Security Target

ST introduction

The reference of this ST is **Secure Element N5B2M002C3A50000 SN200 with MIFARE DESFire EV2 1.0.17.0Q Security Target version 1.0, dated November 2, 2020.**

TOE

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

TOE reference

The TOE is referred to as **Secure Element N5B2M002C3A50000 SN200 with MIFARE DESFire EV2 1.0.17.0Q** and is named and uniquely identified using the GetVersion command as follows:

Field	Value
VendorID	**0x04**
HWMajorVersion	**0x62**
HWMinorVersion	**0x01**
SWMajorVersion	**0x02**
SWMinorVersion	**0x00**
CWCY	**0x4319**

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:

Field	Tag	Value
JCOP ID	0x82	**N5B2M002C3A50000**
Hardare ID	0x8C	**0x23**
DeviceType	0x87	**0xC8**

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:

TOE component	Identification	Form of delivery	Certification identifier	Date of certificate issue
Hardware IC	**SN200 B1.1 C04**	**(diced) wafer/module/card**	**ICCN0264**	**2019-05-14**
Crypto libraries	**1.0.0**	**Embedded in the above**	**Included in ICCN**	
JavaCard	**N5B2M002C3A50000**	**Embedded in the above**	**PCN0165.04**	**2019-05-29**

MIFARE applet	**1.0.17.0Q**	**Embedded in the above**	**Functional: D2A_2010_003 Security: MF-2000015-01**	**2020-10-29**

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" in the remainder of this document) under Common Criteria version 3.1, revision 5.
Exactly the SFRs of the PP 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 for this TOE type (MIFARE products).

Security Problem Definition

See PP.

Objectives

See PP.

Extended components definition

There are no extended components, see PP.

Security Requirements

Security Functional Requirements

See PP. Note that the PP has no open operations.

Security Assurance Requirements

See section "Conformance claims".

Rationale

See PP.

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 DESFIRE PP] MIFARE DESFire EV1/EV2/EV3 Protection Profile v1.2
[MIFARE-DES-EV2] MIFARE DESFire EV2 Reference Architecture, ra321914
[JCOP-UGM] JCOP 6.1 R2.03.0 User Guidance Manual Rev. 4.3, 8 September 2020