Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Protection Profile (PP)

Application date/ID	2010-10-25 (ITC-0312)
Certification No.	C0284
Sponsor	Local Authorities Systems Development Center
Name of TOE	Basic Resident Registration Card V2 Embedded Software Protection Profile
Version of TOE	1.00
PP Conformance	None
Assurance Package	EAL4 Augmented with AVA_VAN.5
Developer	Local Authorities Systems Development Center
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2011-02-28

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass

"Basic Resident Registration Card V2 Embedded Software Protection Profile" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Basic Resident Registration Card V2 Embedded Software Protection Profile, Version 1.00" (hereinafter referred to as "the PP") developed by Local Authorities Systems Development Center, and evaluation of the PP was finished on 2011-01 by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Local Authorities Systems Development Center and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the PP that is the appendix of this report together. The operational conditions, details of usage assumptions, corresponding security objectives, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the PP.

This certification report assumes "vender who develops and supplies the Basic Resident Registration Card conforming this PP" to be a reader. The Certification Report presents the certification result based on assurance requirements to which the PP conforms.

1.1 Evaluated PP

Overviews of the security functionalities required by the PP are as follows. Refer to and after Chapter 2 for details.

1.1.1 Assurance Package and Conformance Claim

Assurance Package required by the PP is EAL4 augmented with AVA_VAN.5. And PP or ST that claims conformance to this PP shall claim demonstrable conformance.

1.1.2 PP Overview

This PP prescribes security requirements to the embedded software of the Basic Resident Registration Card (hereinafter referred to as "BRR Card") Version2 which provides the specification for the next generation BRR Card. BRR Card is an elementary component of the Basic Resident Registration Network System.

The TOE is the embedded software for the BRR Card which is running on an Integrated Circuit in the BRR Card. The TOE consists of the platform software providing an application execution environment and the proprietary application program of this TOE BRR-AP (Basic Resident Registration Application) running on the platform software. Although any other application programs, called "additional Application Programs" (hereinafter referred to as "additional APs") in the PP, can be added in the platform software, additional APs are out of scope of the TOE. Fig 1-1 shows the TOE structure.

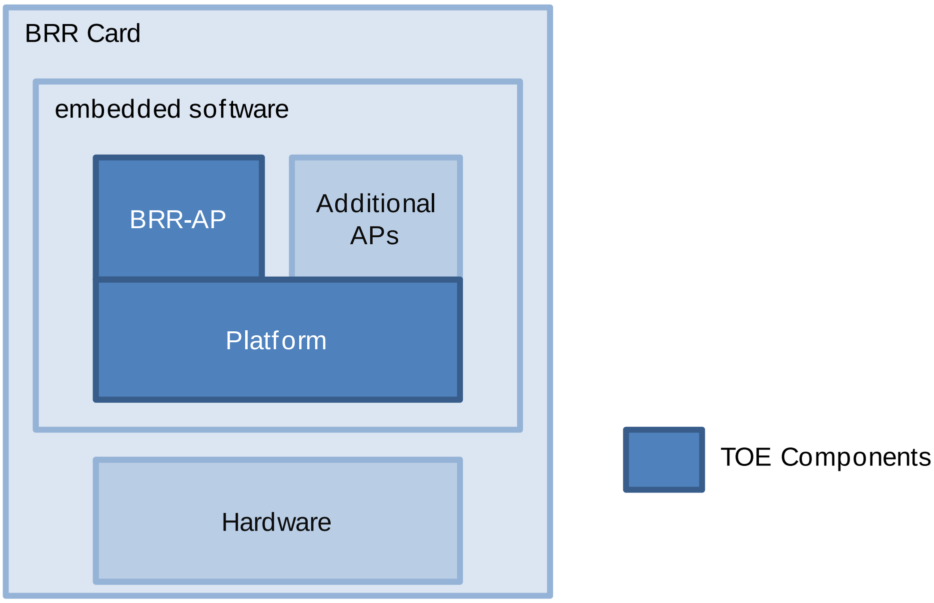

Fig.1-1 TOE structure

Assembled BRR Cards are delivered from developers to each local government, the issuer of BRR Cards. Each local government delivers BRR Cards to resident citizens and the personal data of the BRR Card is initialized (This procedure is called "personalization"). And additional APs may be installed by the issuer. The local government staff who issues BRR Card is called "TOE Administrator" in the PP.

Card holders (the residents) can use services of the Basic Resident Registration Network System through BRR Cards.

1.1.2.1 Security functions

The PP requires the security functions aim at providing the services of the Basic Resident Registration Network through the BRR-AP safely. The major security features of the TOE are as follows:

(1) Secure communication:

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

(2) Mutual authentication:

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

(3) Card holder authentication

BRR-AP authenticates the card holder. This is a function of BRR-AP and additional APs cannot use this function.

(4) Stored data protection

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

1.1.3 Disclaimers

The scope of the TOE conforming to this PP is only the embedded software which is a part of BRR Card. The security requirements for the whole BRR Card including hardware are not provided by this PP.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2011-01 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report[13] and Observation Report(s) prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the PP evaluation is conducted in accordance with the prescribed procedure.Certification oversight reviews are also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. PP Identification

The PP is identified as follows:

Name of PP	Basic Resident Registration Card V2 Embedded Software Protection Profile
Version of PP	1.00
Developer	Local Authorities Systems Development Center

3. Security Policy

This chapter describes security function policies and assumptions required by the TOE conforming to this PP.

This PP requires the security functions to protect data stored in BRR card from illegal access and to meet the organisational security policies.

3.1 Security Function Policies

The TOE conforming to this PP possesses the security functions to counter the threats shown in Chapter 3.1.1 and to meet the organisational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE conforming to this PP assumes the threats shown in Table 3-1 and provides the functions as countermeasures against them.

Table 3-1 Assumed Threats

Identifier	Threat
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. [Note] This is a threat concerning with illegal use of BRR-AP. Threats caused by additional APs would be countered by the Basic Resident Registration Network System side.
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. An external device 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.
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. [Note]

	This threat assumes the misuse or the alteration of the AP which meets Assumption A.AP. "An AP" is BRR-AP or any additional AP.
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.

3.1.1.2 Security Function Policies against Threats

The TOE conforming to this PP counters the threats shown in Table 3-1 by the following security function policies.

(1) Security function to counter the threat "T.Fraud"

This threat assumes that 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.

To counter this threat, the TOE provides the user authentication function that validates the authenticity of the BRR Card holder. The authentication mechanism uses 4-digit PIN, which was replaced from 16-byte temporary password on issuance of BRR Card. An only user who succeeded in the authentication within 3 times retry is allowed to use the BRR-AP as a proper BRR Card holder.

(2) Security function to counter the threats "T.Illegal_attack" and "T.Replay"

The threat "T.Illegal_attack" assumes that the TOE is accessed illegally to the TOE itself and internal data through the external interfaces of BRR Card, the electric contact pads or the contactless communication port. "T.Replay" assumes that the TOE is accessed illegally by replaying the authentication procedures between the TOE and the external device.

To counter these threats, the TOE provides the external device authentication function to verify the authenticity of the external device and allows only the proper external device to access to the TOE data. The access is restricted according to user's authority.
The TOE uses the authentication mechanisms based on RSA public key cryptographic system for the external device. And single-use-authentication data is employed for the authentication mechanism.

(3) Security function to counter the threats "T.AP_abuse"

This threat assumes that the TOE is accessed illegally to the resources of the AP through using the other AP running on the platform of the TOE.

To counter this threat, the TOE allows only authorized users to access user data. Any unauthorized accesses by the users belonging to the other APs will be prohibited.

(4) Security function to counter the threats "T.Eavesdrop"

This threat assumes that an attacker monitors contactless communication data between the TOE and the external device to disclose confidential information or modify communication data.
The symmetric key cryptographic algorithm (T-DES or AES) shown in Table 3-3 is used to protect communication data. The symmetric key (called "session key") is exchanged using the RSA algorithm shown in Table 3-3. The SHA hush operation shown in Table 3-3 is used for signature validation of the key exchange. These procedures provide a secure contactless communication between the TOE and the external device.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE conforming to this PP is shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
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. [Note] P.Delivery is the organisational security policy applied when TOE is under the user's (local government) management, and after TOE is issued to the BRR cardholder, P.Delivery is not applied.
P.Cryptography	Cryptographic algorithms and keys shown in Table 3-3 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-compromisedisposition 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-compromisedisposition 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-compromisedisposition group by the administrators.

Table 3-3 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/ validation	pre-compromise-disposition
RSA	1024	PKCS#1 v2.1	- encryption/decryption - signature generation/ validation	
SHA-1	-	FIPS PUB 180-2	- hush operation	
AES	128	NIST FIPS PUB 197	- encryption/decryption - MAC generation/ validation	post-compromise-disposition
RSA	2048	PKCS#1 v2.1	- encryption/decryption - signature generation/ validation	
SHA-256	-	FIPS PUB 180-2	- hush operation	

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE conforming to this PP provides the security functions to meet the organisational security policies shown in Table 3-2.

(1) Security function to meet the organisational security policy "P.Delivery"

This organisational security policy defines for the TOE under the control the local government which is issuer of BRR Card that only authorized users can have access to the data in the TOE.

The TOE provides the function of making a request for authentication with the initial key and the transport key prior to having access to the data in the TOE and permitting access to the data in the TOE according to the authentication of the relevant key only in case of successful authentication.
The initial key protects the platform and the transport key protects BRR-AP respectively.

(2) Security function to meet the organisational security policy "P.Cryptography"

This organisational security policy defines the cryptographic algorithms and keys for the TOE (See Table 3-3).

The TOE provides capability to select cryptographic algorithms shown in Table 3-3 to the platform, BRR-AP or additional APs.
Cryptographic algorithms shown in Table 3-3 are separated into two groups. One is the pre-compromise-disposition group and the other is the post-compromise-disposition group. The administrator chooses either of the group for BRR-AP. Cryptographic algorithms for the platform and additional APs are employed independently of BRR-AP's one.

3.2 Usage Assumptions

Table 3-4 shows assumptions to operate the TOE conforming to this PP.

The effective performance of the TOE conforming to this PP security functions are not assured unless these assumptions are satisfied.

Table 3-4 Assumptions in Use of the TOE

Identifier	Assumptions
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. [Note] This assumption eliminates the risk that an illicit application developed by untrustworthy developers would be installed into the BRR Card. To meet A.AP, the administrators (responsibilities) of the TOE should accept only additional APs developed by reliable developers.

4. Evaluation conducted by Evaluation Facility and results

4.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3.Details for evaluation activities are reported in the Evaluation Technical Report.In the Evaluation Technical Report, it explains the summary of the PP, the content of evaluation and verdict of each work unit.

4.2 Overview of Evaluation Activity

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on 2010-11 and concluded by completion the Evaluation Technical Report dated 2011-01.The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to the developer. These concerns were reviewed by the developer and all concerns were solved eventually.

Concerns that the Certification Body found about the evaluation process was described as a certification oversight review, and it was sent to Evaluation Facility.

After Evaluation Facility and the developer examine it, these concerns were reflected in the evaluation report.

4.3 Evaluation Results

The evaluator had the conclusion that the PP satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance: none
- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- APE_INT.1,APE_CCL.1,APE_SPD.1,APE_OBJ.2,APE_ECD.1,APE_REQ.2

4.4 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

5. Certification

The certification body conducted the following certification based on each materials submitted by Evaluation Facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.

2. Contents pointed out in the Observation Report shall properly be reflected.

3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification oversight reviews and were sent to Evaluation Facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification oversight reviews were solved in the PP and the Evaluation Technical Report and issued this certification report.

5.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the PP satisfies assurance components APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1, and APE_REQ.2 in the CC part 3.

5.2 Recommendations

As it is described also in 1.1.3, this PP provides a security requirement of the security functions which is consists of the only embedded software.

For the evaluation of BRR Card, it is necessary evaluation and validation of the whole security functions which is include the security function consist of hardware. And ST author should define the security problems, the security objectives, and the security functional requirement about all these security functions in the ST. Additional information for the evaluation of the whole BRR Card is shown in the PP.

The effectivity of the cryptographic algorithms provided in this PP at the time of the TOE evaluation may not be assured. Effectivity and compromise of the cryptographic algorithms should be taken in consideration on the evaluation of the TOE.

6. Annexes

There is no annex.

7. Glossary

The abbreviations relating to CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The definition of terms used in this report is listed below.

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. 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), the adoption of advanced cryptographic technologies replacing compromised cryptographic algorithms 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.

Disposition for cryptographic algorithm

The TOE provides two groups of cryptographic algorithms for BRR-AP use. One group classified as the "pre-compromise-disposition" is being used in the previous

compromise	version of BRR-AP. To address cryptographic algorithm compromise, the change of cryptographic algorithms to another group the "post-compromise-disposition" 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.

8. Bibliography

[1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan, CCS-01

[2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan, CCM-02

[3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001, (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002, (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004, (Japanese Version 1.0, December 2009)

[12] Basic Resident Registration Card V2 Embedded Software Protection Profile, Version 1.00, (January 21, 2011), Local Authorities Systems Development Center

[13] Basic Resident Registration Card V2 Embedded Software Protection Profile Evaluation Technical Report, Version 1.1, January 31, 2011, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center