Security Target

ST introduction
The reference of this ST is Security Target for Mobile FeliCa Applet3 on JCOP 6.6_SN100 v1.0 version v1.1

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 Mobile FeliCa Applet Protection Profile[MFAPP].

TOE reference
The TOE is referred to as Mobile FeliCa Applet3 on JCOP 6.6_SN100 v1.0, and is named and uniquely identified by its response to the Request Product information command sent from a FeliCa Reader/Write, as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FeliCa applet</td>
<td>Request Product information</td>
<td>0x 90 38</td>
</tr>
</tbody>
</table>

In addition, the platform and the hardware can be uniquely identified as per the JCOP user guidance manual [JCOP- UGM], using the GET DATA command with 0xDF4C tag, as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Tag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCOP ID</td>
<td>0x82</td>
<td>N5B2M004C7ED0000</td>
</tr>
<tr>
<td>Hardware ID</td>
<td>0x8C</td>
<td>0x23</td>
</tr>
<tr>
<td>DeviceType</td>
<td>0x87</td>
<td>0x64</td>
</tr>
</tbody>
</table>

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>SN100 B2.1 C25</td>
<td>(diced) wafer</td>
<td>ICCN0254</td>
<td>2018-05-25</td>
</tr>
<tr>
<td>JavaCard</td>
<td>JCOP 6.6 “SN100” R1.06.0</td>
<td>Embedded in the above</td>
<td>PCN0156.20</td>
<td>2018-06-19</td>
</tr>
<tr>
<td>FeliCa Crypto library</td>
<td>FeliCa Crypto-Library v1.0.0 on JCOP 6.6 “SN100” R1.06.0</td>
<td>Embedded in the above</td>
<td>FAST-2400027-01</td>
<td>2024-05-23</td>
</tr>
<tr>
<td>FeliCa applet</td>
<td>Mobile FeliCa Applet3 on JCOP 6.6_SN100</td>
<td>Embedded in the above</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
The TOE claims the following FeliCa Crypto library packages of the [MFAPP] section 6:
- DES1
- DES2
- DES3
- AES1
- AES2

Conformance claims
This ST claims strict compliance to the Mobile FeliCa Applet Protection Profile (called “[MFAPP]” 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 [MFAPP] 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 security evaluation scheme requires compliance to this [MFAPP] for this TOE type (FeliCa products).

Security Problem Definition
Refer to [MFAPP].

Objectives
Refer to [MFAPP].

Extended components definition
Refer to [MFAPP].

Security Requirements

Security Functional Requirements
Refer to [MFAPP].

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 to the FeliCa specification, sufficiently hardened to counter attackers at AVA_VAN.5 level.

References
[MFAPP] FeliCa Networks, Inc. Mobile FeliCa Applet Protection Profile, version 1.0