Security Target

ST introduction
The reference of this ST is “MIFARE_DESFire_EV2_on_N7121_Security_Target” version 1.4_4 date 2022.05.31.

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 “MIFARE DESFire EV2 on N7121”, and is named and uniquely identified using the GetVersion 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>0x42</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>SW Sub-Type</td>
<td>0x05</td>
</tr>
<tr>
<td>BatchNo[4]</td>
<td>0x1C</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>NXP Secure Smart Card Controller N7121 with IC Ded. SW and CL</td>
<td>N7121 B1</td>
<td>wafer</td>
<td>ICCN0258</td>
<td>2018-11-22</td>
</tr>
<tr>
<td>MIFARE applet</td>
<td>v2.0.0.28</td>
<td>Embedded in the above</td>
<td>D2C_2205_004</td>
<td>2022-05-26</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MF-1800002-03</td>
<td>tbd</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