Security Target

ST introduction
The reference of this ST is
ST_NXP_FeliCa_Crypto_Library_v2.1.0_and_NXP_FeliCa_API_on_JCOP_6.2_R5.02.1_v1.0
(version 1.0)
(Security Target template is v1.0)

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 NXP FeliCa Crypto Library v2.1.0 and NXP FeliCa API on JCOP 6.2 R5.02.1. The FeliCa components are part of the JCOP OS and are identified by the same identification. The evaluated TOE carries the following identification data:

<table>
<thead>
<tr>
<th>Platform identifier</th>
<th>JCOP version</th>
</tr>
</thead>
<tbody>
<tr>
<td>N5D2M004AD970600</td>
<td>6.2 R5.02.1</td>
</tr>
</tbody>
</table>

Table 1 TOE identification

The version of each JCOP is identified by means of the Platform Identifier as stated in the TOE guidance [AGD] Section 1. The Platform Identifier is as follows: N5D2M004AD970600.

TOE overview
The TOE consists of the following:

<table>
<thead>
<tr>
<th>TOE component</th>
<th>Identification</th>
<th>Form of delivery</th>
<th>Certification identifier</th>
<th>Certificate issue date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware IC</td>
<td>SN220 B0.1 C37</td>
<td>(diced) wafer</td>
<td>ICCN0281</td>
<td>15-Jul-2021</td>
</tr>
<tr>
<td>JavaCard</td>
<td>JCOP 6.2 R5.02.1</td>
<td>Embedded in the above</td>
<td>PCN0189.06</td>
<td>21-Mar-2024 (PCN 1st issuance: 12-Oct-2021)</td>
</tr>
<tr>
<td>FeliCa Crypto library</td>
<td>FeliCa Crypto-Library v2.1.0</td>
<td>Embedded in the above</td>
<td>FAST-2400017-01 n/a¹</td>
<td>See API checker ‘s Logs</td>
</tr>
<tr>
<td>Security Guidance</td>
<td></td>
<td>JCP 6.2 R5.02.1, User Guidance Manual, Rev. 1.0,</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

¹ FeliCa Crypto library functionality is verified using the API Checker tool [FeliCa-CL-Tool] provided from FeliCa Networks.
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] FeliCa Networks, Inc. Mobile FeliCa Applet Protection Profile, version 1.0
[CL-ETRfc] ETRfc of NXP FeliCa Crypto Library v2.1.0 and NXP FeliCa API on JCOP 6.2 R5.02.1; version v2.0
[AGD] JCOP 6.2 R5.02.1 User Guidance Manual, Rev. 1.0, 05.Mar.2024