

Security Target

ST introduction

The reference of this ST is **Security Target for JPKI Applet on JCOP8.9 R6 SN330 version 0.87**

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]

TOE reference

The TOE is referred to as **JPKI Applet on JCOP8.9 R6 SN330 version 1.0**, 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 and the hardware can be uniquely identified as JCOP-eSE 8.9 R6.01.00.1.1 on SN330 as follows:

GET VERSION QUERY command on wired interface to ISD or CASD; see [P_AGD1], [P_AGD2] ([P_AGD1] gives version information for the JCOP OS, while [P_AGD2] gives the version for the System OS)

	Field	Value
IC	0x8C	0x5F (SN330 A0)
Platform	0x82	N5F0000000030600

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	SN330_SE A0.1.000 J20	Diced wafer	ICCN0313	14 Nov. 2024
Java Card OS ¹	JCOP-eSE 8.9 R6.01.00.1.1 (R6-01)	Embedded in the above	PCN0220	06 Jun 2025
JPKI Applet	04 02	Embedded in the above	n/a	n/a
Applet Guidance documentation	[AGD-Applet]	pdf	n/a	n/a

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.

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 5 conformant:

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

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

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 **highlighted in yellow** or
- as a selection from a two or more options, as **highlighted in blue**.
- 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 <u>SK/PK pair</u> in accordance with a specified cryptographic key generation algorithm <u>RSA</u> and specified cryptographic key sizes <u>2048 bit</u> that meet the following: [assignment: list of standards] ¹	1: FIPS 186-4
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 <u>either overwriting with new ones or deleting ones when JPKI Applet deletion</u> that meets the following: <u>none</u> .	---
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 <u>either overwriting with new ones or deleting ones when JPKI Applet deletion</u> that meets the following: <u>none</u> .	---
FCS_COP.1.1/SK	The TSF shall perform <u>digital signature creation</u> in accordance with a specified cryptographic algorithm <u>RSA</u> and cryptographic key sizes <u>2048 bit</u> that meet the following: <u>RSASSA-PKCS1-v1_5</u> in [PKCS #1].	---
FCS_COP.1.1/PK-EA	The TSF shall perform <u>digital signature verification</u> in accordance with a specified cryptographic algorithm <u>RSA</u> and cryptographic key sizes <u>2048 bit</u> that meet the following: <u>RSASSA-PKCS1-v1_5</u> in [PKCS #1].	---

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

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 1.10
- [P_AGD1] JCOP 8.9 R6 (SN330) User Guidance Manual, Rev. 1.8.0, 08 May 2025
- [P_AGD2] JCOP 8.9 R6 (SN330) User Guidance Manual Addendum System Management, Rev. 1.8.0, 08 May 2025
- [GP] GlobalPlatform Card Specification v2.2.1
- [GP_D] GlobalPlatform Card Specification – Amendment D Secure Channel Protocol ‘03’ v1.1.1
- [JC_SPEC] Java Card Platform Virtual Machine Specification, Classic Edition Version 3.0.4
- [JIWG] Joint Interpretation Library – Application of Attack Potential to Smartcards v3.2.1
- [AGD-Applet] Commercial Applet for Mobile JPKI Projects External Interface Specification v1.0
JPKI Applet User guidance v0.7
JPKI Applet Installation Procedure v0.6
JPKI Applet Delivery and Acceptance procedure v0.6