AGENCE
DU NUMÉRIQUE
EN SANTÉ

Nouvelle version de la carte CPx

Caractéristiques techniques des puces des cartes de la famille CPx

Statut : Validé | *Classification : Publique* | *Version : v2.0*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. PREAMBULE

> ***Le changement de la puce actuelle est imposé par l'arrêt de sa production par son fondeur (la société NXP).***

2. DESCRIPTION DES CARTES CPX DEPLOYEES

2.1. Caractéristiques techniques générales

Trois versions de cartes sont actuellement déployées :

- Les cartes CPx 3.1 puce R1,
- Les cartes CPx 3.1 puce R2,
- Les cartes CPx 3.3 puce R2

> ***Précision :***
> ***On entend par version de carte le couple (version de carte, version de puce).***

Les cartes actuelles possèdent les caractéristiques suivantes :

- un volet CPS 2ter totalement compatible avec le volet existant (usages FSE) : puce R1, R2
- un volet IAS ECC pour les usages authentification et signature : puce R1, R2
- des données DAM (Domaine Assurance maladie) et des données d'exercices : puce R1, R2
- un volet MIFARE Classic : puce R2

2.2. Cartes CPx 3.1 puce R1

Ces cartes CPx ont été déployées avant le 7 février 2018.

Elles embarquent des certificats émis par l'IGC CPS-2ter.

Elles possèdent une puce sans contact qui n'est pas MIFARE Classic.

L'authentification simple sans contact est réalisée sur la base l'UID présent dans la puce.

2.3. Cartes CPx 3.1 puce R2

Ces cartes CPx ont été déployées à partir du 7 février 2018.

Elles embarquent des certificats émis par l'IGC CPS-2ter.

Elles possèdent une puce sans contact qui est MIFARE Classic.

L'authentification simple sans contact est réalisée sur la base de l'UID de la puce MIFARE Classic.

L'UID MIFARE Classic est encodé sur 4 octets.

2.4. Cartes CPx 3.3 puce R2

Ces cartes CPx sont celles produites depuis le 2 juillet 2018.

Elles embarquent des certificats émis par l'IGC-Santé.

Elles possèdent une puce sans contact qui est MIFARE Classic.

L'authentification simple sans contact est réalisée sur la base de l'UID de la puce MIFARE Classic (strictement identique à la puce des cartes CPS 3.1 R2).

2.5. Identification visuelle de la version de la puce

Les cartes CPx équipées de puce R2 ont une référence qui se termine par « R2 » au verso en haut à droite.

Les cartes CPx équipées de puce R1 n'ont pas de suffixe R1 et n'ont pas de code barre.

Les cartes CPx équipées de puce R2 ont un code barre depuis février 2018.

Le code barre contient l'identifiant du porteur de la carte.

3. DESCRIPTION DE LA NOUVELLE CARTE CPX

3.1. Cartes CPx 3.3 puce R3

La nouvelle carte est une carte CPx 3.3 équipée d'une puce dite R3. Les CPx 3.3 équipées de puce R3 offriront exactement les mêmes services – avec rétrocompatibité totale - que les CPx 3.3 équipées de puces R2 :

- ***un volet CPS 2ter***
- ***un volet IAS ECC***
- ***un volet MIFARE Classic***

Cette puce R3 apportera une fonctionnalité complémentaire :

> ***Un volet nouveau MIFARE DESFire EV1 amenant des mécanismes de sécurité supplémentaires par rapport à celles de MIFARE Classic***
> ***MIFARE DESFire EV1 est certifié EAL4+.***
>
> ***Ce volet sans contact sécurisé peut s'adresser spécifiquement aux structures opérateurs de Services essentiels (OSE) du fait des exigences spécifiques de l'ANSSI.***

Remarque sur le visuel des cartes équipées d'une puce R3 :

> ***Comme pour les cartes CPx R2, les cartes CPx R3 auront un numéro de série qui se terminera par « R3 » au verso en haut à droite.***

3.2. Gestion de l'UID dans le volet MIFARE CLASSIC

Pour répondre au succès croissant de la solution MIFARE Classic, la société NXP a étendu la longueur de l'IUD de 4 octets et 7 octets depuis l'année 2010.

En effet ces UID sont majoritairement utilisés comme élément anti-collision. Or du fait du très nombre de puce vendu par NXP, il pouvait y avoir potentiellement des doublons.

Le guide officiel de gestion de l'UID Mifare (dernière mis à jour 5 juillet 2018) est disponible ici :

https://www.nxp.com/docs/en/application-note/AN10927.pdf

3.3. Gestion des clés et niveaux de sécurité : volet DESFIRE EV1

Le nouveau volet DESFIRE EV1 apporte des fonctions qui permettent de sécuriser l'accès à l'identifiant de la carte. Le volet DESFIRE EV1 sera livré avec la configuration d'usine :

> ***La clé maître (MK.PICC) de la puce DESFIRE EV1 sera au format 3DES 128bits et aura comme valeur '0000000000000000'.***
> ***La modification de la configuration, le changement de la valeur de la clé maître ou la suppression d'application devra se faire avec une authentification par cette clé maître.***

La mémoire de la puce sera vide et pourra contenir jusqu'à 14 applications DESFIRE.

Comme indiqué, la puce présentera par défaut un UID à 7 Octets.

La version 3.3 du « Guide de mise en œuvre de la partie sans-contact des cartes CPx » accessible en ligne à l'adresse : https://integrateurs-cps.asipsante.fr/meo-sanscontact détaille l'ensemble des niveaux de sécurité possibles avec les configurations d'enrôlement de la puce DESFIRE EV1 correspondantes.

3.4. Roadmap et planning

A ce stade la bascule de production est prévue à partir de T3 2020 avec une possibilité de commander les premières cartes à T4 2019.

3.5. Compatibilité ascendante

A partir du 10 juin 2020, 4 versions de cartes CPx vont potentiellement cohabiter.

> ***La compatibilité ascendante pour ces 4 versions de cartes sera assurée à l'exception de la longueur de l'UID MIFARE CLASSIC.***

3.5.1. Impacts sur les équipements

> ***Pour assurer la compatibilité ascendante concernant la lecture des nouveaux UID, la mise à jour du firmware des lecteurs est nécessaire a minima.***
> ***Cela permettra de de gérer un parc hétérogène de cartes UID 4 octets et UID 7 octets.***

3.5.2. Solution de contournement

Dans le cas où vos équipements nécessiteraient des mises à jours plus importantes au niveau des lecteurs, une solution de contournement est envisageable :

> ***La fonctionnalité de contrôle d'accès sans contact MIFARE CLASSIC par identifiant UID n'a pas de date d'expiration.***
> ***Vous pouvez continuer à utiliser les anciennes cartes expirées pour les contrôles d'accès physiques.***
> ***En revanche, les fonctionnalités cryptographiques de la cartes CPx pour les accès logiques aux systèmes d'informations ne pourront pas être utilisées sur des cartes CPx expirées.***