

Security Target

ST introduction

The reference of this ST is **Combo CE 4.2.3 v1.2 with MIFARE Desfire EV1/M4Mv2 Security Target** version **1.4**.

TOE

The TOE is **an open platform** implementing the MIFARE specification ~~[MIFARE-DES-EV1]/[MIFARE-DES-EV2]/[MIFARE-DES-EV3]/[MIFARE-PLUS-EV0]/[MIFARE-PLUS-EV1]/[MIFARE-PLUS-EV2]~~ 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 v1.2 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 v1.2)

Identification data Get Data command (tag FE)

Value for this product FE15060A2B060104012A026E01030607D0023F15460109

Field	Value
Javacard version	2B060104012A026E0103
OS information	
- PDM counter	D0023F1546
- OS release	0110 (1.10)

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	0x07
SWMinorVersion	0x00

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Certificate issue date
Hardware IC	ST54J Rev C & D ST54K RevD	(diced) wafer/module/card	ICCN0260 (*)	Nov.30,.2018
Crypto libraries		Included in the PCN	PCN0179.02	Aug.7 2020
JavaCard		Included in the PCN	PCN0179.02	Aug.7 2020
MIFARE applet			MF-2200001-01	
MIFARE applet			MIFARE4Mobile _PCOI_2203_00 3	Mar.22 2022

(*) ICCN0260 valid until 30.11.2022.

~~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]/[MIFARE PLUS PP]~~ (you can select ~~both~~) (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 v1.3
[MIFARE-PLUS-EV0]	MIFARE Plus End To End Reference Architecture, Rev. 2.0 (ds287920)
[MIFARE-PLUS-EV1]	MIFARE Plus EV1 Reference Architecture and Interface Specification, Rev. 1.6 (ra385514)
[MIFARE-PLUS-EV2]	MIFARE Plus EV2 Reference Architecture and Interface Specification rev 3.0
[MIFARE PLUS PP]	MIFARE PLUS EV0/EV1/EV2 Protection Profile v1.3

ST revision history

- 1.0 Creation (Nov.23rd 2021) with MIFARE – ST template – 1.4
- 1.1 Update (Jan.28th 2022) based on latest samples sent on Jan.24 2022 (CP1.9)
- 1.2 Update (Feb.4th 2022) based on CP 1.10
- 1.3 (Apr.13 2022) Correction of versioning + EMVCO certificate validity date
- 1.4 (May 11th 2022) Add LoA number (Mifare functional certificate)