Security Target

ST introduction

The reference of this ST is **Combo CE 4.2.3 v1.1 with MIFARE Desfire EV1/M4Mv2 Security Target** version **4.0, dated 2021.06.30**.

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 **Combo CE 4.2.3 v1.1 with MIFARE Desfire EV1/M4Mv2** and is named and uniquely identified using the GetVersion command as follows:

Platform identification data (Combo CE 4.2.3 v1.1)

Identification data Get Data command (tag FE)

Value for this product FE15060A**2B060104012A026E0103**0607**D0023F15240112**

Field	Value
Javacard version	2B060104012A026E0103
OS information - PDM counter - OS release	 D0023F1524 0112 (1.12)

Applet identification data (DESFIRE EV1)

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

Applet identification data (M4M v2)

Field	Value
VendorID	**0x47454D414C544F** (“GEMALTO” ASCII in Hex)
HWMajorVersion	**Not required**
HWMinorVersion,	**Not required**
SWMajorVersion	**0x05**
SWMinorVersion	**0x00**

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Date of certificate issue
IC	**ST54J Rev C & D ST54K RevD**	**(diced) wafer/module/card**	**ICCN0260 (*)**	**Nov.30,.2018**
Crypto libraries	**See previous sections p.1**	**Included in the PCN**	**PCN0179.01 (**)**	**Aug.7, 2020**
JavaCard	**See previous sections p.1**	**Included in the PCN**	**PCN0179.01 (**)**	**Aug.7, 2020**
MIFARE applet	**See previous sections p.1**		**MF-2000023-01**	
(Pre)personalisation documentation			**n/a**	**n/a**

(*) ICCN0260 renewal completed, and valid until Nov.30, 2021
(**) PCN0179.01 valid until Aug.7 2021

~~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 DESFIRE PP] MIFARE DESFire EV1/EV2/EV3 Protection Profile v1.3

[MIFARE-DES-EV1] MIFARE DESFire EV1 Interface Specification, Rev. 1.1

~~[MIFARE PLUS PP] MIFARE PLUS EV0/EV1/EV2 Protection Profile v1.3~~

ST revision history

1.0 Creation

2.0 Update with TOE identification and PCN (May 11, 2021)

3.0 Update with latest MIFARE ST Template v1.3 (May 24, 2021)

4.0 Update with TrustCB remarks (June 30, 2021)