Security Target

ST introduction

The reference of this ST is **Secure Element J5H1M3022A9F0000 with MIFARE DESFire EV2 1.0.17.0Q Security Target version 9.5, dated May 15, 2020.**

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 J5H1M3022A9F0000 with MIFARE DESFire EV2 1.0.17.0Q** and is named and uniquely identified using the GetVersion command as follows:

Field	Value
VendorID	**0x04**
HWMajorVersion	**0x32**
HWMinorVersion	**0x00**
SWMajorVersion	**0x02**
SWMinorVersion	**0x00**
CWCY	**0x4319**

The DESFire EV2 applet consists of 4 components. Each component can be uniquely identified via the package AID, by checking the card information on the chip, using the following JCShell command:

```
/card
auth
card-info
```

Component	SVN revision	Package AID
DESFire mfcarrier-DFEV2-1.0.17.0Q-20191021	50652	A00000039654530000000101201100
SIO Library interfacesio-1.0.10.0Q-20190116	41581	A00000039654530000000101200A10
MCM mcm-1.0.13.0Q-20191119	51573	A00000039654530000000101500D00
lib-DFEV2-1.0.17.0Q-20191021	50652	A00000039654530000000101201111

TOE overview

The TOE consists of the following:

TOE component	Identification	Form of delivery	Certification identifier	Date of certificate issue
Hardware IC	**P61N1M3PVE-1**	**(diced) wafer/module/card**	**ICCN0203**	**2013-10-20**
Crypto libraries	**2.0**	**Embedded in the above**	**Included in PCN**	

JavaCard	**J5H1M3022A9F0000**	**Embedded in the above**	**PCN0081.17X**	**2013-12-19**
MIFARE applet	**1.0.17.0Q**	**Embedded in the above**	**Functional: D2A_2004_005 Security: MF-1900012-02**	**2020-04-14**

Only (pre-)personalisation guidance is provided [MIFARE-DES-EV2]. 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 Protection Profile v1.0

[MIFARE-DES-EV2] MIFARE DESFire EV2 Reference Architecture, ra321914