

# Security Target

## ST introduction

The reference of this ST is **JCOP-eSE 8.9 R1.06.01.1.1** with **MIFARE DESFire EV2 3.2.1.1NxD Security Target version v1.5\_6, date 23.05.2024**.

## 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 JCOP-eSE 8.9 R1.06.01.1.1** with **MIFARE DESFire EV2 3.2.1.1NxD**, and is named and uniquely identified using the GetVersion command as follows:

Field	Value
VendorID	<b>0x04</b>
HWMajorVersion	<b>0x82</b>
HWMinorVersion,	<b>0x00</b>
SWMajorVersion	<b>0x02</b>
SWMinorVersion	<b>0x01</b>
CWCY	<b>2823</b>

In addition, the TOE can be uniquely identified according to the JCOP Platform on which it is integrated. Using the Version Query command (GET DATA command with tag 0xDF4C) applied to the eSE OS can return the Platform Identifier and the Platform Release String (Version + Release) is returned as: (See [JCOP-UGM-eSE] Section 1 and [JCOP-UGM] Section 1.4.5)

Field	Tag	Length	Valid Value
Platform Identifier	0x82	16	N5F2M500001B0600
JCOP version number	0x83	2	0809
Release version number	0x84	4	10601011

## TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
<b>Hardware IC</b>	SN300_SE B5.1.002 JD	<b>(diced) wafer/module/card</b>	<b>ICCN0302</b>	<b>2022-03-17</b>
<b>JavaCard</b>	JCOP-eSE 8.9 R1.06.01.1.1	<b>Embedded in the above</b>	<b>PCN0206.03</b>	<b>2023-05-16</b>
<b>Crypto libraries</b>	v1.3.0	<b>Embedded in the above</b>	<b>Included in ICCN0302</b>	<b>2023-05-16</b>
<b>MIFARE applet</b>	3.2.1.1Nx D	<b>Embedded in the above</b>	<b>Functional: D2A_2404_001 Security: MF-2300125-01</b>	<b>2024-05-20</b>

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-eSE]	JCOP 8.9 R1 User Guidance Manual for JCOP eSE, Rev. 1.6.0, 29. Jan. 2024
[JCOP-UGM]	JCOP 8.9 R1 User Guidance Manual, Rev. 1.6.0, 29. Jan. 2024