AGENCE
DU NUMÉRIQUE
EN SANTÉ

Webinaire
Impacts des nouvelles cartes CPx en ES

Foire aux questions
(Mise à jour du 16/09/2020)

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

SOMMAIRE

1. Glossaire 1
2. Présentation globale des problematiques 2
2.1. Extension de la longueur d'UID 2
2.2. Bug de « temporisation sans contact » 2
3. Foire aux questions 3
3.1. Problématique de longueur d'UID 3
3.2. Bug « temporisation sans contact » sur les cartes CPx R3V2 4
3.3. Authentification TLS en mode sans contact via un navigateur web 8
4. Annexes 10
4.1. Liens vers les ressources sur les cartes CPx 10
4.2. Adresse mail de contact de l'équipe ANS 10

1. GLOSSAIRE

ANS : Agence du Numérique en Santé

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CPA : Carte de Personnel Autorisé

CPE : Carte de Personnel d'Etablissement

CPF : Carte de Personnel en Formation

CPS : Carte de Professionnel de Santé

ES : Etablissement de Santé

IAS : Identification-Authentification-Signature

NXP : L'éditeur des solutions MIFARE

RFID : Radio Frequency Identification (radio-identification)

SIH : Système d'Information hospitalier

SSA : Service de Santé des Armées

SSO : Single Sign-On (Authentification Unique)

UID : Unique ID (Identifiant unique)

2. PRESENTATION GLOBALE DES PROBLEMATIQUES

Les nouvelles cartes CPS R3v2 émises par l'Agence du Numérique en Santé depuis le 10 juin 2020 contiennent une nouvelle puce qui permet de mettre en œuvre des fonctions de contrôle d'accès MIFARE DESFire EV1.
Pour rappel, ce changement de puce en version R3 fait suite à l'arrêt de production industrielle des puces R2.
Ce changement de puce (R2 vers R3) était planifié initialement pour la fin 2019 et a été décalé à juin 2020.
Des problèmes d'utilisation de ces cartes, principalement pour des usages avec des lecteurs Dual (contact/sans contact), dans les environnements existants ont été remontés à l'Agence du Numérique en Santé.

Trois webinaires ont été organisés le 17 juillet, le 7 août 2020 et le 4 septembre 2020 et ont permis de partager avec les structures les dysfonctionnements constatés ainsi que les premières solutions de contournement mises en place par les utilisateurs impactés.

Ce document décrit les problématiques liées aux nouvelles cartes CPx R3v2 (la version cible étant la R3V3), et reprend les questions posées lors des webinaires.

Deux problématiques ont été abordées dans le webinaire :

- La problématique de l'extension de la longueur d'UID, qui n'est pas un bug en soi, mais une évolution, depuis 2010, du standard MIFARE par son éditeur NXP;
- Le bug de « temporisation sans contact », concernant le fait que les cartes CPx R3v2 (produites à partir du 10/06/2020) deviennent muettes après un usage de la carte en mode « ISO » sans contact.

Un nouveau webinaire sera organisé fin octobre 2020 sur le même thème. Nous vous tiendrons informé de cette de la nouvelle date.

2.1. Extension de la longueur d'UID

Les UID sont majoritairement utilisés comme éléments anticollisions. Or, pour répondre au succès croissant de la solution MIFARE Classic, la société NXP, éditeur des solutions MIFARE, a étendu la longueur de l'UID de 4 octets à 7 octets depuis l'année 2010 pour éviter de potentiels doublons.

En conséquence certains lecteurs MIFARE qui ne sont pas conformes doivent voir leur Firmware mis à jour, pour éviter que les lecteurs tronquent les UID de 7 octets à 4 octets. Dans des cas plus rares et généralement de lecteurs MIFARE anciens (notamment d'avant 2010), cette mise à jour ne peut pas se faire et ils doivent être remplacés.

Les usages impactés par la longueur d'UID concernent notamment l'utilisation des cartes CPx pour le self, les distributeurs automatiques de café ou de boisson, les photocopieuses, ou encore les badgeuses.

2.2. Bug de « temporisation sans contact »

Ce dysfonctionnement est caractérisé comme suit : après un usage sans contact en mode ISO (c'est-à-dire pour les usages d'authentification physique en mode DESFIRE – ou les usages d'authentification logique en mode IAS ECC), la carte devient muette pour un usage avec contact pendant un délai variable allant de 20 secondes à 3 minutes.

Ce dysfonctionnement n'est pas rencontré pour un usage initial en sans contact de type Mifare Classic (modèle typique des badgeuses d'ouverture de porte), et concerne uniquement les cartes CPx R3v2 produites à partir du 10/06/2020.
Tout dispositif qui établit un dialogue en mode DESFIRE (lecteurs de badge, cas de certains distributeurs de boisson) rend la carte muette pour un usage avec contact pendant un délai variable.

Ce phénomène concerne donc essentiellement les ES utilisant la carte CPx en mode sans contact ISO et plus spécifiquement ceux équipés de lecteurs DUAL (avec et sans contact).

Il survient notamment avec des solutions de type SSO nécessitant une authentification initiale en mode avec contact, lors de l'utilisation de lecteur dual : quand le porteur approche sa carte pour l'insérer dans le lecteur, un échange en mode sans contact se fait à son insu et déclenche la temporisation (le phénomène se répète en boucle rendant le lecteur inopérant).

3. FOIRE AUX QUESTIONS

3.1. Problématique de longueur d'UID

Pourquoi la longueur d'UID a-t-elle été étendue ?

Pour répondre au succès croissant de la solution MIFARE Classic, la société NXP, éditeur des solutions MIFARE, a étendu la longueur de l'UID de 4 octets à 7 octets depuis l'année 2010 pour éviter de potentiels doublons.

Que se passe-t-il si l'on possède des cartes ayant une longueur d'UID de 7 octets, et que l'on a des lecteurs de cartes (non mis à jour) ne pouvant lire que 4 octets ?

Lorsqu'ils ne sont pas mis à jour, les lecteurs tronquent les UID de 7 octets à 4 octets : ils ne peuvent pas lire les 7 octets, et cela peut générer des problèmes de collision en ne détectant pas les différentes cartes présentes devant le lecteur.

Quelles sont les solutions envisagées pour palier à ce problème de longueur d'UID ?

Les lecteurs Mifare qui ne sont pas conformes doivent être mis à jour. Ce sont des lecteurs produits avant 2010, et les constructeurs permettent une mise à jour du Firmware.
Dans les cas des lecteurs Mifare obsolètes, une mise à jour du firmware est impossible et ils doivent être remplacés.

Le changement de longueur d'UID peut-il également avoir un impact sur le SI global de l'établissement ?

Il est conseillé de vérifier le comportement du logiciel de gestion des accréditations du système de contrôle d'accès. Si les lecteurs fonctionnent sur 4 octets, il est probable que le système complet fonctionne également sur 4 octets, si le système est basé sur l'UID. Il faut donc vérifier le logiciel de gestion des accréditations, les badgeuses, etc. L'impact global sur les installations de contrôle d'accès physique peut donc être conséquent.

Existe-t-il des solutions palliatives à l'extension de la longueur de l'UID ?

Il n'y a pas de solution palliative à cette problématique. NXP impose cette évolution de la longueur d'UID, il faut donc mettre à jour les lecteurs non conformes.

Les cartes de tests émises avant le 10 juin 2020 intègrent-elles la nouvelle puce ? Faut-il demander de nouvelles cartes de tests ?

Les cartes de tests émises avant le 10 juin 2020 contiennent des puces R3V1, et donc la nouvelle longueur d'UID de 7 octets. Ces cartes de tests ne comportent cependant pas le bug de la carte muette de temporisation sans contact. Concernant les cartes de médecins civils, elles avaient un bug qui empêchaient sous certaines conditions de faire des opérations de signature, mais ce cas reste marginal. Il faudra redistribuer des cartes avec des puces

R3V3, ce qui corrigera à la fois le bug de temporisation sans contact et le bug de signature des feuilles de soins électroniques (rencontré avec la R3V1).

Nous avons récupéré des cartes de tests R3v1 depuis septembre 2019, et avions prévu la mise en place d'un contrôle d'accès ; nous avions donc besoin des puces DESFire. Nous nous sommes dont rapprochés en fin d'année 2019 de l'éditeur pour mettre à jour les différents lecteurs et leur firmware pour prendre en charge la carte R3. L'éditeur s'étant basé sur les cartes R3v1 à l'époque, cela va-t-il causer pour les cartes R3v2 et R3v3 ?

La longueur d'UID a été étendue pour toutes les cartes de la famille R3. Les problématiques gérées pour la longueur d'UID sur des cartes de test R3v1 ne causent donc pas de problèmes pour les cartes R3v2 et R3v3.

Cette problématique concerne-t-elle également les lecteurs sans contact associés aux postes de travail ?

Les lecteurs sans contact associés aux postes de travail présentent des couches et firmware différents ; il n'est donc pas nécessaire de faire de mise à jour sur les lecteurs sans contact associés aux postes de travail qui sont branchés en USB.

Comment les industriels peuvent-ils nous aider dans cette problématique d'extension de la longueur d'UID ?

Le passage de 4 à 7 octets datant de 2010, les industriels devraient avoir la mise à jour du firmware disponibles pour les appareils datant d'après 2010. Ils sont donc sensés connaître le problème, et devraient être en mesure de vous aider.

3.2. Bug « temporisation sans contact » sur les cartes CPx R3V2

Pouvez-vous nous confirmer que le problème ne se produit pas avec les lecteurs OMNIKEY 5321 et 5421 ?

Le problème apparaît en fonction des drivers, des firmware, et des technologies des lecteurs. Il est difficile de savoir si le problème apparaît sans test dans l'environnement concerné.

Dans le cas où le problème apparaît, la solution de contournement est spécifique aux lecteurs Ominkey (cf paragraphe « désactivation de l'interface sans contact des lecteurs dual.

Les cartes CPE et CPA sont-elles également impactées par ce bug ?

Le bug apparaît sur les cartes CPx R3v2, c'est-à-dire les CPS, CPA, CPE et CPF R3v2.

Est-ce que 100% des cartes livrées depuis le 10 juin 2020 sont systématiquement R3v2 ?

Les cartes distribuées depuis le 10 juin 2020 sont pour la quasi-totalité des cartes R3v2, à l'exception marginale des cartes de médecins civils (c'est-à-dire excluant les cartes des médecins militaires du SSA), qui ont été distribuées entre le 10 juin et le 3 juillet en R3v1 Celles-ci ont été renouvelées en R2 courant juillet et la production en R2, pour les médecins civils, maintenue jusqu'au 17 aout. A partir de cette date toutes cartes de médecins civils ont été produites en R3V2.

Comment se fera le renouvellement des cartes R3v2 en R3v3 ?

Le renouvellement d'un parc de carte est d'évidence une perturbation pour les porteurs et en particulier les porteurs salariés en ES. C'est pour cela que les cartes seront renouvelées en urgence uniquement pour les ES ayant rencontré ce bug.
L'ANS prendra contact avec les correspondants qu'auront désigné les établissements concernés, afin de déterminer les modalités du renouvellement du parc de cartes CPx dans la version cible R3V3.

Les modalités de renouvellement des cartes seront définies au cas par cas avec les établissements concernés

L'ANS demande donc à chaque établissement concerné de lui fournir via l'adresse mail infocartecpx-nouvellepuce@sante.gouv.fr l'identité et l'adresse email de ses contacts pour organiser ses modalités de renouvellement. .

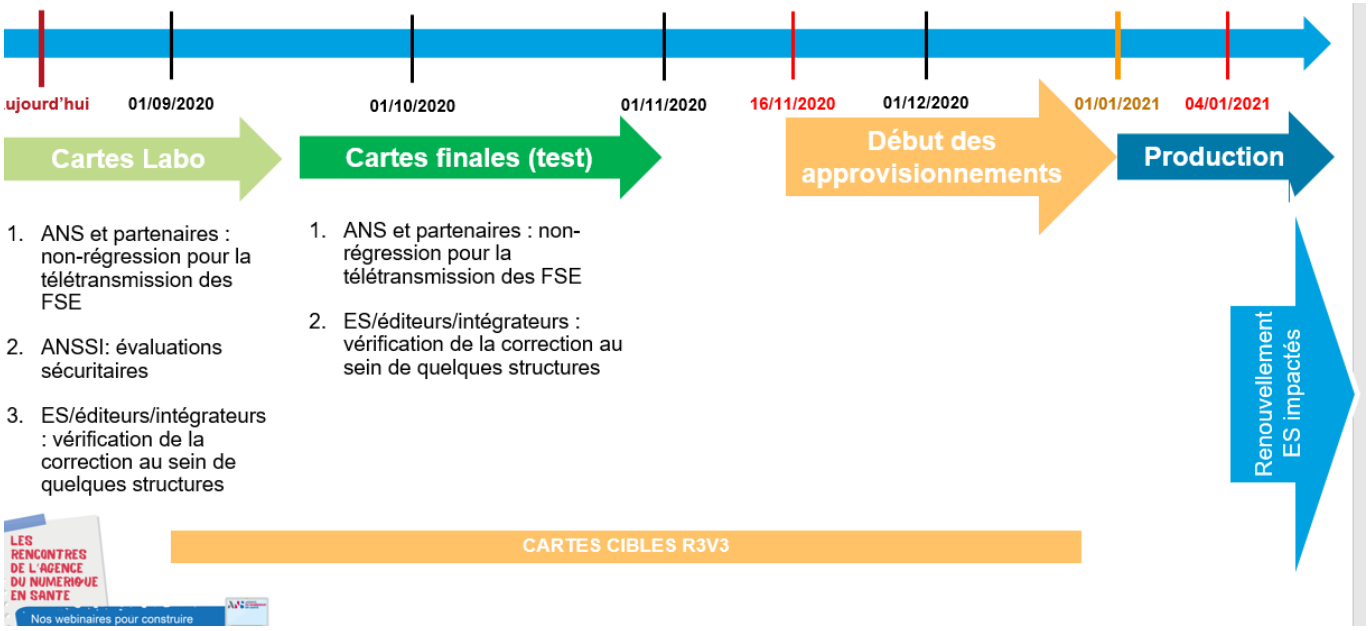
Quel est le calendrier de la correction de ce bug ?

La carte à puce R3V3 a obtenu la qualification de l'ANSSI de la puce.

En parallèle, des tests de qualification et fonctionnels sont en cours.

Le calendrier prévisionnel du renouvellement du parc de cartes R3v2 pour les établissements de santé équipés de lecteurs DUAL a été présenté au webinaire du 07/08/2020 et est rappelé ci-dessous.

Les jalons sont indiqués au plus tôt.



Quelles solutions ont été identifiées pour contourner ce bug ?

Les établissements de santé ont mis en place diverses solutions de contournements techniques mais aussi organisationnelles.

Le principe directeur de ces solutions est d'éviter un reploiement massif de lecteurs ou de scripts sur la totalité des postes de travail impactés.

Solutions de contournement techniques concernant le bug de temporisation sans contact :

1- Désactivation de l'interface sans contact des lecteurs dual

Le SILPC (https://www.silpc.fr/) a implémenté et déployé au CHU de Limoges une solution de contournement concernant le bug de temporisation sans contact.

Cette solution est applicable pour les lecteurs mixtes contact/sans contact car ils possèdent deux pilotes distincts pour l'interface contact et pour l'interface sans contact. C'est le cas des lecteurs Xiring, Ingenico, Gemalto.

Détail de la solution :

Pendant cette période de déploiement des cartes CPx R3v2 et en attendant les nouvelles cartes CPx R3v3, il s'agit de désactiver l'interface sans contact des lecteurs et d'effectuer une communication auprès des utilisateurs.

C'est le seul moyen de s'assurer que ni les services systèmes, ni les cryptolibs CPS, ni les composants SSO n'interagissent sur le mode sans contact de la carte. De plus, on intervient uniquement au niveau des postes de travail (pas de modification sur les serveurs ou les environnements de publication).

Dans la mesure où il faut déployer ces scripts sur les postes de travail concernés, l'application de cette solution peut être complexe.

A chaque fois que l'utilisateur voudra se re-authentifier il devra insérer sa carte dans le lecteur (la saisie du code PIN ne sera nécessaire que pour l'initialisation de la session comme lors du fonctionnement sans le bug).

C'est pourquoi, il est nécessaire de cibler les postes prioritaires (exemple pour les admissions, pour les accès aux téléservices nationaux en authentification forte en mode contact).

/!\ pour passer les commande disable et enable, il est nécessaire d'élever les droits (pour les tests, cmd en mode administrateur).

Exemple, sous Windows 10 avec un lecteur Xiring Diteo :

Commande PowerShell :

Get-PnpDevice -class smartcardreader ➔ *Permet de récupérer la liste des lecteurs*

Exemple :

```
Status  Class           FriendlyName                                  InstanceId
------  -----           ------------                                  ----------
OK      SmartCardReader Lecteur de carte à puce Microsoft Usbccid (WUDF) USB\VID_0A5C...
OK      SmartCardReader Gemalto Virtual PCSC Multi-slots Reader       ROOT\SMARTCA...
OK      SmartCardReader USB Contactless Reader                        CONTACTLESS\...
OK      SmartCardReader USB Smartcard Reader                          USB\VID_04E6...
```

Get-PnpDevice -FriendlyName "USB Contactless Reader" | Disable-PnpDevice -confirm:$false

➔ *Permet de désactiver le lecteur sans contact*

Get-PnpDevice -FriendlyName "USB Contactless Reader" | Enable-PnpDevice -confirm:$false

➔ *Permet de réactiver le lecteur sans contact*

Exemple, sous Windows 7 ou Windows 10 avec un lecteur Xiring Diteo par la commande Devcon[1] :

[1] DevCon (Devcon.exe) est un outil de ligne de commande qui affiche des informations détaillées sur les périphériques sur les ordinateurs Windows (https://download.microsoft.com/download/1/4/0/140EBDB7-F631-4191-9DC0-31C8ECB8A11F/wdk/Installers/787bee96dbd26371076b37b13c405890.cab)

devcon findall =SmartCardReader ➔ *Permet de récupérer la liste des lecteurs*

```
USB\VID_0A5C&PID_5843&MI_01\6&C3AC727&0&0001                    : Lecteur de carte Ó puce Microsoft Usbccid (WUDF)
ROOT\SMARTCARDREADER\0000                                       : Gemalto Virtual PCSC Multi-slots Reader
CONTACTLESS\SCR331-DI_CONTACTLESS_READER\6&353CE04A&0&000       : USB Contactless Reader
USB\VID_04E6&PID_512E\21121048204047                            : USB Smartcard Reader
```

devcon status @"CONTACTLESS\SCR331-DI_CONTACTLESS_READER\6&353CE04A&0&000" ➔
Permet de récupérer le statut du lecteurs

```
CONTACTLESS\SCR331-DI_CONTACTLESS_READER\6&353CE04A&0&000
  Name: USB Contactless Reader
  Driver is running.
```

devcon disable @"CONTACTLESS\SCR331-DI_CONTACTLESS_READER\6&353CE04A&0&000" ➔
Permet de désactiver le statut du lecteurs

```
CONTACTLESS\SCR331-DI_CONTACTLESS_READER\6&353CE04A&0&000   : Disabled
1 device(s) disabled.
```

Exemple, Windows 10 avec un lecteur Ingenico uTrust 102 par la commande Devcon

Affichage de la liste : devcon findall =SmartCardReader

```
USB\VID_0A5C&PID_5843&MI_01\6&C3AC727&0&0001           : Lecteur de carte Ó puce Microsoft Usbccid (WUDF)
USB\VID_076B&PID_5321\OKCM00727041213185797809756200051    : OMNIKEY 5x21
ROOT\SMARTCARDREADER\0000                          : Gemalto Virtual PCSC Multi-slots Reader
CONTACTLESS\SCR331-DI_CONTACTLESS_READER\6&353CE04A&0&000   : USB Contactless Reader
USB\VID_04E6&PID_512E\21121048204047                : USB Smartcard Reader
USB\VID_04E6&PID_5724&MI_00\6&20CB8358&0&0000          : Lecteur de carte Ó puce Microsoft Usbccid (WUDF)
USB\VID_04E6&PID_5724&MI_01\6&20CB8358&0&0001          : Lecteur de carte Ó puce Microsoft Usbccid (WUDF)
```

Status du lecteur : devcon status @"USB\VID_04E6&PID_5724&MI_01*"

```
USB\VID_04E6&PID_5724&MI_01\6&20CB8358&0&0001
  Name: Lecteur de carte Ó puce Microsoft Usbccid (WUDF)
  Driver is running.
1 matching device(s) found.
```

Désactivation du sans contact : devcon disable @"USB\VID_04E6&PID_5724&MI_01*"

```
USB\VID_04E6&PID_5724&MI_01\6&20CB8358&0&0001          : Disabled
1 device(s) disabled.
```

Réactivation du sans contact : devcon enable @"USB\VID_04E6&PID_5724&MI_01*"

/ ! \ Cette solution n'est pas applicable pour les lecteurs HID Omnikey 5321. Ces lecteurs possèdent un pilote unique pour gérer les interfaces contact et sans contact. La désactivation de l'interface sans contact nécessite un reparamétrage du lecteur avec l'outil HID OMNIKEY Workbench Tool.

Exemple Windows 10 avec Lecteur HID 5321

Omnikey publie une documentation sur l'utilisation du mode sans contact sur https://www.hidglobal.com/sites/default/files/5321-903_b.4_omnikey_contactless_developer_guide_en.pdf
La solution retenue :
Création de la clé de registre :
Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CardMan\RFID
ControlFlags=0x00000004
Débrancher / Rebrancher le lecteur pour prise en compte

2- Remplacement des lecteurs dual par deux lecteurs

Deux stratégies sont possibles :

- Ajout d'un lecteur contact à côté du lecteur dual ou bien
- Remplacer chaque lecteur dual par un lecteur contact et un lecteur sans contact sur les postes de travail.

Selon le nombre de poste de travail concernés, ce redéploiement peut être très conséquents.

C'est pourquoi, il est nécessaire de cibler les postes prioritaires (exemple pour les admissions ou dans les salles de réanimation..).

3- Solution de contournement organisationnelle concernant le bug de temporisation sans contact :

Les établissements de santé (ES) impactés ont également mis en place un mode d'organisation dégradé.

Concernant la gestion de l'authentification sur le système d'information hospitalier (SIH), un ES a par exemple réactivé une authentification primaire par login/mot de passe et a continué à utiliser une authentification secondaire en mode sans contact. Cela a impliqué la réinitialisation de nombreux mots de passe et l'envoi de ces informations aux utilisateurs.

Cela demande notamment une organisation au niveau des ressources humaines. Mais cette gestion dégradée de l'authentification n'impacte pas la gestion de l'identification et des habilitations des professionnels sur le SIH.

En effet, les ES veillent à la bonne mise à jour de leur annuaire des professionnels et des habilitations associées. Lorsqu'un un professionnel quitte l'ES, ses entrées dans l'annuaire et ses habilitations sur les applications du système d'information hospitalier sont actualisées.

3.3. Authentification TLS en mode sans contact via un navigateur web

Nous avons détecté un besoin de mise à jour du driver des lecteurs HID OMINKEY pour les cartes R3V2 et sur les cartes labo R3V3 dans le cas d'usage suivant : authentification TLS via un navigateur en sans-contact.
Le test consiste à s'authentifier en mode sans contact sur le site https://testssl.asipsante.fr avec le certificat technique (et sa clé privée) via l'interface Mifare classic de la carte CPS.

Cette authentification échoue avec un lecteur HID sans-contact ou dual Omnikey pour les versions antérieures à la version v5422 (exemple CardMan 5321 Contactless v2, CardMan 5321 V1 et V2) avec tous les navigateurs web.

L’authentification fonctionne avec les lecteur CardMan 5322 et avec les autres modèles :

- Identiv uTrust 4701 F,
- Ingenico DITEO,
- Gemalto Prox DU

Explication :

Les cartes CPS R3v2 et R3V3 labo ne permettent pas un INTERNAL AUTH en sans-contact (Commande APDU utilisée par exemple lors d'une authentification SSL via un navigateur en sans-contact) avec un lecteur sans-contact ou dual Omnikey avec une version < 5421 du fait de l’obsolescence du driver.

Pour information :

- l'ouverture de session Windows n'est pas forcément impactée,
- les lecteurs les plus récents (5422) ne sont pas impactés.

4. ANNEXES

4.1. Liens vers les ressources sur les cartes CPx

Page de présentation des cartes CPx et certificats fournis par l'ANS :
https://esante.gouv.fr/securite/cartes-et-certificats/CPS

Actualité sur la nouvelle puce CPx :
https://esante.gouv.fr/actualites/une-nouvelle-puce-dans-la-carte-cps

L'agence du numérique en santé agit pour les établissements de santé :
https://esante.gouv.fr/lagence-du-numerique-en-sante-agit-pour-les-etablissements-de-sante

Présentation du webinaire de l'ANS sur l'impact des nouvelles cartes CPx :
https://esante.gouv.fr/sites/default/files/media_entity/documents/webinaires_cps_17072020.pdf

Guide officiel de gestion de l'UID Mifare :
https://www.nxp.com/docs/en/application-note/AN10927.pdf

Actualité sur les problèmes d'utilisation des nouvelles cartes :
https://esante.gouv.fr/actualites/etablissements-de-sante-vous-rencontrez-des-problemes-dans-lutilisation-de-vos-nouvelles

Note technique sur les problématiques des nouvelles cartes :
https://esante.gouv.fr/sites/default/files/media_entity/documents/note_point_situation_cpx_r3v2.pdf

Inscription pour le prochain webinaire le 07 août 2020 :
https://www.eventbrite.fr/e/billets-impacts-de-la-nouvelle-carte-cps-dans-les-etablissements-de-sante-114263613544

4.2. Adresse mail de contact de l'équipe ANS

Si vous rencontrez des problèmes dans l'utilisation de vos nouvelles cartes CPx, prenez connaissance des informations de ce document et contactez-nous à l'adresse suivante infocartecpx-nouvellepuce@sante.gouv.fr pour nous signaler les difficultés que vous rencontrez et être accompagnés. N'hésitez pas à nous contacter aux adresses de contact, pour que l'on puisse établir une mailing list, pour échanger plus facilement sur le sujet.