Basic Resident Registration Card Version 2 Embedded Software Protection Profile

Version 1.00

2011-01-21

Local Authorities Systems Development Center

Electronic Commerce Security Technology Laboratory Inc.

Certification number: C0284

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

Foreword

This protection profile “Basic Resident Registration Card V2 embedded software Protection Profile” was developed for the new generation Basic Resident Registration Card. Security and usability were improved. The Protection Profile (hereinafter referred as “the PP”) is issued by the Local Authorities Systems Development Center (LASDEC), Japan.

For Readers

The Basic Resident Registration Card V2

The Basic Resident Registration Card (hereinafter referred as “BRR Card”) is an IC card used for the Basic Resident Registration Network System. It is a multi-purpose public IC card not only for electronic identification but also for a variety of applications offered by local governments.

The current BRR Card has been distributed from 2003. There are two types: the type I card and the type II card. And the next generation BRR Card becomes under the necessity to address the changes in the operational environment; the revision of the Basic Resident Registration Law (2009/7/15), continuous using of BRR Card on moving to the other local government territory, the reinforcement of the cryptographic algorithms for TYPE I and TYPE II card and the introduction of extended administrative services. The new specification of the Basic Resident Registration Card was developed and provided as the Basic Resident Registration Card Version 2 (V2).

Security requirements

This PP provides security requirements to the embedded software conforming with BRR Card V2. IC cards for BRR Card V2 must be validated by the Common Criteria that is international standard of security evaluation. The developer of BRR card shall supply the product satisfying the requirements provided in this PP.

Security evaluation

BRR Card is a product composed of IC chip, wireless antenna (for contactless communication) and embedded software. Those components are unified into a plastic card. The security evaluation of BRR Card would be done for the entire product.

There are two cases for the evaluation of the entire product. They are that the hardware part of the product was evaluated already, and that the hardware part of the product was not evaluated yet. In case of the former, the evaluation method called composite evaluation can be applied. it is explained at the following section “Composite evaluation”.

In case of the latter, the developer has to make a new ST for the entire product. The ST should cover all security requirements for BRR Card. Since this PP provides only security requirements relating the software of BRR Card, the security requirements not covered by this PP need to be added.

The ST for the product must meet all of the requirements in this PP. In addition, the developer has to include any additional security requirements addressed by the hardware and the combination of the hardware and the software as well. The evaluation assurance level for the ST shall be the same or over than the evaluation level of this PP.

For the evaluation of the entire BRR Card product including hardware, the ST authors of the TOE should take any security risks relating the hardware into consideration. Those risks are attacks using physical properties of the hardware. It obstructs security functions of the software. For example, disclosing of a secret key by monitoring variation of power consumption of the IC chip, bypassing of the software security function to access a secret data by manipulating physically the inside of the IC chip. The information assets in BRR Card must be protected from those attacks.

Composite evaluation

Composite evaluation is applicable for the entire BRR Card. For example, the hardware of the IC card (or IC chip) can be evaluated in advance without embedded software. It is capable of reduction of the overlapped evaluation process.

Composite evaluation will be performed according to CCRA (The Common Criteria Recognition Arrangement) supporting documents related to smart cards. The evaluation result will be effective on all schemes joining CCRA. Procedures of composite evaluation are shown below.

The security requirements for the entire BRR Card are addressed as follows:

(a) addresses by the security functionality of the hardware part

(b) addresses by the security functionality of the software part

(c) addresses by the security functionality of combination of the hardware and the software

The hardware part of (a) was evaluated already. The security functionalities corresponding to (b) and (c) have to be evaluated for the entire BRR Card. The security functionalities corresponding to (b) are provided by this PP. The security functionalities of (c) are derived newly from the combination of the hardware and the software.

The case of (c) is that the attacks to physical properties of the TOE are countered by the security functionalities of the combination of the hardware and the software. For example, disclosure of a secret key with power consumption analysis are addressed by the countermeasure that reduces the variation of power consumption by devising software process of the cryptographic algorithm. The other example is the hybrid random number generation method that is the combination of physical generation and software deterministic generation. They are dependent on the specification of the IC chip and the implementation of the software platform. The developers of BRR Card may select their own measures.

On composite evaluation, the ST and the ETR of the platform TOE (IC card hardware) are required. If the evaluation of the IC card hardware and the composite evaluation for the entire IC card are performed in the different CC schemes, the sponsor of the composite evaluation will have to make the ETR and the ST of the IC card hardware available. Cooperation of the certification body and the evaluation facility relating to those documentation will be coordinated.

Information concerning composite evaluation can be obtained from the supporting documents from CCRA. Physical attacks for IC cards are presented on those documents.

Contents

1 PP introduction

1.1 PP reference

Title:	Basic Resident Registration Card V2 Embedded Software Protection Profile
Version number:	1.00
Publication date:	2011-01-21
Sponsor:	Local Authorities Systems Development Center
Author:	Electronic Commerce Security Technology Laboratory Inc.
Certification ID:	C0284
Key words:	IC card, Smart card, Basic Resident Registration, Basic Resident Registration Network System, Basic Resident Registration Card

1.2 TOE overview

1.2.1 TOE type

The TOE is the embedded software for an IC card. The TOE consists of the platform software and the proprietary application program BRR-AP (Basic Resident Registration AP).

1.2.2 TOE usage and major security features

The TOE is the software embedded in BRR Card (Basic Resident Registration Card). BRR Card is used in the system called “The Basic Resident Registration Network System” and it is an elementary component of the system. Each local government delivers BRR Cards to the resident citizens and makes available the administrative services of the Basic Resident Registration Network System with BRR Cards

The TOE consists of BRR-AP and the platform software. BRR-AP is the essential application of BRR Card. It is used commonly on every local government. Any other APs, called “additional APs” in this PP, can be added by each local government. Additional APs are excluded from the scope of the TOE.

Examples of additional APs are “digitization of the personal information printed on the card”, “public ID authentication”, or any APs based on ordinances of local governments. The other APs may be installed by the BRR Card issuer. Installation of additional APs may be done on the development phase or under the control of the issuer after delivery. Additional APs must be installed to the TOE in secure environment managed by authorized administrators. Users without authorization, including card holders, are not allowed to install any programs or data to the TOE.

The TOE has security functionality to protect user data. Major security features of the TOE are shown below.

- Secure communication

  Protects communication channel between BRR Card and the external device. Each of the platform and BRR-AP has its own secure communication function respectively.

- Mutual authentication

  Each of BRR Card and the external device authenticates one another (mutual authentication). Furthermore, each of the platform and BRR-AP independently authenticates the external device. NOTE: Authentication by the external device is not security functionality of the TOE.

- Card holder authentication

  BRR-AP authenticates the card holder. This function belongs to BRR-AP. Additional APs can not use this feature.

- Stored data protection

  Protects stored data within the TOE from illegal attacks. Each of the platform and BRR-AP has its own protection functionality for its own data.

The TOE runs on the IC chip embedded in BRR Card. The hardware, including the IC chip, is the IT environment on which the TOE relies, and is excluded from the TOE. The IT environment for the TOE includes the following.

- IC chip

  The IC chip on which the TOE runs. No specific IC chip is designated for BRR Card in this PP.

  [Note] On the evaluation for the entire BRR Card, the target of the evaluation will be supposed to include the software provided by this PP and also the hardware on which the software runs. An IC chip and an antenna are embedded together in a plastic card. The IC chip loads the software which meets the requirements of this PP.

  On the evaluation for the entire BRR Card, the composite evaluation may be applied. The hardware part is evaluated[1] independently in advance and the entire BRR Card, which

[1] “Security IC Platform Protection Profile Version 1.0 15.06.2007 BSI-PP-0035” receives wide recognition for the PP of IC chip hardware. It claims EAL4+ (augmented with ALC_DVS.2 and AVA_VAN.5). It is acceptable as the security requirements for the hardware part of BRR Card.

includes the software part, will be evaluated subsequently. On a composite evaluation for an IC card, the supporting documents[2] provided by CCRA are applied.

Evaluation assurance level required for BRR Card on the composite evaluation is identical to the evaluation assurance level provided in the PP. On the other hand, the evaluation assurance level required to hardware part of BRR Card is the same or over than the evaluation assurance level of the PP.

The whole of a product, which is composed of hardware and software may be evaluated as an independent evaluation (not composite evaluation). In that case, the CCRA supporting documents for IC card must be applied too, as the TOE includes an IC chip.

- Antenna

  An antenna is equipped for the contactless communication between BRR Card and the external device. The antenna and the IC chip are embedded in a plastic card together.

- Plastic card

  The IC chip and the antenna are embedded in the plastic card. The card has standard electric contact pads. The essential things for BRR Card are printed on the card.

1.2.3 TOE structure

Figure 1-1 shows the TOE structure. The TOE comprises two software parts, a platform and BRR-AP. BRR-AP (and also additional APs) runs on the platform.

The platform provides executing environment of APs. Each executing area of AP is separated from other APs to prevent mutual interferences. And also the executing area of the platform is separated from APs to prevent interferences from APs. As described in the previous chapter, BRR-AP is pre-installed on the platform and comprised in the TOE.

Figure 1-1 shows the TOE components: the platform and BRR-AP. Additional APs are also shown, though they are not common elements for all BRR Card and excluded from the TOE. Examples of additional APs are “digitization of the personal information printed on the card”, “public ID authentication”, or any APs based on ordinances of each local government.

[2] CCDB-2009-03-001: Application of Attack Potential to Smartcards, March 2009, Version 2.7 Revision 1

CCDB-2009-03-002: The Application of CC to Integrated Circuits, March 2009, Version 3.0 Revision 1

CCDB-2007-09-001: Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 Revision 1

The BRR Card issuers (the local governments) may install their own additional APs. Those APs may be installed in the development environment, or in the operational environment as well. Installation of APs in the operational environment is managed by the security functionality of the platform.

Every AP, BRR-AP or additional APs, runs as a process (the internal process of the TOE) of the platform. The TOE security functionality (TSF) comprises parts of the platform and BRR-AP (TSF is not shown in Figure 1-1). Although additional APs are excluded from the TOE, operations of them - install, delete, execute, abort, etc. - are also controlled by the TSF. The encompassed area with the TOE boundary in Figure 1-1 shows the area controlled by the TSF.

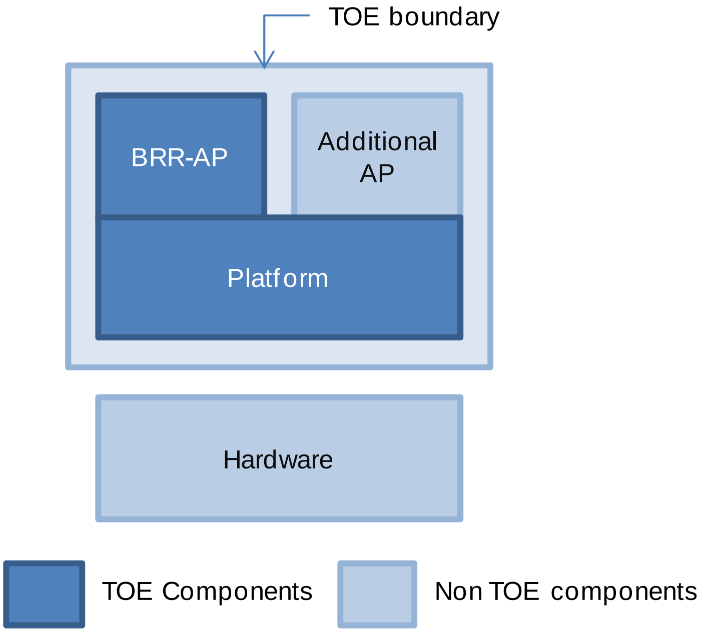

Figure 1-1 TOE structure

1.2.4 TOE life cycle model

The TOE lifecycle model is shown as follows. It presents an example of lifecycle, which helps understanding the TOE. There is no constraint for the actual development of the TOE. The PP/ST authors who refer this PP may define their own lifecycle models without regard to the description here.

Phase 1: IC chip (hardware) development

The developer develops the IC chip for the BRR Card. This phase includes development of photomasks and dedicated software/firmware. This PP does not include IC chip development in the scope of the evaluation. However, on the evaluation of whole BRR Card, this phase is encompassed as the development phase. The development environment security of this phase is required to counter to the high level attacks, the same level of attacks assumed in this PP.

The software installation to an IC chip is done in this phase or the phase 3. The software is developed in the phase 2.

In this phase, the development of the hardware may be done at multiple development sites. Design of hardware circuitry, design and production of the photomasks for the IC chip and the other development processes might be performed in the different development sites.

Phase 2: TOE development

The software (the platform and BRR-AP), which is the TOE of this PP, is developed. The development is done independently from the hardware development of the phase 1.

Phase 3: Card production

The TOE software is embedded in the IC chip (or it may be done in the phase 1). BRR Card is assembled with those components - IC chip including the TOE software, antenna and plastic card. Additional APs might be installed in this phase. This phase and the previous phases correspond to the development phase. Assembled BRR Cards are delivered to the issuers (local governments).

Phase 4: Card personalization

BRR Cards are issued to residents from the local government. On issuance of the card, the personal data of the card is specified. This procedure is called “personalization”. In the lifecycle model of this PP, the phases hereafter correspond to the operational phase. “The TOE user” in this phase is the staff of the BRR Card issuer. He/she is called “the administrator” in this PP.

Phase 5: Additional APs installation

Additional APs are installed to the BRR Cards delivered to the local government. They may be proprietary APs based on ordinances of the local government or the other APs. Additional APs are left the matter of discretion to each local government.

Phase 6: Use by a card holder

The card holder (the resident) can use services of the Basic Resident Registration Network System through the APs installed in BRR Card. The card holders are “general users” of the TOE, and distinguished from “administrative users” of the TOE.

BRR Card is a tool to use the Basic Resident Registration Network System. Illegal exploitation of BRR Card may cause risks to the Basic Resident Registration Network System. The security functionality of BRR Card should counter the threats for the Basic Resident Registration Network System.

2 Conformance claims

2.1 CC conformance claim

The PP claims conformance to CC V3.1 (CC in Japanese version released by JISEC):

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-002
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003

2.2 PP claim

The PP claims no conformance to the other PPs.

2.3 Package conformance

The PP claims package conformance to the assurance package EAL4 augmented.

Augmented assurance requirement is AVA_VAN.5.

2.4 Conformance rationale

There is no PP to which this PP claims conformance.

2.5 Conformance statement

The PP requires *demonstrable conformance* to PPs/STs claiming conformance to the PP.

3 Security problem definition

Security problems concerning the TOE are defined here. Security problems are described on three aspects: threats - countered by the TOE and/or its environment, organisational security policies - enforced by the TOE and/or its environment, and assumptions - made on the operational environment in order to be able to provide security functionality. These problems should be considered in the operational environment of the TOE and solved by the TOE and/or its environment.

Threats, organisational security policies, and assumptions are identified with initial letters “T.”, “P.”, or “A.” respectively. “Application notes” are appended at key points. They are described to give useful information to the readers and are not a portion of the security problem definitions.

3.1 Assets

The assets protected by the TOE security functionality (TSF) are the services of the Basic Resident Registration Network System and the data within the TOE. The user data within the TOE is the primary assets. For example, “BRR code” of BRR-AP is the user data. The user data of additional APs are not explicit assets to be protected, though the objects protected by the security functionality of the platform should be implicit assets of the TOE (See T.AP_abuse in 3.2). The objects protected by the security functionality of the additional AP itself are excluded from the assets of the TOE.

The TOE deals with variety of data excepting user data. Those data are used by the security functionality of the TOE (referred to “TSF data”), or the other management use. If TSF data is disclosed or modified, it may cause disclosure or modification of user data. Therefore, the TSF data is referred to the secondary assets, distinguished form the primary assets which are the essential protection object. Protection of the secondary assets is crucial. However, the TSF data is not described explicitly in the threats here, because it is derived secondarily to protect the user data.

3.2 Threats

Those threats shall be countered by the TOE, its operational environment or a combination of them.

T.Fraud

A BRR Card may be used by the other person (non-possessor of the card) to access services of the Basic Resident Registration Network System.

T.Illegal_attack

An attacker may disclose or modify data or programs in the TOE through the external interface of the TOE without valid authorization. External devices capable of communicating to the TOE is used to access the TOE. Not only regular external devices but irregular devices (ex. skimming tool) might be used for the attack. The TOE is accessed via the electric contact pads or the contactless communication interface of BRR Card.

[Application note 2]

This threat occurs in the operational environment where the TOE is under the control of the issuer or possessed by the card holder. “Modification of program” includes the attack that a program is installed by an unauthorized user.

Authorized users of the TOE are BRR Card holders and authorized persons who administrate and operate BRR Cards (the authorized person is referred to the administrator in this PP) in the local governments. A BRR Card holder is paired with his BRR Card (the TOE), whereas administrators administrate multiple TOEs.

T.AP_abuse

A user of an AP of the TOE may exploit the AP to disclose or modify user data managed by the other AP.

[Application note 3]

“AP” might be BRR-AP which is a part of the TOE or any additional AP outside of the TOE.

T.Eavesdrop

An attacker may interfere contactless communication between the TOE and the external device to disclose private information in communication data or to modify communication data.

T.Replay

An attacker may masquerade as the external device to disclose or modify internal data of the TOE. For masquerade, the attacker may monitor contactless communication between the TOE and the external device, record authentication procedures and replay the procedures.

3.3 Organisational security policies

The organisational security policies shall be enforced by the TOE or the environment of the TOE. The organisation referred in this PP is each of the local government which operates the Basic Resident Registration Network System.

P.Delivery

Internal data of BRR Card is protected from illegal access with an initial key and a transport key during delivery process from developers to issuers. Those keys are used by the TOE security functionality. The initial key protects the platform data and the transport key protects the BRR-AP data, respectively.

[Application note 4]

The TOE during delivery process should be protected by the delivery procedures instead of the security functionality of the TOE. However, the initial key and the transport key, they are belonged to security functionality of the TOE (the authentication mechanisms), are also involved in protecting the data during transport of the TOE. This security functionality is used to validate no security violation during transport of the TOE. And it is also effective in the operational environment as well to prevent illegal use of the TOE. The terms of initial key and transport key in this PP are referred to transport key as general terms for IC cards. P.Delivery is the organisational security policy applied when the TOE is under the control of the user (the local government). P.Delivery is not applicable to the TOE issued to BRR Card holders.

P.Cryptography

Cryptographic algorithms and keys shown in Table 3-1 are used for the cryptographic operation of the TOE. Those cryptographic algorithms can be used by the platform, BRR-AP (both are included in the TOE), or additional APs (non-TOE).

Cryptographic algorithms used by the TOE are separated to two groups. One is the pre-compromise-disposition group and another is the post-compromise-disposition group. The requirement for cryptographic algorithms depends on the entity: the platform, BRR-AP or additional APs. As the selection of cryptographic algorithms also depends on the specification of the system using BRR Card, the TOE has to be capable of providing any cryptographic algorithm required.

If a RSA cryptographic key is imported for the platform, the existing cryptographic key shall not be replaced with a shorter one.

The cryptographic algorithms used by BRR-AP are set as a group either the pre-compromise-disposition group or the post-compromise-disposition group. If the pre-compromise-disposition group was set in BRR Card, the TOE shall be capable to change the group to the post-compromise-disposition group by the administrators.

Table 3-1 Cryptographic algorithms and keys

Cryptographic algorithm	Key length(bit)	Standard	Cryptographic operation	Compromise disposition
T-DES	192	NIST SP 800-67	• encryption/decryption • MAC generation/valida-tion	pre-compromise-disposition
RSA	1024	PKCS#1 v2.1	• encryption/decryption • signature generation/vali-	

			dation	
SHA-1	-	FIPS PUB 180-2	hush operation	
AES	128	NIST FIPS PUB 197	• encryption/decryption • MAC generation/valida-tion	post-compromise-disposition
RSA	2048	PKCS#1 v2.1	• encryption/decryption • signature generation validation	
SHA-256	-	FIPS PUB 180-2	hush operation	

[Application note 5] Disposition for cryptographic algorithm compromise

The platform and BRR-AP are installed to all of BRR Card commonly. The cryptographic algorithms for BRR-AP are selected as follows.

Cryptographic algorithms classified as the “pre-compromise-disposition” group in Table 3-1 are being used in the previous version of BRR-AP. To address cryptographic algorithm compromise, the change of cryptographic algorithms to the “post-compromise-disposition” group is scheduled. The change will be enforced simultaneously in the whole of local governments, after all systems for BRR-AP are replaced to the systems adopting the post-compromise-disposition group. Until then, the pre-compromise-disposition group is being used for BRR-AP.

Developers of BRR Card (vendors) have to make the cryptographic algorithms group for BRR-AP changeable with the post-compromise-disposition group. If the TOE with the cryptographic algorithms of the pre-compromise-disposition group was delivered, change of the cryptographic algorithms to the post-compromise-disposition group may be necessary on issuing of BRR Card. This change must be practicable by the issuer. If the post-compromise-disposition group is installed for BRR-AP, the change of cryptographic algorithms for BRR-AP will be unnecessary.

Cryptographic algorithms for the platform and additional APs are independent from BRR-AP. Requirements to cryptographic algorithms of the platform and additional APs is independent of BRR-AP. Cryptographic algorithms of the platform have to deal with both of the pre-compromise-disposition group and the post-compromise-disposition group in Table 3-1. Additional APs may use the cryptographic function of the platform, though cryptographic keys should be managed by each AP.

The relationship between the cryptographic algorithms installed on the TOE and the scheme’s requirements is represented bellow.

Although CC excludes evaluation of Cryptographic algorithms, most CC evaluation/certification schemes consider that compromised cryptographic algorithms are inappropriate to be assessed secure. Each scheme has its own criterion for acceptance of cryptographic algorithms. The PP/ST authors should consult the certification body of the scheme about the treatment of cryptographic algorithms.

The cryptographic algorithms used by the TOE must counter to the assumed attacks. This PP assumes attacks with high level attack potential. The cryptographic algorithms incapable to counter high level attacks (i.e. compromised cryptographic algorithms) might not prevent violation of the security functionality of the TOE. If the pre-compromise-disposition cryptographic algorithms in this PP are considered to be inappropriate by the scheme, ST authors will have to claim in the PP/ST that the post-compromise-disposition group will meet the SFR of the TOE and that the pre-compromise disposition group will be necessary only to maintain interoperability with existent systems and will not counter high level attacks.

3.4 Assumptions

Assumptions here are made on the operational environment of the TOE in order to be able to provide security functionality.

A.PKI

The TOE is assumed to be used in the PKI system in which the public cryptosystem keys (a pair of the public key and the secret key) are assured to be valid.

A.Administrator

The administrators who set, change or delete data or APs within the TOE are assumed to operate correctly the TOE based on their authorization.

A.AP

Any additional APs are assumed not including malicious codes in the programs and not invading resources of the platform or the other APs in the TOE.

4 Security Objectives

Security objectives for the security problem definition shown in chapter 3 are described here. Security objectives for the TOE and for the environment of the TOE are shown in 4.1 and 4.2 respectively. Rationale demonstrating correctness of the objectives is shown in 4.3.

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

4.1 Security objectives for the TOE

The threats and the organisational security policies defined in the chapter 3 "security problem definition" are addressed by the TOE as follows.

O.I&A

The TOE shall identify and authenticate a user before providing services through the external interfaces of the TOE. The services shall be provided to the user only when the identification and the authentication are completed successfully. The users of the TOE are BRR Card issuers, BRR Card users (holders) and the external devices. The services shall be provided only for the users authenticated, and restricted according to authorization of the user.

The TOE uses the authentication mechanisms shown in Table 4-1 to validate authenticity of the user. If the authentication mechanism is based on cryptographic algorithm, it will use RSA public key cryptosystem in Table 4-1. One of hush algorithms in Table 3-1 will be used for the authentication procedures with RSA algorithm.

The security objective relating to cryptographic keys is described in O.Cryptography. See the application note of Table 3-1 for use of cryptographic keys.

Table 4-1 Authentication mechanisms

Authentication mechanisms	Rules for authentication mechanisms	Use
Authentication of BRR Card issuer (the platform)	Verification with Initial Key (key length is specified in the procurement specification documents)	Authentication of BRR Card issuer for the platform
Authentication of BRR Card issuer (BRR-AP)	Verification with transport key (8-byte)	Authentication of BRR Card issuer for BRR-AP
Authentication of user (BRR Card holder)	Verification with 4-digit PIN (16-byte temporary password is set for verification before issue; it is replaced with 4-digit PIN of the user on BRR	User authentication by BRR-AP ・Authentication of the card holder

	Card issue)	・Protection of illegal use before issue
Authentication of the external device (the platform)	Authentication with public key cryptosystem	The external device authentication by the platform
Authentication of the external device (BRR-AP)	Authentication with public key cryptosystem	The external device authentication by BRR-AP

O.Access_control

Only authorized users shall be allowed to access to user data in the TOE. Unauthorized access to user data shall be prohibited.

O.Secure_messaging

The TOE shall protect communication data (secure messaging) with the symmetric key cryptographic algorithm (T-DES or AES) shown in Table 3-1 to prevent disclosure of personal information in communication data or modification of communication data, by a third party attacker eavesdropping contactless communication data between the TOE and the external device. The secure messaging for the platform protects communication data with encryption and MAC. The secure messaging for BRR-AP protects communication data with encryption. RSA algorithm shown in Table 3-1 is used to exchange a cryptographic key and/or a MAC key. SHA hush operation shown in Table 3-1 is used for validation of signature on a session establishment procedures.

O.Replay

The TOE shall not reuse the same authentication data for the authentication procedures of the external device to prevent replay attack.

O.Delivery

The TOE shall prevent any illegal access to the internal data during delivery from developers to issuers (local governments) with the initial key and the transport key. The initial key protects the platform and the transport key protects BRR-AP respectively.

O.Cryptography

The TOE shall provide capability to select cryptographic algorithms shown in Table 3-1 to the platform, BRR-AP or additional APs.

The TOE shall not replace the existent RSA key with a new key shorter than the old key when the key is imported to the platform.

In case that the pre-compromise-disposition group of the cryptographic algorithms for BRR-AP was installed on BRR Card delivered, the TOE shall provide capability to the administrators of changing the group of cryptographic algorithms to the post-promise-disposition group.

4.2 Security objectives for the environment

The security objectives to be addressed by the operating environment of the TOE to solve the problems relating to the threats and the organisational security policies defined as the security problems are described. Every security objective described here is derived from the assumptions.

OE.PKI

Persons in charge of administration and operation of BRR Card in a local government provide the PKI system that assures validity of the keys installed in the TOE for the public key cryptosystem (a pair of the public key and the secret key) in the operational environment of the TOE.

OE.Administrator

The person in charge of administration and operation of BRR Card in the local government assigns the administrators capable of correct operation of the TOE - setting, changing or deleting of data or APs of the TOE - and reliable not doing adverse actions to the assets of the TOE, and authorizes them to operate the TOE.

OE.AP

On installation of an additional AP to the TOE, the person in charge of administration and operation of BRR Card or the administrator of the TOEs in the local government confirms that the additional AP was developed by the reliable developer who had sufficient experience and knowledge concerning the AP, so that non-reliable AP will not introduced.

4.3 Security objectives rationale

In this chapter, the rationale that each security objective described above is effective for the items of the security problem definitions. In 4.3.1, it is demonstrated that the security objectives for the TOE or the environment can be traced back to one or more security problem definitions. In 4.3.2, it is demonstrated that each security problem is addressed effectively by the corresponding security objectives.

4.3.1 Correspondence between security problem definitions and security objectives

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

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

Security objectives Security problem definition	O.I&A	O.Access_control	O.Secure_messaging	O.Replay	O.Delivery	O.Cryptography	OE.PKI	OE.Administrator	OE.AP
T.Fraud	x								
T.Illegal_attack	x	x							
T.AP_abuse		x							
T.Eavesdrop			x						
T.Replay				x					
P.Delivery	x				x				
P.Cryptography	x		x			x			
A.PKI							x		
A.Administrator								x	
A.AP									x

4.3.2 Sufficiency of security objectives

It is demonstrated that the security objectives address sufficiently the whole of security problems: threats, organisational security policies and assumptions.

T.Fraud

O.I&A requires the user of the TOE to be identified and authenticated so that only the true BRR Card holder can use services of the Basic Resident Registration Network System with his/her BRR Card. O.I&A diminishes sufficiently the threat of T.Fraud.

T.Illegal_attack

O.I&A requires the user of the TOE to be identified and authenticated so that non-authenticated user can use no services mediated by the TSF. O.Access_control restricts the behaviour of the user accessing data or resources of the TOE according to his authorization. So that unauthorized user is not able to disclose or modify any data in the TOE. Those security objectives diminish sufficiently the threat of T.Illegal_attack.

T.AP_abuse

O.Access_control prohibits the subject on behalf of the user of the AP to access any objects belonging to the other APs. O.Access_control diminishes sufficiently the threat of T.AP_abuse.

T.Eavesdrop

O.Secure_messaging protects contactless communication data between the TOE and the external device from being eavesdropped or modified. On secure messaging for the platform, encryption and MAC of communication data diminish sufficiently the threat of T.Eavesdrop. On secure messaging for BRR-AP, encryption of communication data diminishes sufficiently the threat of disclosure. Moreover, if encrypted data of BRR-AP is modified, the modified data will not be decrypted as meaningful document data. It mitigates sufficiently the effects of modification.

T.Replay

If the attacker monitors and records communication for authentication procedures of the external device and attempts to get successful authentication from the TOE by masquerading as the external device, the authentication data monitored will be voided as shown in O.Rplay so that the attacker will not be able to succeed in authentication. O.Replay removes the threat of masquerading with replaying the same authentication procedures shown in T.Replay.

P.Delivery

O.Delivery provides protection measures to counter the attacks during delivery. The security during delivery should be the object of assurance requirement. However, the TOE uses the protection mechanism using the initial key and the transport key, which are specified by the issuer, and the mechanism is applicable to both of the delivery process and the controlled environment of the issuer. Then it is included in the security objectives for the TOE. O.I&A provides authentication properties concerning the initial key and the transport key and is effective to implement protection measures. Those security objectives are suitable to enforce P.Delivery.

P.Cryptography

O.Cryptography covers the policies concerning cryptographic algorithms provided in P.Cryptography. O.I&A and O.Secure_messaging require use of the cryptographic algorithms provided in P.Cryptography. Those security objectives are suitable to enforce P.Cryptography.

A.PKI

OE.PKI addresses directly to A.PKI. This objective is suitable to uphold A.PKI.

A.Administrator

OE.Administrator indicates that the assigned and authorized person in charge of setting, changing or deleting of data or APs of the TOE is capable of doing correct operations of the TOE and reliable not doing adverse actions to the assets of the TOE. This objective is suitable to uphold A.Administrator.

A.AP

OE.AP requires that the developer of the additional AP should be confirmed to be reliable that the additional AP never contains any illegal code nor invades the TOE resources used by the platform and the other APs. OE.AP is suitable to uphold A.AP.

5 Extended components definition

This PP defines no extended components.

6 Security requirements

6.1 Security functional requirements

All SFRs identified in this PP are defined using the components from CC part 2. The SFRs are shown in the list of Table 6-1

Table 6-1 SFR list

Section	Identification	
6.1.1	FCS_CKM.4	Cryptographic key destruction
6.1.2	FCS_COP.1	Cryptographic operation
6.1.3	FDP_ACC.1	Subset access control
6.1.4	FDP_ACF.1	Security attribute based access control
6.1.5	FDP_ITC.1	Import of user data without security attributes
6.1.6	FIA_AFL.1(1)	Authentication failure handling(1)
6.1.7	FIA_AFL.1(2)	Authentication failure handling(2)
6.1.8	FIA_AFL.1(3)	Authentication failure handling(3)
6.1.9	FIA_UAU.1	Timing of authentication
6.1.10	FIA_UAU.4	Single-use authentication mechanisms
6.1.11	FIA_UAU.5	Multiple authentication mechanisms
6.1.12	FIA_UID.1	Timing of identification
6.1.13	FMT_MOF.1	Management of security functions behaviour
6.1.14	FMT_MSA.3	Static attribute initialisation
6.1.15	FMT_MTD.1	Management of TSF data
6.1.16	FMT_SMF.1	Specification of Management Functions
6.1.17	FMT_SMR.1	Security roles
6.1.18	FTP_ITC.1	Inter-TSF trusted channel

Some SFRs are tailored through operations. The notation for operations used in this PP is shown below:

- assignment or selection is expressed with italic: [assignment: *xxx (italic)*], [selection: *xxx (italic)*]
- non-selected items in selection operation are expressed with strike-through: ~~*strike-through*~~
- refinement is expressed with ***italic and gothic*** in the SFR.
- iteration is expressed with an attached number behind the identification: xxx(1), xxx(2)

- non-completed operations are expressed with under-line: [assignment: _xxx_ _(under-line)_]. The ST authors shall complete those incomplete operations in the ST.

SFRs provided in this PP are shown below.

6.1.1 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

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

6.1.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

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

Table 6-2(a) Cryptographic algorithms and keys (pre-compromise-disposition)

crypto-graphic algorithm	*standard*	*key length (bit)*	*cryptographic operation*	*notes (uses)*
T-DES	*NIST SP 800-67*	*192*	• *encryption/de-cryption* • *MAC generation /validation*	• *secure messaging* • *secret key installation*
RSA	*PKCS#1*	*1024*	• *encryption/de-*	• *token validation*

	v2.1		*cryption* • *signature generation /validation*	• *external authentication* • *internal authentication* • *signature generation/validation* • *key exchange for secure messaging*
SHA-1	*FIPS PUB 180-2*	-	*hush operation*	

Table 6-2(b) Cryptographic algorithms and keys (pre-compromise-disposition)

cryptographic algorithm	*standard*	*key length (bit)*	*cryptographic operation*	*notes (uses)*
AES	*NIST FIPS PUB 197*	*128*	• *encryption/decryption* • *MAC generation /validation*	• *secure messaging* • *secret key installation*
RSA	*PKCS#1 v2.1*	*2048*	• *encryption/decryption* • *signature generation /validation*	• *token validation* • *external authentication* • *internal authentication* • *signature generation/validation* • *key exchange for secure messaging*
SHA-256	*FIPS PUB 180-2*	-	*hush operation*	

[Application note 6]

Cryptographic algorithms shown in Table 6-2(a) and Table 6-2(b) are used for communication between the TOE and the external device. Additional APs may use these algorithms, which are provided by the platform.

BRR-AP uses cryptographic algorithms of Table 6-2(a) or Table 6-2(b) alternatively (selection is not required in this SFR). The SFRs related to selection of the cryptographic algorithm group are provided by FMT_MOF.1/FMT_SMF.1.

6.1.3 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **The TSF shall enforce the [assignment: *BRR Card access control SFP*] on [assignment: *subject:<a process within the TOE on behalf of a user>, objects:<files in the TOE>, and operations among subjects and objects covered by the SFP:<create and delete of files; write, read, modify and clear of file data; execute and quit of executable files>*].**

6.1.4 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 **The TSF shall enforce the [assignment: *BRR Card access control SFP*] to objects based on the following: [assignment: *subject:<a process on behalf of a user> and objects:<files in the TOE> controlled under the indicated SFP, and for each, the SFP-relevant security attributes:<for subject: the authentication status, for object: the authentication status requiring to the subject which attempts to access the object and the list of operations allowed to the subject>*].**

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *if the authentication status of the subject meets the authentication status requiring to the subject which attempts to access the object, the list of operations allowed to the subject will be allowed*].**

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *none*].**

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

6.1.5 FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 **The TSF shall enforce the [assignment: *BRR Card access control SFP*] when importing user data, controlled under the SFP, from outside of the TOE.**

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

FDP_ITC.1.3 **The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *in case the user data is RSA cryptographic key for the platform and the data length of the key is shorter than the one of the existent key, importing user data shall be refused*].**

6.1.6 FIA_AFL.1 Authentication failure handling (1)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when [selection: *[assignment: 3]*~~, an administrator configurable positive integer within[assignment: range of acceptable values]~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the initial key shown in Table 6-3*].**

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

6.1.7 FIA_AFL.1 Authentication failure handling (2)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when [selection: *[assignment: 3]*~~, an administrator configurable positive integer within[assignment: range of acceptable values]~~] unsuccessful authentication attempts occur related to [assignment: *authentication with PIN (4-digit PIN or 16-byte temporary password) shown in Table 6-3*].**

FIA_AFL.1.2 **When the defined number of unsuccessful authentication attempts has been [selection: ~~met,~~ *surpassed*], the TSF shall [assignment: *halt the authentication function until it is released by the administrator*].**

6.1.8 FIA_AFL.1 Authentication failure handling (3)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 **The TSF shall detect when [selection: *[assignment: 3]*~~, an administrator configurable positive integer within[assignment: range of acceptable values]~~] unsuccessful authentication attempts occur related to [assignment: *authentication with the transport key shown in Table 6-3*].**

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

6.1.9 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

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

[Application note 7]

The ST authors shall complete the list of the TSF mediated actions performed on behalf of the user before authentication. In the list, it would be better that the actions are described on high level view point, such as “read out of xxx data” instead of specific command name (ex. the commands of ISO/IEC 7816). If there is no action to be performed, FIA_UAU.1 is not applicable. Instead, FIA_UAU.2 should be used. The actions considered to be a part of authentication procedures need not be included in the list.

6.1.10 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 **The TSF shall prevent reuse of authentication data related to [assignment: *authentication for the external devices*].**

6.1.11 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 **The TSF shall provide [assignment: *list of multiple authentication mechanisms shown in Table 6-3*] to support user authentication.**

FIA_UAU.5.2 **The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication shown in Table 6-3*].**

Table 6-3 Authentication mechanisms

Authentication mechanisms	*Rules for authentication mechanisms*	*Use*
Authentication of BRR Card issuer (the platform)	*Verification with Initial Key (key length is specified in the procurement speci-fication documents)*	*Authentication of BRR Card issuer for the platform*
Authentication of BRR Card issuer (BRR-AP)	*Verification with transport key (8-byte)*	*Authentication of BRR Card issuer for BRR-AP*
Authentication of user (BRR Card holder)	*Verification with 4-digit PIN (16-byte temporary password is set for verification before issue; it is replaced with 4-digit PIN of the user on BRR Card issue)*	*User authentication by BRR-AP* *・Authentication of the card holder* *・Protection of illegal use before issue*
Authentication of the external device (the platform)	*Authentication with public key cryptosystem*	*The external device authentication by the platform*
Authentication of the external device (BRR-AP)	*Authentication with public key cryptosystem*	*The external device authentication by BRR-AP*

* ***"Use" is information to help understanding; not a part of the SFR.***

6.1.12 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

[Application note 8]

Typically, a user is identified with the user ID. However, in case of IC card, a user is identified with an action to select an authentication data file. Selecting the authentication data file means that he is claiming to be identified as the owner of the file.

The ST authors shall complete the list of the TSF mediated actions performed on behalf of the user before identification. In the list, it would be better that the actions are described on high level view point, such as "read out of xxx data" instead of specific command name (ex. The commands of ISO/IEC 7816). If there is no action to be performed, FIA_UID.1 is not applicable. Instead, FIA_UID.2

should be used. The actions considered to be a part of identification procedures need not be shown in the list.

6.1.13 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 **The TSF shall restrict the ability to [selection: ~~*determine the behaviour of, disable, enable,*~~ *modify the behaviour of*] the functions [assignment: *cryptographic operations for BRR-AP; the operations shown in Table 6-2(a) the pre-compromise-disposition group may be changed to the operations shown in Table 6-2(b) the post-compromise-disposition group*] to [assignment: *administrators*].**

[Application note 9]

This SFR requires the TOE to be capable the administrator of changing cryptographic algorithms for BRR-AP from the pre-compromise-disposition group shown in Table 6-2(a) of FCS_COP.1.1 to the post-compromise-disposition group shown in Table 6-2(b).

In case that the post-compromise-disposition group is pre-installed to the TOE (ex. on the delivery to the BRR Card issuer) , the modification of the behaviour in this SFR will be considered to be completed. If this is the case, the author of the ST may exclude this SFR with demonstration of rationale.

See [Application note 11] in FMT_SMF.1.

6.1.14 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 **The TSF shall enforce the [assignment: *BRR Card access control SFP*] to provide [selection, choose one of: *restrictive*~~*, permissive, [assignment: other property]*~~] default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the [assignment: *administrators*] to specify alternative initial values to override the default values when an object *related to an additional AP* or information is created.**

[Application note 10]

FMT_MSA.3.1 provides the properties of the default value of security attributes on generation of files for additional AP. The property of the default value means the property of access control before the security attribute of the file is specified by the administrator. “Restrictive” means the property not allowing accesses. The default value may be replaced with the new security attribute specified by the administrator.

Note that this SFR is the requirement relating to file generation in the operational environment. For example, it may be the case that an AP is added to the TOE in the operational environment. This SFR is not applied to the files generated by the developer in advance on delivery, such as the files for BRR-AP.

The authorized person specifying the security attributes on generation of the additional AP is the administrator. The point of this SFR is that the administrator who is a staff of the Local government is authorized to specify the initial security attributes relating to the additional APs

In case that the administrator installs additional APs and generates files in the TOE , it is required that the default values of the security attributes of the files meet the SFR and the mechanism allows only the administrator to replace the default value.

In another case, the program, the files and the initial data of the security attributes of the additional AP are written altogether to the TOE with an installer program. If this is the case, the security mechanism will have to require that writing to the TOE will be done under the authorization of the administrator. If the values of the security attributes were set in advance as secure as intended by the administrator, the security mechanism which provides default values or replaces them is not necessary. Those implementations will also meet this SFR.

6.1.15 FMT_MTD.1 Management of TSF data

Hierarchicalto: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 **The TSF shall restrict the ability to [selection: *~~change_default, query,~~ modify, ~~delete, clear, [assignment: other operations]~~*] the [assignment: user *authentication data for BRR-AP*] to [assignment: *administrator*].**

6.1.16 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 **The TSF shall be capable of performing the following management functions: [assignment: *specification of the initial security attributes of objects, change of the cryptographic algorithms for BRR-AP, modification of user authentication data for BRR-AP*].**

[Application note 11]

The first item of the assignment "specification of the initial security attributes of objects" is the requirement to generate files in the operational environment of the TOE. See the relating [Application note 10] of FMT_MSA.3.

The second item of the assignment "change of the cryptographic algorithms for BRR-AP" is applied as follows. If the cryptographic algorithms of the post-compromise-disposition group were set to the delivered TOE, the administrator never changes the cryptographic algorithms. If this is the case, the ST author may omit the item of "change of the cryptographic algorithms for BRR-AP" from the assignment items of this SFR with a justification rationale.

The management function of "change of the cryptographic algorithms for BRR-AP" is the requirement to address FMT_MOF.1. It requires the TSF mechanism to allow the administrator changing the cryptographic algorithms. Implementation of the mechanism of "change of the cryptographic algorithms for BRR-AP" is left to each developer, since the SFR does not specify the implementation. For example, the cryptographic algorithms can be changed by replacing a part of the program of the TOE. In that case, the mechanism that grants only the administrator to replace the program will be required. It should be noted that the both of the programs before and after of replacing are parts of the TSF and need to be evaluated.

6.1.17 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 **The TSF shall maintain the roles [assignment: *administrators*].**

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

[Application note 12]

"Administrators" means the role to handle BRR Cards on issuing and thereafter with authorization and responsibilities for management in the organisation. It does not indicate the whole of the organisation that is the issuer of BRR Cards.

6.1.18 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 **The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.**

FTP_ITC.1.2 **The TSF shall permit [selection: *~~the TSF,~~ another trusted IT product*] to initiate communication via the trusted channel.**

FTP_ITC.1.3 **The TSF shall initiate communication via the trusted channel for [assignment: *sending and receiving of protected data to/from the external device (ex. read out of resident registration code from the TOE, import of secret key to the TOE)*].**

6.2 Security assurance requirements

The security assurance requirements for the TOE are provided with the assurance components shown in Table 6-4. All those components are from CC part 3.

In this PP, no operation is applied to the assurance components.

Table 6-4 Assurance components

Assurance class	Assurance component
Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1

	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

6.3 Security requirements rationale

6.3.1 Security functional requirements rationale

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

6.3.1.1 Corresponding between the security objectives and the SFRs

The correspondences between the security objectives and the SFRs are shown in Table 6-5. This table shows that each SFR can be traced back to one or more objectives for the TOE.

Table 6-5 Corresponding between the security objectives and the SFRs

TOE security objectives / SFR	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_ITC.1	FIA_AFL.1(1)	FIA_AFL.1(2)	FIA_AFL.1(3)	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.1	FMT_MOF.1*	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FTP_ITC.1
O.I&A		x				x	x	x	x	x	x	x			x	x	x	
O.Access_control			x	x	x									x		x	x	
O.Secure_messaging	x	x	x	x	x													x
O.Replay										x								
O.Delivery									x		x	x						
O.Cryptography	x	x			x								x			x*	x*	x

* See [Application note 13]

[Application note 13]

If FMT_MOF.1 was omitted as shown in [Application note 9], the ST author has to remove the column of FMT_MOF.1 and “x” marks between O.Cryptography and FMT_SMF.1/ FMT_SMR.1.

6.3.1.2 Sufficiency of SFRs

The rationale that the security objectives for the TOE are satisfied with the corresponding SFR(s) is demonstrated. And also it is demonstrated that every SFR is effective to satisfy the security objectives of the TOE.

O.I&A

FIA_UAU.1 and FIA_UID.1 provide that only authorized users are allowed to use services of the TOE. Table 4-1 of O.I&A shows the authentication mechanisms, the rules and the uses of the mechanisms. Those authentication mechanisms are covered by Table 6-3 of FIA_UAU.5. The public key cryptosystem is used to authenticate the external devices. The authentication is done by verifying the electronic signature to a random number. For the authentication mechanism, FCS_COP.1 provides RSA public key cryptographic operation (electronic signature) and hush operation. FIA_UAU.4 provides the requirement to pretend reuse of authentication data.

The actions of the TSF for authentication failure in each authentication mechanism are provided in FIA_AFL(1), FIA_AFL(2) and FIA_AFL(3) respectively. Management requirements of authentication data for BRR-AP user are provided in FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1.

O.I&A is achieved sufficiently with those SFRs.

O.Access_control

O.Access_control requires only authorized users are allowed to access user data specified. This requirement is provided in FDP_ACC.1/FDP_ACF.1. FMT_MSA.3, FMT_SMF.1 and FMT_SMR are used for management of the security attributes concerning FDP_ACF.1. Import of user data into the TOE shall be controlled based on the rules provided in FDP_ITC.1. FDP_ITC.1 is applied to install additional APs and import cryptographic keys. O.Access_control is achieved sufficiently with those SFRs.

O.Secure_messaging

A session key (T-DES or AES) used for secure messaging is encrypted into RSA cryptography by the external device, imported to the TOE and decrypted. Cryptographic operations performed in the TOE are provided in FCS_COP.1. Import of user data into the TOE is provided in FDP_ITC.1. Access control related to the import is provided in FDP_ACC.1/FDP_ACF.1. FCS_CKM.4 provides the rule to destruct the session key. FTP_ITC.1 provides the requirements for secure messaging itself. O.Secure_messaging is achieved sufficiently with those SFRs.

O.Replay

FIA_UAU.4 provides single-use of authentication data. It achieves O.Replay.

O.Delivery

The protection by the initial key and the transport key, which is the requirement of the security objective O.Delivery, can be achieved with the requirements to the authentication functions of the TOE using those keys. FIA_UID.1 and FIA_UAU.1 provide the requirements for identification and authentication. FIA_UAU.5 provides each authentication mechanism. Those SFRs achieves O.Delivery sufficiently.

O.Cryptography

FCS_COP.1 provides cryptographic algorithms and operations required by O.Cryptography. The session key (T-DES or AES) for secure messaging and the public key pair (RSA) are imported into the TOE according to the policy of FDP_ITC.1. FDP_ITC.1 also provides the rule concerning restriction of the key length for RSA algorithm. Protection of the communication channel importing the cryptographic keys is provided in FTP_ITC.1. FCS_CKM.4 provides destruction of the cryptographic keys. The change of the cryptographic algorithms for BRR-AP is provided in FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1. O.Cryptography is achieved sufficiently with those SFRs.

[Application note 14]

If the ST author omits FMT_MOF.1 for the reason shown [Application note 9], the description “The change of the cryptographic algorithms for BRR-AP is provided in FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1.” in this rationale should be removed as well.

6.3.1.3 Dependencies of SFRs

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

The dependencies provided in the components of CC part 2 are shown at “Dependencies” of the Table. “Satisfaction of dependencies” shows how the dependencies are satisfied or the reasons why the dependency need not being satisfied.

Table 6-6 Dependencies of SFRs

SFR	Dependencies	Satisfaction of dependencies
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FDP_ITC.1 is included.
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 and FCS_CKM.4 are included.
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1 is included.
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1 and FMT_MSA.3 are included.

	FMT_MSA.3	
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3 are included.
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.1 is included.
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.1 is included.
FIA_AFL.1(3)	FIA_UAU.1	FIA_UAU.1 is included.
FIA_UAU.1	FIA_UID.1	FIA_UID.1 is included.
FIA_UAU.4	none	-
FIA_UAU.5	none	-
FIA_UID.1	none	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1 are included.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 is not applied because the security attributes need not to be changed after creation of the object. FMT_SMR.1 is included.
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1 are included.
FMT_SMF.1	none	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1 is included.
FTP_ITC.1	none	-

6.3.2 Security assurance requirements rationale

The scope of the TOE is the software embedded in the IC chip, which is hardware. The security of the TOE highly depends on the security functionality of the IC chip. A typical attack to IC chip is an attempt to disclose secret keys within the memory by means of physical attacks. As physical attack measures against IC chip have been highly developed, protection of IC chip is required to stand high level attacks. On consideration of the security of the entire BRR Card, the IC chip part needs to counter to high level attack potential.

As high level attacks are assumed to the hardware part of BRR Card, the software part of BRR Card should counter the same level attacks as well. The security assurance requirements for the TOE should consider high level attack potential, then AVA_VAN.5 on vulnerability assessment is claimed.

Concerning for the security of the IC chip and the software, attack measures and attack points are not vague, but specific and restrictive, even if high level attacks were assumed. Then the whole security assurance requirements do not necessarily address high level attacks. Therefore, EAL4 (augmented with AVA_VAN.5) is considered to be adequate for the TOE. EAL4 is the highest assurance level for COTS without rigorous development practices as EAL5.

The dependencies provided in AVA_VAN.5 are the same as AVA_VAN.3, which is a component of EAL4. Then, all dependencies between assurance components are the same as EAL4 package. The dependencies between each component shown in Table 6-4 are satisfied.

7 Glossary and acronyms

7.1 General CC terms

PP

Protection Profile: implementation-independent statement of security needs for a TOE type. PP is developed by procurers of the TOE or developers interests.

CC

Common Criteria: Criteria of security evaluation for IT products. ISO/IEC 15408 is the counterpart of CC in ISO/IEC standards.

CCRA

The Common Criteria Recognition Arrangement: Each CC evaluation and certification scheme acceding to CCRA recognizes mutually the IT products certified by the other country's scheme.

ST

Security Target: Organized definition of security requirements for the IT product. Evaluation of the TOE is performed based on the ST.

TOE

Target of Evaluation: set of software, firmware and/or hardware possibly accompanied by guidance. A TOE may be whole of the IT product or a part of the IT product. The scope of the TOE is defined by the ST.

7.2 Terms related to the TOE

BRR Card

The Basic Resident Registration Card: The IC card used for the Basic Resident Registration Network System.

It is a multi-purpose public IC card not only for electronic identification but also for a variety of applications offered by local governments.

The current Basic Resident Registration Card has been distributed from 2003. There are two types: the type I card and the type II card.

The next generation Basic Resident Registration Card becomes under the necessity to address the changes in the operational environment; the revision of the Basic Resident Registration Law (2009/7/15), continuous using of BRR Card on moving to the other local government territory, the reinforcement of the cryptographic algorithms implemented TYPE I and TYPE II card and the introduction of extended administrative services. The new specification was developed and provided as the Basic Resident Registration Card Version 2 (V2).

BRR-AP

The essential application of BRR Card. It is used for the Basic Resident Registration Network System.

BRR-AP is used to manage the resident registration code of the card holder. It is installed to all BRR Card and provides security functionality capable of allowing only for the legitimate card holder to use BRR-AP securely.

Composite evaluation IC card is the IT product composed of software and hardware, which consists of an IC chip, an antenna for contactless communication etc. In case that a common hardware provides a base component and is combined with various software, the hardware part alone can be evaluated before evaluating the entire IC card. On the evaluation of the entire IC card, just the additional security functionality derived from the software part and the combination of the software and the hardware will be evaluated. The evaluation of the hardware part, which takes much time and cost, need not be re-evaluated. This is called “composite evaluation”.

In the case of the IC card mentioned above, the target of the composite evaluation will be the software added on the hardware and the combination of the software and the hardware. The former evaluation result of the hardware, ST and the evaluation technical report, can be reused. However, since the ETR is not a public document, the sponsor of the composite evaluation will have to make the ETR available under the authorization of both of the evaluation facility and the certification body concerning the ETR. Especially, in case that the evaluations of the IC chip TOE and the composite TOE are performed on the different schemes, the agreements with all interested parties will be very important.