Note d'information produits - Mars 2018

Migration MIFARE® DESFire® EV1 / DESFire® EV2 - Identifiants et compatibilités lecteurs

Arrêt de la production des puces MIFARE® DESFire® EV1 et migration vers les puces MIFARE® DESFire® EV2

Nous vous informons de la migration de tous nos identifiants en MIFARE® DESFire® EV2 – badges, porte-clés, étiquettes, tags disques (cf. annexe 1 - Tableau des correspondances).

Conformément à la note d'information de NXP « MIFARE-DESFIRE-EV2-FS », les puces MIFARE® DESFire® EV2 sont 100 % rétro-compatibles avec les MIFARE® DESFire® EV1.
Tous les lecteurs 13,56 MHz STid sont compatibles avec cette dernière génération de puces.
Si toutefois vous constatez une incompatibilité avec les équipements d'un autre constructeur nous vous conseillons de le contacter pour mise à jour, seule solution pérenne car l'EV1 n'est plus livrable.

Les nouvelles puces MIFARE® DESFire® EV2 sont rétro-compatibles avec la version DESFire® EV1 et apportent notamment :

- de meilleurs niveaux de sécurité EAL5+ (mêmes niveaux que le secteur bancaire),
- plus de fonctionnalités (cf. annexe 2),
- plus de souplesse dans la gestion des clés et des fichiers,
- un nombre illimité d'applications (dans les limites de la mémoire de la puce),
- une meilleure résistance aux attaques relais,
- de meilleures distances de lecture.

Pour de plus amples informations sur le comparatif des deux générations de puces, nous vous invitons à consulter l'annexe 3.

20 Parc d'Activités des Pradeaux - 13850 GREASQUE - France
Tél. : +33 (0)4.42.12.60.60 - Fax : +33 (0)4.42.12.60.61 - E-Mail : info@stid.com - Web : http://www.stid.com

Compatibilités avec les lecteurs STid

STid est le premier constructeur à proposer ses lecteurs compatibles avec la DESFire® EV2.

Tous les lecteurs des gammes Architect®, Architect® One, Architect® Blue, Architect® One Blue intègrent les fonctions suivantes :

- « Secure Messaging » : nouvelle méthode de sécurisation des transactions basée sur AES-128 qui dispose d'une protection contre les attaques par entrelacement et par rejeu.
- « Proximity Check » : protection contre les attaques relais.

Cette compatibilité est effective à partir des versions de firmwares suivantes :

- Lecture seule (R ou S) ≥ 08 à partir de la version SECard 3.2
- Lecture écriture (W) ≥ 10
- Lecteurs OSDP ≥ 4

Modèles compatibles :

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 et T6

Pour plus d'information sur nos produits, nous vous invitons à vous rapprocher de votre commercial et à consulter notre site web : www.stid-security.com.

Annexe 1 - Tableau des correspondances

- **Badges ISO**

Version	DESFire® EV1	DESFire® EV2
MIFARE® DESFire® 2K avec ou sans piste ISO	CCTW370 / CCTW371	CCTW670 / CCTW671
MIFARE® DESFire® 4K avec ou sans piste ISO	CCTW380 / CCTW381	CCTW680 / CCTW681
MIFARE® DESFire® 8K avec ou sans piste ISO	CCTW390 / CCTW391	CCTW690 / CCTW691
MIFARE® DESFire® 2K + 125 kHz EM4200 avec ou sans piste ISO	CCTWR100 / CCTWR101	CCTWR300 / CCTWR301
MIFARE® DESFire® 4K + 125 kHz EM4200 avec ou sans piste ISO	CCTWR110 / CCTWR111	CCTWR310 / CCTWR311
MIFARE® DESFire® 8K + 125 kHz EM4200 avec ou sans piste ISO	CCTWR120 / CCTWR121	CCTWR320 / CCTWR321
MIFARE® DESFire® 2K + 125 kHz ATA5577 avec ou sans piste ISO	CCTWR130 / CCTWR131	CCTWR330 / CCTWR331
MIFARE® DESFire® 4K + 125 kHz ATA5577 avec ou sans piste ISO	CCTWR140 / CCTWR141	CCTWR340 / CCTWR341
MIFARE® DESFire® 8K + 125 kHz ATA5577 avec ou sans piste ISO	CCTWR150 / CCTWR151	CCTWR350 / CCTWR351
MIFARE® DESFire® 2K + UHF programmable avec ou sans piste ISO	CCTWR160	CCTWR260
MIFARE® DESFire® 4K + UHF programmable avec ou sans piste ISO	CCTWR170	CCTWR270
MIFARE® DESFire® 8K + UHF programmable avec ou sans piste ISO	CCTWR180	CCTWR280

- **Porte-clés**

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

- **Tags disques**

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

- **Étiquettes en polypropylène blanc adhésif**

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

Annexe 2 - Fonctionnalités des puces MIFARE® DESFire® EV2

« Secure messaging EV2 » : nouvelle méthode de sécurisation des transactions basée sur AES-128 qui dispose d'une protection contre les attaques par entrelacement « interleaving » et par rejeu.

« Proximity Check » : amélioration de la protection contre les attaques relais.

« MIsmartApp » : délègue la gestion des applications à des tiers, sans partager la clé maître. Le nombre d'applications est uniquement limité par la mémoire de la puce.

« Transaction MAC » : assure l'authenticité de chaque transaction marchande.

« Multiple key sets per application » : jeux de clés multiples par application (jusqu'à 16 jeux).

« Multiple keys assignment for each file access rights » : attribution de clés multiples pour chaque droit d'accès de fichier (jusqu'à 8 clés).

« Update Record command » : mise à jour des données d'un fichier existant de type « LinearRecord » ou « CyclicRecord ».

« Virtual Card Architecture » : gestion multi-applications transparente entre smartphone et carte sans contact standard.

« Originality Check » : vérification de l'authenticité de la puce DESFire® EV2 pour éviter les contrefaçons.

Annexe 3 - Comparatif entre les puces MIFARE® DESFire® EV1 et EV2

Caractéristiques	DESFire® EV1	DESFire® EV2
Protection de la transmission des données « Secure messaging »	D40 native, EV1	D40 native, EV1, EV2
Cryptographie	Single DES, 2KTDEA, 3KTDEA, AES-128	
Nombre d'applications	Maximum 28	Illimité
Nombre de fichiers par application	32	
Nombre maximum de fichiers avec sauvegarde	32	
Random ID	Oui	
Commandes ISO/IEC816-4	8	8 avec améliorations
ATS configurable	Oui, « historical bytes » seulement	Oui, tous les paramètres (FSCI supporté jusqu'à 128 octets)
Communication maximum mémoire tampon	64 octets	128 octets
Format du transfert des données	Natif (AFh)	Natif (AFh) ou ISO/IEC 1443-4
« Multiple key Sets with rolling »	Non	Oui
« MISmart App »	Non	Oui
« Shared Application Management »	Non	Oui
« Multiple keys per access rights »	Non	Oui
« Update Record command »	Non	Oui
« Transaction MAC »	Non	Oui
« Virtual Card Architecture »	Non	Oui
« Proximity check »	Non	Oui
« Originality check »	Non	Oui