# Security Target

## ST introduction

The reference of this ST is **TESS v7.1 with MIFARE Desfire EV1/M4Mv2 Security Target version 1.1**

## TOE

The TOE is **an open platform** implementing the MIFARE specification [**MIFARE-DES-EV1]** and the access control in the MIFARE services.
See PP(s) for details.

## TOE reference

The TOE is referred to as **TESS v7.1 with MIFARE Desfire EV1/M4Mv2** and is named and uniquely identified using the following:

### Platform identification data (TESS v7.1 OS v1.19)

| | |
|---|---|
| OS Ident. command | Get Data command (tag FE) |
| Expected value | FE15060A**2B060104012A026E0103**0607**D0027115DA0113** |

| Field | Value |
|---|---|
| Javacard version | 2B060104012A026E0103 |
| OS information<br>- PDM counter<br>- OS release | <br>D0027115DA<br>0113 (=v1.19) |

| | |
|---|---|
| Patch Ident. command | Get Data command (tag FD) |
| Expected value | FD04**00010000** |

| Field | Value |
|---|---|
| - Patch major revision | 0001 |
| - Patch minor revision | 0000 |

### Applet identification data (MIFARE DESFIRE EV1)

| | |
|---|---|
| Ident. command | GetVersion command |
| Expected value | **4001000102** |

| Field | Value |
|---|---|
| VendorID | 0x40 (ISO affected value by NXP to GTO) |
| HWMajorVersion | 0x01 |
| HWMinorVersion | 0x00 |
| SWMajorVersion | 0x01 |
| SWMinorVersion | 0x02 |

**Applet identification data (M4M v2.1.1 v11)**

Ident. command

1. Open secure channel with C_DEC, C_MAC, R_MAC, R_ENC
2. INSTALL[forPerso] command to VCM/SM instance
   command:
   80E6200016000010A0000003964D344D10000000000000030000
   0000
3. Store data command with P1 = 81 P2 = 00 and the following data in 0A0404000500
   Command:
   80E28100060A040400050000

Expected value 0A14900004064002024002020508**5448414C45530B00**

| Field | Value |
|---|---|
| VendorID | 5448414C4553 (=THALES) |
| SWMajorVersion | 0B (=11) |
| SWMinorVersion | 00 (=00) |

## TOE overview

The TOE consists of the following:

| TOE component | Identification | Form of delivery | Certification identifier | Certificate issue date |
|---|---|---|---|---|
| **Hardware IC** | **S3NSN6H** | **(diced) wafer/module/card** | **ICCN0304** | **2023-08-31** |
| **Crypto libraries** | **V2.6.0** | **Embedded onto the IC** | **PCN0215** | **2024-12-06** |
| **JavaCard** | **TESS V7.1** | **Embedded onto the IC** | **PCN0215** | **2024-12-06** |
| **MIFARE applet** | | **Embedded onto the IC** | **MIFARE4Mobile_PC0I_2412_001** | **2024-12-11** |
| **(Pre)personalisation documentation** | | | **n/a** | **n/a** |

Only (pre-)personalisation guidance is provided [AGD-DESFIRE] [AGD-M4M]. 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-EV1] | MIFARE DESFire EV1 Interface Specification, Rev. 1.1 (ts335111) |
| [MIFARE DESFIRE PP] | MIFARE DESFire EV1/EV2/EV3 Protection Profile v1.5 |
| [AGD-DESFIRE] | MIFARE – AGD MIFAREDesFireEV1 v1.1.pdf |
| [AGD-M4M] | MIFARE – AGD M4Mv2 v1.1.pdf |

# ST revision history

| | |
|---|---|
| 0.1 | Creation with v1.5 template |
| 0.2 | 06/11/2024 Update: TOE reference (Identification), TOE overview (Lib version) |
| 0.3 | 26/11/2024 Update: TOE reference (Identification with command/response) |
| 1.0 | 16/01/2025 Update: TOE reference (M4M identification), TOE overview (certificate) |
| 1.1 | 30/01/2025 Update: References (AGD) |