Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

Protection Profile (PP)

Reception Date of Application (Reception Number)	2018-04-02 (ITC-8666)
Certification Identification	JISEC-C0612
Protection Profile Name/Identifier	Public Transportation IC Card Protection Profile
Protection Profile Version Number	1.12
Protection Profile Developer	Japan ID Connect with Secure Authentication Promotional association
Protection Profile Sponsor	Japan ID Connect with Secure Authentication Promotional association
Assurance Conformance	EAL5 augmented with ALC_DVS.2 and AVA_VAN.5
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above PP has been certified as follows.

2018-08-22

Shinji Sato, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

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

- Common Criteria for Information Technology Security Evaluation
  Version 3.1 Release 5
- Common Methodology for Information Technology Security Evaluation
  Version 3.1 Release 5

Evaluation Result: Pass

"Public Transportation IC Card Protection Profile" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" 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 is to report the sponsor, Japan ID Connect with Secure Authentication Promotional association as the developer of the IT Security Evaluation of "Public Transportation IC Card Protection Profile Version 1.12" (hereinafter, the "PP" [9]) on certification results, produced through the evaluation of the PP [9] conducted by ECSEC Laboratory Inc. Evaluation Center (hereinafter "Evaluation Facility") with completion date of August, 2018. This report also provides security information to procurement entities and consumers interested in the PP [9].

This Certification Report assumes "developers who develop and supply the product conforming to the PP [9]" to be intended readers. Note that the Certification Report only presents the certification result based on assurance requirements to which the PP [9] confirms, and does not intend to guarantee an individual IT product itself.

Readers of this Certification Report are advised to refer to the PP [9] corresponding to this report. Details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements for the TOE claiming conformance to the PP [9] are specifically described in the PP [9].

Reference should be made to Chapter 8 for the terms used in this Certification Report.

1.1 Evaluated PP

An overview of the PP [9] is provided as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 PP Overview

The PP [9] provides the security requirements for the IC used as a public transportation IC card in Japan.

TOEs conforming to the PP [9] are public transportation IC cards. The TOE consists of an IC with a contactless interface (with optional contact interface) and a smartcard embedded software (hereinafter "PT Software").

The TOE can be used not only for a stored fare card, one-day ticket card and seasonal ticket for public transportation but also for e-money and ID card.

A public transportation operator can implement their own services as well as the interoperation with other public transportation operators. The TOE provides flexible file system that realizes the multi-application for their services where a public transportation operator can configure access permissions and access rules to the internal data of the TOE.

Figure 1-1 shows a typical operation provided by a Ticket Service. Figure 1-2 shows the TOE and non-TOE components assumed by the PP [9].

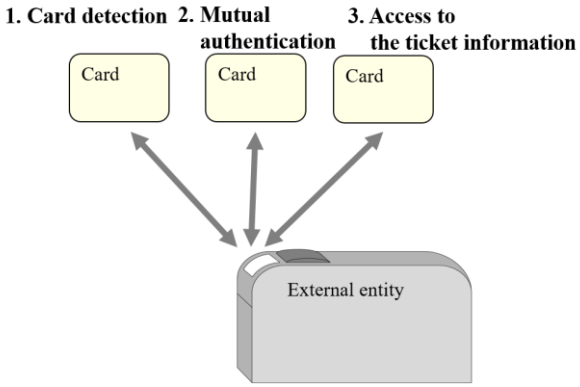

Figure 1-1 Typical operation of the ticket gates

Typical operation of the ticket gates starts from detection of the card by the ticket gate, then the ticket gate and the card perform mutual authentication. If the mutual authentication is successfully completed, the ticket gate reads the ticket information from the card. If the ticket is valid, the ticket gate writes necessary information to the card and then allows the Passenger to pass through the gate.

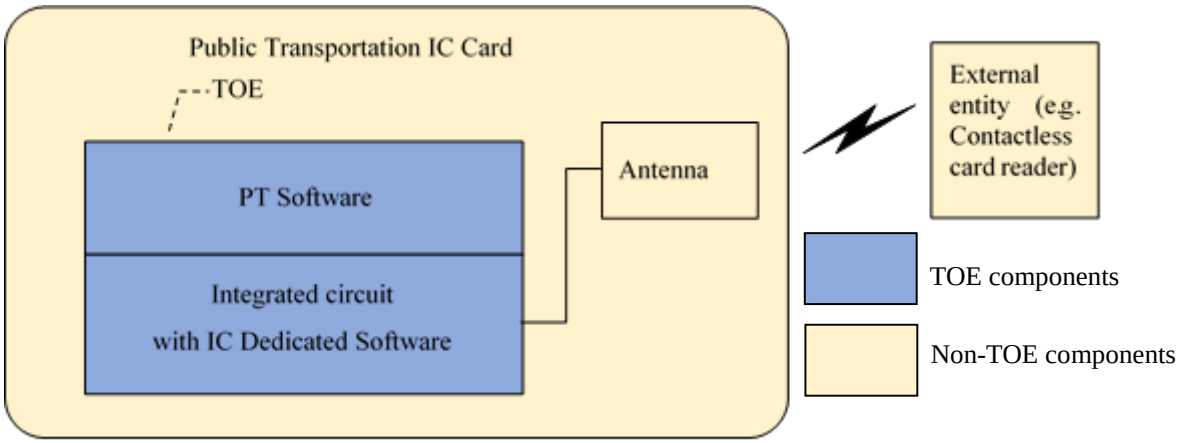

Figure 1-2 Assumed TOE components and non-TOE components

"PT Software" is composed of a public transportation application and an operating system.

"Integrated circuit with IC Dedicated Software" refers to an IC and its associated dedicated software. The IC chip is composed of a processing unit, cryptographic co-processor(s), security components (e.g., security detectors, sensors), a contactless

interface, an optional contact interface, and memories. The dedicated software is used not only during manufacturing, and can contain cryptographic libraries as additional services.

The lifecycle of the TOE is divided into seven phases. Table 1-1 shows the TOE lifecycle.

Table 1-1 TOE Lifecycle

Phase	Description
Phase 1	IC embedded software development
Phase 2	IC development
Phase 3	IC manufacturing
Phase 4	IC packaging
Phase 5	Composite product integration
Phase 6	Personalisation
Phase 7	Operational usage

PT Software is developed in Phase 1. IC and IC Dedicated Software are developed in Phase 2 and manufactured in Phase 3. TOEs are delivered in form of wafers or sawn wafers (dice) when TOEs are delivered after Phase 3. TOEs are delivered in form of packaged modules when TOEs are delivered after Phase 4. The TOE is integrated into the card product in Phase 5, and undergo an issuing process in Phase 6, followed by operational usage in Phase 7.

The PP [9] defines assurance requirements from Phase 1 up until "TOE Delivery".

1.1.1.1 Threats and Security Objectives

The TOE confirming to the PP [9] counters several threats using security functions as follows.

AAPS [8] describes physical attacks, side-channel attacks and perturbation attacks as attacks against IC card. These attacks can be applied to the TOE. The PP [9] requires the tamper-resistant functionalities that protect IC chip itself and counter the impairment of the assets.

During the mutual authentication shown in Figure 1-1, attackers may try to access the assets in the TOE by bypassing the authentication. The PP [9] requires protection of the confidentiality and the integrity of the assets stored in the TOE by the mutual authentication function and the service-dependent access control function.

The TOE communicates with an external entity via contact or contactless interface. Attackers may try to eavesdrop or alter the communication data. The PP [9] requires to counter these attacks by establishing the secure channel.

Attackers may try to access the assets in the TOE by bypassing the security functions and by exploiting the functions that are unavailable after the TOE delivery. The PP [9] requires protection from the exploitation of the functions.

1.1.1.2 TOE configuration requirements and assumptions

The PP [9] assumes that the TOE is manufactured and used in operation under the following configuration and assumptions:

It is assumed that TOEs are configured in a manner that the level of access control to the assets is set explicitly, and the mutual authentication mechanism(s) between external entities and the TOE are provided. In addition, the confidentiality and the integrity of the TOEs and of their manufacturing and test data must be maintained by security procedures after the TOE delivery to the personalisation (issuing the TOE).

1.1.2 Disclaimers in Certification

It should be noted that, as practical security requirements for procurement, requirements for cryptographic algorithms and communication protocols are required in addition to PP [9]. To be more specific, the PP [9] does not provide any requirements for cryptographic algorithms, communication protocols, or associated cryptographic key management, which are inevitably assumed to be used in the mutual authentication shown in Figure 1-1, and so on. In addition, none of underlying threat analysis, security objectives and security functional requirements is described to the above. Therefore, when a TOE confirming to the PP [9] is developed and procured, these requirements additionally need to be defined among developer(s) and a procurement entity, and need to be evaluated and certified.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility has conducted IT security evaluation and completed on August 2018, based on functional requirements and assurance requirements of the PP [9] according to the publicized documents, "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2] and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [10] prepared by the Evaluation Facility, as well as evaluation documentation, and confirmed that the PP [9] evaluation was conducted in accordance with the prescribed procedure. Certification

oversight reviews have also been prepared for those concerns found in the certification process. The Certification Body confirmed that all the concerns have fully resolved and the PP [9] evaluation has been appropriately conducted in accordance with the CC [4][5][6] and the CEM [7]. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2 PP Identification

The PP [9] is identified as follows:

Name of PP:	Public Transportation IC Card Protection Profile
Version of PP:	Version 1.12
Developer:	Japan ID Connect with Secure Authentication Promotional association

3 Security Policy

This chapter describes the security functional policies adopted by the TOE conforming to the PP [9] to counter threats, and organizational security policies.

The PP [9] requires the following functionalities to the TOE:

- Tamper-resistant functionalities
- Access control functions to the assets
- Mutual authentication and secure communication functions between the external entity and the TOE
- Protection from abuse of the functions unavailable after TOE delivery

3.1 Threats

The PP [9] assumes the threats described in Table 3-1 and requests the TOE to provide security functionalities to counter them.

Table 3-1 Assumed Threats

Identifier	Threats
T.Hardware_Attack	An attacker may perform physical attacks, perturbation attacks and side channel attacks against IC chips in order to (i) disclose or manipulate the assets of the TOE or (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE.
T.Logical_Attack	In the operational environment after issuing the TOE, an attacker may try to (i) disclose the assets of the TOE or (ii) alter the assets of the TOE without authentication.
T.Comm_Attack	An attacker may try to (i) disclose the assets that is sent or received through the communication channel or (ii) alter the messages on the communication channel.

Identifier	Threats
T.Abuse_Func	An attacker may use functions of the TOE which may not be used after TOE delivery in order to (i) disclose or manipulate the assets of the TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE, (iii) manipulate (explore, bypass, deactivate or change) functions of the TOE or (iv) enable an attack disclosing or manipulating the assets of the TOE.

3.2 Organisational Security Policies

Table 3-2 shows organizational security policies required for the use of the OTE confirming to the PP [9].

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policies
P.Configure	The TOE is a tool to be used by the Administrator in a system that shall implement specific business rules. The TOE shall provide the means for the level of the access control to be specified explicitly by the Administrator for each asset.
P.Identification	An accurate identification shall be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.
P.TOE_Auth	TOE shall be able to authenticate the external entities and authenticate itself to the external entities.

3.3 Security Function Policies

The PP [9] requires the implementation of the security functions of the TOE to counter the security problem described in 3.1 and 3.2. The security functions are summarized in the following subsections.

3.3.1 Tamper-resistance functionalities

The TOE provides protection against physical probing, physical manipulation, and ensures its correct operation by preventing its operation outside the normal operating conditions, and provides protection against in place to handle the physical interaction. This security function counters T.Hardware_Attack.

3.3.2 Access control functions to the assets

The TOE provides means to configure the level of access control to each asset explicitly, and provides access control mechanism according to the configured level of access control. This security function counters T.Logical_Attack and supports P.Configure.

3.3.3 Mutual authentication and secure communication functions between the external entities and the TOE

The TOE provides the functionality to authenticate the external entities and to let external entities authenticate itself. The TOE provides secure channel with the external entity. Authentication mechanisms and communication protocols will be specified for each version of TOE. These security functions counter T.Comm_Attack and support P.TOE_Auth.

3.3.4 Protection from exploitation of the functions unavailable after TOE delivery

The TOE implements the protection from exploitation of the functions unavailable after TOE delivery. This security function counters T.Abuse_Func and supports P.Identification.

4 Assumptions and Clarification of Scope

This chapter describes assumptions and an operational environment for the operation of the TOE confirming to the PP [9]. If any of the assumptions is not met, effective performance of the security functionalities of the TOE is not assured.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.Process	It is assumed that security procedures are used after delivery of the TOE by the TOE manufacturer up to delivery to the Passenger to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
A.Keys	Access Keys for TOE use are generated outside the TOE, by the supporting system in a controlled environment. This system shall check that all such keys are suitably secure by, for example, weeding out weak keys. Access Keys are then handled correctly without misoperation. The process of key generation and management shall be suitably protected and shall be performed in a controlled environment.

5 Evaluation conducted by Evaluation Facility and Results

5.1 Evaluation Facility

ECSEC Laboratory Inc. Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body as a member of the Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). The Evaluation Facility is periodically checked and confirmed that is meets the requirements on appropriateness of the management and the evaluators for maintaining the quality of evaluation.

5.2 Evaluation Approach

The evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities have been reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the PP [9] as well as the evaluation details and the verdict for the each work unit in the CEM.

5.3 Overview of Evaluation Activity

The history of the evaluation activities is described in the Evaluation Technical Report as follows.

The evaluation started on April 2018 has concluded upon completion of the Evaluation Technical Reports dated August 2018. The Evaluation Facility has received a full set of evaluation deliverables necessary for the evaluation provided the developer, and examined the evidence in relation to a series of evaluation activities.

Any concern found in the evaluation activities for each work unit is included in the Observation Reports, which are issued and reported to the developer. However, no Observation Report has been issued in this evaluation.

Concerns that the Certification Body found in the evaluation process have been described in certification oversight reviews to the Evaluation Facility.

All the above concerns, examined by the Evaluation Facility and the developer have been reflected in the Evaluation Technical Report.

5.4 Evaluation Results

The evaluator has concluded that, upon provision of the Evaluation Technical Report, the PP [9] satisfies all work units prescribed in the CEM.

The following security requirements are confirmed in the evaluation:

Security Functional Recruitments: Common Criteria Part 2 extended

Security Assurance Requirements: Common Criteria Part 2 conformant

As a result of the evaluation, the verdict "PASS" has been confirmed for the following assurance components:

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

5.5 Evaluator Comments/Recommendation

There is no evaluator recommendation to be addressed to procurers.

6 Certification

Based on the materials submitted by the Evaluation Facility during the evaluation process, the Certification Body has conducted certification including the following confirmations:

1. Through checking of the submitted documentation, whether the relevant work units have been evaluated as presented in the Evaluation Technical Report.
2. Whether the rationale for the evaluation verdict made by the evaluator presented in the Evaluation Technical Report is appropriate
3. Whether the evaluator's evaluation methodology presented in the Evaluation Technical Report is complying with the CEM.

Concerns found in the certification process are documented in the certification oversight reviews, which have been sent to the Evaluation Facility. The Certification Body has issued this Certification Report upon confirmation that in the PP [9] and the Evaluation Technical Report such concerns described in the certification oversight reviews have been fully solved.

6.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report and related evaluation documentation, the Certification Body has determined that the PP [9] satisfies assurance requirements APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.2, APE_ECD.1 and APE_REQ.2 in the CC Part 3.

6.2 Recommendations

The PP [9] does not specify the protocol between the TOE and the external entity. The TOE developer claiming conformance to the PP [9] shall specify the protocol in consultation with a procurement entity.

The PP [9] does not specify any cryptographic algorithms used in the mutual authentication between the TOE and an external entity, the specifications of the cryptographic key and the cryptographic key management. The TOE developer claiming conformance to the PP [9] shall specify them in consultation with a procurement entity. When the TOE claiming conformance to the PP [9] is evaluated, it is necessary to confirm that each cryptographic algorithm and cryptographic key management is still valid, and not compromised yet.

7 Annexes

There is no annex.

8 Terms

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

PT Software	Public Transportation Software

The definitions of terms used in this report are listed below.

Access Key	A key that is used to access to the data used as the ticket service.
Passenger	A person who uses Ticket Service
Operator	An entity that provides a specific service to a Passenger. (Public Transportation Operator, Administrator)
Ticket Service	A specific service that is provided by an Operator to a Passenger

9 Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017

[7] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 5, April 2017

[8] Joint Interpretation Library Application of Attack Potential to Smartcards, Version 2.9, January 2013

[9] Public Transportation IC Card Protection Profile, Version 1.12, 01 August 2018, Japan ID Connect with Secure Authentication Promotional association

[10] Protection Profile Evaluation Technical Report, Version 2.0, August 7, 2018, ECSEC Laboratory Inc. Evaluation Center, TPS-ETRPP-0002-00