Personal Number Cards Protection Profile

Version 1.00

24-4-2014

J-LIS

Japan Agency for Local Authority Information Systems

JISEC C0431

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

Preliminary notice

The background of this protection profile “Personal Number Cards Protection Profile” is explained here. Development of the card conforming to this PP is also mentioned.

Security requirements for Personal Number Cards

This PP provides the security requirements for Personal Number Cards. Personal Number Cards must 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 Card is the IC card equipped with both an IC module interface and a contactless interface. The entire IC card, including hardware and software, is subject to CC evaluation.

Composite evaluation is applicable. When the hardware part of the IC 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 IC 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 IC card, whether composite evaluation is applied or not.

This PP requires demonstrable conformance for the ST claiming conformance to. The ST must 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.

Security requirements for the hardware

The TOE type of this PP is IC card (smartcard) including embedded software. Security requirements for the hardware of the TOEs of this category are almost the same. Though this PP does not claim conformance to any PPs, BSI-PP-0035 “Security IC Platform Protection Profile, v1.0, 15.06.2007” is referred partially to provide security requirements for the hardware. Many STs/PPs in the field of smartcard have claimed conformance to BSI-PP-0035. As the security requirements for hardware part of this PP is a subset of the requirements provided by BSI-PP-

0035, any TOEs conforming to BSI-PP-0035 satisfy the requirements for the hardware part of this PP.

JIWG supporting documents are applied to evaluation of IC card TOEs. Those documents address attacks specific to IC cards, mainly physical attacks, and complement CC and CEM. “Physical attacks” are attacks against on hardware of an IC card. The hardware is a part of the TSF, so that those attacks to the TSF are considered in the evaluation from the aspect of vulnerabilities, even if they are not indicated clearly in the threats nor organisational security policies of the ST. JIWG supporting documents are revised independently of the version of CC/CEM. The evaluation of the TOE conforming to this PP will be done based on the newest version of those documents.

Composite evaluation

On the evaluation of Personal Number Card 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 defined by JIWG supporting documents. Results of evaluation and certification are valid in every scheme participating in CCRA.

Composite evaluation is executed as follows:

Security requirements for the IC 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 IC 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 analyzing power consumption during cryptographic operation.

Extreme care should be taken when the schemes for hardware evaluation and composite evaluation are independent. The result of hardware evaluation must be available for the composite product certification body. In order to achieve this, coordination is required in advance between all stakeholders.

Contents

1 PP introduction

1.1 PP reference

Title:	Personal Number Cards Protection Profile
Version number:	1.00
Publication date:	24-4-2014
Sponsor:	J-LIS (Japan Agency for Local Authority Information Systems)
Certification ID:	C0431
Key words:	IC card, Smartcard, Basic Resident Registration, Basic Resident Registration Network System, Personal Number Card, Basic Resident Registration Card, Public ID authentication, JPKI, Input Support for the personal information printed on the card, Digitization of the personal information printed on the card, APs based on ordinances of local governments

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 and major security features

The TOE is the IC 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 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). 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.

Four kinds of APs run on the platform according to a use. Those four APs are “Input Support AP for the personal information printed on the card”, “Basic Resident Registration AP”, “public ID authentication AP” and “AP for digitization of the personal information printed on the card”. 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 local governments (of municipalities) issuing Personal Number Cards may create APs based on ordinances of the local government. Any APs based on ordinances of local governments are created in SSD(s) and distinguished from the basic APs.

Overview of usage of the basic APs are shown below. Detailed explanation is provided in the next section (2).

- Input Support AP for the personal information printed on the card

  It stores the personal number and the four data (name, address, date of birth and gender) of the card holder and provides them to users. Examples of users are the entities that use personal numbers in business and the entities that require authentication of the card holder.

- Basic Resident Registration AP

  It provides the identical functionality as Basic Resident Registration Card for Basic Resident Registration Network System.

- Public ID authentication AP

  It issues “certificate for digital signature” used for electronic application, or “electronic certificate (certificate for user certification)” used for electronic authentication of the card holder.

- AP for digitization of the personal information printed on the card

  It provides the data corresponding to the printed information on the card surface, the four data (name, address, date of birth and gender), personal number, photographic portrait and expiration date.

The construction of the TOE is explained as follows. An example of the internal construction of the TOE is shown in Fig 1-1. The purpose of this figure is to present the major components of the TOE for understanding the behavior of the TOE. It does not intend to specify nor limit the implementation of the TOE.

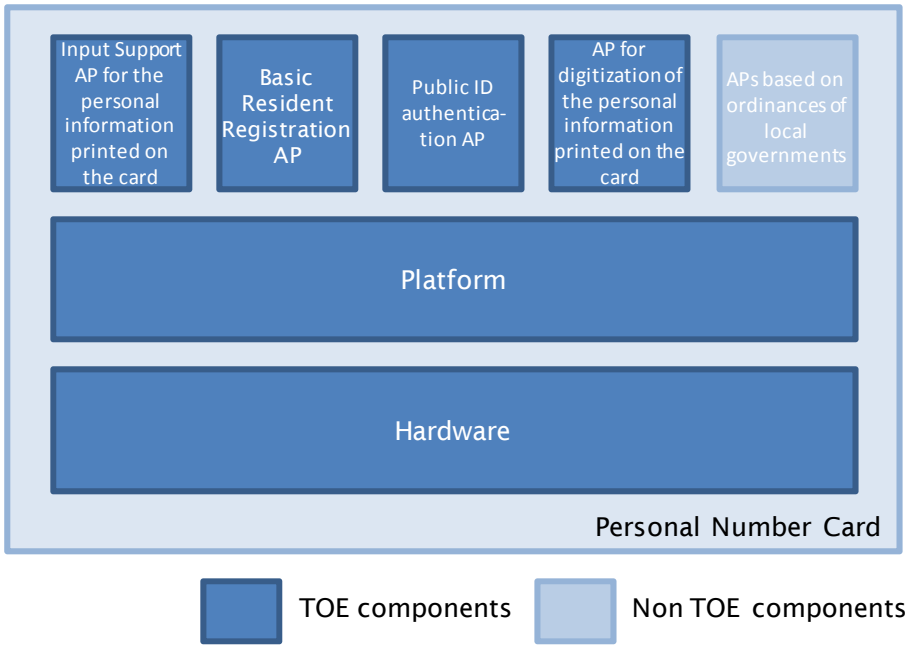

Fig 1-1 Construction of the TOE

The software of the TOE consists of the platform and the four 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 APs based on ordinances of local governments” are optional by local governments and not included in the components of the TOE.

(2) Services provided by the basic APs

Personal Number Cards are issued to residents via local governments. The four basic APs provide services described below. Some of the services can be used in the context of business of private companies, in addition to the context of local government's administrative services. In principle, user authentication is required before using any services. However, some specific data can be read out without user authentication.

[Input Support AP for the personal information printed on the card]

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

[Basic Resident Registration AP]

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

[Public ID authentication AP]

This is the application providing public ID authentication services for individuals. It is used to sign "certificate for digital signature" for electronic application, or "certificate for user certification" for electronic authentication of the card holder. It stores the public key pair and the certificates in the TOE for each use above. It executes cryptographic operation for generating electronic signature in the card.

[AP for digitization of the personal information printed on the card]

This is the application which provides digitization of the personal information printed on the card. The printed information includes the four data, the personal number, the photographic portrait and the expiration date. The digitized image data of the whole printed information is stored in a file of the card. Furthermore, digitized image data of the personal number is stored in another file. When the alteration of the printed information was doubted, it is verified by comparing with those stored data displayed on a terminal. The date of the birth, which is stored as text data, is used for age verification of the card holder. The stored data are not confidential, because they are identical with the printed information on the card. However, to prevent the data

being read out without recognition of the card holder, the TOE requires a password on readout of the data.

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 four 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.

In this chapter, the security features of the TOE as a whole are described. 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 also counters the attacks to the hardware itself.

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. For the communication which needs protection from eavesdropping or modification, the TOE applies “secure messaging” function in order to protect confidentiality and/or integrity of communication data by means of encryption/decryption and/or generation/verification of MAC (Message Authentication Code).

(2) User authentication and access control

The TOE performs user authentication and 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. Examples are; 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 local governments (optional and out of the TOE) 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 arithmetic function of the TOE). The TOE authenticates a 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. Human users refer to card holders, administrators[1] or business operators who use data of the card. 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 an external terminal by the TOE (IC card) is referred to as External Authentication[2] 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), in order to examine that the TOE is not forged. 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 certification for the public ID authentication AP and so on.

(4) Counters physical attacks

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

---

1 "Administrator" refers to the person who is the personnel of the IC card issuers (J-LIS and local governments) and is authorized to administrate the security functionality of the TOE. He/she performs setting data, creating APs based on ordinances of local governments to the card, and also updating data for issued cards.

2 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.

in terms of evaluation of vulnerability analysis, regardless of the threats described in this PP. Evaluation of IC chips for vulnerability analysis is performed with the methodology shown in JIWG supporting documents.

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 an external terminal.

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

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 software/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. Any APs based on ordinances of local governments may be created at this phase. 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

Each Personal Number Card supplied to J-LIS is issued to the resident (card holder) via the relevant local government. Administrators of the local government or of J-LIS write necessary data including information specific to the card holder 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 local governments by the local government

The local government issuing Personal Number Cards may add own APs based on ordinances of the local government. They are optional by the local government and not necessarily created.

(6) Use of Personal Number Cards by card holders

The resident to whom the Personal Number Card is issued is referred to the card holder and uses the services of the card. Various organizations relating to services of Personal Number Cards other than card holders are also able to use services of Personal Number Cards. Examples of the organizations are local governments, government agencies or private companies admitted by laws.

2 Conformance claims

2.1 Conformance claims

This PP claims CC conformance as follows:

- CC conformance: CC Version 3.1 Revision 4 conformant *(The original Japanese version PP conforms to "CC V3.1 R4 translation version 1.0" by IPA)*

  Part 1: Introduction and general model: September 2012 Version 3.1 Revision 4 CCMB-2012-09-001 (Japanese language version; released by IPA, version number 1.0)

  Part 2: Security functional components: September 2012 Version 3.1 Revision 4 CCMB-2012-09-002 (Japanese language version; released by IPA, version number 1.0)

  Part 3: Security assurance components: September 2012 Version 3.1 Revision 4 CCMB-2012-09-003 (Japanese language version; released by IPA, version number 1.0)

- Part2 conformance: CC Part2 extended

  The extended security functional component is FCS_RNG.1 (defined in chapter 5).

- Part 3 conformance: CC Part3 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, organisational 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, organisational 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.

- Card holder — A person to whom Personal Number Card (TOE) is issued by the local government. The card holder uses service functions of the basic APs of the TOE or any APs based on ordinances of the local government (optional and out of the TOE). An external terminal at the local government or the PC owned by the card holder 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 any APs based on ordinances of local governments, data setting/modification for the platform/APs or releasing of blocked password. Administrators belong to J-LIS or each local government.
- Organizations — Various organizations relating to the services of the TOE use the TOE. Examples of organizations are local governments, government agencies or private companies which are admitted to use the services of the TOE

by laws. Organizations are shown as “the system handling xx” in this PP.

- External terminal The TOE exchanges data with external terminals (the IT devices external of the TOE) in operational environment of the TOE. The external terminals are installed at windows and so on of local governments. As there is a potential risk that an illegal terminal violates the assets of the TOE, the external terminal is identified and authenticated as one of the TOE users. On the other hand, some terminals are not required to be identified as users. Examples are, the PC owned by the card holder in the context of using Public ID authentication AP, or terminals for AP for digitization of the personal information printed on the card, used for readout of digitization of the personal information printed on the card and so forth by private companies. Those terminals do not correspond to “external terminal” described here.

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 card holders and is valuable for the card holders. An example of user data is card holder’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 card holder 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.

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 organisational 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 must counter them. The scope of physical attacks to be countered is shown specifically in the JIWG supporting documents. Evaluation of the TOE for physical attacks should be carried out according to the newest supporting documents at the point of the evaluation.

Any “APs based on ordinances of local governments” based on ordinances of municipalities may be created in the TOE. Any APs based on ordinances of local governments are services provided individually by each local government. They are not provided in this PP and the user data for them are not included in the assets of the TOE.

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 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.Replay

An attacker masquerades a legitimate external terminal by monitoring, recording and replaying the authentication procedure between the TOE and the external terminal in order to be authenticated by the TOE. The attack causes disclosure or modification of user data of the TOE, or illegal use of processing function of the TOE.

[Application note_T.Replay] This threat might be considered as a part of T.Illegal_Attack. However, it is defined here as an independent threat because it identifies a specific attack method.

T.Phys_Attack

An attacker attacks components of the TOE – hardware, firmware or software – with physical means. The attack causes disclosure or modification of user data of the TOE, or unauthorized use of processing function of the TOE. Examples of typical attack measures are as follows:

- Monitoring and analyzing variation of power consumption of the TOE during cryptographic operation to determine the cryptographic key used.
- Probing the inside of the TOE to disclose data.
- Disclosing or modifying data or using processing function of the TOE illegally by causing errors or malfunction of the TSF operation with glitches or environmental stresses during operation of the TOE.
- Disclosing or modifying data of the TOE or modifying behavior of the TOE by physically manipulating the inside of TOE.

3.4 Organisational security policies

The organisational security policies applied to the TOE and/or the operational environment of the TOE are described. “The organizations” refer to J-LIS and local governments. They take charge of administration and operation of Personal Number Cards.

P.Secure_messaging

Secure messaging shall be applied to the communication between the TOE and an external terminal indicated, as “applied” in Table 3-1. Applying secure messaging is not mandatory for the communication indicated as “applied or not applied” or “not applied”, as shown in the notes of the table.

Table 3-1 Application of secure messaging

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

*1 [applied or not applied] The TOE shall be equipped with the secure messaging function. The function will be used when an external terminal requests it.

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

P.Delivery

On shipment of Personal Number Cards from developers, the functionality to prevent illegal accesses to the TOE shall be activated. “Illegal accesses” refer to logical accesses to the inside of the TOE by unauthorized entities.

[Application note_P.Delivery] When the TOE is shipped from developers, a part of the security functionality of the TOE shall be enabled to protect the TOE from illegal accesses. The authentication data, called as “transport key” generally in IC cards, is stored in the TOE. Only the users who know the transport key can access the TOE. Even if an attacker steals the TOE in transport, he/she won’t be able to initialize nor use the TOE without the knowledge of the transport key. Transport key is effective not only in transport but also in safekeeping until issuing. “Initial key” and “issuer key” are the authentication data having the similar security property as “transport key”. The “transport key” in this PP is the general term for those keys.

P.Cryptography

The TOE provides the environment where cryptographic functions are available to the platform and the basic APs. The cryptographic functions are used for data protection, signature or authentication. Table 3-2 shows cryptographic algorithms, cryptographic operations, cryptographic key sizes, cryptographic key management policies (key generation/import and destruction) and purposes of cryptographic functions.

Table 3-2 Cryptographic function policies

Crypto-graphic algorithm /Standard	Cryptographic operation	Key size (bit)	Key genera-tion /import	Key dest-ruction	Purpose
AES-CBC mode /FIPS PUB 197, NIST SP 800-38A	Encryption /decryption	128	Import	Destruction methods are not provided in this PP	Secure messaging, private key decryption (at import)
CMAC with AES/FIPS PUB 197, NIST SP 800-38B	MAC generation /verification				Secure messaging

RSASSA-PKCS1-V1.5 /PKCS#1 v2.2	Signature verification with a public key	2048			External authentication
	Signature generation with a private key[*1]				Internal authentication, signature and user certification for Public ID authentication AP
RSA-OAEP /PKCS#1 v2.2	Decryption with a private key				Session key establishment for secure messaging, Secret key establishment[*2] for private key decryption
SHA-256/FIPS PUB 180-4	Hash operation	-	-	-	Used as a supporting technique for RSA cryptographic operation

[*1] For “Input Support AP for the personal information printed on the card”, “Public ID authentication AP” and “AP for digitization of the personal information printed on the card”, meanwhile encoding operation (including hash) specified in the standard is performed at an external device (external terminal), PKCS padding and signature generation with a private key are performed by the TOE. For “Public ID authentication AP”, the TOE also can add “organization code” to the padding. This padding does not conform to the standard.

[*2] Applied on the on-line update of a secret key for Public ID authentication AP.

P.RND

The TSF generates random numbers to be used for the TSF itself. The quality of random numbers is sufficient to prevent prediction by an attacker.

[Application note_P.RND] The quality of random numbers will depend on purposes. The quality should be defined with objective metric. An example of quality metric is a numerical value in the unit of entropy.

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

A person in charge of creating any APs based on ordinances of local governments is assumed to create APs developed by trusted developers with appropriate development methods, on the TOE.

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 and for the environment of the TOE are shown in 4.1 and 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 for the TOE

For the threats and the organisational security policies provided as the security problem definitions, the security objectives that the TOE enforces to solve those problems are shown as follows.

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. Users to be identified and authenticated and their privileges are shown in Table 4-1. 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.

Table 4-1 Users and privileges

Applied to:	User	Privilege
The platform	Administrator of the platform	Initialization/modification of data, Creation/deletion of SSD
	Administrator of any APs based on ordinances of local governments	Creation/deletion of any APs based on ordinances of local governments
Input Support AP for the personal information printed on the card AP	Administrator of Input Support AP for the personal information printed on the card	Initialization/modification of data
	Card holder	Readout of the personal number and the four data,

		Change of the card holder's own PW
	The system handling personal numbers and the four data	Readout of the personal number and the four data
Basic Resident Registration AP	Administrator of Basic Resident Registration AP	Initialization/modification of data
	Card holder	Readout of resident registration code, Change of the card holder's own PW
	The system handling the Basic Resident Registration data	Readout of resident registration code
Public ID authentication AP	Administrator of Public ID authentication AP	Initialization/modification of data
	Card holder	Use of the signature generation function/the user certification function, Change of the card holder's own PW
	The system handling certificate data	Use of the user certification function
AP for digitization of the personal information printed on the card	Administrator of AP for digitization of the personal information printed on the card	Initialization/modification of data
	Card holder	Readout of the digitized personal information printed on the card
	The system handling digitized personal information printed on the card	Readout of the digitized personal information printed on the card, Change of card holder's PW
	The system handling personal number	Readout of the personal number
	The system handling date of birth	Readout of the date of birth
Common to the platform and the basic APs	External terminal	Readout of the public key for session key encryption (except for AP for digitization of the personal information printed on the card), Readout of the public key for Internal Authentication

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 based on ordinances of local

governments, SSDs or processing functions in the TOE. Operations include input and output of user data, execution of processing functions or creation/deletion of objects.

Subjects, objects and operations of objects by subjects are controlled based on the access control rules of the TOE. The access control rules are shown in Table 4-2. When a user of the TOE is authenticated successfully, the subject on behalf of the user will be permitted to operate objects as shown in Table 4-2.

Table 4-2 Access control of the TOE

Applied to:	Subject (Associated User)	Object	Operation
The platform	Administrator of the platform	User data files*	read and/or write*
		SSD	create/delete
	Administrator of Any APs based on ordinances of local governments	any APs based on ordinances of local governments	create/delete
Input Support AP for the personal information printed on the card AP	Administrator of Input Support AP for the personal information printed on the card AP	User data files*	read and/or write*
	Card holder	The personal number file The four data file	read
	The system handling the personal number and the four data		
Basic Resident Registration AP	Administrator of Basic Resident Registration AP	User data files*	read and/or write*
	Card holder	Resident registration code file	read
	The system handling the Basic Resident Registration data		
Public ID authentication AP	Administrator of Public ID authentication AP	User data files*	read and/or write*
	Card holder	The signature generation function with the private key for signing The signature generation function with the private key for user certification	sign
	The system handling certificate data	The signature generation function with the private key for user certification	
AP for digitization of the personal information printed on the	Administrator of AP for digitization of the personal information printed on the card	User data files*	read and/or write*
	Card holder	The data file for digitized	read

card	The system handling digitized personal information printed on the card	personal information printed on the card	
	The system handling personal number	The data file for the personal number	
	The system handling date of birth	The data file for the date of birth	
Common to the platform and the basic APs	External terminal	The data files of public keys for session key encryption (except for AP for digitization of the personal information printed on the card) The data files of public keys for Internal Authentication	read

* Objects “user data files” and operations for the objects are not specified in this PP. The specification will be provided separately from the procurement authority.

O.Replay

For External Authentication by the TOE, the same authentication data must not be reused to prevent duplication and reuse of authentication data by an attacker.

O.Secure_messaging

The TOE shall apply secure messaging for communication with an external terminal according to Table 3-1. In the secure messaging, communication data shall be protected from disclosure/modification with encryption/decryption and/or generation/verification of MAC (Message Authentication Code) by applying the secret key cryptographic algorithm shown in Table 3-2.

Communication between the TOE and an external terminal consists of command (input) and response (output). The same type of secure messaging shall be applied to the both of command and response. The RSA cryptographic algorithm and the SHA function shown in Table 3-2 of P.Cryptography are used for mutual authentication with an external terminal on the session establishment procedures for the secure messaging. For establishment of session keys (a cryptographic key and a MAC key), the RSA cryptographic algorithm for “session key establishment for secure messaging” shown in Table 3-2 is used.

O.Delivery

Personal Number Cards shipped from developers 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 four basic APs individually.

O.Cryptography

The TOE shall provide cryptographic operational function and cryptographic key management function for the platform and the basic APs.

The cryptographic function applied to the platform and the basic APs shall enforce the policies shown in Table 3-2 of P.Cryptography. In Table 3-2, cryptographic algorithms, cryptographic operations, cryptographic key sizes, management of cryptographic keys (generation/import and destruction) and purposes required by the TOE are provided.

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/firmware/software).

The physical attacks to be countered by the TSF are shown in JIWG supporting documents.

[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 for the environment

For the threats, the organisational 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

Persons in charge of administration and operation of Personal Number Cards in the organizations relating to the issue of the cards 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

Persons responsible for the administration and operation of Personal Number Cards issuing organization appoint administrators who set up, 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 persons grant them the right to perform said duties. Furthermore, those persons select and introduce reliable IT devices.

OE.AP

Persons in charge of administration and operation of Personal Number Cards or administrators of the TOE in local governments of municipalities confirm that any APs based on ordinances of local governments have been developed by trusted developers with proper development methods so that unreliable APs are not introduced.

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 4-3. It shows that all security objectives trace back to one (or more) security problem definitions.

Table 4-3 Tracing between security problem definitions and security objectives

Security problem definitions \ Security objectives	O.I&A	O.Access_Control	O.Replay	O.Phys_Attack	O.Secure_messaging	O.Delivery	O.Cryptography	O.RND	OE.PKI	OE.Administrator	OE.AP
T.Illegal_Attack	x	x									
T.Replay			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

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 organisational security policies and uphold all assumptions.

T.Illegal_Attack

O.I&A provides that the TOE identifies and authenticates a 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.Replay

When an attacker monitors and records data of authentication procedures of an external terminal and makes an authentication attempt to the TOE by impersonating the external terminal, O.Replay will invalidate the authentication data which has been used once and reject the request of authentication. O.Replay removes the threat of impersonation by replaying the same authentication procedures shown in T.Replay.

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 JIWG supporting documents, therefore the threat T.Phys_Attack is diminished sufficiently.

P.Secure_messaging

O.Secure_messaging protects communication data between the TOE and an 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 four basic APs. Therefore, secure messaging is applied where necessary as shown in Table 3-1 of P.Secure_messaging. 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 objective is a secret data called as “transport key” for IC card. O.Delivery addresses P.Delivery by requiring authentication mechanism using 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 3-2 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 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 setting up, 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. Furthermore, it also indicates that reliable external terminals should be provided for use of administrators. 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.

5 Extended components definition

This PP defines an extended component not provided in CC part2 to describe an extended security functional requirement.

5.1 Extended security functional components

The extended component and the family to which it belongs are shown in 5.1.1. They belong to FCS class, an existing class of CC part2 (security functional component). They are created based on the family and component model of CC part2.

5.1.1 Definition of the Family FCS_RNG

Random number generation is one of cryptographic operations performed by the cryptographic function, which is a part of the TOE. Random numbers are used for key generation of secret key cryptography, secure key exchange, mutual authentication and so on. Generation of random numbers with sufficient entropy is needed to prevent being easily guessed by an attacker. As there was no component to provide a requirement for random number generation, an extended component about random number generation is defined. In this section, “FCS_RNG” family is defined first, and an extended component belonging to the family is defined. These extended family and component are quoted from the PP below:

“Security IC Platform Protection Profile” Version 1.0, 15.06.2007; BSI-PP-0035

Following is the reproduction of the definition in the PP above.

To define the security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG Generation of random numbers

Family Behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component leveling:

FCS_RNG: Generation of random numbers	1

FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

FCS_RNG.1 Random number generation

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

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

[Application note_EXT_FCS_RNG.1] A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

6 Security requirements

6.1 Security functional requirements

SFRs in this PP are defined using the components from CC part2. The SFRs are shown in the list of Table 6-1

Table 6-1 SFR list

Section	Identification	
6.1.1	FCS_CKM.4	Cryptographic key destruction
6.1.2	FCS_COP.1(1)	Cryptographic operation (AES)
6.1.3	FCS_COP.1(2)	Cryptographic operation (MAC)
6.1.4	FCS_COP.1(3)	Cryptographic operation (RSA_crpt)
6.1.5	FCS_COP.1(4)	Cryptographic operation (RSA_sign)
6.1.6	FCS_COP.1(5)	Cryptographic operation (SHA256)
6.1.7	FCS_RNG.1	Random number generation
6.1.8	FDP_ACC.1	Subset access control
6.1.9	FDP_ACF.1	Security attribute based access control
6.1.10	FDP_IFC.1	Subset information flow control
6.1.11	FDP_IFF.1	Simple security attributes
6.1.12	FDP_ITC.1(1)	Import of user data without security attributes (a session key/a public key for External Authentication)
6.1.13	FDP_ITC.1(2)	Import of user data without security attributes (except session keys/public keys for External Authentication)
6.1.14	FIA_AFL.1	Authentication failure handling
6.1.15	FIA_UAU.1	Timing of authentication
6.1.16	FIA_UAU.4	Single-use authentication mechanisms
6.1.17	FIA_UAU.5	Multiple authentication mechanisms
6.1.18	FIA_UID.1	Timing of identification
6.1.19	FMT_MSA.3	Static attribute initialisation
6.1.20	FMT_MTD.1	Management of TSF data
6.1.21	FMT_SMF.1	Specification of Management Functions
6.1.22	FMT_SMR.1	Security roles
6.1.23	FPT_PHP.3	Resistance to physical attack
6.1.24	FTP_ITC.1	Inter-TSF trusted channel

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 is expressed with italic: [assignment: *xxx (italic)*], [selection: *xxx (italic)*].
- Non-selected items in selection operation are expressed with strike-through: ~~strike-through~~
- Refinement is expressed with ***italic and gothic*** in the SFR.
- Iterated operation is expressed with information for distinction in parenthesis behind the SFR name, and with the short name attached a number such as (1), (2).
- Uncompleted operations are expressed with under-line: [assignment: *xxx (italic/under-line)*]. ST authors shall complete those uncompleted operations.

SFRs provided in this PP are shown below.

6.1.1 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**

6.1.2 FCS_COP.1(1) Cryptographic operation (AES)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [assignment: *encryption/decryption of APDU* for secure messaging, decryption of private key imported*] in accordance with a specified cryptographic algorithm [assignment: *AES-CBC mode*] and cryptographic key sizes [assignment: *128-bit*] that meet the following: [assignment: *FIPS PUB 197/NIST SP800-38A*].**

* *Application Protocol Data Unit: A data block for command/response transmitted to/from an IC card.*

6.1.3 FCS_COP.1(2) Cryptographic operation (MAC)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **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: *128-bit*] that meet the following: [assignment: *FIPS PUB 197/NIST SP 800-38B*].**

6.1.4 FCS_COP.1(3) Cryptographic operation (RSA_crpt)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [assignment: *decryption of the session key for secure messaging, decryption* of the secret key for decryption of private keys*] in accordance with a specified cryptographic algorithm [assignment: *RSA-OAEP*] and cryptographic key sizes [assignment: *2048-bit*] that meet the following: [assignment: *PKCS#1 v2.2*].**

* *applied to online modification of the secret key for public ID authentication AP*

6.1.5 FCS_COP.1(4) Cryptographic operation (RSA_sign)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [assignment: *the operations shown in Table 6-2*] in accordance with a specified cryptographic algorithm [assignment: *the cryptographic algorithm shown in Table 6-2*] and cryptographic key sizes [assignment: *2048-bit*] that meet the following: [assignment: *the standards shown in Table 6-2*].**

Table 6-2 Cryptographic operation for RSA signature and verification

Standard	*Cryptographic algorithm*	*Operation*
PKCS#1v2.2	*RSASSA-PKCS1-V1.5*	*signature generation to a message for Internal Authentication in the context of the platform and Basic Resident Registration Card AP*
		signature verification for External Authentication in the context of the platform and each basic AP
RSASSA-PKCS1-V1.5 padding in PKCS#1v2.2	*RSA*	*signature generation for a message with PKCS padding using a private key* *for Internal Authentication in the context of Input Support AP for the personal information printed on the card,* *Public ID authentication AP and* *AP for digitization of the personal information printed on the card,* *and for signature in the context of Public ID authentication AP*
None (proprietary code+ RSASSA-PKCS1-V1.5 padding in PKCS#1v2.2		*signature generation for a message using a private key, with PKCS padding accompanied with non-standard code, for a signature in the context of Public ID authentication AP*

6.1.6 FCS_COP.1(5) Cryptographic operation (SHA256)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [assignment: *message digest computation in connection with RSA cryptographic operation (decryption, signature generation/verification)*] in accordance with a specified cryptographic algorithm [assignment: *SHA-256*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *FIPS PUB 180-4*].**

6.1.7 FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 **The TSF shall provide a [selection: *physical, ~~non-physical true, deterministic,~~ hybrid*] random number generator that implements: [assignment: *none*].**

FCS_RNG.1.2 **The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].**

6.1.8 FDP_ACC.1 Subset access control

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

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 6-3>,

Object:<entities shown at the object column of Table 6-3>,

***Operations among subjects and objects covered by the SFP:<operations shown at the operation column of Table 6-3>*].**

Table 6-3 Subjects/objects/operations

Applied to:	*Subject*	*Object*	*Operation*
The platform	*Process on behalf of the administrator of the platform*	*[assignment: list of user data files*]*	*[selection: write, read]**
		SSD	*create/delete*
	Process on behalf of the administrator of Any APs based on ordinances of local governments	*Any APs based on ordinances of local governments*	*create/delete*
Input Support AP for the personal information printed on the card AP	*Process on behalf of the administrator of Input Support AP for the personal information printed on the card AP*	*[assignment: list of user data files*]*	*[selection: write, read]**
	Process on behalf of the card holder	*The personal number file* *The four data file*	*read*
	Process on behalf of the system handling the personal number and the four data		
Basic Resident Registration AP	*Process on behalf of the administrator of Basic Resident Registration AP*	*[assignment: list of user data files*]*	*[selection: write, read]**
	Process on behalf of the card holder	*Resident registration code file*	*read*

	Process on behalf of the system handling the Basic Resident Registration data		
Public ID authentication AP	*Process on behalf of the administrator of Public ID authentication AP*	*[assignment: list of user data files*]*	*[selection: write, read]**
	Process on behalf of the card holder	*The signing function with the signature private key* *The signing function with the user certification private key*	*sign*
	Process on behalf of the system handling certificate data	*The signing function with the user certification private key*	
AP for digitization of the personal information printed on the card	*Process on behalf of the administrator of AP for digitization of the personal information printed on the card*	*[assignment: list of user data files*]*	*[selection: write, read]**
	Process on behalf of the card holder	*The data file for digitized personal information printed on the card*	*read*
	Process on behalf of the system handling digitized personal information printed on the card		
	Process on behalf of the system handling personal number	*The data file for personal number*	
	Process on behalf of the system handling date of birth	*The data file for date of birth*	
The platform and the basic APs	*Process on behalf of the external terminal*	*The data files of public keys for session key encryption (except for AP for digitization of the personal information printed on the card)* *The data files of public keys for Internal Authentication*	*read*

* *Objects "user data files" 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).*

6.1.9 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset 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 column of Table 6-3>,

Objects:<entities shown at the object column of Table 6-3>,

SFP relevant security attributes for each subject:<authentication result of the user associated with the subject>,

***SFP relevant security attributes* for each object:<types of operations allowed to the subject>*]**.

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 authorise 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*]**.

* *Security attributes of objects include information of operation types allowed to authenticated subjects. Specified information for each object will be provided separately by the procurement authority (See the note of Table 6-3, FDP_ACC.1).*

6.1.10 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 **The TSF shall enforce the [assignment: *cryptographic key import information flow control SFP*] on [assignment:**

Subjects:<the process of the TOE importing a cryptographic key (a session key or a public key for External Authentication) from an external terminal>,

Information:<a cryptographic key (a session key or a public key for External Authentication)>, and

***Operations:<import>*]**.

6.1.11 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 **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 session key and the process of the TOE importing a public key for External Authentication from an external terminal>,

Information:<a session key and a public key for External Authentication)>,

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 **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 verification will be determined to be successful, if:

Case of a session key: Assuming that the data is encrypted by an external terminal with the public key of the TOE, the TOE decrypts encrypted data with the private key of the TOE and verifies that the decrypted data includes a given character string (here the private key and the given character string correspond to the reference data for information verification),

Case of a public key for External Authentication: 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 **The TSF shall enforce the [assignment: *none*].**

FDP_IFF.1.4 **The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].**

FDP_IFF.1.5 **The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].**

6.1.12 FDP_ITC.1(1) Import of user data without security attributes (a session key/a public key for External Authentication)

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

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

FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].**

6.1.13 FDP_ITC.1(2) Import of user data without security attributes (except session keys/public keys for External Authentication)

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 **The TSF shall enforce the [assignment: *Personal Number Cards access control SFP*] when importing user data *(except for session keys for secure messaging, public keys for External Authentication)*, controlled under the SFP, from outside of the TOE.**

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

FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].**

6.1.14 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].**

FIA_AFL.1.2 **When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].**

[Application note_FIA_AFL.1] An example of assignment for FIA_AFL.1.2 is a block of authentication function. If the block needs to be released by a management function, an ST author should add the management function.

6.1.15 FIA_UAU.1 Timing of authentication

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*] on behalf of the user to be performed before the user is authenticated.**

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.**

6.1.16 FIA_UAU.4 Single-use authentication mechanisms

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

FIA_UAU.4.1 **The TSF shall prevent reuse of authentication data related to [assignment: *the authentication mechanism applied to the user authentication shown in Table 6-4*].**

Table 6-4 Authentication mechanism to prevent reuse of authentication data

User authentication entity	*Purpose of authentication*	*Authentication mechanism*

The platform	*External authentication*	*Challenge-response system based on public key cryptosystem*
Input Support AP for the personal information printed on the card		
Basic Resident Registration AP		
Public ID authentication AP		
AP for digitization of the personal information printed on the card		

6.1.17 FIA_UAU.5 Multiple authentication mechanisms

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

FIA_UAU.5.1 **The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.**

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

6.1.18 FIA_UID.1 Timing of identification

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

FIA_UID.1.1 **The TSF shall allow [assignment: *list of TSF-mediated actions*] 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.**

6.1.19 FMT_MSA.3 Static attribute initialisation

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 **The TSF shall allow the [assignment: *administrator of objects (any APs based on ordinances of local governments, SSDs)*] to specify alternative initial values to override the default values when *the object* ~~*or information*~~ *is* created.**

[Application note_FMT_MSA.3] The default property of security attributes on creation of objects (any APs based on ordinances of local governments, SSDs) is provided by FMT_MSA.3. 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.

6.1.20 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 **The TSF shall restrict the ability to [selection: ~~*change_default, query, modify, delete, clear, [assignment: other operations]*~~] the [assignment: *TSF data shown in Table 6-5*] to [assignment: *the administrators shown in Table 6-5*].**

Table 6-5 TSF data managed

Applied to:	*TSF data*	*Administrator of TSF data*
The platform	*Not applicable*	–
Input Support AP for the personal information printed on the card	*Card holder PW*	*Card holder, and Administrator of Input Support AP for the personal information printed on the card*
	PW for personal number readout *PW for the four data readout*	*Administrator of Input Support AP for the personal information printed on the card*
Basic Resident	*Card holder PW*	*Card holder, and*

Registration AP		*Administrator of Basic Resident Registration AP*
Public ID authentication AP	*PW for signing* *PW for user certification*	*Card holder, and Administrator of Public ID authentication AP*
AP for digitization of the personal information printed on the card	*PW for date of birth* *PW for printed information on the card* *PW for personal number*	*Administrator of AP for digitization of the personal information printed on the card*
	Card holder PW	*Administrator of AP for digitization of the personal information printed on the card, and the system handling digitized personal information printed on the card*[*]

[*] *The system handling digitized personal information printed on the card has the privilege to modify card holder PW. The modified PW is informed to the card holder.*

6.1.21 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 **The TSF shall be capable of performing the following management functions: [assignment: *management functions shown in Table 6-6*].**

Table 6-6 Management functions

Applied to:	*Management function*
The platform	*none*
Input Support AP for the personal information printed on the card	*Modifies each PW*
Basic Resident Registration AP	*Modifies the card holder PW*
Public ID authentication AP	*Modifies each PW*
AP for digitization of the personal information printed on the card	*Modifies each PW*

6.1.22 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 **The TSF shall maintain the roles [assignment: *the roles shown in Table 6-7 for the platform and the basic APs each*].**

Table 6-7 Security roles

Applied to:	*Role*
The platform	*Administrator of the platform,* *Administrator of any APs based on ordinances of local governments*
Input Support AP for the personal information printed on the card	*Card holder,* *Administrator of Input Support AP for the personal information printed on the card*
Basic Resident Registration AP	*Card holder,* *Administrator of Basic Resident Registration AP*
Public ID authentication AP	*Card holder,* *Administrator of Public ID authentication AP*
AP for digitization of the personal information printed on the card	*Administrator of AP for digitization of the personal information printed on the card,* *The system handling digitized personal information printed on the card (See Table 6-5)*

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

6.1.23 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 **The TSF shall resist [assignment: *attacks with physical means and included in the IC evaluation method provided by the JIWG supporting documents*] to the [assignment: *the TSF*] by responding automatically such that the SFRs are always enforced.**

[Application note_FPT_PHP.3] The newest JIWG supporting documents at the time of evaluation shall be applied. The document when this PP was written was "Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 2.9, January 2013".

6.1.24 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 **The TSF shall 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/or MAC generation/verification are applied to, as shown in Table 6-8*].**

Table 6-8 Application methods of secure messaging

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

[*1] *[applied or not applied] The TOE shall be equipped with the secure messaging function. The function will be used when an external terminal requests it.*

[*2] *[not applied]The TOE may be equipped or not with the secure messaging function. If equipped, the function may be used depending on the request of an external terminal.*

6.2 Security assurance requirements

Security assurance requirements applied to the TOE are defined by the assurance components in Table 6-9. All of these components are taken from CC part3.

In this PP, no operation was applied to the components in Table 6-9.

Table 6-9 Assurance components

Assurance class	Assurance component
Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2

	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

6.3 Security requirements rationale

6.3.1 Security functional requirements rationale

In this chapter, the security functional requirements rationale shows that the SFRs defined achieve the security objectives for the TOE appropriately. It is shown that each SFR can be traced back to one or more security objectives for the TOE and that each objective is satisfied appropriately by the corresponding SFRs, in 6.3.1.1 and 6.3.1.2 respectively.

6.3.1.1 Tracing between the security objectives and the SFRs

The tracing between the security objectives and the SFRs is shown in Table 6-10. This table shows that each SFR can be traced back to one or more objectives for the TOE.

Table 6-10 Tracing between the security objectives and the SFRs

TOE security objective / SFR	FCS_CKM.4	FCS_COP.1(1)	FCS_COP.1(2)	FCS_COP.1(3)	FCS_COP.1(4)	FCS_COP.1(5)	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1(1)	FDP_ITC.1(2)	FIA_AFL.1	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_PHP.3	FTP_ITC.1
O.I&A	x				x	x		x	x	x	x	x	x	x	x	x	x	x		x	x	x		
O.Access_Control								x	x				x						x			x		
O.Replay																x								
O.Secure_messaging	x	x	x	x				x	x	x	x	x	x											x
O.Delivery															x		x	x						
O.Cryptography	x	x	x	x	x	x		x	x	x	x	x	x											x
O.Phys_Attack																							x	
O.RND							x																x	

6.3.1.2 Justification for tracing

In this section, 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(4) RSA signature generation/verification operation and FCS_COP.1(5) message digest computation are applied. For import of cryptographic keys used for public key cryptographic operations, two sets of SFRs are applied: FDP_ITC.1(1), FDP_IFC.1 and FDP_IFF.1 are applied to public keys for External Authentication. FDP_ITC.1(2), FDP_ACC.1, FDP_ACF.1 are applied for the rest of cryptographic keys used for public cryptosystem operations. Destruction of cryptographic key is provided by FCS_CKM.4. 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 any APs based on ordinances of local governments. 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 from outside. The cryptographic keys imported are access-controlled as user data. This requirement is addressed by FDP_ITC.1(2). These SFRs achieve O.Access_Control sufficiently.

O.Replay

FIA_UAU.4 describes single-use of authentication data. This SFR agrees with the security objective O.Replay.

O.Secure_messaging

Confidentiality and integrity of session data are protected by secure messaging using AES encryption/MAC. Session keys (AES) are created by an external terminal, encrypted with an RSA key, imported into the TOE and then decrypted. The AES cryptographic operation is provided by FCS_COP.1(1)/FCS_COP.1(2), and the RSA cryptographic operations are provided by FCS_COP.1(3), respectively. Import of the session keys for secure messaging is provided by FDP_ITC.1(1), FDP_IFC.1 and FDP_IFF.1. Destruction of a session key used for secure messaging is provided by FCS_CKM.4. Import of keys used for RSA public cryptosystem is provided by FDP_ITC.1(2)/FDP_ACC.1/FDP_ACF.1. Destruction of the keys imported is provided by FCS_CKM.4. Requirement for secure messaging itself (protection of communication channel data) is provided by 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 password, which is the secret information (often referred as a transport key). 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. These SFRs achieve O.Delivery sufficiently.

O.Cryptography

Cryptographic algorithms, cryptographic operations and cryptographic key management (key size, cryptographic key import, cryptographic key destruction) required in O.Cryptography are specified in Table 3-2 of P.Cryptography, which is referred to by O.Cryptography. The

requirements for cryptographic algorithms and cryptographic operations are provided by FCS_COP.1(1) – (5). All cryptographic keys are generated outside of the TOE and imported into the TOE. Requirements to import cryptographic keys are provided by FDP_ITC(1)/FDP_ITC(2). SFRs FDP_ACC.1/FDP_ACF.1/FDP_IFC.1/FDP_IFF.1 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.4. 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. If the TSF is not violated with physical attacks, the TSF will prevent security violation of data and functions of the TOE, with the logical security functionality of 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 a random number to be generated has sufficient quality and makes it difficult to be guessed by an attacker. FCS_RNG.1 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.

6.3.1.3 Dependencies of security functional requirements

Dependencies provided in each SFR and the dispositions are shown in Table 6-11.

The dependencies provided in the components of CC part 2 are shown at “Dependencies” column. “Satisfaction of dependencies” column shows how the dependencies are satisfied or the rationale justifying that the dependency is not satisfied.

Table 6-11 Dependencies of SFR

SFR	Dependencies	Satisfaction of dependencies
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Cryptographic keys to be destructed are imported from external terminals. Import of keys are addressed by FDP_ITC.1(1)/FDP_ITC.1(2) and the dependency is satisfied.
FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Cryptographic keys (session keys, secret keys to decrypt private keys) are imported from external terminals. Import of session keys and secret keys to

	FCS_CKM.4	decrypt private keys are addressed by FDP_ITC.1(1) and FDP_ITC.1(2) respectively. Key destruction is addressed by FCS_CKM.4 and the dependency is satisfied.
FCS_COP.1(2)		Cryptographic keys (session keys) are imported from external terminals. Import of session keys are addressed by FDP_ITC.1(1) and the dependency is satisfied. Key destruction is addressed by FCS_CKM.4 and the dependency is satisfied.
FCS_COP.1(3)		Cryptographic keys are imported from external terminals. Import of public keys for External Authentication are addressed by FDP_ITC.1(1) and the other keys are addressed by FDP_ITC.1(2). Key destruction is addressed by FCS_CKM.4
FCS_COP.1(4)		
FCS_COP.1(5)		This SFR describes only hash operation, which uses no cryptographic keys. Therefore, Import, generation and destruction of keys are not applied.
FCS_RNG.1	none	Not applicable
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1 is included and the dependency is satisfied.
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 is included and the dependency is satisfied. All objects except for any APs based on ordinances of local governments and SSDs are created in the development environment. Therefore, FMT_MSA.3 does not need to be applied. For any APs based on ordinances of local governments and SSDs, FMT_MSA.3 is applied and the dependency is satisfied.
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1 is included and the dependency is satisfied.
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 is included and the dependency is satisfied. FMT_MSA.3 is not applied, because the target information controlled under this SFR (session keys) is created at the external terminal.
FDP_ITC.1(1)		
FDP_ITC.1(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 is included and the dependency is satisfied. FMT_MSA.3 is not applied, because all objects storing user data relating this SFR are created as files in the development environment.
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1 is included and the dependency is satisfied.
FIA_UAU.1	FIA_UID.1	FIA_UID.1 is included and the dependency is satisfied.
FIA_UAU.4	None	Not applicable
FIA_UAU.5	None	Not applicable
FIA_UID.1	None	Not applicable
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	The objects managed by FMT_MSA.3 are any APs based on ordinances of local governments and SSDs. Their security attributes are not changed once after

		having been set. Accordingly, FMT_MSA.1 is not applied. The role creating objects is addressed by FMT_SMR.1 and the dependency is satisfied.
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1 are included and the dependencies are satisfied.
FMT_SMF.1	None	Not applicable
FMT_SMR.1	FIA_UID.1	FIA_UID.1 is included and the dependency is satisfied.
FPT_PHP.3	None	Not applicable
FTP_ITC.1	None	Not applicable

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 IC card have been highly developed, sufficient security cannot be assured without the assumption of high level attacks. That is, the TOE must counter attack potential of high, including physical attacks. Accordingly, AVA_VAN.5 was added to the assurance requirements for appropriate evaluation of vulnerabilities. Namely, for both of the 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, too. High level confidentiality and integrity for those data are required. Sufficient development security must 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 shown in Table 6-9 are satisfied.

7 Glossary and acronyms

7.1 General CC terms

PP Protection Profile: implementation-independent statement of security needs for a TOE type.

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; CC 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.

ST Security Target: Implementation-dependent statement of security needs for a specific identified TOE.

TOE Target of Evaluation: set of software, firmware and/or hardware possibly accompanied by guidance.

TSF TOE security functionality: combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

7.2 Terms related to the TOE

Personal Number Cards Official versatile IC card which includes the 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 IC card, the four APs are included: Input Support AP for the personal information printed on the card, the Basic Resident Registration AP, Public ID authentication AP and AP for digitization of the personal information printed on the card. Furthermore, each local government issuing the card may create any APs based on ordinances of the local government.

Composite evaluation An IC 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. IC 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 IC 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 ex-ante coordination among all interested parties will be required.