

JREM KM67S3B2 Contactless Smart Card IC chip with fast processing function for transport Security Target

ST introduction

The reference of this ST is **JS4-ST-E01-30** version **1.3**

TOE

The TOE is an IC Platform composed with the FeliCa Crypto Lib and the FeliCa Applet. Designed to meet the security functionality of the Public Transportation IC Card PP (PTPP)

TOE reference

The TOE is referred to as **JREM KM67S3B2 Contactless Smart Card IC chip with fast processing function for transport Version 1.0** and is named and uniquely identified by its response to the Polling command sent from a FeliCa Reader/Write, as follows:

Field	Field	Value
IC	Hardware identifier	0x0101
IC	Hardware version	0x0000
IC dedicated software	HAL version	0x000C
FeliCa OS v5.0	OS revision	0x0211

The user can check Hardware version, HAL version and OS revision by inputting “Request Product Information” command, and Hardware identifier by “Get Chip ID” command. For more details, see “JREM KM67S3B2 Contactless Smart Card IC chip with fast processing function for transport Inspection Procedure”.

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	KM67S3B2	wafer	ANSSI-CC-2024/35	2024-12-06
IC dedicated software	KM67S3B2	Embedded in the above	ANSSI-CC-2024/35	2024-12-06
FeliCa OS v5.0		Embedded in the above	FAST-2500029-01	
(Pre)personalisation documentation	M1260-E00-40	PDF	n/a	n/a
Operational guidance	None	None	n/a	n/a

Only (pre-)personalisation guidance is provided. No operational guidance other than the FeliCa specifications is provided.

Any (pre-)personalisation performed by the developer of the TOE on behalf of its customers will lead to a state identical to states possible by executing the FeliCa commands for personalisation.

Conformance claims

This ST claims strict compliance to the Public Transportation IC Card PP (called “[PTPP]” in the remainder of this document) under Common Criteria version 3.1, revision 5.

This ST is CC Part 2 conformant:

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

The ST is CC Part 3 conformant:

- The assurance package is **EAL5 augmented with AVA_VAN.5 and ALC_DVS.2**.

The rationale behind these claims is the requirement that the FeliCa security evaluation scheme requires compliance to this [PTPP] for this TOE type (FeliCa products).

Security Problem Definition

Refer to [PTPP].

Objectives

Refer to [PTPP].

Extended components definition

Refer to [PTPP].

Security Requirements

Security Functional Requirements

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

- 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**.

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

SFR Reference	SFR	Assignment value/selection
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: memory area] ¹	1: memory areas protected by an access control system in the Flash memory
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: integrity errors] ² on all objects, based on the following attributes: [assignment: user data attributes] ³	2: bit corruption 3: data integrity checksum
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [assignment: action to be taken] ⁴ .	4: return an error code
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required] ¹⁵ .	15: Secure_read ¹ , Secure_write ² , management of security attribute
FIA_UID.1.1	The TSF shall allow Polling, Public read, Public write and [selection: [assignment: other list of TSF mediated actions], none] ¹⁷ on behalf of the user to be performed before the user is identified.	17: Requests ³ , Echo Back ⁴ , Reset Modes ⁵
FIA_UAU.1.1	The TSF shall allow Polling, Public_read, Public_write and [selection: [assignment: other list of TSF mediated actions], none] ¹⁸ on behalf of the user to be performed before the user is authenticated.	18: Requests ³ , Echo Back ⁴ , Reset Modes ⁵
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)] ¹⁹ .	19: all authentication mechanisms
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects	25: none

	based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] ²⁵ .	
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] ²⁶ .	26: none
FMT_MSA.1.1	The TSF shall enforce the Service Access Policy ²⁷ to restrict the ability to set and [selection: [assignment: other operations], none] ²⁸ the security attributes ACL ²⁹ to Administrator ³⁰	28: none
FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery ³⁴ with the capability to store Initialisation Data and [selection **: [assignment: other data], none] ³⁵ in the [assignment: type of persistent memory] ³⁶	35: none 36: Flash memory

¹ Secure_read is a read operation to the user data files that require authentication with the Access Key corresponding to the Service.

² Secure_write is a write operation to the user data files that require authentication with the Access Key corresponding to the Service.

³ Requests is an operation to retrieve a configure, status or version information from the TOE that does not required authentication.

⁴ Echo Back is an operation to perform the communication test that does not required authentication.

⁵ Reset Mode is an operation to reset authentication status to “Not authenticated”.

Security Assurance Requirements and Rationale

See section “Conformance claims”.

TOE Summary Specification

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

References

- [PTPP] JICSAP (Japan ID Connect with Secure Authentication Promotional association) Public Transportation IC Card Protection Profile, version 1.12, 1 August 2018.