



La transformation commence ici 

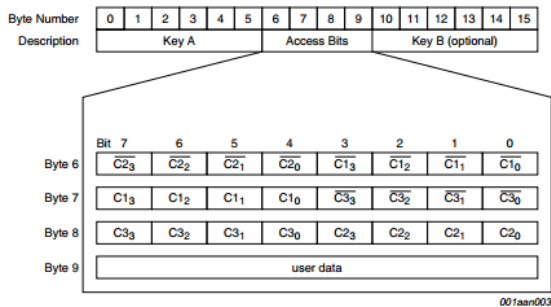
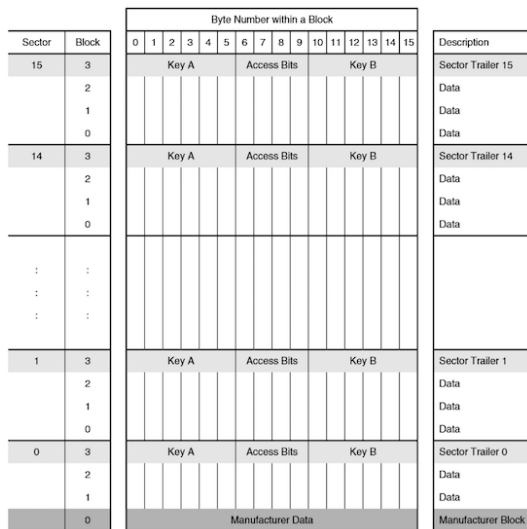


Précisions sur les impacts du passage mifare Classic au mifare DESFire

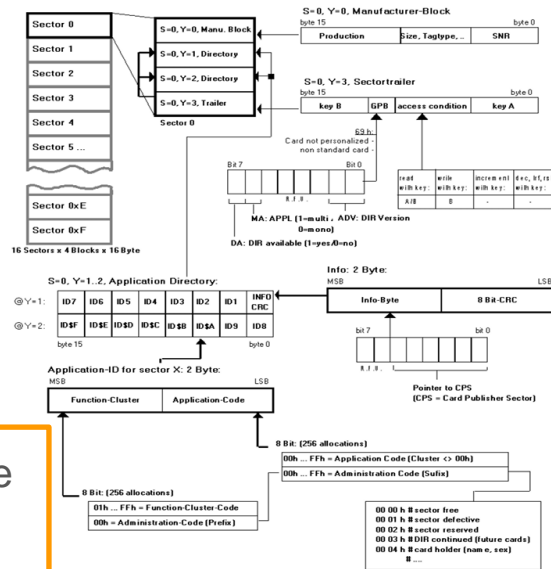
16 janvier 2024 | Joachim METZGER – Florian CATTEAU

- La CPSv3 intègre le mifare Classic et le mifare DESFire EV1
- Le mifare Classic est « cassé » depuis ~2008
- La CPSv4 intègre le mifare DESFire EV3
- ***Le mifare Classic ne sera plus disponible sur la CPSv4***

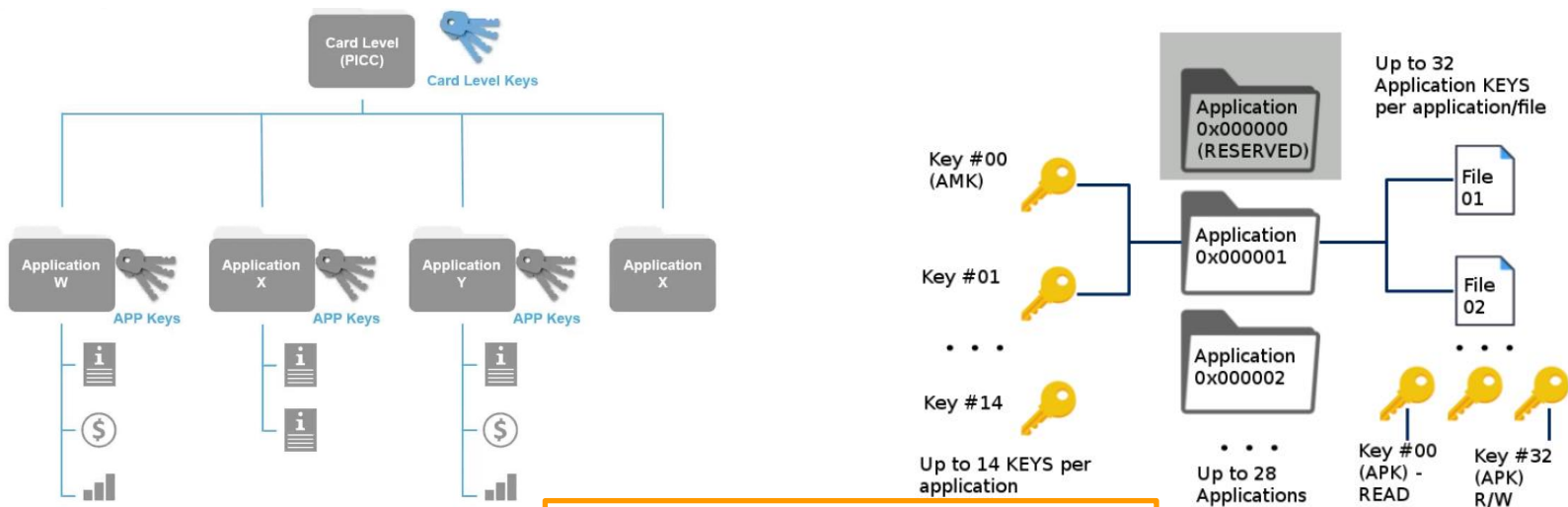
C'est une carte mémoire divisée par secteur protégé par 2 clefs. Une gestion multi-applicative est possible à l'aide du MIFARE Application Directory (MAD).



Historiquement l'UID du mifare Classic est de 4 octets de longueur



C'est carte mémoire nativement multi-applicative associée à des algorithmes cryptographiques à jour.



L'UID du mifare DESFire est de 7 octets de longueur

DESFire EV1 vs DESFire EV3

Les solutions en EV1 sont compatibles de l'EV3.

En EV1, la mémoire est limitée à 28 applications simultanées tandis que pour les puces EV3 il n'y a aucune limite.

En EV3, il est possible de générer un code d'authentification unique et sécurisé à chaque fois qu'un tag est lu, soit une sorte de générateur de clé jetable : chaque fois qu'un tag est lu, une ligne différente est générée et permet d'éviter les copies de contenu.

Quels usages du sans contact ?

1. Accès aux locaux, Parking, Casier, Cantine, Distributeur de boisson, Imprimante

- ▶ Nécessite une installation compatible mifare DESFire : depuis 10 ans, toutes les solutions de contrôle d'accès sont compatibles.
- ▶ Cependant cf. diapo suivante ...

2. Ouverture de session Windows

- ▶ En mifare Classic, seule la lecture d'UID permet cet usage : c'est une simple identification sans sécurisation.
- ▶ En mifare DESFire, des solutions en 1FA et 2FA existent.

Focus contrôle d'accès physique

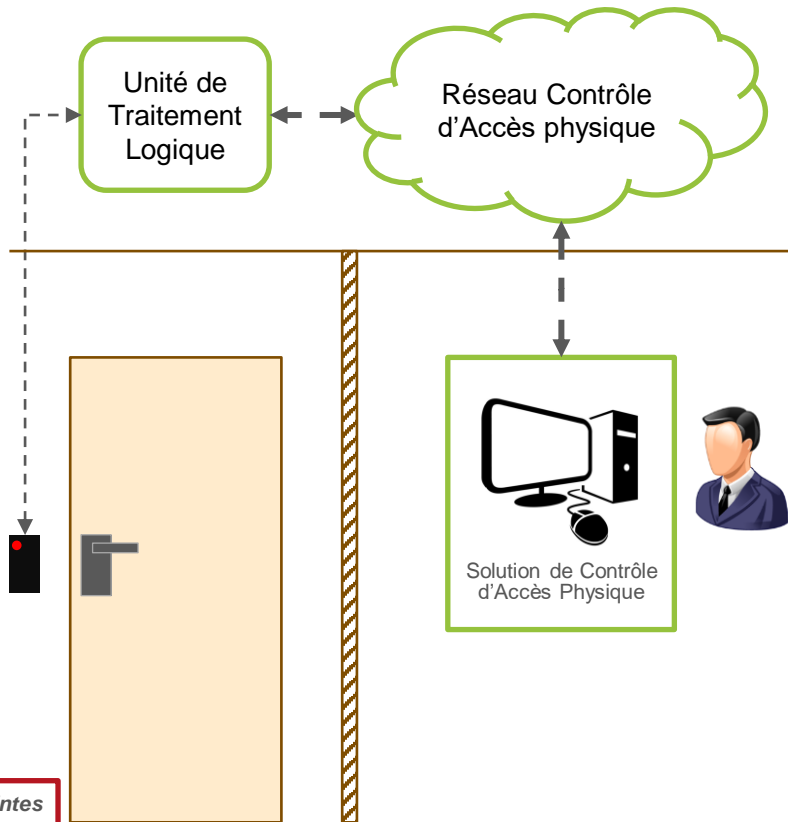
Il est nécessaire que l'ensemble de la chaîne du contrôle d'accès ait été mis à niveau :

- les lecteurs : la technologie DESFire peut nécessiter des lecteurs avec des capacités cryptographiques supérieures à des modèles mifare Classic standards;
 - En effet, le composant RFID est toujours compatible (Attention pour certains lecteurs la gestion de l'UID mifare DESFire sur 7 octets au lieu de 4 octets en mifare Classic peut poser problème dû à une configuration interne figée).
 - Mais le support des secteurs du mifare Classic est natif dans ce composant contrairement au DESFire.
 - Il faut un composant supplémentaire à minima pour la cryptographie ou alors que cette dernière soit déportée dans l'UTL)
- les câbles : entre les lecteurs et les UTL afin de supporter des protocoles réseaux classiques.
- les UTL : elles doivent supporter la gestion des clefs.
- et la solution de gestion des accès (intégration d'un KMS)

Il existe des solutions DESFire « standalone » : sans problématique câble et UTL. En revanche, elles ne semblent pas déployées sur la totalité d'un système de contrôle d'accès mais sur des accès à des portes en particulier.

Parfois seul le lecteur a été modifié face aux contraintes organisationnelles et techniques locales.

La sécurité a même pu être réduite en passant d'un mifare Classic à une lecture d'UID d'un mifare DESFire.



Quelles utilisations du sans contact ?

1. Lecture de l'Unique Identifiant UID

- ▶ Bien qu'elle soit très fortement répandue, cette solution n'a jamais été sécurisée.
- ▶ Cette fonctionnalité est indispensable au protocole d'anticollision lors de la présence de plusieurs cartes sans contact devant le lecteur (ex : CPS, carte bancaire et badge immeuble).

2. Lecture de données d'identité ou d'accès

- ▶ mifare Classic et mifare DESFire offre les mêmes possibilités.

3. Authentification 1FA ou 2FA

- ▶ Seul le mifare DESFire permet cette fonctionnalité (si elle est correctement configurée).

Quelques problèmes connus ...

- **Les lecteurs ne reconnaissent pas la CPS :**
 - Le lecteur peut être limité dans sa configuration pour ne supporter que des mifare Classic dans la lecture de l'UID : l'UID en mifare Classic est de 4 octets or il est de 7 en mifare DESFire. Une mise à jour voir un remplacement est nécessaire. Dans ce dernier cas, le lecteur n'est probablement pas au standard de sécurité attendu.
- **Les lecteurs ne reconnaissent pas la partie DESFire de la CPS mais sont compatibles avec une carte DESFire :**
 - La CPS supporte le mifare DESFire ET le mifare Classic. D'un point de vue protocolaire (ISO14443), le mifare Classic (ISO14443-3) est détecté avant le mifare DESFire (ISO14443-4) lors des échanges RF. Il est donc nécessaire que le lecteur soit capable d'être configuré pour s'adapter à cette situation approuvée par NXP (Industriel propriétaire des technologies mifare).

Vos questions ...



La transformation commence ici 



esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.



@esante_gouv_fr



[linkedin.com/company/agence-du-numerique-en-sante](https://www.linkedin.com/company/agence-du-numerique-en-sante)