Security Target

ST introduction

The reference of this ST is **D1644959 JPKI ST – Connected eSE 5.3.4 v1.2** version **1.1**

TOE

The TOE is an IC Platform composed with the JPKI Applet. Designed to meet the security functionality of the Japanese Public Key Infrastructure PP [JPKIPP]
The product exists in two TOE configurations corresponding to two versions of Java Card OS with two EMVCo certificates:

- **Connected eSE 5.3.4 v1.2** (the initial version)
- **Connected eSE 5.3.4 v1.2 Rev 01** (corrected with functional patch)

TOE reference

The TOE is referred to as **JPKI Applet on Connected eSE 5.3.4 v1.2**, and is named and uniquely identified by its response to the GET DATA command, as follows:

	Field	Value
JPKI Applet	**Tag 0x00A5**	**04 02**

In addition, the platform can be uniquely identified using GET DATA command as follows:

OS Identification

- Identification data: GET DATA command on ISD application using tag 00FE
- Value for this product for both configurations:
  - FE 17
    - 06 0C 2B060104012A026E01030100
    - 06 07 D0026A15FA0109 (see below for interpretation)

OS Update (patch info)

- Identification data: GET DATA command on ISD application using tag 00FD
- Value for each configuration of this product:
  - FD 04 (see below for interpretation)
    - 00000000 for **Connected eSE 5.3.4 v1.2** configuration
    - 00010000 for **Connected eSE 5.3.4 v1.2 Rev 01** configuration

Field	Value
OS identification: - Java Card version	2B060104012A026E01030100
OS identification: - PDM counter - OS release	 D0026A15FA 0109 (meaning OS Release / Check Point 1.09)

Field	Value
OS update	00000000 (meaning No Patch, for **Connected eSE 5.3.4 v1.2**) 00010000 (meaning Patch 01.00, for **Connected eSE 5.3.4 v1.2 Rev 01**)

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	ST54L	(diced) wafer/module/card	ICCN0300 valid until April 04, 2026	2023-04-04
Java Card OS[1]	Connected eSE 5.3.4 v1.2	Embedded in the above	PCN0199.02 valid until June 30, 2026	2023-06-30
	Connected eSE 5.3.4 v1.2 Rev 01	Embedded in the above	PCN0199.03 valid until June 30, 2026	2023-06-30
JPKI Applet	04 02	Embedded in the above	n/a	n/a
Applet Guidance documentation	[AGD-Applet]	pdf	n/a	n/a

Conformance claims

This ST claims strict compliance to the Japanese Public Key Infrastructure PP [JPKIPP] under CC:2022 Release1.

This ST is CC Part 2 conformant:

- Exactly, the SFRs of the [JPKIPP] are included by reference.
- Assignments for all open operations in the [JPKIPP] are provided in this ST.

The ST is CC Part 3 conformant:

- The assurance package is **EAL4 augmented with ALC_DVS.2 and AVA_VAN.5**.

The ST is CC Part 3 conformant:

- **Composite product package (COMP)** is selected

The rationale behind these claims is the requirement that the JPKI-MD scheme requires compliance to this [JPKIPP] for this TOE type (JPKI products).

[1] The Java Card Platform component includes all the guidance required by the user, as it is listed in its own certificate, relevant for the correct operation and usage of this component after TOE delivery. Therefore, this guidance is also considered part of the TOE. See the Java Card certificate for further details.

Security Problem Definition

Refer to [JPKIPP].

Objectives

Refer to [JPKIPP].

Extended components definitions

Refer to [JPKIPP].

Security Requirements

Security Functional Requirements

The [JPKIPP] defines the SFRs. TOE specific information is required to be assigned to the following SFRs, either:

- predefined according to the latest JPKI specification with underlined text,
- by the addition of the requested information
- as a selection from a two or more options
- Iterations are denoted by showing a slash "/"

In all cases, the JPKIPP should be referenced for relevant application notes and other guidance.

SFR Reference	SFR	Assignment value/selection
FCS_CKM.1.1	The TSF shall generate SK/PK pair in accordance with a specified cryptographic key generation algorithm RSA and specified cryptographic key sizes 2048 bit that meet the following: [assignment: *list of standards*][1].	1: [ISO-18032] and [ETSI-102176]
FCS_CKM.6.2/SK	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method either overwriting with new ones or deleting ones when JPKI Applet deletion that meets the following: none.	---
FCS_CKM.6.2/PK-EA	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method either overwriting with new ones or deleting ones when JPKI Applet deletion that meets the following: none.	---
FCS_COP.1.1/SK	The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 2048 bit that meet the following: RSASSA-PKCS1-v1_5 in [PKCS #1].	---
FCS_COP.1.1/PK-EA	The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 2048 bit that meet the following: RSASSA-PKCS1-v1_5 in [PKCS #1].	---

FCS_RNG.1.1	The TSF shall provide a [selection: *physical, hybrid physical, hybrid deterministic*][2] random number generator that implements: [assignment: *list of security capabilities*][3].	2: hybrid deterministic 3: hybrid design, forward secrecy, enhanced backward secrecy, enhanced forward secrecy, entropy input quality
FCS_RNG.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]][4] that meet [assignment: *a defined quality metric*][5].	4: bits 5: Test Procedure A of BSI AIS-31
FIA_UID.1.1	The TSF shall allow: (1) select files, (2) verify the digital signature verification, (3) read user data on behalf of the user to be performed before the user is identified.	---
FIA_UAU.1.1	The TSF shall allow: (1) select files, (2) verify the digital signature verification, (3) read user data on behalf of the user to be performed before the user is authenticated.	---
FIA_AFL.1.1	The TSF shall detect when 5 in user authentication for digital signature or 3 in user authentication for user certification unsuccessful authentication attempts occur related to consecutive failed authentication attempts.	---
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for (1) generation of SK/PK pair, export of PK and import of Certificate (2) creation and unblocking of PW (3) update of user data (4) none	---

Security Assurance Requirements and Rationale

See section “Conformance claims”.

TOE Summary Specification

The TOE implements the SFRs by access control to the JPKI services in accordance with the JPKI specification, sufficiently hardened to counter attackers at AVA_VAN.5 level.

References

[JPKIPP] Digital Agency, Government of Japan, JPKI Applet Protection Profile version 1.1

[AGD-Applet] Commercial Applet for Mobile JPKI Projects External Interface Specification v1.0
JPKI Applet User guidance v0.5
JPKI Applet Installation Procedure v0.5
JPKI Applet Delivery and Acceptance procedure v0.5

[ISO-18032] ISO/IEC 18032:2020, Information security — Prime number generation. Edition 2, 2020

[ETSI-102176] ETSI TS 102 176-1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. V2.0.0 (2007-11)

ST revision history

0.1 Creation (July 28, 2025)
1.0 Final version conform to ST-Template 0.9 and PP v1.0 (January 9, 2026)
1.1 Update to ST-Template 0.91 and PP v1.1 (January 22, 2026)