Security Target

ST introduction

The reference of this ST is **TESS v5.1 with MIFARE Desfire EV1/M4Mv2 Security Target** version **v1.1**

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 v5.1 with MIFARE Desfire EV1/M4Mv2**, and is named and uniquely identified using the GetVersion command as follows:

Platform identification data (TESS v5.1)

Identification data Get Data command (tag FE)

Value for this product FE15060A2B060104012A026E01030607D0026115C60114

Field	Value
Javacard version	2B060104012A026E0103
OS information - PDM counter - OS release	 D0026115C6 0115 (1.21)

Applet identification data (DESFIRE EV1)

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

Applet identification data (M4M v2)

Field	Value
VendorID	**47454D414C544F**
HWMajorVersion	**-**
HWMinorVersion,	**-**
SWMajorVersion	**04**
SWMinorVersion	**01**

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	**S3NSEN6**	**(diced) wafer/module/card**	**ICCN0291**	**June 20 2022**
Crypto libraries		**Included in PCN**	**PCN0203.01**	**Feb.24 2023**
JavaCard		**Included in PCN**	**PCN0203.01**	**Feb.24 2023**
MIFARE applet			**MIFARE4Mobile_PC0I_2312_001**	**Dec.20 2023**
(Pre)personalisation documentation			**n/a**	**n/a**

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-DES-EV2] MIFARE DESFire EV2 Reference Architecture, Rev. 1.4 (ra321914)

[MIFARE-DES-EV3] MIFARE DESFIRE EV3 Reference Architecture and Interface Specification, Rev. 3.0

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

ST revision history

1.0 Creation (September 11 2023) with v1.5 template

1.1 Updates (January 5 2024)