Certification Report

SAITO Yutaka, Commissioner
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

Protection Profile (PP)

Reception Date of Application (Reception Number)	2025-08-04 (ITC-5919)
Certification Identification	JISEC-C0859
PP Name	JPKI Applet Protection Profile
PP Version	1.10
PP Developer	Digital Agency, Government of Japan
PP Sponsor	Digital Agency, Government of Japan
Assurance Package	EAL4 Augmented with AVA_VAN.5, ALC_DVS.2, COMP
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.
2026-02-25

HASHIMOTO Toru, 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 CC:2022 Release 1
- Common Methodology for Information Technology Security Evaluation CEM:2022 Release 1
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1

Evaluation Result: Pass

"JPKI Applet Protection Profile, Version 1.10" 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 describes the content of the certification result in relation to IT Security Evaluation of "JPKI Applet Protection Profile, Version 1.10" (hereinafter referred to as "the PP [11]") developed by Digital Agency,Government of Japan and the evaluation of the TOE was completed on 2026-01-30 by ECSEC Laboratory Inc. Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Digital Agency, Government of Japan and provide security information to procurement entities and consumers who are interested in this PP [11].

Readers of the Certification Report are advised to read the corresponding PP [11] together with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the PP [11] are described in the PP [11].

This Certification Report assumes developers who develop products conforming to the PP [11] and product procurement entities to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the PP [11] conforms and does not guarantee an individual IT product itself.

1.1 Evaluated PP

An overview of the security functions required by the PP [11] is described below. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the PP [11] is EAL4 augmented by AVA_DVS.2 and AVA_VAN.5, and COMP.
In addition, any PP and any Security Target (ST) that claims conformance to the PP [11] shall claim strict conformance.

1.1.2 Overview of the PP

In the PP [11], the TOE is an embedded secure element (eSE) in a mobile phone.
The TOE operates as a Java Card system that provides a Secure Signature Creation Device (SSCD) with a key generation function for signature creation and user authentication. The TOE consists of the JPKI Applet, the Java Card platform, and the Integrated Circuit (IC). The IC and the platform are certified separately. The JPKI Applet operating on the IC and Java Card platform is subject to composite certification.
Figure 1-1 shows the configuration of the TOE. The TOE corresponds to the yellow portion in the figure.

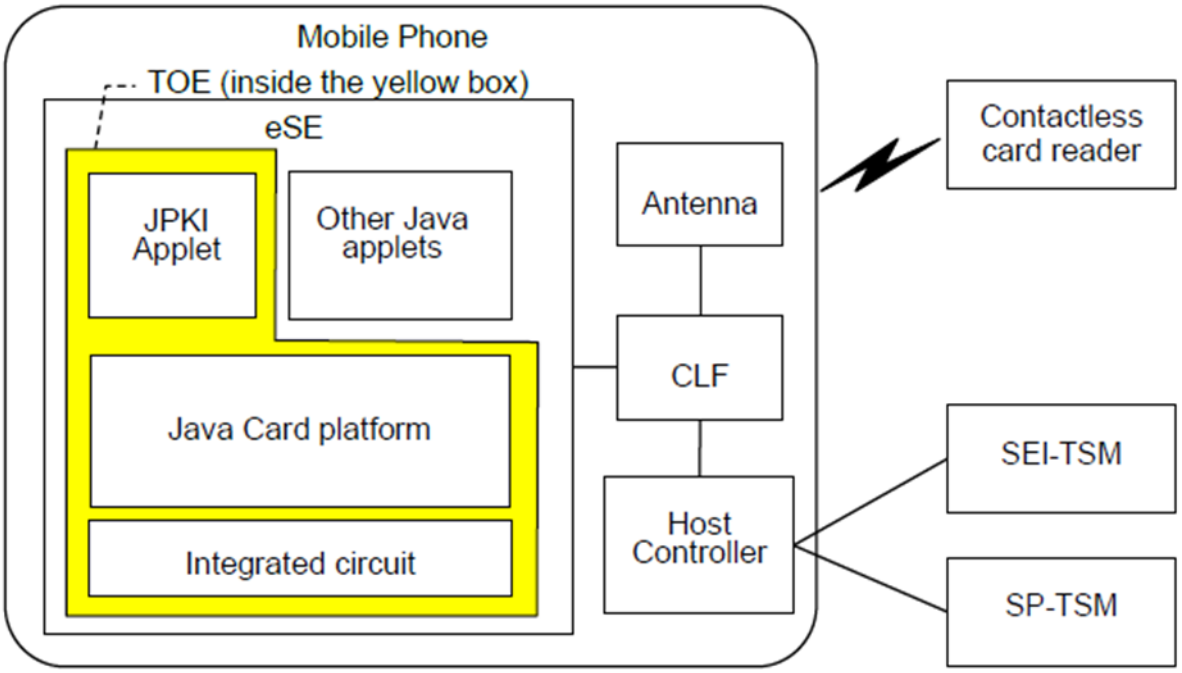

Figure 1-1 TOE Physical Scope

The TOE components are as follows:

- The JPKI Applet constitutes the part of the TOE responsible for generating key pairs for signature creation and user authentication. It manages access control for use of the signature creation function and access control for execution of cryptographic operations for signature creation. The JPKI Applet is installed post-issuance in the operational environment.

- The Java Card platform manages and executes applets. It provides APIs to develop APIs in accordance with the Java Card specifications. The Java Card platform includes a GlobalPlatform package that provides a common interface for managing communication with the smart card and applications in a secure manner in accordance with the GlobalPlatform specification [14].

- The IC is the hardware platform of the TOE. The hardware platform provides basic cryptographic functions and security-related detectors, sensors, and circuits to protect the TOE.

Non-TOE components are as follows:

- Other Java applets may coexist with the JPKI Applet, but they are independent of each other.

- The antenna is used to transmit and receive radio waves for communication with a contactless card reader.

- The CLF (Contactless Front-end) manages routing between the antenna and the Host Controller, controls transmission of the carrier wave of the antenna, and, as a card function, performs anti-collision and card selection.

- The TOE is assumed to operate on a mobile phone. Therefore, the above non-TOE components are also part of the mobile phone.

1.1.2.1 Security Functions Overview

In the PP [11], the TOE is required to provide the security functions required for an eSE that hosts the JPKI Applet, and the functions typically required for an IC. The main functions are as follows:

1. Protection of communication data
   Secure messaging is applied to communications between the TOE and the Certificate Generation Application (CGA) to protect the confidentiality and integrity of communication data.
2. User authentication and access control
   To provide functions according to user roles, the TOE performs user identification and authentication and enforces access control.
3. Cryptographic operations
   The TOE provides cryptographic functions for hash functions, generation of Secret Keys (SKs) / Public Keys (PKs), and signature generation/verification.
4. Countermeasures against physical attacks
   The security functions of the TOE also counter physical attacks against its own hardware components. The assumed attacks are the same as those for general ICs.

1.1.2.2 Threats and Security Objectives

A TOE conforming to the PP [11] counters threats by means of security functions as described below.
An attacker may attempt unauthorized access to disclose or modify data inside the TOE, or to use TOE functions illegally. Therefore, after identifying and authenticating a user, the TOE permits logical access to internal TOE resources only within the privileges corresponding to the user's role.
In addition, in communications between the TOE and an external terminal, there is a threat that an attacker eavesdrops and records the communication contents corresponding to external authentication and then reuses the recorded contents to impersonate a legitimate external terminal. To counter this threat, it is required that the authentication data used for external authentication (which is generated by the TOE) not be reused and that different data be used each time.
Due to the physical characteristics of IC chips, information being processed internally may leak via power consumption or electromagnetic emissions. It is also necessary to consider exposure of internal information by physical probing, physical tampering with circuits on the IC chip, and malfunction induced by applying environmental stress. Therefore, functions are required to protect the TSF from such physical attacks.

1.1.3 Disclaimers

None.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed in 2026-01, based on functional requirements and assurance requirements of the TOE according to the publicised 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 of Evaluation

The Certification Body verified the Evaluation Technical Report [12] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation and confirmed that the PP [11] evaluation was conducted in accordance with the prescribed procedure.

The certification oversight reviews were also prepared for those concerns found in the certification process.

The Certification Body confirmed that all the concerns pointed out by the Certification Body were fully resolved, and that the PP [11] evaluation had been appropriately conducted in accordance with the CC ([4][5][6][7][8]) and the CEM ([9]) and Errata and Interpretation ([10]).

The Certification Body prepared this Certification Report based on the Evaluation Technical Report and fully concluded certification activities.

2. PP Identification

The PP [11] is identified as follows:

PP Name:	JPKI Applet Protection Profile
PP Version:	1.10
Developer:	Digital Agency, Government of Japan

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organisational security policies.

In the PP [11], the TOE is required to provide security functions required for the services provided by the JPKI Applet and the security functions typically required of an IC. The security functions required of the TOE are broadly the following four:

- Protection of communication data
- User authentication and access control
- Cryptographic operations
- Resistance to physical attacks

3.1 Security Function Policies

The PP [11] possesses the security functions to counter the threats shown in Section 3.1.1.1 and to satisfy the organisational security policies shown in Section 3.1.2.1.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The PP [11] presumes the threats shown in Table 3-1 and provides TOE the security functions to counter them.

Table 3-1 Threats

Identifier	Threat
T.Illegal_Attack	An unauthorised user accesses the TOE via external interfaces to disclose or modify internal data of the TOE, or to use processing function of the TOE. "An unauthorised user" is the entity that does not have the authentication data needed to access the assets of the TOE.
T.Replay	An attacker masquerades a legitimate external terminal by monitoring, recording and replaying the authentication procedure between the TOE and the external terminal in order to be authenticated by the TOE. The attack causes disclosure or modification of user data of the TOE, or illegal use of processing function of the TOE.
T.Phys_Attack	An attacker attacks components of the TOE − hardware, firmware or software − with physical means. The attack causes disclosure or modification of user data of the TOE, or unauthorised use of processing function of the TOE.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in **Table 3-1** by the following security function policies.

1. Countermeasures against threat "T.Illegal_Attack" and "T.Replay"

The threat "T.Illegal_Attack" assumes unauthorized access to internal TOE data and functions via the TOE interface. "T.Replay" assumes unauthorized access to the TOE by reusing an authentication procedure in communications with an external terminal.
To counter these threats, the TOE identifies and authenticates users and, upon successful authentication, permits operations according to the user's role. The TOE also provides a function to prevent reuse of authentication data.

2. Countermeasures against threat "T.Phys_Attack"
The threat "T.Phys_Attack" assumes that, due to the physical form factor of an IC, it is exposed to physical tampering (observation, analysis, or modification). The TOE behavior is also affected by operating conditions such as voltage, frequency, and temperature.
To counter this threat, the TOE provides protection functions for the TSF to withstand attacks described in the mandatory technical document on smartcards and similar devices [13].

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 PP [11] are shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.Multiple_authentication	The TOE provides multiple authentication methods for user authentication. In addition to password authentication, the user can also select cryptographic-key-based authentication.
P.Secure_messaging	Secure messaging is applied to communications between the TOE and the CGA.
P.Cryptography	The TOE provides cryptographic functions used for data hashing, data protection, SK/PK generation, signature generation, and authentication.
P.RND	The TSF generates random numbers used for the TSF itself. The random numbers have sufficient quality to prevent prediction by attackers.

Table 3-3 Cryptographic Functional Policy

Function	Key length, specifications, etc.
Key pair generation	RSA 2048 bits or more [to be specified by the ST author at TOE certification] (this function is used to generate signatures over DTBS).
Signature generation	RSA 2048 bits or more [to be specified by the ST author at TOE certification] (this function is used to generate signatures over DTBS).
Signature verification	RSA 2048 bits or more [RSASSA-PKCS1-v1_5, PKCS #1] (this function is used for external authentication using PK-EA).
Hash	SHA-256 [FIPS 180-4].
Random number generation	Physical, hybrid-physical, or hybrid-deterministic random number generator.
Random number generation	Destroy the SK/PK pair and PK-EA when they are no longer needed.

3.1.2.2 Security Function Policies for Organisational Security Policies

The PP [11] provides the security functions to satisfy the organisational security policies shown in Table 3-2 and Table 3-3.

1. Means for organisational security policy “P.Multiple_authentication”
   The TOE provides the authentication mechanisms listed in Table 3-4.

Table 3-4 Multiple authentication mechanism

Authentication mechanism	Rules
Mutual authentication described in GlobalPlatform Card Specification – Amendment D [15]	This mutual authentication is used to authenticate the user as an administrator.
Password authentication	Password authentication is used as default authentication mechanism for authentication of Signatory.
External authentication using PK-EA	External authentication is used as alternative authentication mechanism for authenticating user as Signatory. To activate the method, the PK-EA corresponding to the individual Signatory needs to be registered.

2. Means for organisational security policy “P.Secure_messaging”
   This is addressed by the TOE providing an inter-TSF trusted channel.

3. Means for organisational security policy “P.Cryptography” and “P.RND”
   This is addressed by the TOE providing the cryptographic functions listed in Table 3-3.

4. Assumptions and Clarification of Evaluation Scope

This chapter describes the assumptions and the operational environment to operate a TOE as useful information for the assumed readers to determine whether to use of a TOE conforming to the PP [11].

4.1 Assumptions on Use and Environment

Table 4-1 shows assumptions to operate the TOE conforming to the the PP [11].
The effective performances of the TOE conforming to the PP [11] of security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Identifier	Assumptions
A.PKI	For the effective operation of the TSF, it is assumed that the PKI environment, where the keys for public key cryptosystem (a pair of public and private keys) of the TOE are assured to be effective, is provided.
A.Administrator	The administrator, who creates, changes or deletes data on the TOE, is assumed to be a trusted user and to operate the TOE properly based on the privileges.
A.Protect_VAD	The confidentiality and integrity of VAD is assumed to be guaranteed when VAD is imported from an external device to the TOE.

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, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

5.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance requirements in the CC Part 3.

Details for evaluation activities were reported in the Evaluation Technical Report.

The Evaluation Technical Report explains the summary of the PP [11] as well as the content of the evaluation and the verdict of each work unit in the CEM.

5.3 Overview of Evaluation Activity

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

The evaluation started in 2025-08 and concluded upon completion of the Evaluation Technical Report dated 2026-01.

The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer and examined the evidence in relation to a series of evaluation conducted.

Concerns found in evaluation activities were issued as the Observation Reports and reported to the developer.

The concerns were reviewed by the developer, and all of them were solved eventually.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

5.4 Evaluation Results

The evaluators had concluded that the PP [11] satisfies all work units prescribed in the CEM as per the Evaluation Technical Report.

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 and APE_REQ.2

5.5 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

6. Certification

Based on the evidence submitted by the Evaluation Facility during the evaluation process, the Certification Body has performed certification by checking that the following requirements are satisfied:

1. Contents pointed out in the Observation Reports shall be adequate.
2. Contents pointed out in the Observation Reports shall properly be solved.
3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of the evaluation verdict by the evaluators 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 the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the PP [11] and the Evaluation Technical Report and issued this Certification Report.

6.1 Certification Result

As a result of verification of the Evaluation Technical Report, Observation Reports and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the PP [11] evaluation satisfies all assurance requirements for 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

When conducting TOE evaluations, it is necessary to evaluate resistance not only against the threats specified in the PP [11] but also against threats described in the mandatory technical document on smartcards and similar devices [13]. This document covers attack potentials to smartcards and similar devices, including those specific to Java Card systems, because the TOE conformant to the PP [11] is hardware implementing Java Card systems. Authors of ST conformant to the PP [11] should note that definitions of security problems, security objectives, and security functional requirements addressing those threats are required, for example, by also conforming to a PP for Java Card systems.

7. Annexes

There is no annex.

8. Glossary

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
COMP	Composite Product Package
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

Certificate generation application (CGA)	collection of application components that receive the PK from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate
Data to be signed (DTBS)	all electronic data to be signed including a user message and additional information that is signed together with a user message
Data to be signed or its unique representation (DTBS/R)	data received by a SSCD as input in a single signature creation operation
Japanese Public Key Infrastructure (JPKI)	a safe and secure identity verification service that uses electronic certification installed in My Number Card's IC chips (My Number is not used) to officially authenticate users and confirm that documents such as contracts have not been tampered with online.
JPKI Applet	a java Card applet that is responsible for generating a key pair for digital signature and for user certification
JPKI Application	a mobile phone application responsible for CGA and Signature Creation Application (SCA).
Public Key (PK)	public cryptographic key that can be used to verify a digital signature. JPKI Applet has two PKs, which are “the public key for digital signature” and “the public key for user certification”.
PK-EA	Public key for external authentication
Secure Signature Creation Device (SSCD)	hardware or software that is used in creating a digital signature
Secure Element Issuer Trusted Service Manager (SEI-TSM)	responsible for managing the end-to-end security of the SE, including the deployment of applications and services.
Service Provide Trusted Service Manager (SP-TSM)	entity that issues certificates or provides other services related to digital signatures
Signature creation	application complementing a SSCD with a user

application (SCA)	interface with the purpose to create a digital signature
Secret Key (SK)	secret cryptographic key stored in the SSCD under exclusive control by the signatory to create a digital signature. JPKI Applet has two SKs, which are “the secret key for digital signature” and “the private key for user certification”.
Verification authentication data (VAD)	data provided as input to a SSCD for authentication

9. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, September 2025, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, December 2023, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CC:2022 Revision 1, November 2022, CCMB-2022-11-001(Japanese Version 1.0, September 2023)

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CC:2022 Revision 1, November 2022, CCMB-2022-11-002(Japanese Version 1.0, September 2023)

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CC:2022 Revision 1, November 2022, CCMB-2022-11-003(Japanese Version 1.0, September 2023)

[7] Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities CC:2022 Revision 1, November 2022, CCMB-2022-11-004(Japanese Version 1.0, September 2023)

[8] Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements CC:2022 Revision 1, November 2022, CCMB-2022-11-005(Japanese Version 1.0, September 2023)

[9] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, CEM:2022 Revision 1, November 2022, CCMB-2022-11-006 (Japanese Version 1.0, September 2023)

[10] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 2024, CCMB-2024-07-22 (Japanese Version 1.0, December 2024)

[11] JPKI Applet Protection Profile, Version 1.10, (January 2026), Digital Agency, Government of Japan

[12] Evaluation Technical Report, JPU-ETRPP-0001-05, Version 1.5, January 30, 2026, ECSEC Laboratory Inc. Evaluation Center

[13] Joint Interpretation Library - Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, February 2024

[14] GlobalPlatform Card Specification v2.3.1

[15] GlobalPlatform Card Specification – Amendment D v1.2, Secure Channel Protocol '03'

[16] Observation report JPU-EOR-0001-00, (September 17, 2025), ECSEC Laboratory Inc. Evaluation Center

[17] Observation report JPU-EOR-0002-00, (October 3, 2025), ECSEC Laboratory Inc. Evaluation Center