Xaica-alphaPLUS

Security Target Lite

Ver.1.1

4 Mar, 2015

Revised by NTT DATA CORPORATION

Revision History

Date	Version	Change	Description of Change
22/10/2014	1.0	Newly Created	
4/3/2015	1.1	Updated	Updated ST version

Table of Contents

1. ST introduction

This chapter describes ST reference, TOE reference and TOE overview.

1.1. ST reference

Title; Xaica-alphaPLUS Security Target Lite
Version number: 1.1
Date of Issue: March, 4, 2014
Sponsor: NTT DATA CORPORATION
Author: NTT DATA CORPORATION

1.2. TOE reference

TOE Name; Xaica-alphaPLUS
TOE version: 0116(PQV)
SPI version: SPI-001-03
Soft mask version:0100
Key Word: Smart Card, IC card, Smart card, Personal Number Card(PN Card)
Developer: NTT DATA CORPORATION

1.3. TOE overview

This section defines the type of the Target of Evaluation (TOE) and describes its main security features and intended usages.

1.3.1. TOE Type

The TOE is the IC card for the Social Security and Tax Number System. It is the product composed of dedicated hardware and software for its purpose. The sotware side of TOE consists of the platform software and the proprietary application program BANGO-AP(Input Support AP for the personal information printed on the card), JUKI-AP(Basic Resident Registration Card AP), KENMEN-AP(AP for digitization of the personal information printed on the card) and JPKI-AP(public ID authentication AP). The TOE securely manages the applications residing in IC memory and data according to following specifications.

- ・Personal Number card specification (Dec, 2013,ver.1.00 [PF-spec])
- ・BANGO-AP(Input Support AP for the personal information printed on the card) specification(Dec, 2013, ver.1.00 [BANGO-spec])
- ・JUKI-AP(Basic Resident Registration AP)(Dec, 2013, ver.1.00 [JUKI-spec])

・KENMEN-AP(AP for digitization of the personal information printed on the card)(Dec, 2013, ver.1.00 [KENMEN-spec])

・JPKI-AP(Public ID authentication AP)(Dec, 2013,ver.1.00 [JPKI-spec])

Application note:

These specifications are only Japanese version.

1.3.2. TOE Architecture

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 ST. 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.

The construction of the TOE is explained as follows. An example of the internal construction of the TOE is shown in Figure 1-1. This figure shows the major components 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.

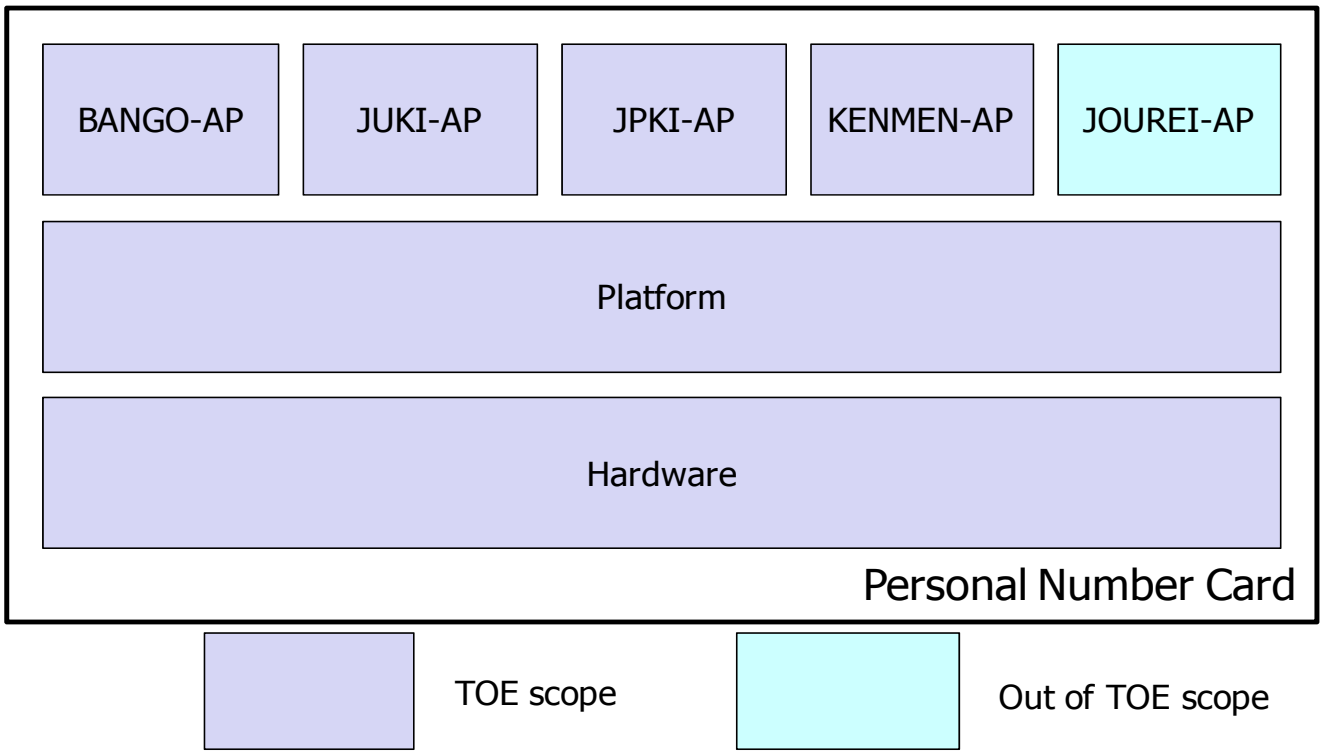


Figure 1-1: TOE Architecture (Overview)

1.3.3. TOE Usage

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.

[BANGO-AP(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. Examples of users are the entities that use personal numbers in business and the entities that require authentication of the card holder.

[JUKI-AP(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.

[JPKI-AP(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.

[KENMEN-AP(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.

1.3.4. TOE 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

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, administrators1 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 Authentication2 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 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.

1.3.5. 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.

1.3.6. TOE Life Cycle

(1) IC chip (hardware) development

The IC chip developer(STMicro erectronics) 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).

(2) Development of the platform and the basic APs
The software (the platform, the basic APs and the script) are developed by software developer(NTT DATA). The development of the software is performed independently from the development of the hardware (1).

(3) Personal number Card production
Personal Number Cards are manufactured through the processes embedding the software corresponding to the TOE of this ST into the IC chip by IC chip manufacturer(STMicro electronics) and embedding the IC chip in the plastic card together with an antenna for contactless communication by card manufacturer. After then, TOE become deliverable status by secure perasonalization with the script. 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) Personal number Card issuance
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) Additional APs(JOUREI-AP) activation
The local government issuing Personal Number Cards may activate own APs based on ordinances of the local government. They are optional by the local government and not necessarily created.

(6) Use by a Personal number Card holder
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. TOE conformance claim

In this chapter, CC conformance claim, PP claim and Package claim and their rationales are described.

2.1. CC conformance claim

This ST conforms to the standards including:

- Common Criteria for Information Technology Security Evaluation Version 3.1, Part 1: Introduction and general model Revision 4 (CCMB-2012-09-001);
- Common Criteria for Information Technology Security Evaluation Version 3.1, Part 2: Introduction and general model Revision 4 (CCMB-2012-09-002);
- Common Criteria for Information Technology Security Evaluation Version 3.1, Part 3: Introduction and general model Revision 4 (CCMB-2012-09-003);
- CC Part 2 extended;
  FCS_RNG.1 and FPT_EMSEC.1 are defined as extend SFR. (These definitions are described in chapter 5.)
- CC Part 3;
- Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1 (CCDB-2007-09-001).

2.2. PP claim

This ST is demonstrably conformant to [PP-PN] as presented below.

- Personal Number Cards Protection Profile, version1.0, 2014-4-24

2.3. Package claim

The assurance level for the evaluation of this ST is EAL4+ augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2 and AVA_VAN.5 components.

3. Security problem definition

In this chapter, users, assets, threats, organizational security policies and assumptions are set out.

3.1. Users

The users are The entities that interact with the product through the physical or logical external interfaces of the TOE.

Application note:

For the TOE, Subjects and their functions are defined as follows.

Table 3-1 definition of User

User	Definition
Card manufacturer	This user manufacturs the Personal number card(TOE) and executes the script. After then, TOE is delivered to the local government.
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.
Organs	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.
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

User	Definition
	“external terminal” described here.

Table 3-2 definition of Subject

Subject ID	Definition
SUB_CARD_MANUFACTURER_PROCESS	Process on behalf of Card Manufacturer.
SUB_PN_CARD_HOLDER	Process on behalf of Card Holder.
SUB _Platform_ADMIN_PROCESS	Process on behalf of Platform Administrator.
SUB _JOUREI-AP_ADMIN_PROCESS	Process on behalf of JOREI-AP Administrator.
SUB _BANGO-AP_ADMIN_PROCESS	Process on behalf of BANGO-AP Administrator.
SUB _JUKI-AP_ADMIN_PROCESS	Process on behalf of JUKI-AP Administrator.
SUB _JPKI-AP_ADMIN_PROCESS	Process on behalf of JPKI-AP Administrator.
SUB _KENMEN-AP_ADMIN_PROCESS	Process on behalf of KENMEN-APAdministrator.
SUB_BANGO_SYSTEM_PROCESS	Process on behalf of a BANGO system using the Personal number and The Four informations.
SUB_JUKI_SYSTEM_PROCESS	Process on behalf of a JUKI system using JUKI data.
SUB_KENMEN_DAY_SYSTEM_PROCESS	Process on behalf of a KENMEN system using a birthday.
SUB_KENMEN_IMG_SYSTEM_PROCESS	Process on behalf of a KENMEN system using a KENMEN data.
SUB_KENMEN_NUM_SYSTEM_PROCESS	Process on behalf of a KENMEN system using the Personal number.
SUB_JPKI_SYSTEM_PROCESS	Process on behalf of a JPKI system using certification data.
SUB_EXTERNAL_TERMINAL_PROCESS	Process on behalf of the External terminal.

Table 3-3 definition of Role

Role	ID	Definition
Card Manufacturer	ROL_CARD_MANUFACTURER	Card format and setting of card configuration by executing the script
Platform administrator	ROL_Platform_ADMIN	Entity to manage Platform(ISD&SSD)
JOUREI-AP administrator	ROL_JOUREI-AP_ADMIN	Entity to manage JOUREI-AP

Role	ID	Definition
PN Card holder	ROL_PN_CARD_HOLDER	The end user of a PN card
BANGO-AP administrator	ROL_BANGO-AP_ADMIN	Entity to manage BANGO-AP
JUKI-AP administrator	ROL_JUKI-AP_ADMIN	Entity to manage JUKI-AP
JPKI-AP administrator	ROL_JPKI-AP_ADMIN	Entity to manage JPKI-AP
KENMEN-AP administrator	ROL_KENMEN-AP_ADMIN	Entity to manage KENMEN-AP
KENMEN-AP system	ROL_KENMEN-AP_SYSTEM	Entity to use KENMEN-AP

The correlation between the Subject, User and Role are shown as below.

Table 3-4 Relationship between Subject, User and Role

Subject ID	User	Role
SUB_CARD_MANUFACTURER_PROCESS	Card Manufacturer	ROL_CARD_MANUFACTURER
SUB_PN_CARD_HOLDER	Card Holder	ROL_PN_CARD_HOLDER
SUB _Platform_ADMIN_PROCESS	Organs	ROL_PLATFORM_ADMIN
SUB _JOUREI-AP_ADMIN_PROCESS	Administrator, Organs	ROL_JOUREI-AP_ADMIN
SUB _BANGO-AP_ADMIN_PROCESS	Administrator, Organs	ROL_BANGO-AP_ADMIN
SUB _JUKI-AP_ADMIN_PROCESS	Administrator, Organs	ROL_JUKI-AP_ADMIN
SUB _JPKI-AP_ADMIN_PROCESS	Administrator, Organs	ROL_JPKI-AP_ADMIN
SUB _KENMEN-AP_ADMIN_PROCESS	Administrator, Organs	ROL_KENMEN-AP_ADMIN
SUB_BANGO_SYSTEM_PROCESS	Administrator, Organs	ROL_BANGO-AP_ADMIN
SUB_JUKI_SYSTEM_PROCESS	Administrator, Organs	ROL_JUKI-AP_ADMIN
SUB_KENMEN_DAY_SYSTEM_PROCESS	Administrator, Organs	ROL_KENMEN-AP_ADMIN ROL_KENMEN-AP_SYSTEM
SUB_KENMEN_IMG_SYSTEM_PROCESS	Administrator, Organs	ROL_KENMEN-AP_ADMIN ROL_KENMEN-AP_SYSTEM
SUB_KENMEN_NUM_SYSTEM_PROCESS	Administrator, Organs	ROL_KENMEN-AP_ADMIN ROL_KENMEN-AP_SYSTEM
SUB_JPKI_SYSTEM_PROCESS	Administrator, Organs	ROL_JPKI-AP_ADMIN
SUB_EXTERNAL_TERMINAL_PROCESS	External terminal	ROL_CARD_ADMIN, ROL_JOUREI-AP_ADMIN, ROL_PN_CARD_HOLDER, ROL_BANGO-AP_ADMIN, ROL_JUKI-AP_ADMIN, ROL_JPKI-AP_ADMIN, ROL_KENMEN-AP_ADMIN

Application note:

If the assets of the TOE are infringement by illegal terminal device, user uses TOE according to own role after confirming the authenticity of the terminal device.

3.2. Assets

The information assets protected by the TOE security functionality (TSF) are the user data stored in the TOE and the processing functions of the TOE for users. The user data is the data used for 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 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.

Application Note:

The following table provides the definition of the objects in the PN Card for the TOE.

Table 3-5 Objects

Application	ID	Object
Platform	OBJ_ SCRIPT	The script for secure personalizing initial TOE.
	OBJ_PLATFORM_DATA	User data files
	OBJ_PLATFORM_JOUREI-AP_AREA	SSD*This object is not included in the asset to be protected by TOE.
	OBJ_PLATFORM_JOUREI_AP	JOUREI-AP(any APs based on ordinances of local governments)*This object is not included in the asset to be protected by TOE.

Application	ID	Object
BANGO-AP	OBJ_BANGO_DATA	User data files
	OBJ_BANGO_MYNUM&4INFO	Data files for the personal number and the four data
	OBJ_BANGO_ENCRYPTION_KEY *1	Data file of public key for session key encryption *1
	OBJ_BANGO_IA_PUBLIC_KEY *1	Data file of public key for internal authentication *1
JUKI-AP	OBJ_JUKI_DATA	User data files
	OBJ_JUKI_RESIDENTIAL_CODE	Data file for the Basic Resident Registration Code
JPKI-AP	OBJ_JPKI_DATA	User data files
	OBJ_JPKI_SIGNATURE_FUN	Function of signature
	OBJ_JPKI_USER_CERT_FUN	Function of user certification
KENMEN-AP	OBJ_KENMEN_DATA	User data files
	OBJ_KNEMEN_KENMEN_INFO	Data files for printed information
	OBJ_KENMEN_MYNUM&4INFO	Data files for birth date, digitized personal information printed on the card, personal number
The platform and the basic APs	OBJ_COMMON_ENCRYPTION_KEYS	Data files of public keys for session key encryption (except KENMEN-AP)
	OBJ_COMMON_PUBLIC_KEYS *2	Data files of public keys for internal authentication*2

*1 These objects are not lead from Access control definition written in PP directly, but product specification document provided from the procurement authority defines Access control which these objects and operations are needed..

*2 Public key for internal authentication in JUKI-AP is not used according to product specification document provided from the procurement authority.

3.3. Threats

This section describes threats to be countered by the TOE. These threats shall be countered by the TOE or its operational environment independently or in combination with them.

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:

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:

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:

- Monitors and analyses power consumption of the TOE during cryptographic operation to infer the cryptographic key.
- Probes the inside of TOE to disclose data.
- Discloses or modifies data or uses processing function of the TOE illegally by causing errors or malfunction of the TSF with glitches or environmental stresses during operation of the TOE.
- Discloses or modifies data of the TOE or modifies behavior of the TOE by physical manipulation the inside of TOE.

3.4. Organizational security policies

The organizational 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 3-6. 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 3-6 Application of secure messaging

Applied to:	Encryption/Decryption	MAC generation/verification
Platform	applied	applied
BANGO-AP (Input Support AP for the personal information printed on the card)	applied or not applied*1	applied or not applied*1*3
JUKI-AP (Basic Resident Registration A)	applied (readout of resident registration code)	not applied *2
JPKI-AP (Public ID authentication AP)	applied or not applied*1	applied or not applied*1
KENMEN-AP (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.

Application Note:

**3 In this TOE, MAC generation/verification is not applied to BANGO AP according to product specification document provided from the procurement authority.*

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:

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 ST 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 3-7 shows cryptographic algorithms, cryptographic operations, cryptographic key sizes, cryptographic key management policies (key generation/import and destruction) and purposes of cryptographic functions.

Table 3-7 Criptographic function policies

Cryptographic algorithm/ Standards	Cryptographic operation	Key sizes (bit)	key generation /Import	key destruction	Purpose
AES-CBC mode /FIPS PUB 197 ・ NIST SP 800-38A	Encryption/decryption	128	Import	Unspecified in [PP-PN]	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		Unspecified in [PP-PN]	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 PUB180-4	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:

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

The assumptions are as follows.

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

In this chapter, Security Objectives for the TOE, Security Objectives for the operational environment and Security Objectives rationale are described.

4.1. Security objectives for the TOE

This section describes security objectives for the TOE.

O.I&A

The TOE shall identify/authenticate a user of the TOE and authorize the user who has been authenticated successfully to perform the actions corresponding to the role of the user. 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.

Table 4-1 users and privileges

Applied to:	User	Privilege
The platform	Card manufacturer	The script execution
	Administrator of the platform	Initialization/modification of data Creation/deletion of SSD
	Administrator of JOUREI-AP(any APs based on ordinances of local governments)	Creation/deletion of any APs based on ordinances of local governments
BANGO-AP (Input Support AP for the Personal information printed on the card AP)	Administrator of BANGO-AP(Input Support AP for the personal information printed on the card)	Initialization/modification of data
	Card holder	Readout the personal number and the four data Change of the card holder's own PW Readout of the public key for session key encryption*1 Readout of the public key for internal authentication*1
	The system handling personal numbers and the four data	Readout of the personal number and the four data Readout of the public key for session key encryption*1 Readout of the public key for internal

		authentication*1
JUKI-AP (Basic Resident Registration AP)	Administrator of JUKI-AP(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 JUKI data(Basic Resident Registration data)	Readout of resident registration code
JPKI-AP (Public ID Authentication AP)	Administrator of JPKI-AP(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 certificate function
KENMEN-AP (AP for digitization of the personal information printed on the card)	Administrator of KENMEN-AP(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 KENMEN-AP(AP for digitization of the personal information printed on the card))*3 Readout of the public key for internal authentication*2*4

Application Note:

**1 These objects and operations are not lead from Access control definition written in PP directly, but product specification document provided from the procurement authority defines Access control which these objects and operations are needed.*

**2 Public key for internal authentication in JUKI-AP is not used according to product specification document provided from the procurement authority.*

**3Public keys for session key encryption of PF can be read out without authentication according to product specification document provided from the procurement authority.*

**4Public keys for international authentication of except BANGO-AP can be read out without authentication according*

to product specification document provided from the procurement authority.

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	Card manufacturer	The script	The script execution
	Administrator of the platform Administrator	User data files	Read and/or write
		SSD	Create/Delete
	Administrator of JOUREI-AP(Any APs based on ordinances of local governments)	JOUREI-AP(any APs based on ordinances of local governments)	Create/Delete
BANGO-AP (Input Support AP for the Personal information printed on the card AP)	Administrator of BANGO-AP(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 The public key for session key encryption*1 The public key for internal authentication*1	Read
	The system handling the personal number and the four data.		
JUKI-AP (Basic Resident Registration AP)	Administrator of JUKI-AP(Basic Resident Registration AP)	User data files	Read and/or write
	Card holder	Resident Registration Code file	Read
	The system handling the JUKI data(Basic Resident Registration data)		

JPKI-AP (Public ID Authentication AP)	Administrator of JPKI-AP(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	
KENMEN-AP (AP for digitization of the personal information printed on the card)	Administrator of KENMEN-AP(AP for digitization of the personal information printed on the card)	User data files	Read and/or write
	Card holder	The Data file digitized	Read
	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 KENMEN-AP(AP for digitization of the personal information printed on the card))*3 The data files of public keys for internal authentication*2*4	Read

Application Note:

**1 These objects and operations are not lead from Access control definition written in PP directly, but product specification document provided from the procurement authority defines Access control which these objects and operations are needed.*

**2 Public key for internal authentication in JUKI-AP is not used according to product specification document provided from the procurement authority.*

**3Public keys for session key encryption of PF can be read out without authentication according to product specification document provided from the procurement authority.*

**4Public keys for international authentication of except BANGO-AP can be read out without authentication according to product specification document provided 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 3-6. 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 3-7. 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 3-7 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 3-7 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 3-7 of P.Cryptography. In Table 3-7, 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:

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.

O.Secure_LOAD&INSTALL

TOE must check integrity and authenticity of the additional code before this code is installed in the initial TOE must insure that the installation of the additional code is executed in the targetd way even in case of interruption. Identification data of the final TOE must be updated at the same time the additional code is installed on the initial TOE.

4.2. Security objectives for the operational environment

The following are the Security Objectives for the operational environment.

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 theTOE.

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 section, the measures presented in the Security Objectives are verified for their effectiveness against the threats defined in the security challenge definition, organizational security policies and assumptions.

4.3.1. Threats

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. In case of secure personalize , O.Secure_LOAD&INSTALL requires the user of the TOE to be identified and authenticated so that only users are allowed to execute the script. 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.

4.3.2. Organizational Security Policies

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 3-6 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 3-7 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.

4.3.3. Assumptions

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.

4.3.4. SPD and Security Objectives

The following tables Table 4-3 T to Table 4-5 show the relationship between the SPD and the Security Objectives.

Table 4-3 Threats and Security Objectives

Security Objectives / Security Problem Definition	O.I&A	O.Access_control	O_Secure_messaging	O_Replay	O.Phys_Attack	O.Delivery	O.Cryptography	O.RND	O.Secure_LOAD&INSTALL	OE.Administrator	OE.PKI	OE.AP
T.Illegal_attack	x	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.Administrator										x		
A.PKI											x	
A.AP												X

Table 4-4 Security Problem Definitions and Security Objectives

Threats	Security Objectives	Rationale
T.Illegal_attack	O.I&A, O.Access_Control, O.Secure_LOAD&INSTALL	Section 4.3.1
T.Replay	O.Reply	Section 4.3.1
T.Phys_Attack	O.Phys_Attack	Section 4.3.1
P.Secure_messaging	O.Secure_messaging, O.cryptgraphy	Section 4.3.1
P.Delivery	O.I&A , O.Delivery	Section 4.3.2
P.Cryptography	O.Cryptography	Section 4.3.2
P.RND	O.RND	Section 4.3.2
A.Administrator	OE.Administrator	Section 4.3.3
A.PKI	OE.PKI	Section 4.3.3
A.AP	OE.AP	Section 4.3.3

Table 4-5 Security Objectives and Security Problem Definitions

Security Objectives	Threats
O.I&A	T.Illegal_attack,P.Delivery
O.Access_control	T.Illegal_attack

Security Objectives	Threats
O_Secure_messaging	P.Secure_messaging
O_Replay	T.Replay
O.Delivery	P.Delivery
O.Cryptography	P.Secure_messaging, P.Cryptography
O.Phys_Attack	T.Phys_Attack
O.RND	P.RND
O.Secure_LOAD&INSTALL	T.Illiegal_Attack
OE.Administrator	A.Administrator
OE.PKI	A.PKI
OE.AP	A.AP

5. Extended components definition

5.1. 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.

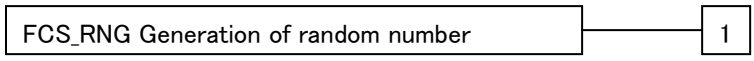
To define the security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG Generation of random numbers

Family behavior

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

Component leveling



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

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.

5.2. Definition of the Family FPT_EMSEC

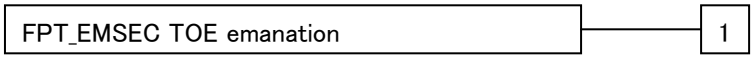
The additional family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), electromagnetic analysis(EMA), differential electromagnetic analysis(DEMA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC2].

The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMSEC.1 TOE emanation has two constituents:

FPT_EMSEC.1.1 Limit of Emissions requires not to emit intelligible emissions enabling access to TSF data or user data.

FPT_EMSEC.1.2 Interface Emanation requires not to emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMSEC.1

There are no management activities foreseen.

Audit: FPT_EMSEC.1

There are no actions defined to be auditable.

FPT_EMSEC.1 TOE Emanation

Hierarchical to: No other components.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Dependencies: No other components.

6. Security requirements

This chapter describes Security functional requirements, Security assurance requirements and Security requirements rationale of TOE.

6.1. Security functional requirements

This section describes Security functional requirements,

The following table and rational apply to Security Target.

Table 6-1 SFRs

Section	Identification	
6.1.1.PP SFRs	FCS_CKM.4/PN	Cryptographic key destruction
	FCS_COP.1(1) /PN	Cryptographic operation (AES)
	FCS_COP.1(2) /PN	Cryptographic operation (MAC)
	FCS_COP.1(3) /PN	Cryptographic operation (RSA_crypt)
	FCS_COP.1(4) /PN	Cryptographic operation (RSA_sign)
	FCS_COP.1(5) /PN	Cryptographic operation (SHA256)
	FCS_RND.1/PN	Random number generation
	FDP_ACC.1/PN	Subset access control
	FDP_ACF.1/PN	Security attribute based access control
	FDP_IFC.1/PN	Subset information flow
	FDP_IFF.1/PN	Simple security attributes
	FDP_ITC.1(1) /PN	Import of user data without security attributes (session key and public key for external authentication)
	FDP_ITC.1(2) /PN	Import of user data without security attributes (except session keys/public keys for external authentication)
	FIA_AFL.1/PN	Authentication failure handling
	FIA_UAU.1/PN	Timing of authentication
	FIA_UAU.4/PN	Single-use authentication mechanisms
	FIA_UAU.5/PN	Multiple authentication mechanism
	FIA_UID.1/PN	Timing of identification
	FMT_MSA.3/PN	Static attribute initialization
	FMT_MTD.1/PN	Management of TSF data
	FMT_SMF.1/PN	Specification of Management Functions
	FMT_SMR.1/PN	Security roles
	FPT_PHP.3/PN	Resistance to physical attack

	FTP_ITC.1/PN	Inter-TSF trusted channel
6.1.2. Additonal SFRs	FPT_FLS.1/Other	Failure with preservation of secure state
	FPT_TST.1/Other	TSF testing
	FPT_EMSEC.1/Other	TOE emanation has two constituents
	FDP_ITC.1/Other	Import of user data without security attributes (the key)
	FDP_IFC.1/Other	Subset information flow(the key)
	FDP_IFF.1/Other	Simple security attributes(the key)
	FTP_ITC.1/Other	Inter-TSF trusted channel(the script)
	FDP_UIT.1/Other	Data exchange integrity(the script)
	FDP_UCT.1/Other	Basic data exchange confidentiality(the script)
	FCS_COP.1/Other	Cryptographic operation(the script)
	FCS_CKM.4/Other	Cryptographic key destruction(the Key)

6.1.1. PP SFRs

FCS_CKM.4/PN 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/PN The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: deleting keys on volatile memory by shutting down, rewriting a key with a new key and disabling a key with a flag]*** that meets the following: ***[assignment: none]***.

FCS_COP.1(1) /PN 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 /PN 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].***

FCS_COP.1(2)/PN 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 /PN 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]***.

FCS_COP.1(3) /PN Cryptographic operation (RSA2048)

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 /PN 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]***.

FCS_COP.1(4) /PN 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 /PN 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	RSASSAPKCS1-V1.5	signature generation to a message forInternal Authentication in the context of the platform and JUKI-AP
		signature verification for External Authentication in the context of the platform

		and each basic APs
RSASSA-PKCS1-V1.5 padding specified in PKCS#1v2.2	RSA	signature generation for a message with PKCS padding using a private key for Internal Authentication in the context of BANGO-AP, JPKI-AP and KENMEN-AP and for signature in the context of JPKI-AP
None (proprietary code+ RSASSAPKCS1-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 JPKI-AP

FCS_COP.1(5) /PN 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/PN 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]***.

FCS_RNG.1 /PN Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 /PN The TSF shall provide a ***[assignment: physical]*** random number generator that implements ***[assignment: none]***.

FCS_RNG.1.2 /PN The TSF shall provide random numbers that meet **[assignment: *AIS-31*]**.

FDP_ACC.1/PN Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 /PN 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 Subject/Objects/Operations

Applied to:	Subject	Object	Operation
Platform	[assignment: Card manufacturer]	[assignment: the script]	[assignment: Secure personalize]
	Platform administrator	User data files	Read and/or write
		SSD	Create/Delete
	Administrator of JOUREI-AP(Any APs based on ordinances of local governments)	JOUREI-AP(any APs based on ordinances of local governments)	Create/Delete
BANGO-AP (Input Support AP for the Personal information printed on the card AP)	Administrator of BANGO-AP(Input Support AP for the personal information printed on the card AP)	User data files	Read and/or write
	Card holder	Data files for the personal number and the four data [assignment: Data file of public key for session key encryption*1 data file of public key for internal authentication*1]	Read
	System which uses the personal number and the four data		
JUKI-AP (Basic Resident Registration AP)	Administrator of Basic Resident Registration AP	User data files	Read and/or write
	Card holder	Data file for the Basic Resident Registration Code	Read
	System which uses the JUKI data		
JPKI-AP (Public ID authentication AP)	Administrator of Public ID authentication AP	User data files	Read and/or write
	Card holder	Function of signature by a secret key for signning Function of user certification by a secret key for user certification	signature
	System which uses the certification data	Function of user certification by a secret key	

Applied to:	Subject	Object	Operation
		for user certification	
KENMEN-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	User data files	Read and/or write
	Card holder	Data files for printed information	Read
	System which uses digitized personal information printed on the card	Data files for digitized personal information printed on the card	
	System which uses personal number	Data files for personal number	
	System which uses birth date	Data files for birth date	
The platform and basic APs	External terminal	Data files of public keys for session key encryption*3 (exception KENMEN-AP) Data files of public keys for internal authentication*2*4	Read

Application note

**1 These objects and operations are not lead from Access control definition written in PP directly, but product specification document provided from the procurement authority defines Access control which these objects and operations are needed.*

**2 Public key for internal authentication in JUKI-AP is not used according to product specification document provided from the procurement authority.*

**3 Public keys for session key encryption of PF can be read out without authentication according to product specification document provided from the procurement authority.*

**4 Public keys for international authentication of except BANGO-AP can be read out without authentication according to product specification document provided from the procurement authority.*

FDP_ACF.1/PN Access control based on security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/PN 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 /PN 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/PN The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[assignment: none].*

FDP_ACF.1.4/PN The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *[assignment: none].*

FDP_IFC.1 /PN 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>].

FDP_IFF.1 /PN Simple security Attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1/PN 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/PN 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 /PN The TSF shall enforce *[assignment: none]*.

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

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

FDP_ITC.1(1)/PN Import of user data without security attributes(Session key and 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 initialization

FDP_ITC.1.1/PN The TSF shall enforce the *[assignment: the encryption 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/PN The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/PN 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]*.

FDP_ITC.1(2)/PN Import of user data without security attributes (except session key and 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 initialization

FDP_ITC.1.1/PN The TSF shall enforce the **[assignment: Personal number Card 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/PN The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/PN 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]***.

FIA_AFL.1/PN Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/PN The TSF shall detect when ***[selection: an administrator configurable positive integer within [assignment: Specified number]]*** unsuccessful authentication attempts occur related to ***[assignment: authentication events]***.

FIA_AFL.1.2/PN When the defined number of unsuccessful authentication attempts has been ***[selection: met]***, the TSF shall ***[assignment:*** permanently stop authentication with the key or halt the authentication function of passwrord until it is released by the administrator***]***.

FIA_UAU.1/PN Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1/PN The TSF shall allow ***[assignment: list of TSF mediated actions]*** on behalf of the user to be performed before the user is authenticated.

Application note:

list of TSF mediated actions

- Booting

- *MPU Setting*
- *Rollback Operation*
- *Select File*
- Read some files

FIA_UAU.1.2/PN The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/PN Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1/PN The TSF shall prevent reuse of authentication data related to ***[assignment: External authentication]***.

Application note:

The authentication method related to Get Challenge＋External Auth supports this.

FIA_UAU.5/PN Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1/PN The TSF shall provide ***[assignment: list of multiple authentication mechanisms shown in Table 6-4]*** to support user authentication.

FIA_UAU.5.2/PN The TSF shall authenticate any user's claimed identity according to the ***[assignment: rules describing how the multiple authentication mechanisms provide authentication shown in Table 6-4]***.

Application note:

Table 6-4 Authentication mechanisms

Application	Key	Name of Authentication Mechanism	Rule of authentication mechanism
Platform	Transport key	Transport key authentication (for the platform)	Verification with transport Key (PIN)
	Public key	The External terminal authentication (for the platform)	Authenticity validation of the authentication target by the public key cryptographic System
Basic APs	Transport key	Transport key authentication (for the basic APs)	Verification with transport Key (PIN)
	Password	Password authentication	Verification with Password (PIN)

Application	Key	Name of Authentication Mechanism	Rule of authentication mechanism
		(for the basic APs)	
	Public key	The External terminal authentication (for the basic APs)	Authenticity validation of the authentication target by the public key cryptographic System

FIA_UID.1/PN Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1/PN The TSF shall allow ***[assignment: list of TSF-mediated actions]*** on behalf of the user to be performed before the user is identified.

Application note:

- Booting
- MPU Setting
- Rollback Operation
- Select file
- Read some files

FIA_UID.1.2/PN The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FMT_MSA.3/PN Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1/PN The TSF shall enforce the ***[assignment: Personal Number Card access control SFP]*** to provide ***[selection: restrictive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/PN The 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 is created.

Application note:

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.

FMT_MTD.1/PN 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/PN The TSF shall restrict the ability to ***[selection: modify]*** the ***[assignment: TSF data shown in Table 6-5]*** to ***[assignment: administrator shown in Table 6-5]***.

Table 6-5 TSF data managed

Applied to:	TSF data	Administrator of TSF data
Platform	Not applicable	–
BANGO-AP (Input support AP Platform)	Card holder PW	Card holder
		Administrator of BANGO-AP
	PW for Personal number readout	Administrator of BANGO-AP
	PW for the four data readout	
JUKI-AP (Basic Resident Registration AP)	Card holder PW	Card holder
		Administrator of JUKI-AP
JPKI-AP (Public ID Authentication AP)	PW for signing	Card holder
		Administrator of JPKI-AP
	PW for user certification	Card holder
		Administrator of JPKI-AP
KENMEN-AP (Confirmation AP)	PW for date of birth	Administrator of KENMEN-AP
	PW for printed information on the card	
	PW for Personal number	
	Card holder PW	The system handling digitized personal information printed on the card.*
		Administrator of KENMEN-AP

* 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.

FMT_SMR.1/PN 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 6-6 for the platform and Basic APs each]***.

Table 6-6 Security roles

Application	Role	ID
Platform	Card Manufacaturer	ROL_CARD_MANUFACTURER
	Administrator of the platform	ROL_PLATFORM_ADMIN
	Administrator of JOUREI-AP	ROL_JOUREI-AP_ADMIN
BANGO-AP	Card Holder	ROL_PN_CARD_HOLDER
	Administrator of BANGO-AP	ROL_BANGO-AP_ADMIN
JUKI-AP	Card Holder	ROL_PN_CARD_HOLDER
	Administrator of JUKI-AP	ROL_JUKI-AP
JPKI-AP	Card Holder	ROL_PN_CARD_HOLDER
	Administrator of JPKI-AP	ROL_JPKI-AP_ADMIN
KENMEN-AP	Card Holder	ROL_PN_CARD_HOLDER
	The system handling digitized personal information printed on the card (See Table 6-5)	ROL_KENMEN-AP_SYSTEM
	Administrator of KENMEN-AP	ROL_KENMEN-AP_ADMIN

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

FMT_SMF.1/PN Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/PN The TSF shall be capable of performing the following management functions: ***[assignment: management functions are shown in Table 6-7].***

Table 6-7 Management functions

Applied to:	Management functions
Platform	None

BANGO-AP	・Modifies each PW ・Unlocks the authentication function
JUKI-AP	・Modifies each PW ・Unlocks the authentication function
JPKI-AP	・Modifies each PW ・Unlocks the authentication function
KENMEN-AP	・Modifies each PW ・Unlocks the authentication function

FPT_PHP.3/PN Physical attack resistance

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_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:

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".

FTP_ITC.1/PN Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/PN 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/PN The TSF shall permit ***[selection: 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
Platform	applied	applied

BANGO-AP (Input Support AP for the personal information printed on the card)	applied or not applied*1	applied or not applied*1*3
JUKI-AP (Basic Resident Registration A)	applied (reading of the Basic Resident Registration Code)	not applied *2
JPKI-AP (Public ID authentication AP)	applied or not applied*1	applied or not applied*1
KENMEN-AP (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.

Application Note:

**3 In this TOE, MAC generation/verification is not applied to BANGO AP according to product specification document provided from the procurement authority,*

6.1.2. Additional SFRs

FPT_FLS.1/Other Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1/Other The TSF shall preserve a secure state when the following types of failures occur: ***[assignment: the following list of types of failures in the TSF]***.

[*List of types of failures in the TSF*]

- Detection of an abnormal status of the granted check code during EEPROM read-out
- Detection of a recalculation error during the private key calculation
- Detection of an abnormal status of a security sensor of chip hardware
- Detection of self-check test error upon resetting
- Detection of bypass processing not correctly perform

FPT_TST.1/Other TSF testing:

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1/Other The TSF shall run a suite of self tests ***[selection: during initial start-up, at the conditions[assignment: After chip H/W initialization]]*** to demonstrate the correct operation of ***[selection: [assignment: RNG, SF.MemoryManager, SF.DomainSeparation], the TSF]***.

FPT_TST.1.2/Other The TSF shall provide authorized users with the capability to verify the integrity of ***[selection: [assignment: Transport Key], TSF data]***.

FPT_TST.1.3/Other The TSF shall provide authorized users with the capability to verify the integrity of ***[selection: [assignment: parts of TSF]]***

FPT_EMSEC.1/Other TOE emanation has two constituents:

FPT_EMSEC.1.1/Other

The TOE shall not emit ***[assignment: electromagnetic emissions]*** in excess of ***[assignment: levels which could be measured and analyzed]*** enabling access to ***[assignment: none]*** and ***[assignment: assets shown in*** Table 3-5***]***.

Application note:

STMicrosystems assigns "none" in [assignment: list of types of user data].

FPT_EMSEC.1.2/Other

The TSF shall ensure ***[assignment: any unauthorized users]*** are unable to use the following interface ***[assignment: smart card circuit contacts and contactless]*** to gain access to ***[assignment: none]*** and ***[assignment: assets shown in*** Table 3-5***]***.

Dependencies: No other components.

Application note:

The TOE (IC card) has contact and contact-less interfaces physically.

FDP_ITC.1/ Other Import of user data without security attributes (the key)

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 initialization

FDP_ITC.1.1/Other The TSF shall enforce the ***[assignment: The key import information control SFP]*** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

FDP_IFC.1/Other Subset information flow control(the key)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Other The TSF shall enforce ***[assignment: the key import access control SFP to subject <the TOE process to execute the script>, information <the key>, operation <import>].***

FDP_IFF.1/Other Simple security Attributes(the key)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1/Other The TSF shall enforce ***[assignment: the key import access control SFP]*** depends on ***[assignment: subject <the TSF process to execute the script>, information <the key>, the subject security attribute <the key related to subject>, information security attribute <authentication by the key related to subject>]***.

FDP_IFF.1.2/Other The TSF shall enforce information flow between controlled subject and controlled information when the following rules are maintained ***[assignment: the TSF allows to access to the information subject, only when the security attribute of imported information is in authentication status by the key related to the subject]***.

FDP_IFF.1.3/Other The TSF shall enforce ***[assignment: SFP rules of additional access control: none]***.

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

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

FTP_ITC.1/Other Inter-TSF trusted channel(the script)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/Other 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/Other The TSF shall permit ***[selection: another trusted IT product]*** to initiate communication via the trusted channel.

FTP_ITC.1.3/Other The TSF shall initiate communication via the trusted channel for ***[assignment: the script transfer].***

FDP_UIT.1/Other Data exchange integrity(the script)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or
FDP.IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/Other The TSF shall enforce **[assignment: Personal number card *access control SFP*]** to ***[selection: receive]*** user data in a manner protected from ***[selection: modification, deletion, insertion]*** errors.

FDP_UIT.1.2/Other The TSF shall be able to determine on receipt of user data, whether ***[selection: modification, deletion, insertion]*** has occurred.

FDP_UCT.1/Other Basic data exchange confidentiality(the script)

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control or
FDP.IFC.1 Subset information flow control]

FDP_UCT.1.1/Other The TSF shall enforce ***[assignment: Personal number card access control SFP]*** to be able to ***[selection: receive]*** user data in a manner protected from unauthorized disclosure.

FCS_COP.1/Other Cryptographic operation(the script)

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/Other The TSF shall perform ***[assignment:cryptgraphic operation shown in Table 6-9]*** in accordance with a specified cryptographic algorithm ***[assignment: cryptographic algorithm shown in Table 6-9]*** and cryptographic key sizes ***[assignment: cryptographic key sizes shown in Table 6-9]*** that meet the following: ***[assignment: Table 6-9].***

Table 6-9 Crypt algorithm

cryptographic algorithm	key length (bit)	standard	cryptographic operation
T-DES	192	NIST SP 800-67	Encryption/Decryption
RSA	1024	PKCS#1 v2.1	Signature Verification
SHA-1	-	FIPS PUB 180-2	Hash operation

FCS_CKM.4/Other Cryptographic key destruction(the Key)

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/Other The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***[assignment: rewriting by the key]*** that meet the following: ***[assignment: none]***.

6.2. Security assurance requirements

The security assurance requirement level is EAL4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2 and AVA_VAN.5.

6.3. Security requirements rationale

6.3.1. Objectives

Verifying the effectiveness of the Security requirements against Security Objectives.

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.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.Replay

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

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 3-7 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.

O.Secure_LOAD&INSTALL

In secure personalize mechanism, the integrity of the script are protected by the encryption. The key is generated in the External terminal, then it is imported to the TOE. FCS_COP.1/Other is respectively provided in the cryptographic operation. Access control related to Load the script to the TOE is provided in FDP_ACC.1/FDP_ACF.1. Inport of the key into the TOE is provided in FDP_ITC.1/Other. FDP_ITC.1/Other is provided in import of the key for Loding the script. Information flow control defined in FDP_IFC.1/FDP_IFF.1 is applied as only the valid the key is imported. FCS_CKM.4/Other provides the rule to destruct the key. Protection of the script is provided by FTP_ITC.1/Other. Integrity of the script is protected by FDP_UIT.1/Other. Confidentiality of the script is protected by FDP_UCT.1/Other. O.Secure_LOAD&INSTALL is achieved sufficiently with those SFRs.

6.3.2. Security Objectives and Security Functional Requirements

The relationship between Security Objectives and Security Functional Requirements are shown in Table 6-10 .
In Table 6-10 , the section numbers where rationale of such relationship is described are also shown.

Table 6-10 Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.RND	FCS_RNG.1/PN, FPT_PHP.3/PN	Section 6.3.1
O.I&A	FCS_CKM.4/PN, FDP_ACC.1/PN, FDP_ACF.1/PN, FDP_IFC.1/PN, FDP_IFF.1/PN, FDP_ITC.1(1) /PN, FDP_ITC.1(2) /PN, FIA_AFL.1/PN, FIA_UAU.4/PN, FIA_UAU.5/PN, FIA_UID.1/ PN, FCS_COP.1(4)/ PN, FCS_COP.1(5)/PN, FIA_UAU.1/PN, FMT_MTD.1/PN, FMT_SMF.1/ PN, FMT_SMR.1/ PN	Section 6.3.1
O.Access_control	FDP_ACC.1/ PN, FDP_ACF.1/ PN, FMT_MSA.3/PN, FDP_ITC.1(2)/PN, FMT_SMR.1/ PN	Section 6.3.1
O.Secure_messaging	FCS_CKM.4/ PN, FCS_COP.1(1)/ PN, FCS_COP.1(2)/PN, FCS_COP.1(3)/PN, FTP_ITC.1/PN, FDP_ACC.1/ PN, FDP_ACF.1/ PN, FDP_IFC.1/PN, FDP_IFF.1/PN, FDP_ITC.1(1)/PN,	Section 6.3.1

Security Objectives	Security Functional Requirements	Rationale
	FDP_ITC.1(2)/PN	
O.Delivery	FIA_UAU.5/PN, FIA_UID.1/ PN, FIA_UAU.1/PN	Section 6.3.1
O.Replay	FIA_UAU.4/PN	Section 6.3.1
O.Cryptography	FCS_CKM.4/PN, FCS_COP.1(1)/PN, FCS_COP.1(2)/PN, FCS_COP.1(3)/PN, FCS_COP.1(4)/PN, FCS_COP.1(5)/PN, FDP_ITC.1(1)/PN, FDP_ITC.1(2)/PN, FTP_ITC.1/PN, FDP_ACC.1/PN, FDP_ACF.1/PN, FDP_IFC.1/PN, FDP_IFF.1/PN	Section 6.3.1
O.Phys_Attack	FPT_PHP.3/PN, FPT_EMSEC.1/PN, FPT_FLS.1/Other, FPT_TST.1/Other	Section 6.3.1
O.RND	FCS_RNG.1/PN, FPT_PHP.3/PN	Section 6.3.1
O.Secure_LOAD&INSTALL	FDP_ITC.1/ Other, FDP_IFC.1/Other, FDP_IFF.1/Other, FTP_ITC.1/Other, FDP_UIT.1/Other, FDP_UCT.1/Other, FCS_COP.1/Other, FCS_CKM.4/Other, FDP_ACC.1/ PN、FDP_ACF.1/ PN	Section 6.3.1

The relationship between Security Objectives and Security Functional Requirements are shown in Table 6-11 .

Table 6-11 SFRs and Security Objectives

Security Functional Requirements	Security Objectives
FCS_CKM.4/ PN	O.Cryptography, O.Secure_messaging, O.I&A
FCS_COP.1(1)/ PN	O.Secure_messaging, O.I&A, O.Cryptography
FCS_COP.1(2)/PN	O.Secure_messaging, O.I&A, O.Cryptography
FCS_COP.1(3)/PN	O.Cryptography, O.Secure_messaging
FCS_COP.1(4)/PN	O.I&A, O.Cryptography
FCS_COP.1(5)/PN	O.I&A, O.Cryptography
FCS_RNG.1/PN	O.RND
FDP_ACC.1/ PN	O.Access_control, O.Secure_messaging, O.Secure_LOAD&INSTALL, O.I&A. Cryptography
FDP_ACF.1/ PN	O.Access_control, O.Secure_messaging, O.Secure_LOAD&INSTALL, O.I&A. Cryptography
FDP_IFC.1/PN	O.Secure_messaging, O.I&A. Cryptography
FDP_IFF.1/PN	O.Secure_messaging, O.I&A. Cryptography
FDP_ITC.1(1)/PN	O.Secure_messaging, O.Cryptography, O.I&A
FDP_ITC.1(2)/PN	O.Access_control, O.Secure_messaging, O.Cryptography, O.I&A
FIA_AFL.1/PN	O.I&A
FIA_UAU.1/PN	O.I&A, O.Delivery
FIA_UAU.4/PN	O.I&A, O.Replay
FIA_UAU.5/PN	O.I&A, O.Delivery
FIA_UID.1/ PN	O.I&A, O.Delivery
FMT_MSA.3/PN	O.Access_control
FMT_MTD.1/PN	O.I&A
FMT_SMF.1/ PN	O.I&A, O.Access_control
FMT_SMR.1/ PN	O.I&A, O.Access_control
FPT_PHP.3/PN	O.Phys_Attack, O.RND
FTP_ITC.1/PN	O.Secure_messaging, O.Cryptography
FPT_FLS.1/Other	O.RND, O.Phys_Attack
FPT_TST.1/Other	O.Phys_Attack
FPT_EMSEC.1/Other	O.Phys_Attack
FDP_ITC.1/ Other	O.Secure_LOAD&INSTALL

Security Functional Requirements	Security Objectives
FDP_IFC.1/Other	O.Secure_LOAD&INSTALL
FDP_IFF.1/Other	O.Secure_LOAD&INSTALL
FTP_ITC.1/Other	O.Secure_LOAD&INSTALL
FDP_UIT.1/Other	O.Secure_LOAD&INSTALL
FDP_UCT.1/Other	O.Secure_LOAD&INSTALL
FCS_COP.1/Other	O.Secure_LOAD&INSTALL
FCS_CKM.4/Other	O.Secure_LOAD&INSTALL

6.3.3. SFRs dependencies

Table 6-12 shows the dependency provided in CC which is to be supported by the Security Functional Requirements as well as the dependencies supported or not supported by the TOE. The indication "-" in the table means no dependency.

For those requirements whose dependency is not supported, the rationales of the exclusion of such dependency are described below.

Table 6-12 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.4/PN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1(1)/PN FDP_ITC.1(2)/PN
FCS_COP.1(1)/PN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1(1)/PN FDP_ITC.1(2)/PN FCS_CKM.4/PN
FCS_COP.1(2)/PN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1(1)/PN FCS_CKM.4/PN
FCS_COP.1(3)/PN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1(1)/PN FDP_ITC.1(2)/PN FCS_CKM.4/PN
FCS_COP.1(4)/PN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1(1)/PN FDP_ITC.1(2)/PN FCS_CKM.4/PN
FCS_COP.1(5)/PN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	Dependency is not satisfied (1)
FCS_RNG.1/PN	No dependencies	-
FDP_ACC.1/PN	(FDP_ACF.1)	FDP_ACF.1/PN
FDP_ACF.1/PN	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/PN FMT_MSA.3/PN Dependency is not satisfied (4)
FDP_IFC.1/PN	(FDP_IFF.1)	FDP_IFF.1/PN

Requirements	CC Dependencies	Satisfied Dependencies
FDP_IFF.1/PN	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/PN Dependency is not satisfied (3)
FDP_ITC.1(1)/PN	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3	FDP_IFC.1/PN, Dependency is not satisfied (3)
FDP_ITC.1(2)/PN	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3	FDP_ACC.1/PN, Dependency is not satisfied (2)
FIA_AFL.1/PN	FIA_UAU.1	FIA_UAU.1/PN
FIA_UAU.1/PN	FIA_UID.1	FIA_UID.1/ PN
FIA_UAU.4/PN	No dependencies	–
FIA_UAU.5/PN	No dependencies	–
FIA_UID.1/PN	No dependencies	–
FMT_MSA.3/PN	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1/PN Dependency is not satisfied (4)
FMT_MTD.1/PN	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1/ PN, FMT_SMF.1/ PN
FMT_SMF.1/PN	No dependencies	–
FMT_SMR.1/PN	(FIA_UID.1)	FIA_UID.1/PN
FPT_PHP.3/PN	No dependencies	–
FTP_ITC.1/PN	No dependencies	–
FPT_FLS.1/Other	No dependencies	–
FPT_TST.1/Other	No dependencies	–
FPT_EMSEC/Other	No dependencies	–
FDP_ITC.1/ Other	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3	FDP_IFC.1/Other
FDP_IFC.1/Other	(FDP_IFF.1)	FDP_IFF.1/Other
FDP_IFF.1/Other	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Other Dependency is not satisfied (5)
FTP_ITC.1/Other	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3	FDP_ACC.1/PN FMT_MSA.3/PN
FDP_UIT.1/Other	(FDP_ACC.1 or FDP_IFC.1) (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/PN FTP_ITC.1/Other
FDP_UCT.1/Other	(FTP_ITC.1 or FTP_TRP.1) (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/Other FDP_ACC.1/PN
FCS_COP.1/Other	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FTP_ITC.1/Other FCS_CKM.4/Other
FCS_CKM.4/Other	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FTP_ITC.1/Other

Rationale for the exclusion of dependencies

(1) This SFR prescribes only hash operation. Cryptographic key is not used. Therefore, Import, generation or destruction of keys is not necessary.

(2) FMT_MSA.3 is not applied, as all objects storing user data are created in the development environment.
For JOUREI-AP(any APs based on ordinances of local governments) and SSD, FMT_MSA.3 satisfied the dependency.
(3) FMT_MSA.3 is not applied as information (a session key) is created at the external terminal.
(4) The objects managed by FMT_MSA.3 are JOUREI-AP(any APs based on ordinances of local governments) and SSD. Their security attributes are not changed once after having been set. Accordingly, FMT_MSA.1 is not applied.
For any APs based on ordinances of local governments, FMT_MSA.3 is applied.
(5)As the target information (the key) of this SFR is generated in the External terminal, FMT_MSA.3 is not applied nor is satisfaction of dependency.

6.3.4. SARs dependencies

Table 6-13 shows the dependency provided in CC which is to be supported by the Security Assurance Requirements as well as the dependencies supported or not supported by the TOE. The indication "-" in the table means no dependency.

Table 6-13 SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.1
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.1) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.4)	ADV_FSP.5
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No dependencies	-
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No dependencies	-
ALC_DEL.1	No dependencies	-
ALC_DVS.2	No dependencies	-
ALC_LCD.1	No dependencies	-
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies	-
ASE_INT.1	No dependencies	-
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies	-
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and	ADV_ARC.1, ADV_TDS.4,

Requirements	CC Dependencies	Satisfied Dependencies
	(ATE_FUN.1)	ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

6.3.5. Rationale for the Security Assurance Requirements

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 of EAL4 are satisfied.

7. TOE summary specification

In this chapter, the security functions of TOE are provided.

7.1. Security Functions and Security Functional Requirements

This section presents the compliance to the security functional requirements by describing the TOE security function summary specifications. The Table 7-1 shows the relationship between the security functional requirements and the security functions. The indication "*" appearing at the intersection of the security function and security functional requirement shows the valid combination of specific security requirement and a security function.

Table 7-1 Security Functions and Security Functional Requirements

Security Functional Requirements \ Security Functions	7.1.1 SF.Init	7.1.2 SF.Rollback	7.1.3 SF.Crypt	7.1.4 SF.SecureMessaging	7.1.5 SF.KeyManager	7.1.6 SF.FileManager	7.1.7 SF.LifecycleManager	7.1.8 SF.MemoryManager	7.1.9 SF.DomainSeparation	7.1.10 SF.PrivilegeManager	7.1.11 SF.Authentication	7.1.12 SF.AccessControl	7.1.13 SF.Supervisor	7.1.14 SF.CmdIap	7.1.15 SF.CmdCm	7.1.16 SF.CmdJcd	7.1.17 SF.PhysicalTamper
FCS_CKM.4/PN					*	*											
FCS_COP.1(1)/PN			*														
FCS_COP.1(2)/PN			*														
FCS_COP.1(3)/PN			*														
FCS_COP.1(4)/PN			*														
FCS_COP.1(5)/PN			*														
FCS_RND.1/PN			*														*
FDP_ACC.1/PN							*					*					
FDP_ACF.1/PN							*					*					
FDP_IFC.1/PN			*		*										*	*	
FDP_IFF.1/PN			*		*										*	*	
FDP_ITC.1(1)/PN					*										*	*	
FDP_ITC.1(2)/PN												*					
FIA_AFL.1/PN											*						
FIA_UAU.1/PN	*								*								
FIA_UAU.4/PN											*						
FIA_UAU.5/PN											*						
FIA_UID.1/PN	*								*								
FMT_MSA.3/PN																*	
FMT_MTD.1/PN												*					
FMT_SMF.1/PN									*							*	
FMT_SMR.1/PN									*							*	
FTP_ITC.1/PN				*													
FPT_PHP.3/PN	*		*										*				*
FPT_FLS.1/Other	*		*														*
FPT_TST.1/Other	*																*
FPT_EMSEC/Other			*														*

Security Functions / Security Functional Requirements	7.1.1 SF.Init	7.1.2 SF.Rollback	7.1.3 SF.Crypt	7.1.4 SF.SecureMessaging	7.1.5 SF.KeyManager	7.1.6 SF.FileManager	7.1.7 SF.LifecycleManager	7.1.8 SF.MemoryManager	7.1.9 SF.DomainSeparation	7.1.10 SF.PrivilegeManager	7.1.11 SF.Authentication	7.1.12 SF.AccessControl	7.1.13 SF.Supervisor	7.1.14 SF.CmdIap	7.1.15 SF.CmdCm	7.1.16 SF.CmdJcd	7.1.17 SF.PhysicalTamper
FDP_ITC.1/ Other														*			
FDP_IFC.1/Other			*											*			
FDP_IFF.1/Other			*											*			
FTP_ITC.1/Other									*								
FDP_UIT.1/Other			*						*								
FDP_UCT.1/Other			*						*								
FCS_COP.1/Other			*														
FCS_CKM.4/Other														*			

The summary specification of TOE security functions (TSF) is described below.

7.1.1. SF.Init

The function of SF.Init performs the initialization..

7.1.2. SF.Rollback

The function of SF.Rollback performs to rollback data.

7.1.3. SF.Crypt

The function of SF.Crypt performs cryptographic operations.

7.1.4. SF.SecureMessaging

The function of SF.SecureMessaging performs the secure messaging..

7.1.5. SF.KeyManager

The function of SF.KeyManager manages a key data.

7.1.6. SF.FileManager

The function of SF.FileManager manages data files.

7.1.7. SF.LifecycleManager

The function of SF.LifecycleManager manages life cycle for card.

7.1.8. SF.MemoryManager

The function of SF.MemoryManager ensures the confidentiality.

7.1.9. SF.DomainSeparation

The function of SF.DomainSeparation divides the memory into multiple segments and manages.

7.1.10. SF.PrivilegeManager

The function of SF.PrivilegeManager manages privilege information.

7.1.11. SF.Authentication

The function of SF.Authentication implements external authentication.

7.1.12. SF.AccessControl

The function of SF.AccessControl performs access control.

7.1.13. SF.Supervisor

The function of SF.Supervisor manages the privilege of segment.

7.1.14. SF.CmdIap

The function of SF.CmdIap is to implement IAP command function to perform initial card issuance.

7.1.15. SF.CmdCm

The function of SF.CmdCM is to implement CM command function used in Operation Mode.

7.1.16. SF.CmdJcd

The function of SF.CmdJCD is to implement AP command function used in Operation Mode.

7.1.17. SF.PhysicalTamper

The function of SF.PhysicalTamper averts attacks trying to disclose confidential information with security IC.

Application note:

Description of this function is described in IC chip's ST[STSTM].

8. References

In this chapter, terms used in this ST and references are listed

8.1. Terms

Table 8-1 Terms

Terms	Definition
ADV	Development class
AGD	Guidance Documents class
ALC	Life-Cycle Support class
API	Application Programming Interface
ATE	Tests class
AVA	Vulnerability Assessment class
CC	Common Criteria
CCRA	The Common Criteria Recognition Arrangement
CCS	Cryptographic Checksum Message Authentication Code (MAC) provided in secure messaging for message Authentication
CM	Card Manager which manages single Issuer Security Domain (ISD) and multiple Supplementary Security Domain (SSD).
CRC	Cyclic Redundancy Check An error detection mechanism to ensure that there are no errors in the data transmission
Demonstrable conformance	The relation between ST and PP with which ST provides the solution for the security issues in PP in general.
DPA	Differential Power Analysis A very strong power analysis attack based on a statistical method to classify traces of power consumed during several algorithm runs.
EAL	Evaluation Assurance Level
ELF	(1) Executable Load Files (GP term) (2) ELF(Executable and Linked Format) is the file format for an object generated by a compiler and a library-linked executable file. The format is widely adopted as a successor of a.out format and COFF.
EMA	ElectroMagnetic Analysis Electromagnetic Analysis (EMA) attacks measure electromagnetic emissions from an IC during its operation and inferences to the data processed knowing such magnetic emissions is related to the logical value or the content of the processing.
fault injection	Fault injection is the attack dealing with the insertion or simulation of faults during the operation of Smart Card in order to infer the cryptographic key. Sometimes, such insertion of faults could affect destructive damage.
Global Platform	Global Platform (GP) is the international smart card association which was established in 1999 for the Open Platform technology developed by VISA and others and is responsible for the multi application Smart Card management system.
IAP	Initialize AP.Initializing the smart card.
invasive attacks	Invasive attacks start with the removal of the chip package. The direct access to the chip allows chip research or chip operation to steal private key.
ISD	ISD(Issuer Security Domain) ISD is an On-Card Entity which controls Issuer Security Domain or provides supports to security and communication request from the Card Manager.

Terms	Definition
J-LIS	Japan Agency for Local Authority Information Systems
MF	Master File
MPU	Memory Protection Unit The memory protection function provided by ST23R160
perturbation attacks	Perturbation attacks change the normal behavior of an IC under the condition outside specification (voltage, frequency, temperature etc.) in order to create an exploitable error in the operation of a TOE.
physical manipulation	A kind of attack which destroys or manipulates the specific circuit (e.g. sensor circuit) on an IC chip.
PP	Protection Profile A document used as part of the certification process according to the Common Criteria (CC). A security requirement specification for security. The security description described in it is independent from implementation and satisfies user's requirements.
probing	An invasive attack to read signals (information) by establish electrical contact with on-chip bus lines without damaging them using micro-prober etc
RNG	Random Number Generator
SFR	Security Functional Requirement
SPA	Simple Powering Analysis Simple power analysis is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device in order to extract cryptographic keys and other secret information from the device.
SSD	Supplementary Security Domain. Security Domains other than Issuer Security Domain.
ST	Security Target
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
TSF data	The data generated by TOE or those generated in connection with TOE, which may affect the behaviors of TOE.
Integer data	The data whose integrity must be fully protected
Object	The passively acting entity which receives or stores information and is the object of the operations by a subject.
Card AP	The processing definitions and information required for using card application services.
Card Holder	Card user
Confidential data	The data which needs to be kept confidential
Subject	The actively acting entity which performs operation on the Object.
Brute Force Attack	Brute Force Attack A strategy used to break the encryption of data which involves traversing the search space of possible keys until the correct key is found.
User Data	The data generated by a user or those generated in connection with a user, which may affect the behaviors of TSF.

8.2. Reference Materials

Table 8-2 Reference Materials

Identifier	Document Name
[CC1]	Common Criteria for Information Technology Security Evaluation Version 3.1, Part 1: Introduction and general model Revision 3 (CCMB-2009-07-001)
[CC2]	Common Criteria for Information Technology Security Evaluation Version 3.1, Part 2:

Identifier	Document Name
	Introduction and general model Revision 3 (CCMB-2009-07-002)
[CC3]	Common Criteria for Information Technology Security Evaluation Version 3.1, Part 3: Introduction and general model Revision 3 (CCMB-2009-07-003)
[CEM]	Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CCMB-2009-07-004)
[PP-PN]	Personal Number card protection profile (Apr, 2014,ver.1.00)
[PF-spec]	Personal Number card specification (Dec, 2013,ver.1.00)
[BANGO-spec]	BANGO-AP(Input Support AP for the personal information printed on the card) specification(Dec, 2013, ver.1.00)
[JUKI-spec]	UKI-AP(Basic Resident Registration AP)(Dec, 2013, ver.1.00)
[KENMEN-spec]	KENMEN-AP(AP for digitization of the personal information printed on the card)(Dec, 2013, ver.1.00)
[JPKI-spec]	JPKI-AP(Public ID authentication AP)(Dec, 2013,ver.1.00)
[PP0035]	Security IC Platform Protection Profile -BSI-PP-0035- Version 1.0, 15.06.2007
[CRYPTO]	MécaniSMes cryptographiques. Règles et recommendations concernant le choix et le dimensionnement deSMécaniSMes cryptographiques. Version 1.11, 24 October 2008, ANSSI.
[STSTM]	ST23YR80A Security Target, Rev 01.00, February 2009
[REQ200]	New Smart Card Definition on technical requirement, January 31, 2011, Ver.2.00
[CCDB1]	Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1 (CCDB-2007-09-001)
[CCDB2]	Application of Attack Potential to Smartcards, May 2013, Version 2.9 (CCDB-2013-05-002)
[GP]	GlobalPlatform Card Specification Ver.2.2 March 2006
[ISO14443]	ISO/IEC 14443-3(2001) Identification cards — Contactless integrated circuit(s) cards — Proximity Cards — Part 3: Initialization and anti-collision ISO/IEC 14443-4(2001) Identification cards — Contactless integrated circuit(s) cards — Proximity cards —Part 4: Transmission protocol