

## Product information notice - March 2018

### Migration from DESFire® EV1 to DESFire® EV2 - Credentials and reader compatibility

---

#### **MIFARE® DESFire® EV1 chip production discontinued and migration towards MIFARE® DESFire® EV2 chips**

We are writing to inform you of the migration of all our credentials to MIFARE® DESFire® EV2 - cards, keyrings, labels, disc tags (see Appendix 1 - Table of equivalent part numbers).

In accordance with the NXP “MIFARE-DESFIRE-EV2-FS” notice, MIFARE® DESFire® EV2 chips are fully backward compatible with MIFARE® DESFire® EV1.

All STid 13.56 MHz readers are compatible with this latest generation of chips.

However, should you observe any incompatibility of equipment by another manufacturer, please contact them for an update, which is the only long-term solution as EV1 can no longer be supplied.

The new MIFARE® DESFire® EV2 chips are backward compatible with the DESFire® EV1 version, providing:

- better security levels: EAL5+ (same levels as the banking sector),
- more functionalities (see Appendix 2),
- greater flexibility for key and file management,
- an unlimited number of applications (limited only to the chip memory),
- better resistance to relay attacks,
- larger reading ranges.

Please see Appendix 3 for more information on the comparison between the two generations of chips.

## Compatibility with STid readers

---

STid is the first manufacturer to offer readers compatible with DESFire® EV2.

All Architect®, Architect® One, Architect® Blue, Architect® One Blue readers have the following functions:

- Secure Messaging EV2: new secure transaction method based on AES-128 with protection against interleaving and replay attacks.
- Proximity Check: protection against relay attacks.

This compatibility is effective from the following firmware versions:

- Read only (R or S)  $\geq$  08 from version SECard 3.2
- Read/Write (W)  $\geq$  10
- OSDP readers  $\geq$  4

### Compatible models:

**ARC1 / ARC1S  
ARC1S/BT**



**ARC-A / ARCS-A  
ARCS-A/BT**



**ARC-B / ARCS-B  
ARCS-B/BT**



**ARC-C / ARCS-C  
ARCS-C/BT**



**ARC-D / ARCS-D**



**ARC-E / ARCS-E**



**ARC-F / ARCS-F**



**ARC-G / ARCS-G  
ARCS-G/BT**



**ARC-I / ARCS-I  
ARCS-I/BT**



**ARC-J / ARCS-J  
ARCS-J/BT**



**MA1 / MA1S  
MA1S/BT**



**ATX 13,56 MHz  
T5 & T6**



Please contact your sales representative or visit our website for more information on these products:  
[www.stid-security.com](http://www.stid-security.com).

## Appendix 1 - Table of equivalent part numbers

- ISO cards

Version	DESFire® EV1	DESFire® EV2
MIFARE® DESFire® 2K with/without magstripe	CCTW370 / CCTW371	CCTW670 / CCTW671
MIFARE® DESFire® 4K with/without magstripe	CCTW380 / CCTW381	CCTW680 / CCTW681
MIFARE® DESFire® 8K with/without magstripe	CCTW390 / CCTW391	CCTW690 / CCTW691
MIFARE® DESFire® 2K + 125 kHz EM4200 with/without magstripe	CCTWR100 / CCTWR101	CCTWR300 / CCTWR301
MIFARE® DESFire® 4K + 125 kHz EM4200 with/without magstripe	CCTWR110 / CCTWR111	CCTWR310 / CCTWR311
MIFARE® DESFire® 8K + 125 kHz EM4200 with/without magstripe	CCTWR120 / CCTWR121	CCTWR320 / CCTWR321
MIFARE® DESFire® 2K + 125 kHz ATA5577 with/without magstripe	CCTWR130 / CCTWR131	CCTWR330 / CCTWR331
MIFARE® DESFire® 4K + 125 kHz ATA5577 with/without magstripe	CCTWR140 / CCTWR141	CCTWR340 / CCTWR341
MIFARE® DESFire® 8K + 125 kHz ATA5577 with/without magstripe	CCTWR150 / CCTWR151	CCTWR350 / CCTWR351
MIFARE® DESFire® 2K + UHF programmable with/without magstripe	CCTWR160	CCTWR260
MIFARE® DESFire® 4K + UHF programmable with/without magstripe	CCTWR170	CCTWR270
MIFARE® DESFire® 8K + UHF programmable with/without magstripe	CCTWR180	CCTWR280

- Key holders

Version	DESFire® EV1	DESFire® EV2
PCD - MIFARE® DESFire® 2K	PCDW37-y	PCDW67-y
PCD - MIFARE® DESFire® 4K	PCDW38-y	PCDW68-y
PCD - MIFARE® DESFire® 8K	PCDW39-y	PCDW69-y
PCG - MIFARE® DESFire® 2K	PCGW37-y	PCGW67-y
PCG - MIFARE® DESFire® 4K	PCGW38-y	PCGW68-y
PCG - MIFARE® DESFire® 8K	PCGW39-y	PCGW69-y
PCR - MIFARE® DESFire® 2K	-	PCRW67-y
PCR - MIFARE® DESFire® 4K	-	PCRW68-y
PCR - MIFARE® DESFire® 8K	-	PCRW69-y

- Disc tags

Version	DESFire® EV1	DESFire® EV2
MIFARE® DESFire® 2K - 20 mm	DTAW370/20	DTAW670/20
MIFARE® DESFire® 2K - 26.5 mm	DTAW370/26	DTAW670/26
MIFARE® DESFire® 2K - 40 mm	DTAW370/40	DTAW670/40
MIFARE® DESFire® 4K - 20 mm	DTAW380/20	DTAW680/20
MIFARE® DESFire® 4K - 26.5 mm	DTAW380/26	DTAW680/26
MIFARE® DESFire® 4K - 40 mm	DTAW380/40	DTAW680/40
MIFARE® DESFire® 4K - 50 mm	DTAW380/50	DTAW680/50
MIFARE® DESFire® 8K - 20 mm	DTAW390/20	DTAW690/20
MIFARE® DESFire® 8K - 26.5 mm	DTAW390/26	DTAW690/26
MIFARE® DESFire® 8K - 40 mm	DTAW390/40	DTAW690/40
MIFARE® DESFire® 8K - 50 mm	DTAW390/50	DTAW690/50

- White adhesive label

Version	DESFire® EV1	DESFire® EV2
MIFARE® DESFire® 4K	ETPW3805080	ETPW6805080

## Appendix 2 - MIFARE® DESFire® EV2 chip functionalities

---

**Secure Messaging EV2:** new secure transaction method based on AES-128 with protection against interleaving and replay attacks.

**Proximity Check:** improved protection against relay attacks.

**MIsmartApp:** delegates application management to third parties without sharing the master key. The only limit on the number of applications is the chip memory.

**MAC transaction:** ensures the authenticity of each sales transaction.

**Multiple key sets per application:** up to 16 key sets.

**Multiple keys assignment for each file access rights:** up to 8 keys.

**Update Record command:** update data from an existing “LinearRecord” or “CyclicRecord” file.

**Virtual Card Architecture:** transparent multi-application management between a smartphone and standard contactless card.

**Originality Check:** checks the originality of the DESFire® EV2 chip to avoid counterfeits.

### Appendix 3 - Comparison between MIFARE® DESFire® EV1 and EV2 chips

---

Characteristics	DESFire® EV1	DESFire® EV2
Secure Messaging data transmission protection	D40 native, EV1	D40 native, EV1, EV2
Cryptography	Single DES, 2KTDEA, 3KTDEA, AES-128	
Number of applications	Maximum 28	Unlimited
Number of files per application	32	
Maximum number of files with backup	32	
Random ID	Yes	
ISO/IEC816-4 commands	8	8 with improvements
ATS configurable	Yes, historical bytes only	Yes, all parameters (FSCI supported up to 128 bytes)
Maximum communication buffer memory	64 bytes	128 bytes
Data transfer format	Native (AFh)	Native (AFh) or ISO/IEC 1443-4
Multiple key Sets with rolling	No	Yes
MISmart App	No	Yes
Shared Application Management	No	Yes
Multiple keys per access rights	No	Yes
Update Record command	No	Yes
Transaction MAC	No	Yes
Virtual Card Architecture	No	Yes
Proximity Check	No	Yes
Originality Check	No	Yes