1 describe the requirements of services for the authorized users. Multiple authentication mechanisms applied are provided by FIA_UIA.5. For External Authentication based on public key cryptosystem, FCS_COP.1/ExtAuth ECDSA signature verification operation and FCS_COP.1/Hash message digest computation are applied. Importing of public keys for external authentication and public keys for key agreement used for public key cryptographic operations is specified in FDP_ITC.1/PubKey, FDP_IFC.1/PubKey and FDP_IFF.1/PubKey. Furthermore, FIA_UAU.4 is applied to describe prohibition of reuse of the same authentication data to prevent authentication with illegal means. FIA_AFL.1 describes the TSF action for authentication failures for each authentication mechanism. The administrative requirements for authentication data of the TOE users are provided by FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1. These SFRs achieve O.I&A sufficiently.

O.Access_Control

Security objective O.Access_Control requires that only the legitimate users are allowed to access user data within their own privileges. This requirement is provided by FDP_ACC.1/FDP_ACF.1. FMT_MSA.3 is applied to manage the security attributes used by FDP_ACF.1. FMT_MSA.3 relates only to creation of SSDs and non-TOE AP. The other objects are not managed by FMT_MSA.3, because they are created in the development environment. FMT_SMR.1 is used to specify administrator roles relating to FMT_MSA.3. The TOE imports cryptographic keys and user data from outside. The cryptographic keys imported are access-controlled as user data. This requirement is addressed by FDP_ITC.1/UData. These SFRs achieve O.Access_Control sufficiently.

O.Secure_messaging

Secure messaging is applicable when the secure messaging attribute is assigned to the access target by FTP_ITC.1. In SCP 11a, the ephemeral key pair is generated by FCS_CKM.1, FCS_RNG.1/ES and FCS_RNG.1/DRBG, and the ephemeral public key is sent to the external terminal by FCS_CKM.2. The session key is derived by FCS_CKM.5 from the generated ephemeral private key, the ephemeral public key received from the external terminal, the public key extracted from the certificate received from the external terminal, and the private key for key agreement corresponding to the public key certificate for

key agreement to be sent to the external terminal. In SCP11b, the ephemeral key pair is generated by FCS_CKM.1 FCS_RNG.1/ES and FCS_RNG.1/DRBG, and the ephemeral public key is sent to the external terminal by FCS_CKM.2. The session key is derived by FCS_CKM.5 from the generated ephemeral private key, the ephemeral public key received from the external terminal, and the private key for key agreement corresponding to the public key certificate for key agreement to be sent to the external terminal.

Confidentiality and integrity of session data are protected by secure messaging using AES encryption/MAC. The session key (AES) is derived from the ephemeral keys exchanged with the external terminal, the public key extracted from the certificate received from the external terminal and the private key for key agreement stored in the TOE. Importing of the public key for external authentication and the public key for key agreement used for key derivation is specified in FDP_ITC.1/PubKey, FDP_IFC.1/PubKey and FDP_IFF.1/PubKey. Providing of the public key certificate for key agreement and the public key certificate for internal authentication to external terminals is specified in FDP_ACC.1, FDP_ACF.1, FIA_API.1. Destruction of the ephemeral secret keys is provided by FCS_CKM.6. AES cryptographic operations are specified in FCS_COP.1/ED and FCS_COP.1/MAC. The destruction of the session key used for secure messaging is specified in FCS_CKM.6. The import of the public key certificates for key agreement and the private keys for key agreement used in public key schemes is specified in FDP_ITC.1/UData, FDP_ACC.1 and FDP_ACF.1. The requirements for secure messaging itself (protection of communication channel data) are specified in FTP_ITC.1. These SFRs achieve O.Secure_messaging sufficiently.

O.Delivery

"Protection of internal data of the card by secret information" required by the security objective O.Delivery is achieved with the SFRs that require authentication function using transport keys as passwords. Identification is needed for authentication. The requests of identification and authentication are provided by FIA_UAU.1/FIA_UID.1. Each authentication mechanism is provided by FIA_UAU.5. FMT_LIM.1 and FMT_LIM.2 are specified to disable the access function after successful authentication by the transport key. These SFRs achieve O.Delivery sufficiently.

O.Cryptography

Cryptographic algorithms, cryptographic operations and cryptographic key management (key generation and key derivation) required in O.Cryptography are specified in Table 4-1. The cryptographic algorithms and cryptographic operations are specified in FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_COP.1/ED, FCS_COP.1/MAC, FCS_COP.1/Receipt, FCS_COP.1/SigGen, FCS_COP.1/PersoAuth, FCS_COP./1/TOEAuth, FCS_COP.1/ExtAuth, and FCS_COP.1/Hash. The generation of nonce in signature generation is specified in FIA_SOS.2 and FCS_RNG.1/DRBG. Requirements to import cryptographic keys are provided by FDP_ITC.1/PubKey、FDP_ITC.1/UData. FCS_COP.1/KeyDec, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1/PubKey, FDP_IFF.1/PubKey are also used for secure import of those keys. Protection of communication channels used to import cryptographic keys is provided by FTP_ITC.1. Requirement of destruction for unnecessary cryptographic keys is provided by FCS_CKM.6. Regarding private letter, the generation of shared secret is specified in FCS_COP.1/ShSes, and the reading of public key certificates for the private letter is specified in FDP_ACC.1 and FDP_ACF.1. The import of the ephemeral public key for the private letter is specified in FDP_IFC.1/Pri, FDP_IFF.1/Pri, and FDP_ITC.1/Pri, and the export of the shared secret for the private letter is specified in FDP_ETC.1. These SFRs achieve O.Cryptography sufficiently.

O.Phys_Attack

O.Phys_Attack requires countermeasures against security violation of data and functions of the TOE with physical attacks. FPT_PHP.3 requires resistance to physical attacks to the TSF. Therefore, if this SFR is met, O.Phys_Attack will be achieved sufficiently.

O.RND

The security objective O.RND requires countermeasures that the random number to be generated has sufficient quality and makes it difficult to be guessed by an attacker. FCS_RNG.1/ES requires generation of random numbers satisfying a quality metric needed. Furthermore, FPT_PHP.3 counters the physical attack to guess output of the RNG. These SFRs achieve O.RND sufficiently.

6.3.1.1 Dependencies of security functional requirements

Dependencies provided in each SFR and the dispositions are shown in Table 6-12.

Table 6-12 Dependencies of SFR

SFR	Dependencies	Satisfaction of dependencies
FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1], [FCS_RBG.1 or FCS_RNG.1], FCS_CKM.6	FCS_CKM.2, FCS_CKM.5, FCS_RNG.1/ES, FCS_RNG.1/DRBG, FCS_CKM.6
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.1
FCS_CKM.5	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.6	FCS_COP.1/ED, FCS_COP.1/MAC, FCS_COP.1/Receipt, FCS_CKM.6, Note 1
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, or FCS_CKM.5]	FCS_CKM.1, FCS_CKM.5
FCS_COP.1/ED	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5], FCS_CKM.6	FCS_CKM.5, FCS_CKM.6
FCS_COP.1/MAC		
FCS_COP.1.1/Receipt		
FCS_COP.1/KeyDec		FDP_ITC.1/UData, Note 2
FCS_COP.1/SigGen		
FCS_COP.1/PersoAuth		
FCS_COP.1/ExtAuth		FDP_ITC.1/PubKey, Note 3
FCS_COP.1/Hash		Note 4
FCS_COP.1/ShSes		FDP_ITC.1/Pri, FDP_ITC.1/UData, Note 2, Note 3
FCS_RNG.1/ES	None	NA
FCS_RNG.1/DRBG	None	NA
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, Note 5
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/Pri
FDP_IFC.1/PubKey	FDP_IFF.1	FDP_IFF.1/PubKey
FDP_IFC.1/Pri		FDP_IFF.1/Pri

SFR	Dependencies	Satisfaction of dependencies
FDP_IFF.1/PubKey	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1/PubKey, Note 6
FDP_IFF.1/Pri		FDP_IFC.1/Pri, Note 6
FDP_ITC.1/PubKey	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	FDP_IFC.1/PubKey, Note 6
FDP_ITC.1/Pri		FDP_IFC.1/Pri, Note 6
FDP_ITC.1/UData		FDP_ACC.1, Note 7
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_API.1	None	NA
FIA_SOS.2	None	NA
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	None	NA
FIA_UAU.5	None	NA
FIA_UID.1	None	NA
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_SMR.1, Note 8
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	None	NA
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_PHP.3	None	NA
FTP_ITC.1	None	NA

Note 1: For FCS_COP.1/KeyDec, FCS_COP.1/SigGen, FCS_COP.1/PersoAuth, FCS_COP.1/TOEAuth and FCS_COP.1/ExtAuth, no dependency from FCS_CKM.5 is required because the cryptographic keys for these SFRs are written before the TOE is issued.

Note 2: Due to OE.Card, Keys written to the TOE by FDP_ITC.1/UData are properly disposed of after the expiration of personal number cards or when it is returned at the request of the cardholder.

Note 3: Cryptographic keys imported by FDP_ITC.1/PubKey and FDP_ITC.1/Pri are not destructed due to public keys.

Note 4: No cryptographic keys are used, so the required dependencies are not necessary.

Note 5: For non-TOE AP and SSDs, FMT_MSA.3 is applied, and all objects except for basic APs are created in the development environment. The dependency is satisfied.

Note 6: Public keys for external authentication and the ephemeral public key for the private letter are used temporarily and therefore do not require a dependent SFR.

Note 7: file has already been set up in the development environment and no dependencies need to be fulfilled.

Note 8: The objects managed by FMT_MSA.3 are non-TOE AP and SSDs. Their security attributes are not changed once after having been set. Accordingly, Therefore, there is no need to fulfill dependencies.

6.3.2 Security assurance requirements rationale

The security functionality of the TOE will be implemented with three means, security functionality of software, hardware (IC chip) or combination thereof.

Most of security functionalities required for the TOE may be implemented with software security mechanisms. The main objective of software security mechanisms is protection of the primary assets such as personal information (e.g. the personal number) and Public ID authentication service. These assets should be credible from the point of view for social information infrastructure. Therefore, sufficient security evaluation is needed and EAL4 the highest level for COTS is appropriate for the evaluation assurance level.

On the other hand, the TOE includes security functionality based on the hardware of the IC card. As the attack methods exploiting vulnerabilities of the IC card have been highly developed, sufficient security cannot be assured without the assumption of high-level attacks. That is, the TOE shall counter the attack potential of high, including physical attacks. Accordingly, AVA_VAN.5 is added to the assurance requirements for appropriate evaluation of vulnerabilities. Namely, for both software and the hardware of the TOE, it is defined as the assurance requirements relating to vulnerabilities to counter high level attacks.

All files of the TOE except for any APs based on ordinances of local governments are created in the development environment (production environment). Some cryptographic keys and authentication data are set in the environment as well. High level confidentiality and integrity for those data are required. Sufficient development security shall be assured for them together with the development environment for the hardware. Therefore, ALC_DVS.2 was added for development environment.

Dependencies derived from AVA_VAN.5, that is an augmented assurance requirement, are identical to those for the AVA_VAN.3 (for EAL4). ALC_DVS.2 does not depend on other assurance requirements. Therefore, the dependencies of the assurance requirements are identical to EAL4 assurance package, and all dependencies among each assurance component are satisfied.

7 References

[CC] Common Criteria for Information Technology Security Evaluation CC:2022 Revision1
Part 1: Introduction and general model CCMB-2022-11-001
Part 2: Security functional components CCMB-2022-11-002
Part 3: Security assurance components CCMB-2022-11-003
Part 4: Framework for the specification of evaluation methods and activities CCMB-2022-11-004
Part 5: Pre-defined packages of security requirements CCMB-2022-11-005

[CEM] Common Methodology for Information Technology Security Evaluation CEM:2022 Revision1 CCMB-2022-11-006

[ERT] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Unique identifier: 002, Version: 1.1, Date of issue: 2024-07-22

[FIPS180_4] FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), August 2015

[FIPS186_5] FIPS PUB 186-5, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Digital Signature Standard (DSS), Published: February 3, 2023

[FIPS197] FIPS 197 Federal Information Processing Standards Publication Advanced Encryption Standard (AES), Published November 26, 2001; Updated May 9, 2023

[GPC093] GlobalPlatform Technology Secure Channel Protocol '11' Card Specification v2.3 - Amendment F, Version 1.2, Public Release July 2018

[ISOIEC9797_1] ISO/IEC 9797-1:2011, Information technology - Security techniques - Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, Edition 2, 2011

[ISOIEC10116] ISO/IEC 10116:2017, Information technology - Security techniques - Modes of operation for an n-bit block cipher, Edition 4, 2017

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

[KS2011] A proposal for: Functionality classes for random number generators Version 2.0 18 September 2011

[SP800_90A] NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[TR03111] Technical Guideline BSI TR-03111, Elliptic Curve Cryptography, Version 2.10, Date: 2018-06-01

[X9.63] ANSI X9.63. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011

End of document