Security Target

ST introduction
The reference of this ST is Secure Element N5B2M00386D20000 SN100 with MIFARE DESFire EV2 1.0.17.0Q Security Target version 3.0, dated May 12, 2022.

TOE
The TOE is an open platform implementing the MIFARE specification [MIFARE-DES-EV2] and the access control in the MIFARE services. See PP(s) for details.

TOE reference
The TOE is referred to as Secure Element N5B2M00386D20000 SN100 with MIFARE DESFire EV2 1.0.17.0Q and is named and uniquely identified using the Get Version command as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VendorID</td>
<td>0x04</td>
</tr>
<tr>
<td>HWMajorVersion</td>
<td>0x62</td>
</tr>
<tr>
<td>HWMinorVersion</td>
<td>0x00</td>
</tr>
<tr>
<td>SWMajorVersion</td>
<td>0x02</td>
</tr>
<tr>
<td>SWMinorVersion</td>
<td>0x00</td>
</tr>
<tr>
<td>CWCY</td>
<td>0x4319</td>
</tr>
</tbody>
</table>

In addition, the TOE 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>N5B2M00386D20000</td>
</tr>
<tr>
<td>Hardware ID</td>
<td>0x8C</td>
<td>0x08</td>
</tr>
<tr>
<td>DeviceType</td>
<td>0x87</td>
<td>0x64</td>
</tr>
</tbody>
</table>

The DESFire EV2 applet consists of 4 components, as follows:
- DESFire mfcarrier-DFEV2-1.0.17.0Q-20191021 (SVN revision 50652)
- SIO Library interfacesio-1.0.10.0Q-20190116 (SVN revision 41581)
- MCM mcm-1.0.13.0Q-20191119 (SVN revision 51573)
- lib-DFEV2-1.0.17.0Q-20191021 (SVN revision 50652)

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>Date of certificate issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware IC</td>
<td>SN100 B2.1 C25</td>
<td>(diced) wafer/module/card</td>
<td>ICCN0254</td>
<td>2018-05-25</td>
</tr>
</tbody>
</table>
**Crypto libraries**

<table>
<thead>
<tr>
<th>Library</th>
<th>Version</th>
<th>Embedded in the above</th>
<th>Included in the ICCN</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaCard</td>
<td>JCO 6.4 “SN100” R1.06.0</td>
<td>Embedded in the above</td>
<td>PCN0156.16</td>
<td>2018-06-19</td>
</tr>
<tr>
<td>MIFARE applet</td>
<td>1.0.17.0Q</td>
<td>Embedded in the above</td>
<td>D2A_2204_002</td>
<td>2022-04-22</td>
</tr>
</tbody>
</table>

Only (pre-)personalisation guidance is provided. No operational guidance other than the MIFARE 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 MIFARE commands for personalisation.

**Conformance claims**

This ST claims strict compliance to [MIFARE DESFIRE PP] (called “PP(s)” in the remainder of this document) under Common Criteria version 3.1, revision 5. Exactly the SFRs of the PP(s) are included by reference, no omissions nor additions have been made. The ST is therefore CC Part 2 conformant. The assurance package is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. The ST is therefore CC Part 3 conformant. The rationale behind this claim is the requirement that the MIFARE security evaluation scheme requires compliance to this PP(s) for this TOE type (MIFARE products).

**Security Problem Definition**

See PP(s).

**Objectives**

See PP(s).

**Extended components definition**

There are no extended components, see PP(s).

**Security Requirements**

**Security Functional Requirements**

See PP(s). Note that the PP has no open operations.

**Security Assurance Requirements**

See section “Conformance claims”.

**Rationale**

See PP(s).
TOE Summary Specification
The TOE implements the SFRs by access control to the MIFARE services in accordance to the MIFARE specification, sufficiently hardened to counter attackers at AVA_VAN.5 level.

References
[MIFARE-DES-EV2] MIFARE DESFire EV2 Reference Architecture, Rev. 1.4 (ra321914)
[MIFARE DESFIRE PP] MIFARE DESFire EV1/EV2/EV3 Protection Profile v1.3
[JCOP-UGM] JCOP 6.4 R1.06.0 User Guidance Manual Rev. 5.7 – March 31, 2022