

Security Target

ST introduction

The reference of this ST is **ST_SN300_FeliCa_v6.1.5_JCOP-eSE_8.9_R1-01.doc** version **1.6**

TOE

The TOE is an IC Platform composed with the FeliCa Crypto Library. Designed to meet the security functionality of the package “FeliCa Crypto Library” defined in Mobile FeliCa Applet Protection Profile[MFAPP].

TOE reference

The TOE is referred to as (long form) “**NXP FeliCa Crypto-Library v6.1.5 on JCOP-eSE 8.9 R1.06.01.1.1**” (short form **JCOP-eSE 8.9 R1-01**), and is named and uniquely identified by its response to the ~~Polling command sent from a Felica Reader/Write~~ GET VERSION QUERY command on wired interface to ISD or CASD as follows:

Field	Field	Value
JCOP ID	0x82	N5F2M500001B0600
HW ID	0x8C	0x4B (SN300 B5)

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	SN300_SE B5.1.002 JD	(diced) wafer	ICCN0302	17-03-2022
JavaCard	JCOP-eSE 8.9 R1.06.01.1.1 (R1-01)	Embedded in the above	PCN0206.03	16 May 2023 (PCN back date)
FeliCa Crypto library	FeliCa Crypto-Library v6.1.5	Embedded in the above	FAST-2300101-01¹	See API checker ‘s Logs
Security Guidance	JCOP 8.9 R1 User Guidance Manual, Rev. 1.6, 29 Jan. 2024 JCOP 8.9 R1 User Guidance Manual Addendum System Management, Rev. 1.6, 29 Jan. 2024	Documentation	Part of PCN	Part of PCN

¹ FeliCa Crypto library functionality is verified using the API Checker tool [FeliCa-CL-Tool] provided from FeliCa Networks.

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
	<p>JCOP-eSE 8.9 R1 User Guidance Manual for JCOP eSE, Rev. 1.6, 29 Jan. 2024</p> <p>JCOP-eSE 8.9 R1 User Guidance Manual Addendum for JCOP eSE, Rev. 1.6, 29 Jan. 2024</p> <p>JCOP 8.9 R1 CSP User Manual Addendum, Rev. 1.6, 29 Jan. 2024</p> <p>JCOP 8.9 R1 Amd I SEMS Application User Manual Addendum, Rev. 1.6, 29 Jan. 2024</p> <p>JCOP 8.9 R1 Anomaly Sheet, Rev. 1.6, 29 Jan. 2024</p>			

Note: JCOP-SE 8.9 R1.06.02.1 is a system level identifier. It can also be referred as JCOP-SE 8.9 R1-02. The System hosts multiple guest OS which use a 4th identifier byte to differentiate.

<u>JCOP 8.9</u>	<u>OS</u>
JCOP-SE 8.9 R1.06.02.1	<u>System Identifier</u>
JCOP-eSE 8.9 R1.06.01.1.1	<u>eSE OS Identifier</u>
JCOP-eUICC 8.9 R1.06.00.1.2	<u>eUICC OS Identifier</u>

Only the eSE OS “JCOP-eSE 8.9 R1.06.01.1.1” (short form JCOP-eSE 8.9 R1-01) supports Felica, therefore user guidance documents related to the eUICC OS are not relevant. Further JCOP-eUICC and related JCOP-SE can exist.

The TOE claims the following FeliCa Crypto library packages of the [MFAPP] section 6:

DES1 DES2 DES3 AES1 AES2

Information for Composite Evaluations

[CL-ETRFC] has to be assessed as part of any composite evaluation using this Crypto Library.

Conformance claims

This ST does not claim compliance to any PP but it is based on [MFAPP] as it uses the FeliCa Crypto Library packages defined in [MFAPP] Section 6.

This ST claims to be conformant to the Common Criteria version 3.1, revision 5.

This ST is CC Part 2 conformant:

- Exactly, the SFRs of the [MFAPP] Section 6 are included by reference.

The ST is CC Part 3 conformant:

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

The rationale behind these claims is the requirement that the FeliCa Approval for Security and Trust (FAST) scheme requires compliance to this [MFAPP] for this TOE type (FeliCa products).

Security Problem Definition

Refer to [MFAPP] Section 6.

Objectives

Refer to [MFAPP] Section 6 and TOE FeliCa Crypto Library algorithms selected in section "TOE overview".

Extended components definition

Refer to [MFAPP] Section 6.

Security Requirements

Security Functional Requirements

Refer to [MFAPP] Section 6 and TOE FeliCa Crypto Library algorithms selected in section "TOE overview".

Security Assurance Requirements and Rationale

See section "Conformance claims".

TOE Summary Specification

The TOE implements the SFRs in accordance to the FeliCa CL specification, sufficiently hardened to counter attackers at AVA_VAN.5 level.

References

[FeliCa-CL-Tool] FAST FeliCa Crypto Library API Checker tool list version 1.0

[MFAPP]
[CL-ETRfc]
[AGD]

FeliCa Networks, Inc. Mobile FeliCa Applet Protection Profile, version 1.0
FeliCa Shared Evaluation report / ETRfc, version 3, 2024-02-27
JCOP 8.9 R1 User Guidance Manual, Rev. 1.6, 29 Jan. 2024