Security Target

ST introduction

The reference of this ST is **N5D2M003D0430600** version **MIFARE DESFire EV2** `2.2.2.1JxU` **Security Target version v1.5_2, date 14.12.2022.**

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 N5D2M003D0430600** with **MIFARE DESFire EV2** 2.2.2.1JxU, and is named and uniquely identified using the GetVersion command as follows:

Field	**Value**
VendorID	**0x04**
HWMajorVersion	**0x72**
HWMinorVersion,	**0x00**
SWMajorVersion	**0x02**
SWMinorVersion	**0x02**
CWCY	**5021**

In addition, the TOE can be uniquely identified as per the JCOP user guidance manual [JCOP-UGM], using the GET DATA command with 0xDF20 tag, as follows:

Field	**Value**
JCOP ID	N5D2M003D0430600

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	SN220 Series B0.1 C37	**(diced) wafer/module/card**	**ICCN0281**	**2021-07-15**
Crypto libraries	Crypto Library v 2.3.1	**Embedded in the above**	**Included in ICCN**	**2021-07-15**
JavaCard	N5D2M003D0430600	**Embedded in the above**	**PCN0189.02**	**2021-10-12**
MIFARE applet	2.2.2.1JxU	**Embedded in the above**	**Functional: D2A_2210_005 Security: MF-2000029-03**	**2022-10-24**

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 v1.5
[JCOP-UGM] JCOP 6.2 R2.01.1 User Guidance Manual Rev. 1.2, 30. Sep 2022