Security Target

ST introduction

The reference of this ST is **Secure Element N5E0000001100000 SN300B2 with MIFARE DESFire EV2 1.0.23.0B Security Target version 1.0, dated April 25, 2024**

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 N5E0000001100000 SN300B2 with MIFARE DESFire EV2 1.0.23.0B**, 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	**0x5022**

In addition, the TOE can be uniquely identified by the same identification as per the JCOP user guidance manual [AGD1] [AGD2], using the GET DATA command with 0xDF4C tag, as follows:

Field	Tag	Value
JCOP ID	0x82	**N5E0000001100000**
HW ID	0x8C	**0x49**

The DESFire EV2 applet consists of 4 components, as follows:

- DESFire mfcarrier-DFEV2-1.0.23.0B-20221214 (SVN revision 93270)
- SIO Library interfacesio-1.0.13.0Q-20220831 (SVN revision 90875)
- MCM mcm-1.0.18.0Q-20220831 (SVN revision 90863)
- lib-DFEV2-1.0.23.0B-20221214 (SVN revision 93270)

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	**SN300 B2.1.001 JB**	**(diced) wafer/module/card**	**ICCN0297**	**2022-03-17**
Crypto libraries	**1.0.0**	**Embedded in**	**Included in the**	**-**

		the above	**PCN**	
JavaCard	**JCOP 8.1 "SN300B2" R1.06.0.1**	**Embedded in the above**	**PCN0200.02**	**2023-05-16**
MIFARE applet	**1.0.23.0B**	**Embedded in the above**	**D2A_2403_004**	**2024-03-26**

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) Specification, Rev. 3.0

[MIFARE DESFIRE PP] MIFARE DESFire EV1/EV2/EV3 Protection Profile v1.5

[AGD1] JCOP 8.1 R1.06.0.1 User Guidance Manual Feb. 2024

[AGD2] JCOP 8.1 User Guidance Manual Addendum for JCOP eSE Feb. 2024