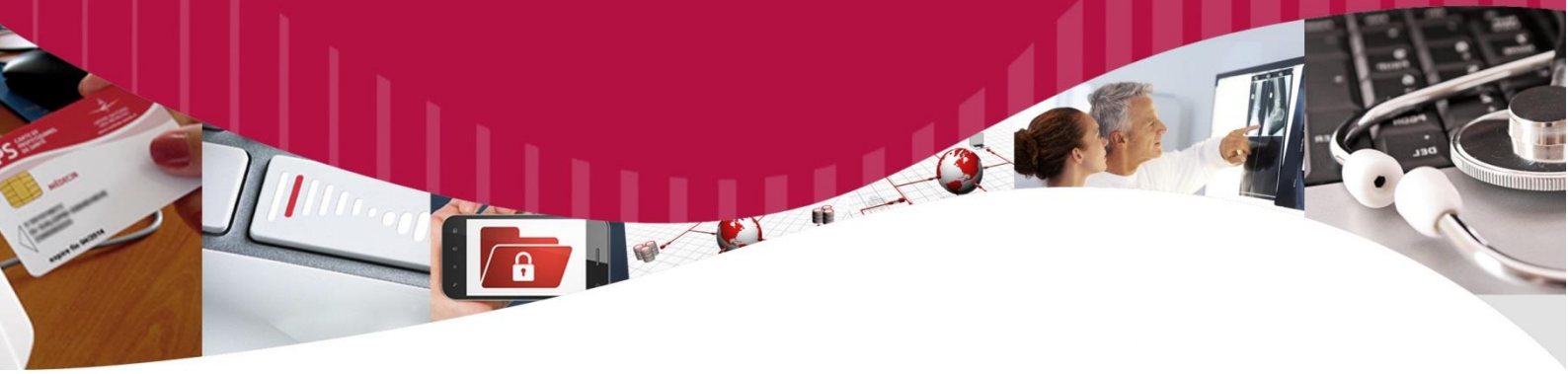


Guide de mise en œuvre de la partie sans-contact des cartes CPx

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

V3.3.0 du 25/04/2019

Guide de mise en œuvre de la partie sans-contact des cartes CPx

Version 3.3.0 du 25/04/2019

Historique du document			
2.3.7	06/02/2015	ASIP Santé	Version publiée sur le site integrateurs-cps.asipsante.fr
2.3.8	30/09/2015	ASIP Santé	Cryptolib CPS 5.0.24 Prise en compte de l'IGC-Santé
3.0.0	31/03/2017	ASIP Santé	+ Annexe 15: Commande OpenSSL "rsautl" + Annexe 19: Cartes CPS3.3 et Mifare Classic 1K
3.1.0	31/03/2017	ASIP Santé	Annexe 19: Cartes CPS3.3, Mifare Classic 1K et HID 5321
3.2.0	22/05/2017	ASIP Santé	Annexe 15.2.5: Exemples de production de signature en sans-contact
3.3.0	25/04/2019	ASIP Santé	Rajout des données de configuration du volet DESFIRE EV1 de la CPx 3.3 R3

1 Références

N°	Version	Date	Auteur	Document
[1]	5.0.9	12/09/2014	ASIP Santé	**Manuel d'installation et d'utilisation de la Cryptolib CPS**
[2]	2.0.1	01/05/2011	ASIP Santé	**Présentation de la carte CPS3**
[3]	1.5.0	16/10/2013	ASIP Santé	**Manuel de programmation de la Cryptolib CPS v5**
[4]	1.1.0	29/05/2011	ASIP Santé	**Documentation programme d'exemple de la Cryptolib CPS v5**
[5]	1.0.1	10/10/2012	ASIP Santé	**Spécifications externes PKCS#11 de la Cryptolib CPS v5**
[6]	2.5.8	24/09/2014	ASIP Santé	**Guide de mise en œuvre d'un Smartcard logon avec une Carte de Professionnel de Santé (CPS)**
[7]			ISO	**ISO/IEC 7810 : Identification cards — Physical characteristics**
[8]		2011	ISO	**Standards "Identification cards — Integrated circuit(s) cards with contacts":** ISO/IEC 7816-1 Part 1: Physical characteristics ISO/IEC 7816-2 Part 2: Dimensions and location of the contacts ISO/IEC 7816-3 Part 3: Electrical interface and transmission protocols ISO/IEC 7816-4 Part 4: Organization, security and commands for interchange

N°	Version	Date	Auteur	Document
[9]			ISO	**Standards "sans-contact":** ISO/IEC 14443-1 Part 1: Physical characteristics ISO/IEC 14443-2 Part 2: Radio frequency power and signal interface ISO/IEC 14443-3 Part 3: Initialization and anticollision ISO/IEC 14443-4 Part 4: Transmission protocol
[10]	1.0.1	21/03/2008	GIXEL / ACSIEL	**EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS [IAS ECC]**
[11]	1.0.2	10/10/2012	ASIP Santé	**Les données métier de la CPS3 Volets CPS2ter et IAS**
[12]	1.0	22/11/2012	ANSSI	**Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques**
[13]	2.0	11/2012	CNPP	**APSAD D83 - Contrôle d'accès - Document technique pour la conception et l'installation**
[14]	2.0	09/2014	Denis BODOR	**OpenSilicium n°12 – Prise en main des technologies RFID / NFC**
[15]	1.0.0	31/03/2017	ASIP Santé	**Echanges courriers CPS3**
[16]	1.0.0	02/04/2013	ASIP Santé	**Procédure de concessions des spécifications de la carte CPS3**
[17]	1.0.0	26/09/2013	ASIP Santé	**PGSSI-S, Authentification des acteurs de Santé**
[18]	1.0	10/02/2011	ASIP Santé	**IGC - CPS2ter, Les certificats X.509 des cartes CPS2ter et CPS3.1 et les CRLs**
[19]	3.0	03/03/2014	NXP	**MF1S50yyX/V1 MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development**
[20]	1.3	02/10/2012	NXP	**AN1305 MIFARE Classic as NFC Type MIFARE Classic Tag**

N°	Version	Date	Auteur	Document
[21]	5321-903 Rev. B.4	01/2015	HID	**OMNIKEY Contactless Smart Card Readers Developers Guide, 5321-903, Rev. B.4**
[22]	3.2.0	31/03/2017	ASIP Santé	**OpenSSL et mod_ssl avec les produits de certification ASIP Santé**
[23]	4.1	05/07/2018	NXP	**AN 10927 MIFARE product and handling of UIDs**
[24]	1.0	03/10/2017	NXP	**AN 12057 Making reader infrastructures ready for multi-application cards and devices**
[25]	1.3	25/04/2019	ASIP Santé	**Prochaine version de la carte CPx**

Tableau 1 : Documents de référence

2 Résumé

Ce document est un **guide pratique et technique** destiné aux porteurs de projet qui souhaitent **mettre en œuvre la partie sans-contact des cartes de la famille CPS** (CPx) à court et à moyen terme. Il s'adresse prioritairement :

- Aux éditeurs de solutions logicielles, fournisseurs de composants matériels (lecteurs,...) et constructeurs de bâtiments destinés aux acteurs de santé (public : architectes, développeurs, chefs de projet)
- Aux établissements de santé qui ont un projet de sécurisation des accès à leur système d'information et aux bâtiments par carte CPx (public : Responsable de la sécurité des systèmes d'information, chefs de projet).

Les cartes CPx sont des cartes à puce délivrées aux professionnels du secteur santé et médico-social. Elles permettent de mettre en œuvre :

- **l'authentification forte du professionnel** (porteur de carte) et la **signature numérique** : en **mode contact** pour réaliser pleinement les opérations cryptographiques permettant de sécuriser le partage et l'échange d'informations médicales à caractère personnel
- **l'authentification simple de la carte** : en **mode sans-contact** (lecture de la carte à moins de 5 cm du lecteur ; conforme à la norme ISO 14443) pour **faciliter l'usage de la carte en situation de mobilité** au sein d'une organisation de santé.

Le **volet sans-contact** de la carte CPx est utilisé :

- d'abord pour faciliter l'utilisation de la carte CPx dans les projets de **sécurisation de l'accès au système d'information** des structures de santé (contrôle d'accès logique) : la carte CPx peut permettre de concilier une authentification primaire du porteur (avec saisie de code porteur) en mode contact et une authentification secondaire de la carte en mode sans-contact, particulièrement adapté pour le personnel médical et soignant en situation de mobilité au sein de la structure de santé.
- ensuite pour **sécuriser l'accès aux locaux** (portes sécurisées) et **au parking** (contrôle d'accès physique); et d'une manière plus générale, pour permettre **l'accès à tout système compatible avec une carte sans-contact de proximité** (cantine, accès aux files d'attente des photocopieuses…) lorsqu'une structure de santé souhaite généraliser les usages de la carte CPx après avoir mené son projet de sécurisation des accès au système d'information par CPx. L'usage d'une seule carte multi-services renforce la dépendance du porteur à sa carte permettant d'éviter les oublis. Plusieurs niveaux de sécurité sont possibles à mettre en place au niveau de la CPx 3.3R3.

Les cartes CPx contiennent un volet IAS permettant de mettre en œuvre un niveau de sécurité renforcé (conformité à la norme européenne IAS-ECC) en mode contact et sans-contact, à la fois pour du contrôle d'accès logique et physique. **Cette mise en œuvre s'inscrit dans un véritable projet d'intégration** et fait appel à des lecteurs compatibles.
L'expression de besoin associée au projet sans-contact doit être formalisée en précisant la cible et la trajectoire.

Le guide se présente en 3 grandes parties:

1. Présentation des **fonctionnalités attachées aux cartes de la famille CPx** et **comparaison** des fonctionnalités sans-contact de la CPx **aux technologies Mifare largement diffusées** ;

2. Description de **scénarios d'utilisation et d'intégration du mode sans-contact de la carte CPx** :
   - pour le **contrôle d'accès physique**, en s'appuyant sur les recommandations du **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** édité par l'*Agence Nationale de Sécurité des Systèmes d'Information* (novembre 2012)
   - pour le **contrôle d'accès logique** quel que soit l'environnement (Smartcard logon, TSE et Citrix, client léger de type navigateur web,…) ; préconisations sur l'utilisation de la zone dédiée dans la carte CPx permettant le stockage et l'usage de jetons
3. Un exemple d'intégration complet dans le SI pour du contrôle d'accès physique et logique est proposé dans le chapitre 8.5.

4. **Recommandations de mise en œuvre**.

De nombreuses annexes complètent ce guide ; en particulier l'annexe 13 qui propose plusieurs exemples d'implémentation pour faciliter **l'enrôlement local de la partie sans-contact de la carte**. L'enrôlement est nécessaire car il n'existe aucun fichier de correspondance entre le numéro de série sans-contact et la carte physique, dans le respect des exigences de la CNIL (les données accessibles via le volet sans-contact des cartes CPx sont des données non nominatives qui ne peuvent pas être reliées au porteur de la carte).

Pour faciliter la mise en œuvre et l'évolutivité des systèmes de contrôle d'accès utilisant les fonctions sans-contact de la carte CPx, l'ASIP Santé recommande la mise en place :
1. d'un système local de gestion du parc de cartes CPx utilisées
2. de lecteurs sans-contact en mode « transparent », c'est-à-dire des lecteurs qui ne font que transformer les ondes en commandes filaires et vice versa dans le cadre des échanges entre la carte CPS et l'Unité de Traitement Local (UTL)
3. d'UTL « intelligents » (capables de communiquer avec la carte CPS au moyen de commandes APDUs normalisées par la norme IAS-ECC), supportant le mode transparent, et susceptibles d'être mis à jour facilement
4. de processus d'enrôlement local simples
5. de câblages normalisés

Accompagnement	Pour toute question et échange sur ce document : editeurs@asipsante.fr Les structures de santé et leur maîtrise d'œuvre, désireuses de revoir leurs systèmes d'accès en s'appuyant sur les fonctionnalités apportées par la carte CPx, peuvent se faire connaître auprès de l'ASIP Santé à l'adresse editeurs@asipsante.fr

Tableau 2 : Contrôle d'accès : contact accompagnement ASIP Santé

3 Sommaire

4 Glossaire

Abréviation	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
ATS	Answer To Select, réponse de la carte à puce sans-contact à la sélection par le lecteur sans-contact
ATR	Answer To Reset, réponse de la carte à puce à la mise sous tension
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPP	Centre National de Prévention et de Protection
CPx	Famille de cartes à puce émises par l'ASIP Santé comprenant CDA, CDE, CPA, CPE, CPF et CPS
ES	Etablissement de Santé
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS-ECC	Identification Authentification Signature - European Citizen Card
IGC	Infrastructure de Gestion de Clés, PKI en anglais ou Infrastructure à Clés Publiques i.e. ICP
ISO	International Organization for Standardization
LPS	Logiciel de Professionnel de Santé
MITM	Man In The Middle
NUID	Non-Unique IDentifier
OS	Operating System – Système d'exploitation
OSI	Open Systems Interconnection
PFCNG	Plate-Forme de Certification Nouvelle Génération : plate-forme technique offrant les services de la nouvelle "IGC-Santé" remplaçant les IGCs 2bis et 2ter

Abréviation	Signification
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PKCS	Public Key Cryptographic Standards
PIV	Personal Identification Verification
PKI	Public Key Infrastructure (IGC)
PKIX	X-509 based PKI
PoE	Power over Ethernet
PS	Professionnel de Santé
PUPI	Pseudo-Unique PICC (Proximity Integrated Circuit Card) Identifier
RFID	Radio-Frequency IDentification
RGS	Référentiel Général de Sécurité
SI	Système d'Information
SSL	Secure Sockets Layer
SSO	Single Sign On
TLS	Transport Layer Security
TSE	Terminal Server Edition
UID	Unique IDentifier
URL	Uniform Resource Locator
UTL	Unité de Traitement Local

Tableau 3 : Glossaire

5 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants:

Nom	Site Web	Lien avec le sans-contact CPx
ANSSI	www.ssi.gouv.fr	Co-rédacteur du RGS, Recommandations sans-contact
Apple	www.apple.com	Mac OS X
Citrix	www.citrix.com	Environnements TSE/Citrix
GIXEL	www.gixel.fr	Standard IAS-ECC
HID	www.hidglobal.fr	Fabricant de lecteurs
Ingenico/Xiring	healthcare-eid.ingenico.com	Fabricant de lecteurs
Microsoft	www.microsoft.com	Windows, CSP, Windows Active Directory
NXP Semiconductors	www.nxp.com	Société propriétaire de Mifare, technologie sans-contact souvent mise en relation avec la partie sans-contact de la CPx
OpenSC	OpenSC	Outils et librairies pour la carte à puce
PC/SC Workgroup	www.pcscworkgroup.com	Responsable du standard PC/SC visant l'intégration de la carte à puce et des lecteurs de cartes dans les systèmes informatiques
RSA Security Inc.	**www.rsa.com**	**PKCS, RSA**

Tableau 4 : Entreprises citées

6 Avertissements

Sur le nécessaire strict respect des procédures décrites dans le document L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent document. Toutes les procédures qui y sont décrites ont été préalablement testées par l'ASIP Santé. Elles doivent permettre à l'utilisateur d'évaluer la technologie sans-contact de la carte CPx sur un poste de travail ou tout autre dispositif informatique. En cas de non-respect de ces procédures, cette mise en œuvre est susceptible d'engendrer des dysfonctionnements dans l'environnement de travail de l'utilisateur. En cas de dysfonctionnement, quel qu'il soit, l'ASIP Santé prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent document.
Sur les liens externes Le présent document contient des liens vers des sites Internet. Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ASIP Santé et l'ASIP Santé n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ASIP Santé quant à leur contenu. L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.
Sur les copies d'écran et les lignes de commande Les lignes de commandes données ci-après le sont à titre indicatif. Elles documentent des cas « passants » qui peuvent différer d'un système à l'autre. Les copies d'écran présentées dans ce document sont données à titre illustratif. Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.
Citations L'ASIP Santé est contrainte de citer le nom de certaines entreprises recensées au Tableau 4 afin d'apporter toute l'aide nécessaire au lecteur. Les entreprises citées peuvent prendre contact avec l'ASIP Santé à l'adresse email editeurs@asipsante.fr pour toute demande en lien avec la citation les concernant. Les entreprises non citées dans ce manuel et ayant une activité en lien avec la technologie sans-contact peuvent également se faire connaître auprès de l'ASIP Santé en la contactant à la même adresse.
Contact Toute question en rapport avec le contenu du présent manuel doit être adressée à l'adresse suivante: editeurs@asipsante.fr

Tableau 5 : Avertissements

7 Présentation générale de la CPx et du sans-contact

7.1 La famille de cartes CPx

Les cartes CPx permettent d'effectuer des opérations cryptographiques dont l'objectif est de sécuriser des actions ou des échanges informatiques.

Les cartes CPx sont exhaustivement présentées en **[Présentation de la carte CPS3]** et permettent de mettre en œuvre le palier 3 de l'authentification publique des acteurs de Santé comme décrit en **[PGSSI-S, Authentification des acteurs de Santé]**.

En résumé, les cartes CPx offrent deux grandes fonctions cryptographiques:

1. L'authentification[1]
    a. qui permet d'identifier et d'authentifier le porteur de la carte CPx
2. La signature numérique
    a. qui permet de vérifier l'authenticité et l'intégrité d'un document lors de sa réception

7.2 Présentation du sans-contact

La carte CPx se présente en fait comme trois cartes en une :

1. une carte CPS2ter ;
2. une carte IAS-ECC ;
3. une carte sans-contact qui s'appuie sur l'ISO 14443

Le document de référence décrivant les nouvelles fonctionnalités sans-contact de la carte CPx est **[Présentation de la carte CPS3]**.

La partie sans-contact est destinée à améliorer l'ergonomie d'usage de la carte CPx ainsi qu'à ouvrir la carte CPx à de nouveaux usages, notamment dans les établissements de santé (ES). Elle permet à l'utilisateur d'exploiter sa carte sans avoir à l'insérer dans la fente d'un lecteur, réduisant de ce fait les manipulations à effectuer et plus secondairement l'usure du support.

Cet usage nécessite l'utilisation d'un lecteur disposant de la fonctionnalité sans-contact. Cette technologie permet, selon le lecteur utilisé, un fonctionnement jusqu'à une distance maximale d'environ 10 cm[2] par rapport au lecteur.

La partie sans-contact de la carte CPx est conforme au standard IAS-ECC, norme promue par l'ANTS et le GIXEL[3], conforme au standard européen ECC visant à renforcer la sécurité tout en améliorant les performances des systèmes qui la sous-tendent.

[1] Dans ce document, l'authentification est une identification au moyen de secrets révocables.

[2] **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** conseille 5 cm.

[3] Le site du GIXEL n'est plus disponible. La norme IAS-ECC semble être distribuée par l'ACSIEL (www.acsiel.fr).

7.4 Accès physique et accès logique

Le contrôle d'accès fait souvent la distinction entre 2 types d'accès différents :

D'un côté, l' « accès physique » qui couvre les cas d'usages liés aux ouvertures de portes, aux accès à des locaux.

Carte CPx et ISO 14443	La carte CPx est compatible avec les lecteurs ISO 14443 type A et type B d'ores et déjà largement installés.

Tableau 6 : CPx Sans contact, accès physique et ISO 14443

D'un autre côté, l' « accès logique » qui couvre les cas d'usage liés à l'ouverture de sessions applicatives (ouverture de sessions de travail, accès à des applications, droits dans des applications particulières).

Cryptolib CPS v5	La Cryptolib CPS v5 permet d'accéder aux fonctionnalités sans-contact de la carte CPx depuis des postes de travail utilisant Microsoft Windows, Apple Mac OS X ou Linux.

Tableau 7 : CPx Sans contact, accès logique et Cryptolib CPS v5

7.5 Sans-contact et authentification simple du support

Afin d'améliorer l'ergonomie d'usage dans un contexte de mobilité, une « **authentification simple** » sans-contact est proposée par la carte CPx.

L' « **authentification simple** » s'entend relativement à l'expression « **authentification forte** » :

1. L' « **authentification forte** » met en œuvre au moins 2 facteurs d'authentification
    a. Dans le cas d'une authentification en mode contact avec une carte CPx, les 2 facteurs d'authentification sont :
        i. « **ce que j'ai** » : le fait d'être porteur de la carte
        ii. « **ce que je sais** » : connaissance du code porteur
2. L' « **authentification simple** » met en œuvre 1 seul facteur d'authentification
    a. Dans le cas d'une authentification en mode sans-contact avec une carte CPx, le facteur d'authentification est :
        i. « **ce que j'ai** » : le fait d'être porteur de la carte

Le volet sans-contact de la carte CPx:

- **permet** d'effectuer une « **authentification simple** » du **support** (la carte)
- **ne permet pas** d'effectuer une **authentification du porteur**, qu'elle soit simple ou forte
    - ceci provient du fait que le volet sans-contact de la CPx **ne contient ou n'expose aucune information** « reliable » à une personne physique

Deux exemples:

1- Le volet sans-contact de la carte CPx permet par exemple de faire une authentification SSL via un navigateur internet (mis en place sur testssl.asipsante.fr) : cette authentification ne doit pas être traitée par le serveur qui la met en œuvre de la même manière qu'une authentification en mode contact car il s'agit d'une authentification simple du support physique « carte CPx » et non d'une authentification forte d'un porteur de carte CPx.

2- Le volet sans-contact de la carte CPx permet de faire une signature. La signature produite est une signature technique, destinée à la fonction d'authentification simple du support, qui n'a pas du tout la même valeur juridique qu'une signature effectuée avec le bi-clé de signature en mode contact.

7.6 Comparaison avec la technologie Mifare

Le volet sans-contact de la carte CPx est souvent comparé au Mifare.

Les produits Mifare s'appuient eux-aussi sur l'ISO 14443 pour le niveau physique et le niveau transmission afin de gérer la communication entre le lecteur et la carte (voir aussi Annexe – ISO 14443 et IAS-ECC pour la partie sans-contact de la carte CP pour plus de détails).

Le produit Mifare Classic est le précurseur des produits sans-contact et n'est pas totalement conforme à l'ISO 14443 : ce produit ne fait pas de distinction entre la couche physique et la couche applicative.

Au niveau applicatif, les produits CPx/IAS-ECC et Mifare sont totalement différents : ils ne supportent pas les mêmes fonctions, ils n'utilisent pas les mêmes algorithmes cryptographiques.

La partie applicative de Mifare, activée depuis février 2017 dans la carte CPS3.3 (cf. Annexe – Carte CPS 3.3 et support de Mifare Classic 1K), fait l'objet de consignes de vigilance de la part de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) communiquées par les services du Haut Fonctionnaire de Défense et de Sécurité du ministère des affaires sociales et de la santé aux différents acteurs Santé&Social.

	CPx	**Mifare Classic**
Facteur de forme	ISO 7810 ID-1	ISO 7810
Fréquence	13,56 Mhz	13,56 Mhz
Modulation	ISO 14443 Type A ou Type B	ISO 14443 Type A
Protocole de communication	ISO 7816-1 à 4	ISO7816-1 à 3
Identifiants uniques	UID (Type A) PUPI (Type B) Numéro de série IAS Numéro de carte logique Certificat Technique Identifiant Aléatoire	UID

Tableau 8 : Tableau comparatif CPx / Mifare Classic

La carte CPx est compatible avec les installations sans-contact basées sur les cartes Mifare Classic.

De plus, elle permet d'accéder à des mécanismes d'un niveau de sécurité supérieur.

Un même système de contrôle d'accès peut faire cohabiter deux familles de cartes en parallèle :

- Des cartes d'accès Mifare d'un côté (« accès historique »).

- Des cartes CPx

7.7 Absence de code porteur en sans-contact

Il n'y a pas de saisie de code porteur sur le volet sans-contact de la carte CPx (authentification simple du support physique).

7.8 Protection des données personnelles

Le volet sans-contact de la carte CPx tient compte des considérations de sécurité induites par le « sans fil ». En particulier, les données exposées en sans-contact peuvent être lues à l'insu du porteur de la carte (cas d'un attaquant équipé d'un lecteur de cartes sans-contact dans un lieu public par exemple).

Dans ce contexte, les données accessibles via le volet sans-contact de la carte CPx sont des données non nominatives non reliables au porteur de la carte :

- Le certificat X.509v3 sans-contact est un certificat « technique » non nominatif ;
- Il n'existe aucun fichier de correspondance entre numéro de série sans-contact et carte physique, par construction même de l'IGC de Santé ;
    - l'exigence de non-traçabilité de l'individu imposée par la CNIL est ainsi respectée ;
    - l'ASIP Santé ne dispose pas elle-même de ces listes.

Pour ces deux raisons (légale puis technique), l'ASIP Santé ne peut pas fournir de fichiers de correspondance associant l'identifiant (UID/PUPI) de l'interface sans contact carte CPx avec le numéro de série de la partie Contact.

Les établissements qui souhaitent mettre en œuvre le volet sans-contact de la carte CPx doivent donc mettre en œuvre un processus d'enrôlement local des cartes (cf. le chapitre « Enrôlement » et l'annexe « Annexe – Exemples d'implémentation d'enrôlement sans-contact»).

8 Scénarios d'utilisation et d'intégration du mode sans-contact

La technologie des cartes sans-contact est principalement utilisée en accès physique lorsqu'il est nécessaire voire indispensable :

- que le temps d'exposition soit court :
  - barrière de péage
- que le nombre d'expositions quotidiennes soit élevé :
  - contrôle d'accès physique à un bâtiment
- que les traitements logiques soient limités :
  - pointage horaire

Le volet sans-contact de la CPx est essentiellement tourné vers ce type d'usages.

Pour l'heure, la technologie sans-contact est moins utilisée pour faire de l'accès logique.

Le volet sans-contact de la CPx permet cependant d'anticiper dès maintenant des usages en accès logique.

8.1 Accès sans-contact et modèle « AAA »

Les principes appliqués dans le domaine des accès sans-contact, qu'ils soient « physique » (portes…) ou « logiques » (ouverture de session), suivent les mêmes grandes règles d'implémentation que l'on trouve traditionnellement dans l'édition logicielle. Ces règles sont bien formalisées et largement adoptées.

Dans les scénarios qui intéressent ce document, le porteur de carte CPx utilise sa carte CPx pour s'**authentifier** auprès du système, qui l'**autorise** (ou non). L'opération laisse généralement une **trace** : l'événement, qu'il soit ok ou ko est conservé sous la forme d'une association {date ; carte ; lieu d'accès ; référence vers l'identité associée} par chacun des éléments techniques composant le système.

Il s'agit donc d'un modèle AAA (Authentication, Authorization and Accounting, pour Authentification, Autorisation et Traçabilité) dans lequel le « vecteur d'authentification » est la carte CPx, utilisée via son volet sans-contact.

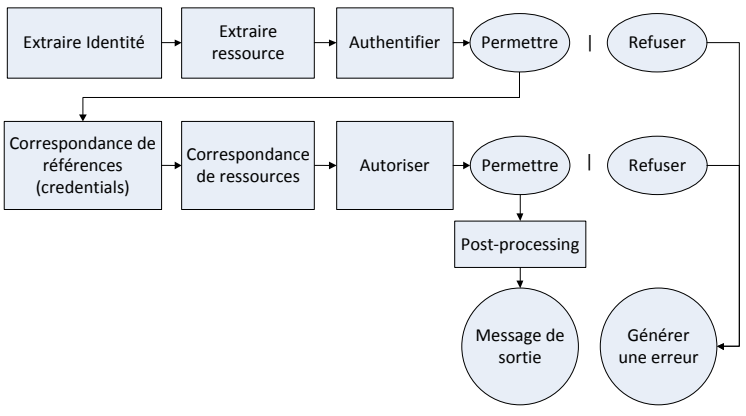


Figure 1 : Principe général du AAA (source : IBM)

Ce modèle est un modèle en « tunnel » - ou en « filtres » - dans lequel chaque élément assume un rôle précis, bénéficiant du travail de son prédécesseur et dont le travail bénéficie à son successeur. Il est intéressant d'avoir à minima les 3 éléments Authentification, Autorisation et Traçabilité en tête afin de disposer des éléments sémantiques permettant la réflexion, la compréhension et, plus avant, l'échange avec les interlocuteurs du secteur. Une recherche ultérieure sur les principales implémentations AAA permet d'affiner cette compréhension.

[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques] reprend et analyse exhaustivement les principaux éléments d'architecture que l'on rencontre en sans-contact. Résumés et vus sous l'angle du AAA, ils peuvent être présentés dans le schéma ci-après.

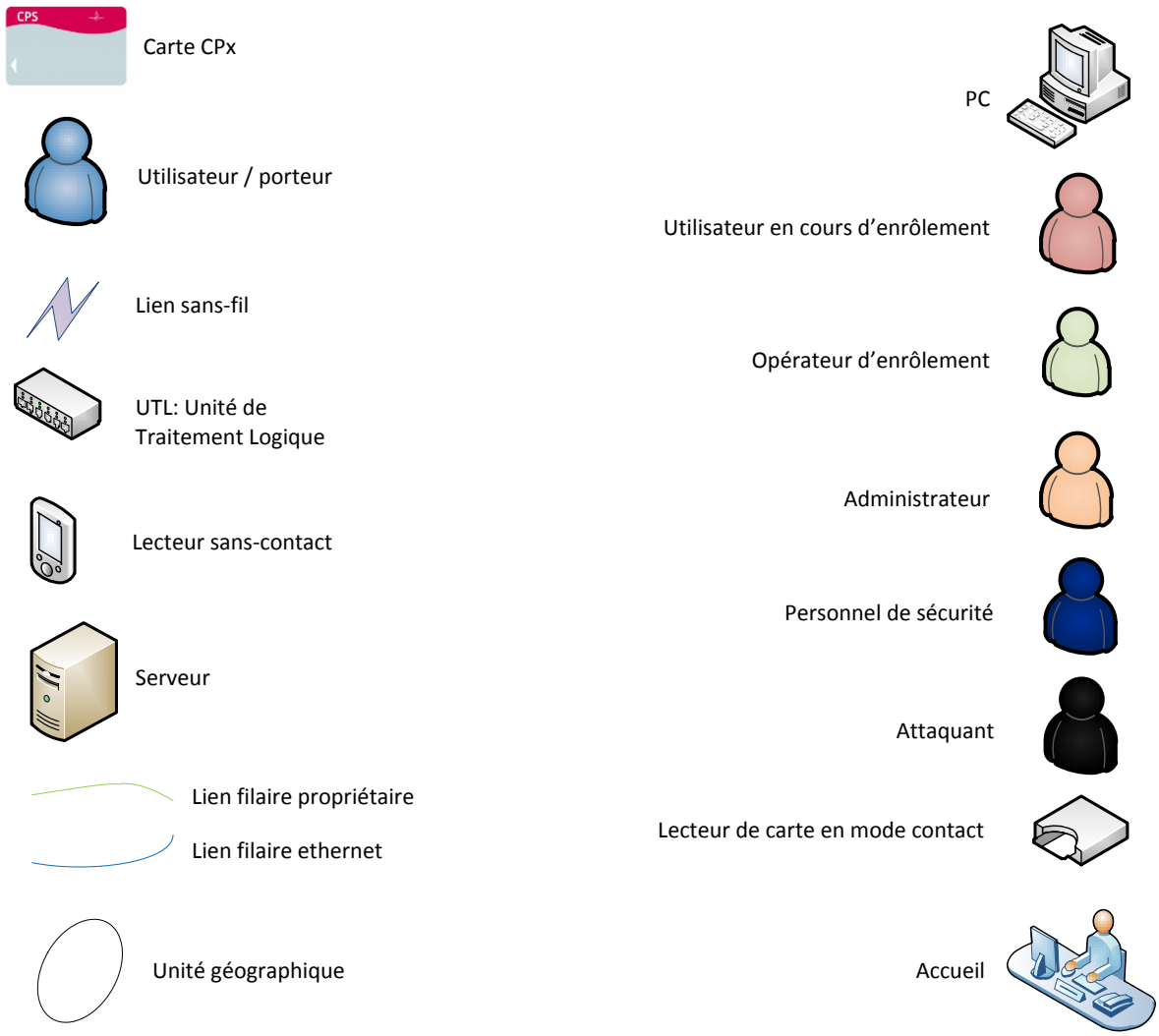


Figure 2 : Légende des schémas présentés dans le document

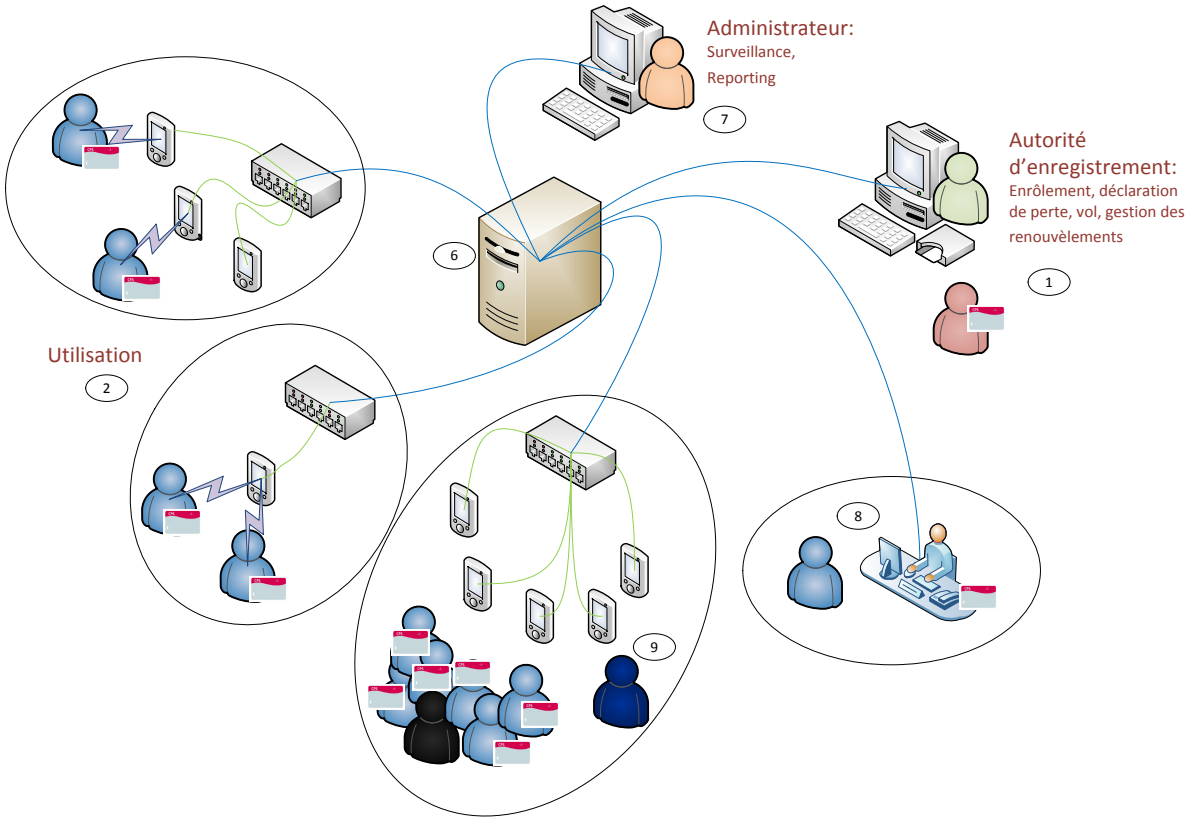


Figure 3 : Architecture d'un système d'accès sans-contact

#	Description
1	L'utilisateur et sa carte sont « enrôlés » - enregistrés - par une « autorité d'enregistrement » dans une base de données. Cette opération peut être automatique ou manuelle.
2	Une fois le porteur enrôlé, il devient « utilisateur » du système et peut utiliser sa carte en sans-contact pour accéder aux locaux ou aux différents services du SI.
3	Dans les faits, dans le cas des accès physiques, l'« utilisateur » passe sa carte devant un « lecteur de cartes sans-contact » qui est géré par une « Unité de Traitement Local » (UTL) généralement située à proximité immédiate de la porte protégée par contrôle d'accès. L'UTL ressemble à un petit routeur de type « box internet » relié au réseau de l'entreprise.
4	Le lecteur lit depuis la carte de l'utilisateur, en sans-contact, des informations qui sont remontées du lecteur à l'UTL puis, éventuellement, de l'UTL au serveur.
5	Ces informations sont discriminantes : elles permettent au serveur d'**authentifier** de manière non-équivoque l'utilisateur après examen des informations créées lors de la phase d'enrôlement.
6	Les informations d'**authentification** récupérées par le serveur lui permettent ensuite de récupérer des **autorisations** pour cet utilisateur et la zone géographique où il essaye de pénétrer.
7	Cette tentative d'accès et son résultat sont journalisés dans le lecteur, dans l'UTL et dans le serveur (**traçabilité**). L'analyse des traces collectées permet une forme de surveillance et d'effectuer des reportings.
8	En cas de perte ou d'oubli de carte, un utilisateur applique une procédure préétablie qui lui permet d'accéder aux locaux sans sa carte (par exemple en se rendant à l'accueil qui lui délivre une carte temporaire).
9	Certaines zones sensibles ou à fort passage sont surveillées.
10	Cette surveillance permet de fluidifier les accès aux heures de pointe, d'aider les utilisateurs qui rencontrent des problèmes et de dissuader les intrus, dont on cherche à s'affranchir par essence même du projet.

Tableau 9 : Architecture et scénario général du contrôle d'accès

8.2 Le contrôle d'accès physique

L'utilisation historique de la carte sans-contact est le contrôle d'accès à des zones de sensibilité variée. Il est ainsi aisé de la généraliser pour :

- l'entrée au bâtiment,
- l'entrée au parking,
- la définition d'une zone plus sensible en limitant les accès à un certain nombre d'identifiants.
- …

L'intérêt réside principalement :

- dans la réduction de coûts humains des contrôles d'accès
  - moins de personnels dédiés à vérifier des identités aux entrées
  - une image : le péage autoroutier par rapport au télépéage
- dans la réduction des temps de contrôle
  - une image : une nouvelle fois, le péage autoroutier par rapport au télépéage
- dans la réduction de fuite dans le système de contrôle
  - par échanges oraux ou papiers
  - la carte servant aussi de badge d'identification, son prêt à un tiers devient plus délicat.
- par rapport au « mode contact », le mode « sans-contact » permet de s'affranchir des problèmes d'usure du support

8.2.1 Principe du contrôle d'accès physique en type A sur la base de l'UID Mifare

Conformément au principe général, le contrôle d'accès physique se fait historiquement en lisant l'UID Mifare de la carte sans-contact type A.

Le principe est le suivant :

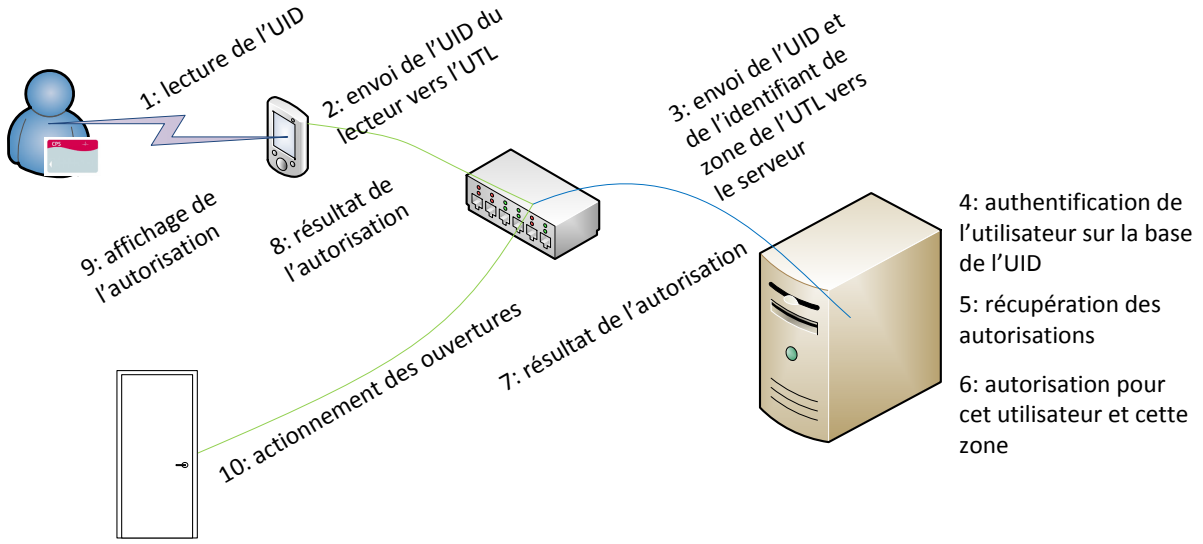


Figure 4 : Principe de l'accès physique type A sur la base de l'UID Mifare

Les phases 4, 5 et 6 peuvent aussi se passer sur les UTL s'ils sont « intelligents » et que le serveur leur a préalablement distribué des listes d'approbations.

8.2.1.1 *Diagramme de séquence associé au contrôle d'accès physique en type A sur la base de l'UID Mifare (situation communément rencontrée)*

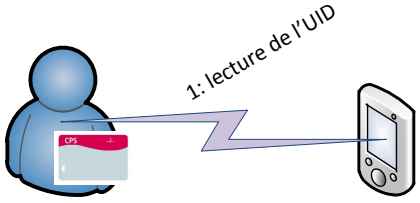
Ce scénario est illustré en « Annexe – Diagramme de séquence associé au contrôle d'accès physique en type A sur la base de l'UID Mifare ». Les remarques liées à ce scénario sont les suivantes :

#	Remarque
[a1]	La courte ligne de vie de la carte CPx dans les échanges carte-lecteur est due au fait que seul le niveau ISO 14443 est utilisé.
[C]	L'absence d'authentification CPx.
[D2]	Une simple vérification de présence de l'UID détecté dans une liste blanche en guise de vérification.

Tableau 10 : remarques liées au diagramme de séquence associé au contrôle d'accès physique en type A sur la base de l'UID Mifare

8.2.1.2 *Problèmes liés à l'accès physique type A sur la base de l'UID Mifare*

Ce principe souffre néanmoins de problèmes de sécurité sur le lien {carte – lecteur sans-contact} et est déconseillé « tel quel » par **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** qui lui attribue le niveau de sécurité 1, i.e. le plus faible : c'est ce scénario qui fait l'objet de consignes de vigilance de la part de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) évoquées plus haut.



P1: clonage de carte et rejeu

P2: logique incompatible avec le type B / PUPI

Figure 5 : Problèmes liés à l'accès physique type A sur la base de l'UID

La technologie Mifare Classic ne doit plus être utilisée pour implémenter un nouveau système d'accès.

Si la technologie Mifare Classic est utilisée pour implémenter un système d'accès, le système d'accès ne doit pas reposer sur les seules données du « bloc 0 », qui est le bloc de données réservé aux fabricants de composants et qui contient notamment l'UID.

Les problèmes de sécurité qui imposent ces précautions sont illustrés en « Annexe – Attaques de cartes sans-contact. »

Dans le cas de la carte CPx, lorsque le niveau applicatif IAS-ECC n'est pas utilisé, le niveau de sécurité obtenu est équivalent au Mifare Ultralight avec la CPS3.1 et au Mifare Classic 1K avec la CPS3.3R2.

En Mifare Ultralight, seul l'UID Mifare peut servir de discriminant en contrôle d'accès physique. Mifare Ultralight étant une adaptation non sécurisée de Mifare Classic, les 2 recommandations citées ci-dessus s'appliquent.

Ce scénario est repris dans le paragraphe « Exemple d'intégration complet : l'accès physique » et le processus d'enrôlement associé est illustré en « Annexe – Exemples d'implémentation d'enrôlement sans-contact », ce dernier étant une brique commune avec tous les autres scénarios envisageables.

8.2.2 Principe du contrôle d'accès physique basé sur l'utilisation du volet DESFIRE EV1 de la CPx3.3 R3

La mise à jour du composant de la CPx3.3 de la R2 vers la R3 ramène un nouveau volet sans contact (DESFIRE EV1) avec un niveau de sécurisation renforcée [25]. La rétrocompatibilité est garantie par rapport aux usages existants avec la CPx3.3 R2. [23-24]

8.2.2.1 Configuration initiale du volet DESFIRE EV1 de la CPx 3.3 R3 :

La CPx 3.3 R3 est livrée avec la configuration suivante :

- La clé maitre (MK.PICC) de la puce DESFIRE EV1 est au format 3DES 128bits et aura une valeur nulle.
- La modification de la configuration, le changement de la valeur de la clé maitre ou la suppression d'application devra se faire avec une authentification par cette clé maître MK.PICC.
- La mémoire de la puce sera vide.
- La puce présentera par défaut un UID à 7 Octets.

8.2.2.2 Configurations recommandées :

Plusieurs combinaisons de configuration sont possibles au niveau de la DESFIRE EV1. On en recommande deux qui présentent un niveau de sécurité suffisant mais deux niveaux de complexité d'implémentation.

Identification basée sur l'UID

Il est fortement recommandé d'éviter de baser l'identification de la carte sur l'UID. Ceci équivaut à utiliser le composant DESFIRE EV1 comme un composant MIFARE CLASSIC.

Pour toutes les configurations, les recommandations sont les suivantes :

- Il est conseillé de créer une application dédiée à chaque usage (contrôle d'accès, pointage horaire, parking, …) avec un jeu de clés dédié.
- Chaque application doit contenir un fichier contenant l'identifiant de la carte.
- **L'identifiant généré doit être aléatoire et non inscrit sur la carte CPx.**
- Il est fortement recommandé d'utiliser exclusivement des clés symétriques de type AES.
- L'activation du paramètre du chiffrement des échanges lecteur-CPx est aussi recommandée.

La CPx est reconnue par un identifiant encodé au niveau de chaque CPx au moment de son enrôlement initial et non par son UID. L'accès à cet identifiant nécessite la connaissance par le système de contrôle d'accès des données suivantes :

1. Clé de lecture du fichier
2. AID (Application IDentifier) de l'application
3. FID (File IDentifier) du fichier contenant l'identifiant
4. Longueur de l'identifiant
5. Type d'encodage de l'identifiant dans le fichier

Lors de l'échange entre le lecteur et la CPx, on peut distinguer deux types d'implémentation :

Cas d'usage 1 : (Implémentation simple) authentification par une clé partagée

La CPx donne accès à l'identifiant lorsque le lecteur présente le chemin d'accès (AID+FID) et la clé de lecture du fichier qui est commune à toutes les CPx.

Cas d'usage 2 : (Implémentation complexe) authentification par une clé diversifiée

La CPx donne accès à l'identifiant lorsque le lecteur présente le chemin d'accès (AID+FID) et une clé de lecture qui est propre à chaque CPx. Cette clé est obtenue par diversification de la clé de lecture et de l'UID se basant sur un algorithme prédéfini au moment de la configuration du système de contrôle d'accès.

8.2.2.3 Gestion des clés :

La génération ainsi que l'insertion des clés dans le système d'encodage ou de contrôle d'accès sont considérés comme des opérations sensibles : il est recommandé que ces opérations se fassent lors d'une cérémonie des clés lors de la mise place de la configuration initiale du système. Il est recommandé que l'ensemble des clés soient exclusivement connues et gérées par les équipes internes de l'établissement de santé. On distingue deux types de clés : des clés à partager avec le lecteur ou l'UTL pour échanger avec la carte et d'autres qui ne seront utilisés que lors de l'encodage initial de la CPx.

Liste des clés pour une configuration type :

1. Clé « MX » : clé maitre de la carte (exclusive au poste d'encodage)
2. Clé « MAID » : clé d'accès à l'application créée (exclusive au poste d'encodage)
3. Clé « FileRead » : clé de lecture du fichier contenant l'identifiant (partagée avec le système de contrôle d'accès)
4. Clé « FileWrite » : clé d'écriture du fichier contenant l'identifiant (exclusive au poste d'encodage)

Il est aussi important de distinguer entre les CPx et les cartes dites « blanches » (anonymes ou dédiés aux visiteurs) par un jeu de clés différent. Ceci permet de séparer les deux lots et se prémunir d'une éventuelle compromission de clés.

8.2.2.4 Séquence d'encodage type :

A titre d'exemple, voici un séquencement type d'opération pour l'encodage de la CPx3.3R3 :

1. S'authentifier avec une clé 3DES nulle au niveau de l'application 00
2. Changer la clé maitre MK.PICC à une nouvelle clé en AES 128 bits : « MX »
3. S'authentifier avec la clé « MX » au niveau de l'application 00
4. Modifier la configuration comme suit :
    a. Activation du chiffrement de la communication entre le lecteur et la carte
    b. Imposer l'authentification pour accéder à l'UID
    c. Imposer l'authentification pour créer une application
    d. Imposer l'authentification pour explorer la carte
5. S'authentifier avec la clé « MX » au niveau de l'application 00
6. Créer une application avec les données suivantes :
    a. AID : à initier et à partager avec le système de contrôle d'accès
    b. Clé d'accès à l'application : à initier en AES 128 bits : « MAID »
    c. Imposer l'authentification de la clé pour pouvoir la changer
7. S'authentifier avec la clé MAID au niveau de l'application créée
8. Créer un fichier avec les données suivantes :
    a. FileID : à choisir (0 par défaut) : la valeur « 1 » est recommandée
    b. Clé de lecture : à initier en AES 128 bits : « FileRead »
    c. Clé d'écriture : à initier en AES 128 bits : FileWrite »
    d. Taille du fichier : à définir en fonction de la taille de l'identifiant
9. S'authentifier avec la clé d'écriture du fichier
10. Générer un identifiant et l'écrire au niveau du fichier créé

8.2.3 Principe du contrôle d'accès physique basé sur SSL (situation cible)

A l'opposé de la méthode précédente, il est possible de mettre en place une architecture de contrôle d'accès basée sur PKIX.

Carte CPx et certificat X.509v3 sans contact	La carte CPx est compatible avec l'architecture de contrôle d'accès physique basée sur SSL

Tableau 11 : CPx et accès sans-contact SSL

Le principe général est le suivant :

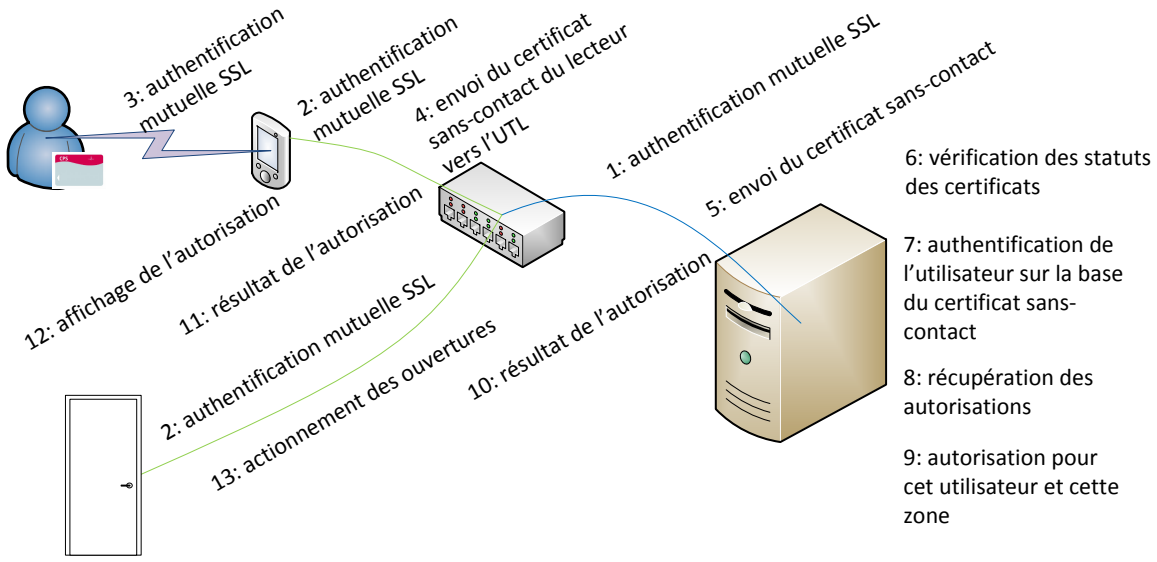


Figure 6 : Principe du contrôle d'accès sans-contact SSL avec la CPS

	Description
1	Chaque équipement s'authentifie à l'aide de son certificat propre auprès de ses correspondants: • La porte auprès de l'UTL et vice versa • Les UTL auprès du serveur et vice versa Dans ce scénario, la distribution des clés entre les différents acteurs du système et leurs répudiations sont plus abouties que dans un scénario proche basé sur de la cryptographie symétrique, ce dernier scénario étant par ailleurs sans doute plus performant (latences).
2	Une fois les authentifications mutuelles réalisées, des liens sécurisés par SSL, point à point, sont créés et permettent l'envoi et la réception de commandes dans des canaux sécurisés.
3	Lorsqu'un utilisateur passe sa carte devant le lecteur, le même principe s'applique entre la carte et le lecteur sans-contact: la carte CPx s'authentifie à l'aide du certificat X.509v3 technique qu'elle porte auprès du lecteur et vice versa. Si lecteur supporte le « mode transparent », l'authentification mutuelle peut avoir lieu entre la carte et l'UTL..
4	Les statuts des certificats (consultation des listes de révocation, vérification des dates de validité…) sont vérifiés (voir sur ce sujet l'Annexe – Vérification des statuts des certificats techniques sans-contact de l'ASIP Santé, la vérification des certificats technique sans-contact contenus dans les cartes CPx présentant des particularités du fait des mesures de confidentialité prises par l'ASIP Santé et présentées dans le paragraphe Protection des données personnelles plus haut).

Tableau 12 : Description du principe du contrôle d'accès sans-contact SSL avec la CPS

Sécurité des liens avec les ouvertures

Au sujet des ouvertures, il faut rappeler qu'il n'y a pas de sécurité d'accès si le lien « porte-UTL » n'est pas « durci » (câbles inaccessibles, secret des échanges de commandes et de leur mise en œuvre, protections électriques des relais….)

Sécurité du lien carte CPx-lecteur sans-contact

Ce scénario s'inscrit complètement dans l'esprit de la norme IAS-ECC qui a prévu des usages sans-contact dans ses spécifications.

Ce scénario repose sur la capacité de distribuer des secrets entre les différents acteurs du système, capacité que l'on rencontre habituellement en contrôle d'accès dans des scénarios basés sur de la cryptographie symétrique.

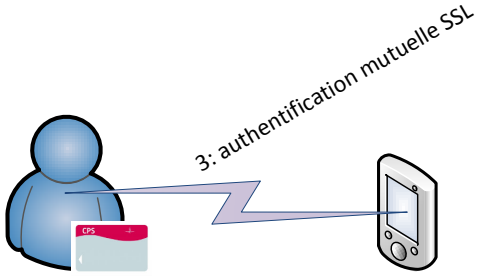
Qualité des composants CPx

Le composant électronique CPx est qualifié EAL4+, ce qui garantit la qualité du stockage des secrets contenus dans la carte.

Les autres composants du système d'accès (lecteur, UTL, serveur) devraient en cible être eux-aussi qualifiés, tant il est important d'assurer que les secrets, qu'ils soient symétriques ou asymétriques, soient bien gardés.

CPx sans-contact : clé RSA de 2048b

Le volet sans-contact de la CPx intègre un bi-clé d'authentification « technique » RSA de 2048b conforme au RGS



Le lien carte-lecteur sans-contact est assuré par une authentification mutuelle: le lecteur – ou l'UTL, si le lecteur supporte le mode transparent – communique avec la carte au moyen de commandes APDUs normalisées par la norme IAS-ECC et utilise pleinement les fonctions PKI de la carte CPS3

Figure 7 : Carte CPx sans-contact : dans l'esprit de l'IAS-ECC

A titre indicatif, ce scénario est le scénario retenu par le gouvernement américain pour l'identification des fonctionnaires et des prestataires fédéraux (projet PIV).

Exemple d'implémentation de contrôle d'accès basé sur PKIX

PIV est un exemple opérationnel de contrôle d'accès physique basé sur SSL.

La carte PIV contient une clé CAK pour Card authentication Key définie par la NIST et généralement implémentée sous forme d'un bi-clé RSA 1024 ou 2048 bits avec un certificat associé.

Parallèlement, une liste de lecteurs homologués, exploitant la CAK, est disponible : http://www.idmanagement.gov/approved-products-list.

De tels lecteurs, hors capacités biométriques, coûtent plus chers qu'un lecteur RFID classique du fait qu'ils embarquent un microcontrôleur puissant et du code et un jeu d'instructions spécifiques à la carte PIV.

Lecteur sans-contact compatible IAS-ECC ou CPx

A cette date, il n'existe pas encore de lecteur sans-contact compatible IAS-ECC (utilisation générique de IAS-ECC via la mise en œuvre de l'interopérabilité offerte par PKCS#15) ou CPx (utilisation directe et spécifique des containeurs de clés sans-contact CPx)

Les pistes possibles pour palier à cette situation sont :

- Spécification d'un lecteur sans-contact « Santé&Social » CPx
  1. Choix de fournisseurs et mises en fabrication
  2. Ou mise en place d'un processus d'homologation

Lecteur sans-contact compatible IAS-ECC ou CPx

De tels lecteurs pourraient fonctionner avec des cartes IAS-ECC sans-contact autres que la CPx :

- s'ils sont « génériques IAS-ECC »
- pour peu que ces cartes reprennent la structure de la CPx en sans-contact (peu de containeurs à implémenter).

- Spécification d'un bi-clé d'authentification sans-contact
  1. Propre au Ministère de la Santé (fait via la CPx)
  2. Inter-ministériel / français
  3. Européen

Norme commune pour un bi-clé d'authentification sans-contact

Chaque état de l'UE, voire chaque ministère de chaque état de l'UE, a créé ses propres cartes IAS-ECC. La disparité des implémentations qui en résulte n'est pas un problème, cette disparité venant de différences de besoins et d'usages.

Les besoins et usages en contrôle d'accès physique sont par contre communs à beaucoup d'institutions. Il serait sans doute nécessaire de « fermer » un peu mieux sa partie sans-contact, en spécifiant non pas une personnalisation de carte IAS-ECC complète pour toute l'Europe ou tous les ministères mais plutôt une ou des clés sans-contact communes et implémentables ensuite dans chaque personnalisation IAS-ECC.

Cela créerait les conditions d'un marché qui justifieraient les investissements financiers nécessaires au développement du scénario « sans-contact SSL ».

8.2.3.1 Diagrammes de séquence associés au contrôle d'accès physique basé sur SSL

Ce scénario peut être adapté avec notamment des déports des phases 6, 7, 8 et 9 :

- Soit dans les UTL
- Soit dans les lecteurs
- Soit dans les UTL et les lecteurs qui se répartissent alors la complexité de 6, 7, 8 et 9

via une distribution préalable des éléments d'approbation depuis le serveur vers les UTL et/ou les lecteurs, qui sont plus proches géographiquement du porteur de carte.

Ce scénario peut aussi être adapté en écartant l'idée d'une authentification des UTL ou des lecteurs auprès de la carte pour ne conserver qu'une authentification de la carte.

8.2.3.2 Cas du « lecteur générique IAS-ECC et autonome »

En conjonction avec l'idée de repousser au plus près du porteur la complexité des vérifications pour éviter des latences gênantes pour l'ergonomie, et de choisir un lecteur sans contact générique IAS-ECC « sur étagère », on obtient un scénario dit de « **lecteur IAS-ECC autonome** » et la séquence d'échanges décrite en « Annexe – Diagramme de séquence associé au cas du « lecteur générique IAS-ECC et autonome ».

Les remarques particulières liées à ce scénario sont :

#	Remarque
[A1]	De façon générique, seule la liste des autorités de certification de confiance est distribuée sur les lecteurs depuis un serveur de gestion centralisé. Mais, en pratique : • il faudrait aussi distribuer des CRLs • il vaudrait mieux constituer des listes blanches de certificats (pour ne pas accepter systématiquement les cartes de l'ES voisin par exemple)
[A2]	Les lecteurs doivent alors avoir les capacités mémoires (ROM et RAM) nécessaires afin d'exploiter les listes reçues.
[a1]	La ligne de vie de la carte CPx est plus longue que précédemment du fait que le lecteur demande à la carte de s'authentifier (échanges d'APDU supplémentaires après la récupération de l'UID).
[B]	La phase de récupération de l'UID est une brique de base, commune à tous les scénarios envisageables.
[C]	La phase générique d'authentification de la carte CPx impose la lecture et l'interprétation des structures PKCS#15 contenues dans la carte CPx. Ces structures assurent l'interopérabilité de la carte CPx et permettent ici de retrouver l'identifiant de clé sans-contact afin de lui demander d'effectuer l'opération d'authentification.
[D]	La phase de vérification est plus simple que la précédente mais reste coûteuse en temps.
[a3]	L'UTL ne porte aucune complexité dans ce scénario.

Tableau 13 : remarques liées au diagramme de séquence associé au cas du « lecteur générique IAS-ECC et autonome »

8.2.3.3 Cas du « lecteur transparent et UTL générique IAS-ECC autonome »

Un « lecteur transparent » est un lecteur qui fait « passe-plat » entre la carte et l'UTL.

Sa seule fonction est de transformer des ondes en commandes filaires et vice versa.

Appliqué dans le cas d'usage précédent, cela transforme le scénario « lecteur générique IAS-ECC et autonome » en scénario « UTL générique IAS-ECC et autonome ».

La différence entre lecteur autonome **[A]** et lecteur en mode transparent **[B]** est la suivante :

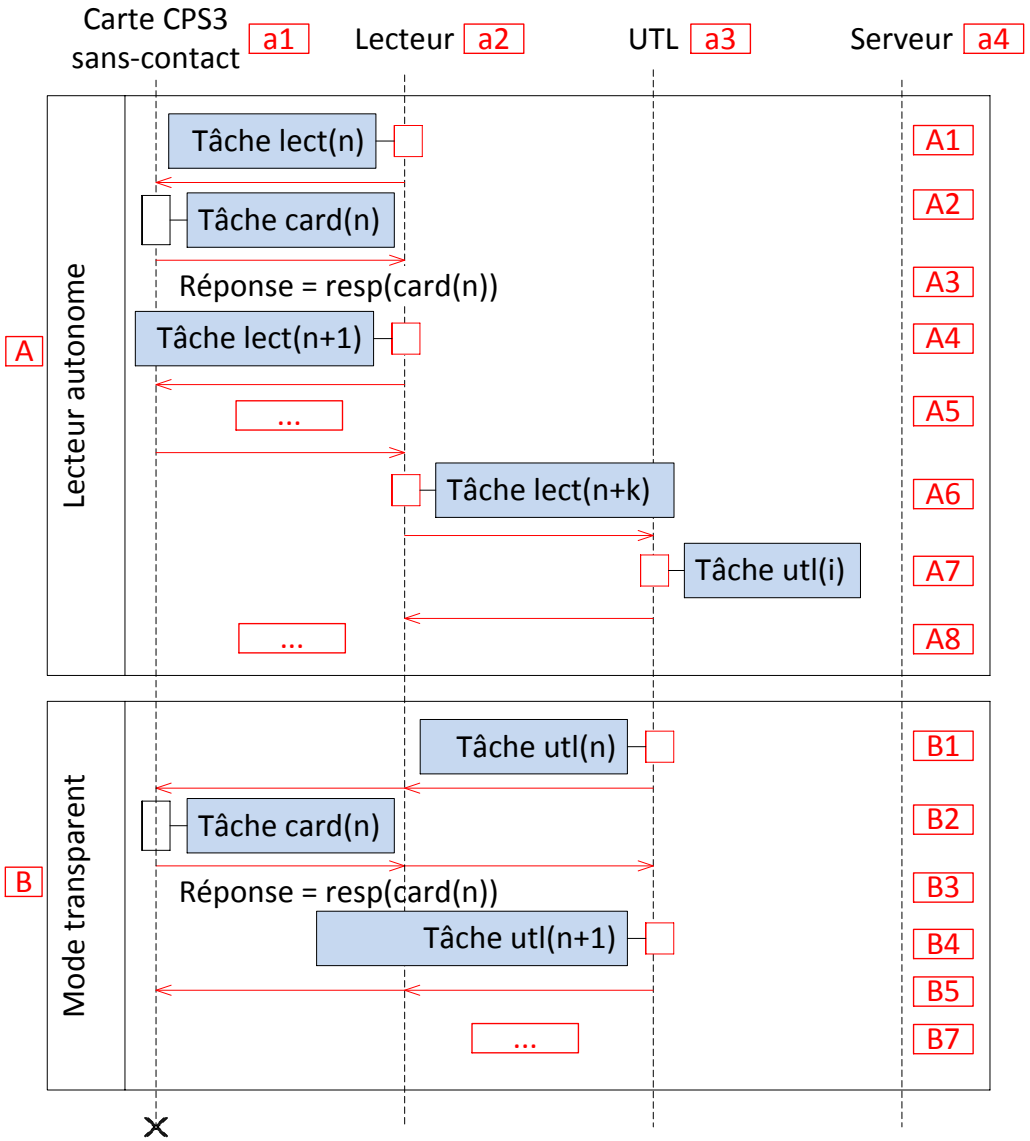


Figure 8 : Différence entre lecteur autonome et lecteur en mode transparent

Un lecteur autonome dialogue seul avec la carte via des commandes de bas niveau. Il « remonte » des informations consolidées quand cela lui est nécessaire à l'UTL [A6] qui lui répond après analyse [A7] par une commande de haut niveau. Le lecteur transforme cette commande de haut niveau en commandes unitaires de bas niveau et le dialogue entre lecteur et carte reprend jusqu'à la consolidation suivante. La logique est portée conjointement par le lecteur et par l'UTL.

En mode transparent, le lecteur transforme des ondes en commandes filaires unitaires en direction de l'UTL et vice versa, sans procéder à aucune interprétation. La logique est complètement portée par l'UTL.

Les remarques particulières liées à ce scénario sont :

Avantage 1	Pas de changement des lecteurs si ces derniers supportent le mode transparent. D'où l'importance de retenir ce type de lecteur lors de tout nouveau projet.
Avantage 2	Capacités des UTL plus en adéquation avec la cryptographie et la complexité mise en œuvre.

Tableau 14 : remarques liées à l'utilisation de lecteur en mode transparent

8.2.3.4 Cas du « lecteur transparent et UTL intelligent »

Le scénario « lecteur transparent et UTL intelligent » mixe :

- L'utilisation d'un lecteur en mode transparent
- La suppression de la complexité d'interprétation du PKCS#15 et de récupération du certificat
  - utilisation « en dur » de l'identifiant de la clé privée sans-contact de la carte CPx et distribution des certificats admis par le système sous forme de liste blanche.

Ce scénario nécessite un enrôlement {UID, certificat} préalable et une distribution des certificats sous forme de liste blanche depuis un serveur centralisé vers les UTL.

Il est illustré en « Annexe – Diagramme de séquence associé au cas du « lecteur transparent et UTL intelligent » ».

Les remarques particulières liées à ce scénario sont :

#	Remarque
[A1]	La liste blanche (WL) à consolider nécessaire à ce scénario peut par exemple prendre la forme de quadruplets (UID, Type carte = "CPS3.1", Certificat d'authentification sans-contact de la carte CPx, autorisations). La mise en place d'un système d'enrôlement permet de construire quotidiennement une WL. Cette opération est l'occasion de vérifier le statut des certificats et d'en extraire les clés publiques. ⇨ L'inclusion du type de carte ("CPS3.1" seulement pour l'instant) permet d'anticiper les situations où plusieurs générations de carte CPx cohabitent, ce qui n'est pas exclu à moyen-long terme mais aussi de faire cohabiter le sans-contact CPx avec d'autres cartes sans-contact. ⇨ Compter 1600 octets par enregistrement (16 + 16 + 1024 + 512) ○ 300 cartes : 480 ko ○ 2000 cartes : 3 Mo ○ 20000 cartes : 30 Mo ○ 120000 cartes : 183 Mo ⇨ Pour les 2 derniers cas ○ La gestion d'un grand nombre de cartes est souvent liée à une dispersion sur plusieurs sites différents ▪ subdiviser la liste principale en listes nominales de cartes par site ▪ gérer les déplacements inter-site en « lazy-loading » ⇨ En lieu et place du certificat, seule la clé publique peut être distribuée (256 bytes au lieu de 1024) ce qui divise la taille des fichiers par 2.

#	Remarque
[a2]	Pas de changement des lecteurs si ces derniers supportent le mode transparent. ⇨ D'où l'importance de retenir ce type de lecteur lors de tout nouveau projet. Le nombre total de lecteurs à installer dépend de la configuration des sites, de la stratégie sans-contact retenue (en conjonction avec d'autres moyens d'accès -sas, portiques…) et des fonctionnalités retenues (l'anti-passback requiert des lecteurs en sortie par exemple). A titre indicatif, compter : • 8 lecteurs par zone d'accueil + 1 UTL • 4 lecteurs par couloir (2 portes, 2 accès de secours) + 1 UTL • 2 lecteurs par niveau de parking + 1 UTL • 1 lecteur par zone spéciale (locaux informatiques, UTL factorisé avec celui de l'étage) • Y ajouter les lecteurs pour les postes de travail et les imprimantes si ces scénarios sont retenus
[a3]	Capacités des UTL plus en adéquation avec la cryptographie et les vérifications induites.
[C][D]	Bonne réactivité du système • **4 APDUs** IAS-ECC pour **300 bytes** transmis seulement et **50 ms** d'exécution, voir « Annexe – IAS-ECC avec la CPx en sans-contact » ○ attention à la compatibilité de ce volume de données avec Wiegand (mots de 64bits) • Pas d'APDU de lecture des structures PKCS#15 • Pas de temps d'analyse des structures PKCS#15 • Pas d'APDU de lecture du certificat
Point d'attention	UTL avec des capacités spécifiques liées à la carte CPx. ⇨ D'où l'importance de retenir des UTL susceptibles d'être facilement mis à jour.

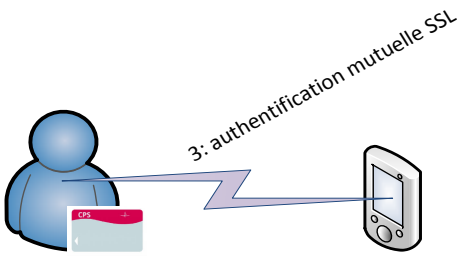
Tableau 15 : remarques liées à l'utilisation en « lecteur transparent et UTL intelligent »

Préconisation court-terme	Ce mode « lecteur transparent et UTL intelligent » est le mode à privilégier à court terme.

Tableau 16 : Préconisation mode « lecteur transparent et UTL intelligent »

8.2.3.5 Problèmes liés au contrôle d'accès physique basé sur SSL

Pour résumer ce qui vient d'être présenté, les problèmes liés au contrôle d'accès physique basé sur SSL sont inhérents aux principes de la PKI et en particulier de PKIX avec ses opérations asymétriques et ses chaînes de confiance.



P0: solution lourde nécessitant la mise en œuvre d'une PKI complète

P1: lenteur de l'authentification mutuelle SSL

P2: microcontrôleurs des lecteurs ou des UTL puissants embarquant des capacités cryptographiques asymétriques

P3: microcontrôleurs des lecteurs ou des UTL embarquant du code spécifique CPx

P4: Pour réduire les coûts et la complexité des lecteurs, il est possible de déporter les fonctions cryptographiques et le code spécifique CPx dans les UTL ou même dans le serveur en utilisant les lecteurs en « mode transparents ». Ce scénario se heurte alors à des problèmes de latences incompatibles avec les exigences du contrôle d'accès physique.

Figure 9 : Problèmes liés à l'accès physique basé sur SSL

Les principaux obstacles à ce scénario sont :

- La complexité de mise en œuvre
- Les latences
- Les lecteurs et les UTL (disponibilité, coûts, diversité des fournisseurs)

Aujourd'hui, ces problèmes sont résolus au cas par cas. Ce scénario coûte donc cher mais rien à ce jour ne permet de l'exclure d'une feuille de route visant à élever les niveaux de protection offerts par les systèmes de contrôle d'accès en appliquant les principes de la cryptographie asymétrique à ce domaine.

Marché des UTLs	Le scénario « lecteur transparent et UTL intelligent » est envisageable à court terme – et performant – si les conditions d'un marché pour des UTL supportant la CPx sont créées.

Tableau 17 : CPx Sans contact : accès physique basé sur SSL à court terme

8.3 Le contrôle d'accès logique

8.3.1 Accès aux services internes

Il est possible de généraliser l'utilisation sans-contact à des usages tels que :

- le compte de restauration ;
- le pointage horaire (voir remarques de **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** sur ce sujet);
- les photocopieuses (authentification du porteur en sans-contact plutôt que par code aux travaux d'impression en cours) ;
- …

Les technologies employées (UID simple, authentification simple du support CPx, SSL…) sont à évaluer en fonction du besoin et au regard de la sécurité requise (l'accès à une file d'attente d'impression ou à la réserve d'argent de la cantine peuvent ne pas être anodin !).

8.3.2 Smartcard logon

Les capacités sans-contact d'une carte à puce permettent d'éviter les inconvénients liés aux ouvertures de sessions par identifiant et mot de passe. Ces deux informations sont amenées à être oubliées par les utilisateurs, générant un support régulier et utilisant toujours un minimum de ressources de la Direction des Services Informatiques (DSI).

La carte CPx est une carte fournie par une autorité gouvernementale (précisément par l'ASIP Santé). Elle peut donc servir comme vecteur d'authentification auprès d'un service tel que :

- la gestion de la paye : accès réservés aux ressources humaines ;
- le suivi de la disponibilité des lits : accès réservés à tout le personnel soignant ou administratif de l'établissement ;
- l'accès aux consoles de monitoring.

Cryptolib CPS v5.0.24	Le volet sans-contact de la carte CPx est compatible avec les mécanismes de Smartcard logon Windows Server 2008 ou supérieur. Leur intégration dans ce type d'architecture fait l'objet d'un guide dédié.

Tableau 18 : CPx Sans contact, Cryptolib CPS v5 et Smartcard logon

IGC-Santé : mise en œuvre du Smartcard logon Windows	Le format des DN des certificats change avec la mise en production de la nouvelle "IGC-Santé". Le principe de « mapping » décrit dans le guide de Smartcard logon et applicable au Smartcard logon sans-contact reste cependant valable avec l'IGC-Santé.

Tableau 19 : IGC-Santé : mise en œuvre du Smartcard logon Windows

Idéalement, cette solution remplace la saisie d'un identifiant et d'un mot de passe par un simple geste.

L'ergonomie proposée par le Winlogon présent par défaut dans Microsoft Windows nous éloigne un peu de ce scénario : il est en effet indispensable de saisir un « hint » dont Windows se sert pour rattacher le certificat présent au compte utilisateur :

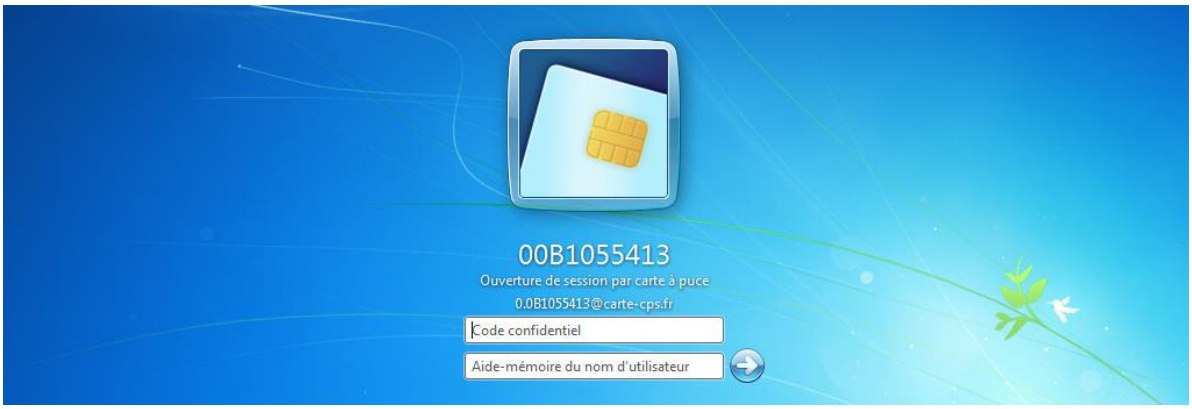


Figure 10 : Smartcard logon sans-contact : Ecran de Smartcard logon après lecture du certificat sans-contact

En sans-contact, l'utilisateur laisse la section « Code confidentiel » vide et tape son compte dans le champ « hint » :

Figure 11 : Smartcard logon sans-contact : Saisie du « hint »

La session s'ouvre :

Figure 12 : Smartcard logon sans-contact : Ouverture de session Windows

Ces aspects ergonomiques doivent être anticipés et faire l'objet de solutions spécifiques si besoin.

Ergonomie du Smartcard logon sans-contact	Si ce fonctionnement est un peu pénalisant, il apporte tout de même un peu de « ce que je sais » dans le processus. Une évolution raisonnable pourrait donc simplement consister à paramétrer le « hint » pour qu'il puisse être saisi masqué… Les bénéfices du port de la carte restent par ailleurs présents (limitation des transmissions, pas de gestion de mot de passe à prévoir).

Tableau 20 : Remarques ergonomie du Winlogon sans-contact

Il est nécessaire de s'occuper des statuts des certificats (voir sur ce sujet l'Annexe – Vérification des statuts des certificats techniques sans-contact de l'ASIP Santé).

8.3.3 TSE et Citrix

Cryptolib CPS v5.0.24	Le volet sans-contact de la carte CPx est compatible avec les architectures client légers implémentés via TSE / Citrix.

Tableau 21 : CPx Sans contact, Cryptolib CPS v5, Smartcard logon en TSE

8.3.4 Client léger du type « navigateur web »

Techniquement, la carte CPx peut servir comme vecteur d'authentification auprès de services Web, l'accès au service Web étant alors réservé aux porteurs munis d'une CPx.

Cryptolib CPS v5.0.13+	A partir de la Cryptolib CPS v5.0.13, la Cryptolib CPS **permet** de faire de l'authentification web avec le certificat sans-contact de la carte CPx (voir http://testssl.asipsante.fr/)

Tableau 22 : CPx Sans-contact, Cryptolib CPS v5 et authentification web avec le certificat sans-contact de la carte CPx

Il est là aussi nécessaire de s'occuper des statuts des certificats (voir sur ce sujet l'Annexe – Vérification des statuts des certificats techniques sans-contact de l'ASIP Santé).

8.3.5 Authentification du support versus authentification de l'utilisateur

A ce stade, il est important de se remémorer les explications présentées dans le paragraphe « Sans-contact et authentification simple du support » :

Le volet sans-contact de la carte CPx:

- **permet** d'effectuer une « **authentification simple** » du **support** (la carte)
- **ne permet pas** d'effectuer une **authentification du porteur**, qu'elle soit simple ou forte
    - ceci provient du fait que le volet sans-contact de la CPx **ne contient ou n'expose aucune information** « reliable » à une personne physique

Dans les cas d'utilisation de la CPx en accès logique via les scénarios présentés plus haut, l'analyse du besoin est essentielle : ce mode d'accès logique par **authentification simple du support** (qu'il se fasse par UID ou par authentification de la carte) ne devrait pas donner accès aux mêmes niveaux d'information qu'en cas **d'authentification simple ou forte de l'utilisateur**.

Un exemple :

- il est envisageable que l'utilisation du sans-contact sur la base de l'UID permette d'accéder à certaines fonctions non critiques d'un LPS, fonctions qu'il convient d'identifier correctement (accès à l'aide, accès aux conseils d'utilisation, à l'agenda public de l'établissement…)
- il n'est pas envisageable que cette utilisation du sans-contact sur la base de l'UID permette d'accéder à des données médicales

Ces considérations peuvent toutefois être revues lors d'analyses de risque si le traitement sans-contact et le SI dans sa globalité sont revus (voir ci-après).

8.4 Contrôle d'accès avec l'utilisation de la zone de données dédiée contenue dans la carte CPx

La carte CPx contient une zone de données libre et exploitable par n'importe quelle application.

Cette zone de données et son utilisation en accès sans-contact sont évoquées en **[Présentation de la carte CPS3]**.

Le principe est le suivant :

1. Après une authentification forte en mode contact et - donc - sous protection du code porteur (**authentification primaire**), une application écrit des informations dans la zone de données libre.
2. Une autre application contenue dans les lecteurs sans-contact ou dans les appareils auxquels les lecteurs sont connectés (UTL ou PC selon les modes d'accès) lisent ces informations au moment où le porteur passe sa carte devant le lecteur en mode sans-contact. Ces informations sont utilisées pour authentifier et autoriser le porteur (**authentification secondaire**)

Ce principe se schématise de la façon suivante :

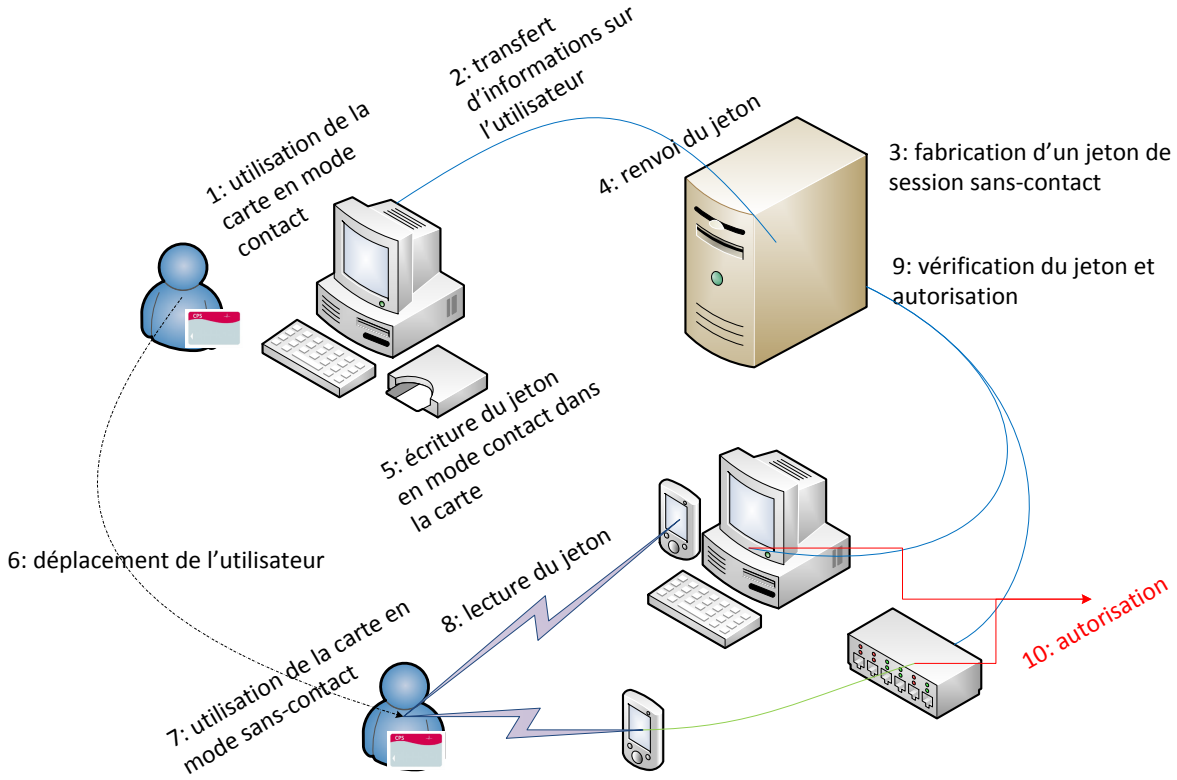
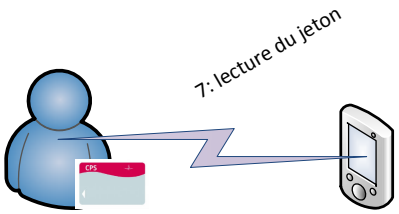


Figure 13 : CPx : Contrôle d'accès avec utilisation de la zone de données carte

Les remarques que l'on peut faire à propos de ce scénario sont les suivantes:



P1: **rejeu du jeton**: le jeton peut être lu par un attaquant à l'approche d'une carte cible, écrit dans une carte blanche et rejoué

P2: microcontrôleurs embarquant du code spécifique CPx

P3: **interopérabilité** du jeton

Figure 14 : Remarques Contrôle d'accès avec utilisation de la zone de données carte

Contrôle d'accès avec utilisation de la zone de données carte : rejeu du jeton

Une application souhaitant exploiter la zone de données carte CPx pour l'authentification doit se pencher sérieusement :

- sur la composition du jeton stocké dans la carte
- ainsi que sur le traitement du jeton
- (la concomitance des 2 conditions étant importante)

faute de quoi :

1. la sécurité ne sera pas meilleure
2. et ce pour des performances moins bonnes
3. et pour un coût (code spécifique dans les lecteurs de cartes sans-contact dédié à l'exploitation de ce jeton via des APDUs IAS-ECC) nettement plus élevé

qu'avec le scénario « authentification par UID » du fait de possibilités de rejeu du jeton

Tableau 23 : Contrôle d'accès avec utilisation de la zone de données carte : la question du rejeu

Interopérabilité du jeton

Ce scénario présente d'emblée un problème d'interopérabilité : deux applications différentes présentes dans le SI ou sur le poste de travail (par exemple celle liée à l'accès physique et une autre liée à l'accès logique) et basées toutes deux sur cette architecture en jeton vont exploiter le jeton de manières différentes ce qui risque de les faire dysfonctionner l'une et l'autre, l'une (re-) écrivant un jeton que l'autre ne comprend pas.

Figure 15 : Contrôle d'accès avec utilisation de la zone de données carte : Problème d'interopérabilité du jeton

Mise en œuvre

La mise en œuvre de ce scénario implique d'embarquer des capacités spécifiques à la CPx, ces capacités recouvrant celles qui permettent de demander une authentification de la carte CPx.

La mise en œuvre de ce scénario implique de faire jouer aux différents acteurs du système les mêmes rôles que ceux décrits dans le scénario « lecteur transparent et UTL intelligent » (lecteur en mode transparent, UTL capable de gérer des APDUs IAS-ECC spécifiques à la CPx).

Il est donc conseillé d'évaluer les scénarios d'authentification simple du support avant d'intégrer la zone de données partagées.

Figure 16 : Contrôle d'accès avec utilisation de la zone de données carte : Mise en œuvre

8.5 Un exemple d'intégration complet dans un SI

3 principes de contrôle d'accès ont été présentés :

1. Type A / UID Mifare: le plus simple et le plus répandu mais aussi le moins sûr
2. SSL : le plus complexe à mettre en œuvre mais le plus sûr
3. La zone de données CPx : quasiment aussi complexe à mettre en œuvre que l'accès SSL, ce scénario nécessite de bien concevoir et de bien traiter le « jeton » mais présente potentiellement un avantage en terme de performances sur le scénario SSL

Les accès applicatifs passent quant à eux essentiellement par

4. Le Smartcard logon
5. Les clients légers : TSE/Citrix/Web Browser

Cette section propose de revisiter ces 5 modes :

- en présentant un cas d'usage envisageable à court-moyen terme
- où le porteur est un médecin
  - porteur d'une carte CPx
- se déplaçant tout au long de sa journée dans son établissement de santé
  - consultations, urgences, cantine, blocs, …
- dont le SI est équipé en machines et serveurs Microsoft Windows.

8.5.1 Exemple d'intégration complet : l'accès physique

Pour l'accès physique, il est difficile de faire autre chose que de l' « UID Mifare »:

- Si l'établissement est déjà câblé et équipé de lecteurs
  - Les lecteurs sont impossibles à changer en faveur de lecteurs faisant de l'IAS-ECC CPx sauf à tout changer de bout en bout (lecteurs, câbles, UTL, serveurs et solution d'identification)
  - Ces lecteurs sont sans doute, par contre, compatibles ISO 14443 ou Mifare et donc CPx dans son mode « UID Mifare »
  - Il est utile de vérifier si les lecteurs sans-contact en parc supportent ou non le « mode transparent » auquel cas seuls les UTL et le serveur peuvent être mis à jour pour passer au sans-contact IAS-ECC
- Si l'établissement n'est pas déjà câblé
  - il ne trouvera pas, sur étagère et à court terme, de fournisseur de lecteurs ou d'UTL et de solutions compatibles IAS-ECC CPx. Il faudra donc qu'il supervise un projet d'intégration complet (BTP, accès physiques, développements logiciels…).
  - Il en trouvera par contre énormément qui sont compatibles ISO 14443 ou Mifare
  - Et il pourra néanmoins imposer un certain nombre de recommandations comme celles d'éviter les liens physiques propriétaires au profit du RJ45, d'éviter les solutions d'enrôlement complètement « fermées », de se pencher sur la traçabilité… (voir Points d'attention sur les projets sans-contact)
  - En visant notamment le scénario « lecteur transparent et UTL intelligent » présenté plus haut et illustré en annexe.

On impose néanmoins à ce cas d'usage :

1. une concession d'autorisations suivant les bonnes pratiques, en particulier en ne donnant que les droits minimaux requis à une personne donnée et en évitant les cartes aux pouvoirs étendus
2. la mise en place d'un système de gestion étroit du parc de carte CPx utilisées
3. de la surveillance (vigile)
4. un monitoring étroit (surveillance des accès parking, attribution de places de parking nominatives, sensibilisations/formations des utilisateurs, définitions de procédures…)
5. l'application des recommandations de **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** pour le niveau 1 avec une analyse d'écarts formalisée, motivée et « mitigée »
6. la mise en place d'une stratégie à moyen et long terme, au niveau de l'établissement de santé, pour basculer vers un mode d'accès plus sécurisé (remplacement des lecteurs par des lecteurs supportant le mode transparent, choix des câblages lors des rénovations…)

On s'assure aussi que les communications entre équipements qui ne sont pas liés directement à l'interaction avec le porteur, et donc qui ne sont pas dimensionnant dans la latence d'accès, sont sûres (exemple avec le lien UTL – porte, modulo la remarque émise plus haut).

Ces équipements doivent par ailleurs pouvoir être mis à jour facilement (mise à jour de firmwares pour améliorer les fonctionnalités dans le temps).

On obtient le schéma suivant :

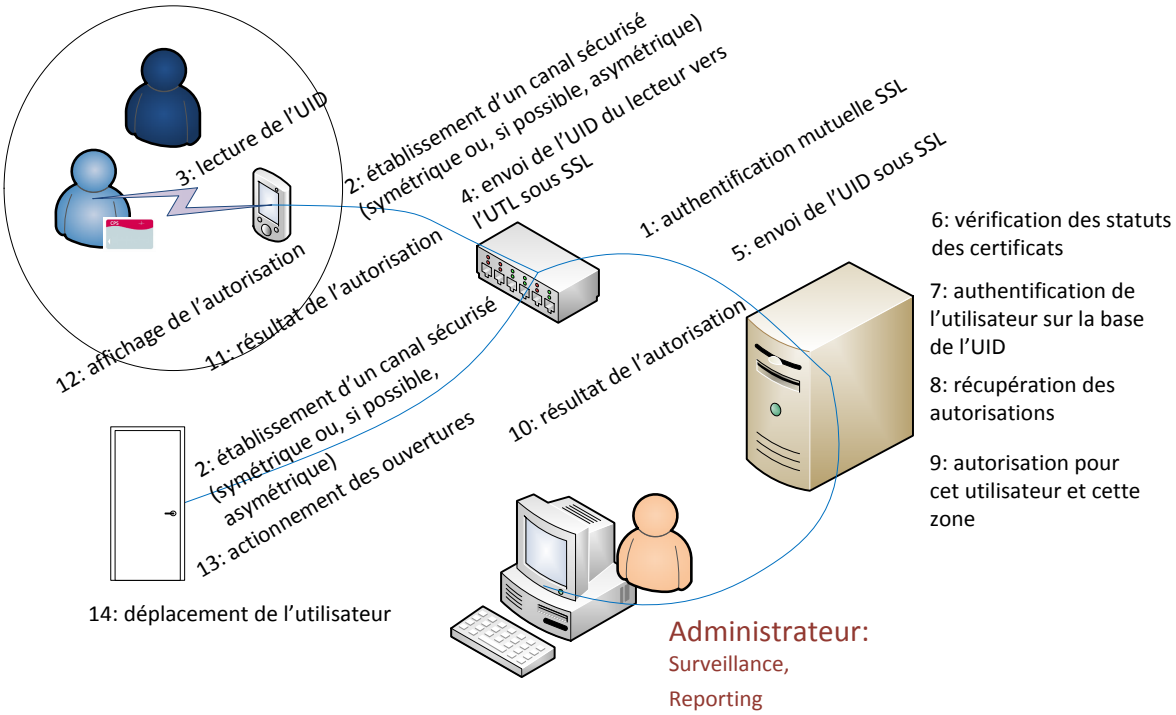
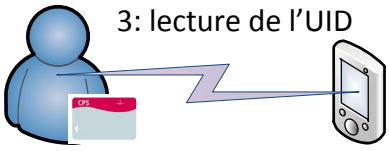


Figure 17 : Exemple d'intégration complète : accès physique : le principe

Les remarques et problématiques sur cette partie sont donc :



Pas de microcontrôleur embarquant du code spécifique CPx, pas de cryptographie

P1: clonage de carte et rejeu

P2: logique incompatible avec le type B / PUPI

Mise en place de reportings dédiés (administrateur, exploitation fine de l'accounting)

Présence humaine (vigiles) dans les zones d'accès

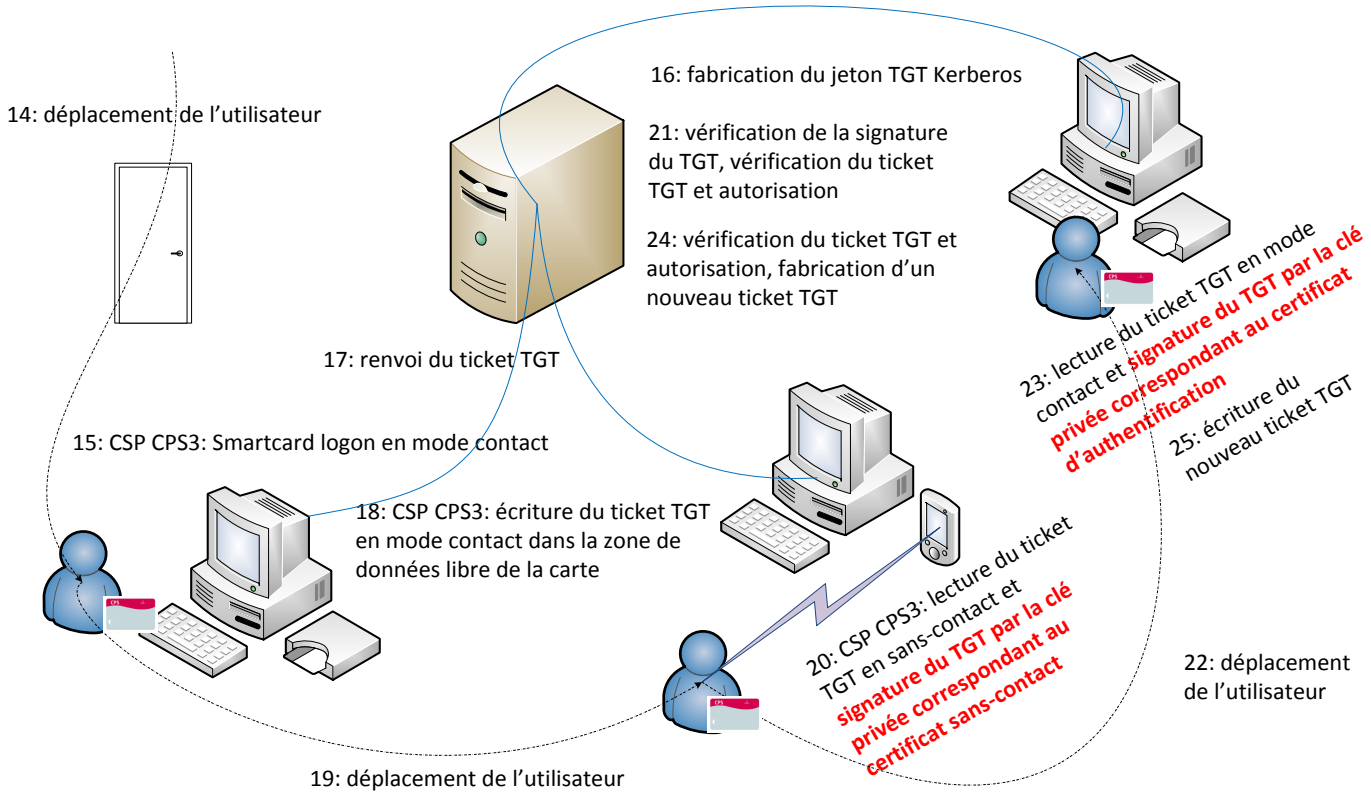
Formation / sensibilisation des personnels à la sécurité et aux procédures

Nécessité de mettre en place une stratégie de migration vers un système plus sûr

Figure 18 : Exemple d'intégration complète : accès physique : les remarques

8.5.2 Exemple d'intégration complet : l'accès logique

En accès logique avec authentifications primaire et secondaire, le porteur de carte doit obtenir préalablement un jeton en mode contact pour l'utiliser par la suite en mode sans-contact. Le système est conçu de sorte à ce que les phases « contact » coïncident avec son activité (logon Windows et lecture de mails ou écriture de comptes rendus par exemple, qui sont des phases où la carte peut rester longtemps dans le lecteur de carte tout en restant dans le périmètre d'attention du porteur). Une fois le jeton écrit dans la carte, le porteur peut ouvrir une session applicative en sans-contact sur le poste de la salle de consultation par exemple ou ouvrir la porte d'un bloc opératoire. Ce scénario se schématise ainsi :

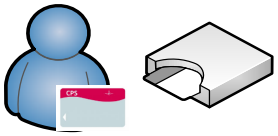


Les principales remarques :

1. **Cas d'usage**
   Idéalement, le porteur n'a pas à se préoccuper de l'existence d'un jeton dans sa carte.
   Si son jeton est invalide :
   - il est remplacé de façon transparente pour l'utilisateur en mode « contact »
   - des lecteurs en mode contact peuvent être mis à disposition (badgeuses « dual » contact / sans-contact, postes avec lecteur contact dédié)
2. **SSO**

Ce scénario réinvestit l'architecture SSO mise en place par Microsoft pour gérer les accès aux services déployés dans un domaine Active Directory. Cette architecture permet à l'utilisateur de ne renseigner son mot de passe qu'une seule fois pour accéder aux services offerts par le SI auxquels il a droit (et non à chaque fois qu'il accède à un des services offerts par le SI).

3. **En Smartcard logon en contact, l'authentification est forte**



Dans cette phase, l'authentification de l'utilisateur est forte

15: CSP CPS3: Smartcard logon en mode contact

4. **Emission du jeton**

Lorsque que le serveur de jetons émet le jeton, il sait pour quelle carte il a émis le jeton et stocke cette correspondance en plus de remplir le jeton avec les droits utilisateurs et la durée de validité.

5. **Les fonctionnalités du CSP CPx doivent être enrichies**

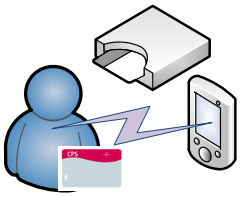
Le CSP CPx écrit le jeton dans la zone de données libre en mode contact sous présentation du code porteur. Idéalement, le jeton est stocké dans la carte tel qu'il a été reçu par le poste client.

En lecture, le CSP CPx lit le jeton puis **demande à la carte de signer le jeton lu :**

- **avec la clé privée correspondant au certificat sans-contact** en mode sans-contact
  - les opérations de lecture de la zone et de signature sont libres en sans-contact
- **avec la clé privée correspondant au certificat d'authentification** en mode contact, sous présentation du code porteur

C'est ce jeton sur-signé qui est renvoyé au serveur de ticket de session.

Ces opérations de lecture / écriture dans la zone de données libre de la carte CPx sont faites de manière transparente pour l'utilisateur et pour le reste du système.



Fonctions assurées par le CSP CPS3

15: CSP CPS3: Smartcard logon en mode contact
18: CSP CPS3: écriture du ticket TGT en mode contact dans la zone de données libre de la carte
20: CSP CPS3: lecture du ticket TGT en sans-contact et signature en mode sans-contact du TGT par la clé privée correspondant au certificat sans-contact
23: CSP CPS3: lecture du ticket TGT en mode contact et signature en mode contact du TGT par la clé privée correspondant au certificat d'authentification

6. La composition du jeton

Ce jeton est idéalement un ticket Kerberos TGT compatible avec les architectures Microsoft ou Linux.

```
[APPLICATION 22] {
  SEQUENCE {
    [0] {
      INTEGER 5
      }
    [1] {
      INTEGER 22
      }
    [2] {
      SEQUENCE {
        [APPLICATION 1] {
          SEQUENCE {
            [0] {
              INTEGER 5
              }
            [1] {
              GeneralString 'ABCDEF.FR'
              }
            [2] {
              SEQUENCE {
                [0] {
                  INTEGER 2
                  }
                [1] {
                  SEQUENCE {
                    GeneralString 'krbtgt'
                    GeneralString 'ABCDEF.FR'
                    }
                  }
                }
              }
            [3] {
              SEQUENCE {
                [0] {
                  INTEGER 18
                  }
                [1] {
                  INTEGER 3
                  }
                [2] {
                  OCTET STRING
                    87 DA 9C FA 52 7D 9C C8 75 55 F6 8A 21 A6 3D D5
```

Figure 19 : Début d'un ticket TGT

La taille du container de données CPx est de 4096 bytes. La taille maximum des tickets TGT est configurable sous Windows (8K par défaut, voir MaxTokenSize) et dépend directement du nombre de groupes auxquels appartient l'utilisateur (40 bytes par groupe, le TGT de l'auteur de ce document fait 1338 bytes).

Si le contrôleur de domaines est en 2012, le blindage Kerberos et les « claims » peuvent être utilisés, auquel cas on peut penser à intégrer la solution avec AD FS (Federation Service, le SSO Microsoft) ou avec la gestion de droits dynamique.

Le poste client transmet le ticket TGT sur-signé par la carte CPS au serveur de ticket de session qui le traite : la régénération d'un ticket TGT est économisée, celui stocké dans la carte servant directement. Si ce scénario est impossible à implémenter, ces informations sorties de la carte peuvent alimenter une requête de pré-authentification Kerberos.

Si le ticket TGT Microsoft n'est pas directement exploitable, le jeton à gérer doit être un jeton dans ce format (RFC 1510) ou dans tout autre format qui puisse ramener ultérieurement à Kerberos. Ceci permet, au passage, **d'assurer l'interopérabilité applicative du jeton** (cf. problématique exposée plus haut).

7. Rejeu

Le rejeu du jeton stocké dans le conteneur CPS, quel que soit son format, reste un sujet de préoccupation puisqu'il peut être lu par un attaquant à l'approche d'une carte cible et écrit dans une carte blanche et rejoué.

Le rejeu du TGT est un point d'attention identifié de façon général en dehors des considérations sans-contact, notamment sous Windows.

Le **rejeu est évité** par la vérification par le serveur de la sur-signature du jeton.

8. Vérification des statuts des certificats

Les statuts des certificats (consultation des listes de révocation, vérification des dates de validité…) doivent être vérifiés (voir sur ce sujet l'Annexe – Vérification des statuts des certificats techniques sans-contact de l'ASIP Santé, la vérification des certificats techniques sans-contact contenus dans les cartes CPx présentant des particularités du fait des mesures de confidentialité prises par l'ASIP Santé et présentées dans le paragraphe Protection des données personnelles plus haut).

9. Performances et bonnes pratiques

Quel que soit le format du jeton écrit dans la carte retenu, il est préférable de le préfixer avec la longueur des données réellement utilisées afin de ne pas devoir lire systématiquement 4096 bytes de données depuis la carte (environ 20 APDUs et 4 secondes en contact, le débit étant plus important en sans-contact) dont beaucoup pourraient être non utilisés.

Le TGT étant écrit au format ASN.1, il remplit cette condition et permet d'optimiser sa lecture depuis la carte en lisant et en interprétant ses premiers octets qui contiennent la longueur totale du ticket (TLV).

La lecture des seules données utiles permet aussi de diminuer la fréquence des erreurs de lecture en sans-contact (plus il y a de données à lire plus la probabilité de rencontrer des erreurs de transmission augmente).

Les applications qui écrivent dans cette zone doivent « reformater » la zone régulièrement en

- Ecrivant 4096 « 00 »
- Réécrivant les nouvelles données ensuite

10. Références

Le point d'entrée dans la documentation Microsoft sur ces questions est l'« Authentication Reference » (voir en particulier l'énumération KERB_PROTOCOL_MESSAGE_TYPE dans la section « Authentication Enumerations »). Voir aussi le projet Windows Credentials Editor et le projet Mimikatz pour des exemples de code source (notons au passage que la CPx rentre complètement dans les préconisations qui découlent de tels projets).

11. Impacts

Ils sont à préciser en collaboration avec les spécialistes de l'identité chez Microsoft.

Ils concernent essentiellement :

- Le poste de travail :
  - CSP CPx
  - Ergonomie de l'ouverture de session / Credential Provider personnalisé « sans-contact »
- Le serveur de jetons (correspondance jeton / certificats du demandeur)

- Le serveur de jetons de session (vérification de la sur-signature en lien avec le serveur de jetons et autres vérifications induites par ce scénario)

8.6 Résumé des usages

Les scénarios d'intégration du mode sans-contact sont donc les suivants :

	Description du scénario
U_01	L'identification simple sans-contact par la lecture d'un numéro de série de composant répond au besoin des applications requérant un niveau de sécurité moins exigeant : • le contrôle d'accès aux locaux ou au parking • le contrôle d'accès aux imprimantes • le contrôle d'accès aux tenues de travail • le contrôle d'accès à la restauration d'entreprise
U_02	L'identification simple sans-contact par la lecture d'identifiant généré par le système et chiffré au niveau de la puce répond au besoin des applications requérant un niveau de sécurité exigeant. Cette lecture se fait en mode chiffré entre le lecteur et la CPx. Le lecteur doit présenter une clé symétrique pour établir le contact avec la carte et déchiffrer l'identifiant. La clé peut être fixe et commune à toutes les cartes ou bien diversifiée et propres à chaque carte.
U_03	L'identification : • simple sans-contact • combinée avec une authentification forte initiale en mode contact apporte la simplicité recherchée tout en garantissant un niveau de sécurité acceptable. La mise en œuvre de ce scénario passe par la composition et la bonne gestion d'un jeton d'authentification, gestion permise par la nouvelle API PKCS#11 de la Cryptolib CPS v5 et décrite en **[Manuel de programmation de la Cryptolib CPS v5]**.
U_04	L'identification : • simple sans-contact • SSL avec authentification mutuelle du support CPx via son certificat X.509v3 sans-contact et du lecteur sans-contact Répond aux exigences de sécurité les plus élevées. Voir **[Manuel de programmation de la Cryptolib CPS v5]**.
U_05	L'identification : • simple sans-contact • combinée avec une authentification forte initiale en mode contact • et aux services d'authentification disponibles dans l'infrastructure du SI apporte la simplicité recherchée tout en garantissant un niveau de sécurité élevé.

Tableau 24 : CPx Sans-contact : scénarios d'utilisation

8.7 Matrice d'intégration

Dans le cas particulier d'utilisation du sans-contact sur un poste de travail, la Cryptolib CPS permet de s'interfacer logiciellement avec la carte CPx à différents niveaux, sur différentes plates-formes et dans différents langages et en particulier avec son volet sans-contact.

#	Domaine	Section	Contact*	Sans-contact
01	**Système exploitation**	Windows	Y	Y (Cryptolib CPS v5)
02		Mac OS X	Y	Y (Cryptolib CPS v5)
03		Linux	Y	Y (Cryptolib CPS v5)
04		Autres dont OS embarqués ou propriétaires	N	N. Deux points importants à ce sujet : • la Cryptolib CPS v5 n'est pas conçue pour être embarquée • du code embarqué est nécessaire et fourni au cas par cas par les fabricants de lecteurs sans-contact afin de rendre le lecteur, si besoin, capable d'envoyer des APDUs IAS-ECC paramétrés pour communiquer avec la CPx • ces développements sont nécessaires sous couvert de la signature de la convention de concessions des spécifications de la carte CPx **[Procédure de concessions des spécifications de la carte CPS3]** (cf. annexe 15.1)
05	**Langage**	C/C++	Y	Y (Cryptolib CPS v5, compilateurs PC et Mac OS X ou Linux cibles x86)
06		Java	Y	Y (Cryptolib CPS v5, compilateurs PC, Mac OS X ou Linux cibles x86)
07		C#	Y	Y (Cryptolib CPS v5, compilateurs PC et Linux, cibles x86)
08	**Fonctionnalités**	Accès concurrents	Y	Y avec Cryptolib CPS v5 à vérifier au cas par cas avec les fabricants de lecteurs sans-contact
09		Evènements lecteurs	Y	Y avec Cryptolib CPS v5
10		Evènements cartes	Y	Y avec Cryptolib CPS v5
11		Optimisation saisie codes porteurs	Y	N/A

#	Domaine	Section	Contact*	Sans-contact
12		Boite de dialogue de saisie du code porteur	Y	N/A
13		SHA-1	Y	Y (nécessite un lecteur sans-contact capable d'envoyer des APDUs IAS-ECC paramétrés pour communiquer avec la CPx)
14		SHA-2 (RGS)	Y	Y (nécessite un lecteur sans-contact capable d'envoyer des APDUs IAS-ECC paramétrés pour communiquer avec la CPx)
15		Signature	Y	N (le certificat sans-contact est un certificat d'authentification : il permet de signer un challenge d'authentification)
16		Signature « IAS-ECC » (RGS)	Y	N
17		Authentification	Y	Y (simple du support)
18		Sans-contact « Accès certificat Tech. »	Y	Y
19		Sans-contact « Accès conteneur de données »	Y (en R/W)	Y (en Read-Only, nécessite un lecteur sans-contact capable d'envoyer des APDUs IAS-ECC paramétrés pour communiquer avec la CPx)
20		Accès aux objets métiers Santé&Social	Y	N
21		« Interopérabilité »	Y	Y
22		« Configurabilité »	Y	Y
23		Performance	Y	Y
24	Architecture	Client lourd	Y	Y
25		Client léger	Y	Y
26		Embarqué	Y	Y
27	Expertises	Expertise carte à puce	Y	N
28		Expertise Crypto	Y	N

#	Domaine	Section	Contact*	Sans-contact
29		Expertise PKI	Y	N
30		Expertise programmation	Y	Y
31	Usages	Accès locaux	N **	Y
32		Accès parking	N **	Y
33		Accès aux services internes (cantine, impression…)	N **	Y
34		Pointage	N **	Y
35		Smartcard logon	Y	Y (3)
36		Smartcard logon TSE	N	Y (3)
37		Authentification Web	Y	Y (simple du support)

Tableau 25 : Cryptolib CPS: Matrice d'intégration

* dépend du niveau d'intégration (PKCS#11, CSP…) et du langage / framework (Java, C#) utilisé, voir Manuel d'installation et d'utilisation de la Cryptolib CPS

** usages déconseillés en « contact » (usures, réactivité)

(3) Avec la Cryptolib CPS 5.0.24 ou supérieure

8.8 Téléchargements logiciels

Les composants logiciels permettant d'évaluer le sans-contact avec la CPx sous Microsoft Windows, Apple Mac OS X ou Linux sont téléchargeables depuis le site « intégrateurs » de l'ASIP Santé:

	Téléchargements logiciels	
1	Cryptolib CPS v5	Espace intégrateurs ASIP Santé

Tableau 26 : Installation: Sources des installeurs

9 Recommandations de mise en œuvre

9.1 Points d'attention sur les projets sans-contact

La carte CPx, par l'intermédiaire de son volet sans-contact, peut devenir un outil indispensable au personnel d'établissement. En la positionnant au cœur des usages, la mobilité du personnel au sein de l'établissement de santé sera améliorée.

La mise en place de systèmes utilisant le volet sans-contact passe par une étude systématique qui marque le début du projet, abouti à l'expression de besoin, aux spécifications fonctionnelles générales et, selon les cas, aux rédactions des différents documents composants les appels d'offre afférents.

A minima, 11 points d'attention sont à adresser lors de la mise en place d'un projet sans-contact :

	Description des points d'attention sur les projets sans-contact
PA_01	Définition du besoin : 1. Niveau(x) de sécurité requis 2. Zonage 3. Identifiant sans-contact vs. intégration au niveau applicatif
PA_02	Matériels : 1. Conformité aux standards 2. Lecteurs déjà déployés : a. Vérification des capacités i. Notamment les capacités ISO 14443 ou Mifare et le support du « mode transparent » b. Vérification des capacités au regard des besoins 3. Lecteur à déployer : a. Choix des modes de câblage i. Privilégier le RJ45 1. Standard répandu 2. Utilisable en PoE et en vidéosurveillance ii. Existence de lecteurs Wifi b. Choix des capacités au regard des besoins c. Choisir des lecteurs supportant le « mode transparent » d. Modalités de mises à jour des firmwares 4. UTL a. Modalités de mises à jour des firmwares b. Support du mode transparent c. Capacités cryptographiques d. Capacités fonctionnelles i. anti-passback : badgeage unique dans un sens donné, cf. **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** ii. imbrication des zones iii. escorte 5. Bagde porte-carte a. Pas de partie métallique b. Sensibilisation des porteurs aux sources possibles d'interférences (clés…)

	Description des points d'attention sur les projets sans-contact
PA_03	Enrôlement : 1. Définition des procédures a. Pour les cartes CPx « en parc » (existantes) b. Pour les nouvelles cartes CPx (renouvèlements…) 2. Développements et/ou choix des logiciels 3 exemples d'enrôlement pour un scénario « Type A » sont fournis en Annexe – Exemples d'implémentation d'enrôlement sans-contact
PA_04	Définition des scénarios de perte / vol / oubli / renouvèlement de carte et de modification des droits adossé à un système de gestion du parc de cartes utilisées: 1. Problématique commune avec le Smartcard logon 2. Accès physiques : Chaperon/Escorte vs carte temporaire ? 3. Accès logiques : Accès normaux vs accès restreints ?
PA_05	Compatibilité et réversibilité des données : 1. Gestion des « copies » de données pour des services différents (photocopieuse, parking, portiques, cantine) 2. Problématique de migration d'une solution technique vers une autre
PA_06	Fonctionnement en mode dégradé (autres que perte / vol / oubli / renouvèlement de carte) 1. Pannes de lecteur sans-contact notamment
PA_07	Conformité de la solution vis-à-vis des standards et des bonnes pratiques • AAA : LDAP, RADIUS… • Capacités réelles et paramétrables d'« accounting », d'audit et d'exploitation des logs • Bonnes pratiques de sécurisation des liaisons à distance • Bonnes pratiques de dimensionnement des infrastructures, de mise en production et de suivi d'exploitation, le système se devant d'être performant et réactif de bout en bout
PA_08	Concomitance / dépendance avec d'autres projets de l'établissement • Inventaires • Expansions des locaux • Rénovations (en particulier, rénovations des accès) • Migrations logicielles (changement d'annuaires internes, changements de logiciels RH, poste de travail, accueil, changement ou évolution d'ERP) • Mise en place de zones de sécurité spécifiques

	Description des points d'attention sur les projets sans-contact

PA_09	Conformité réglementaire
	• Sécurité
	  ○ accès restreint aux bases de données de correspondance {identité porteur ; données sans-contact}
	  ○ accès accordés sur d'autres données que celles contenues en bloc-0
	  ○ niveau de qualification
	  ▪ des cartes (la carte CPx est EAL 4+)
	  ▪ des lecteurs
	  ▪ des équipements intermédiaires
	• CNIL : déclaration de conformité simplifiée n°42, cf. **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]**
	  ○ « Traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration »

PA_10	Formations des personnels
	• Explications de différents rôles (enregistrement, administrateurs, utilisateurs, émetteur de carte temporaire…)
	• Sécurité
	  ○ sensibilisations
	• Procédures
	  ○ Déclarations de perte
	  ○ Renouvèlements
	  ○ Gestion des oublis
	  ○ …

PA_11	Modalités d'administration • Modalités de mises à jour des équipements composants du contrôle d'accès • Déploiement de cartes « d'administrateur » propriétaires ? • Possibilité de spécifier un sous-ensemble de cartes CPx déjà présentes dans le parc comme cartes « d'administrateur » ?

Tableau 27 : CPx Sans-contact : points d'attention

9.2 Recommandations pour le choix de lecteurs sans-contact

	Description de la recommandation pour le choix de lecteurs sans-contact
1	La carte CPx est compatible ISO 14443 type A et type B. Pour les scénarios dans lesquels le lecteur sans-contact est connecté à un PC : les lecteurs à utiliser en sans-contact avec la carte CPx doivent être des lecteurs PC/SC compatibles ISO 14443 en types **A et B** (cf. **[Présentation de la carte CPS3]**), si possible compatibles PC/SC v2. Il n'existe pas d'API équivalente à PC/SC pour les lecteurs muraux.

2	Si tous les lecteurs de cartes sans-contact sont capables de communiquer avec la carte CPx au niveau physique via l'implémentation des volets 1, 2 et 3 de **l'**ISO 14443 :
	• pour le protocole de type A
	  ○ récupération et exploitation de l'UID
	• pour le protocole de type B
	  ○ récupération et exploitation du PUPI
	la grande majorité d'entre eux – en tout cas de ceux qui sont déployés – ne sont pas capables « sur étagère » de transmettre des messages IAS-ECC adaptés à la carte CPx pour faire du « sans-contact IAS-ECC ».
	
	Il convient donc:
	1. Si les lecteurs **ne sont pas** déjà **déployés** :
	  a. **de bien identifier le besoin** pour choisir le bon lecteur
	  b. de privilégier les lecteurs supportant le **mode transparent**
	  c. de privilégier les lecteurs dont le **firmware se met facilement à jour**
	2. Si les lecteurs **sont** déjà **déployés** :
	  a. **de bien vérifier leurs conformités aux standards et leurs capacités** afin de ne pas chercher à implémenter un service qu'ils ne pourront pas rendre

Tableau 28 : CPx Sans-contact : recommandations pour le choix de lecteurs sans-contact

9.3 Enrôlement

L'enrôlement est l'étape cruciale lors de laquelle une personne est autorisée :

- à accéder à une ou plusieurs zones sécurisées
- à utiliser certains services informatiques.

Les applications ou les SI qui souhaitent déployer des services sur la base du volet sans-contact de la carte CPx doivent prévoir une phase d'enrôlement.

Le volet sans-contact de la CPx n'étant pas lié à la personne physique du porteur par construction même de l'IGC de Santé, il n'est pas possible pour l'ASIP Santé de fournir des listes de correspondances {carte CPx; numéro de série du composant sans-contact} afin d'alimenter cette phase.

La phase d'enrôlement doit donc être effectuée au niveau local, au sein du SI souhaitant gérer des accès sans-contact avec un parc de cartes CPx.

9.3.1 Objectif de l'enrôlement

L'objectif de l'enrôlement est l'enregistrement de personnes dans le système de contrôle d'accès. Après l'enregistrement, des données personnelles sont liées à la personne grâce à un identifiant unique en base de données. Après analyse, cet identifiant est distribué aux lecteurs connectés au système de contrôle d'accès. Les autorisations et les badges attribués à chaque personne sont également repérés par l'identifiant unique de la base de données.

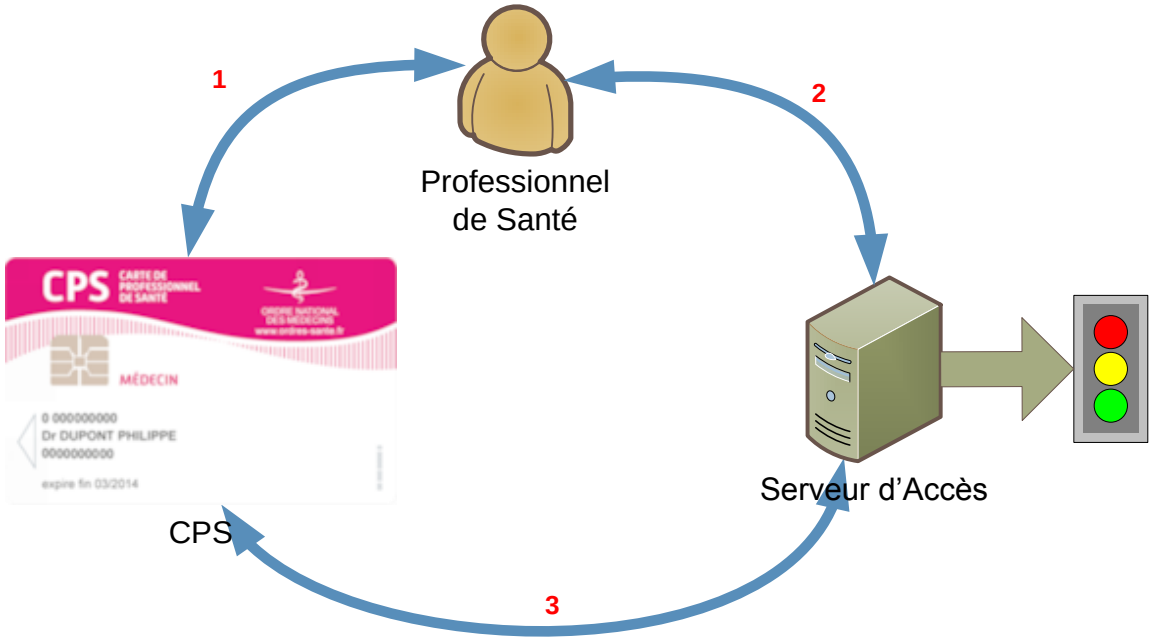


Figure 1 : Objectif de l'enrôlement

	IGC-Santé : enrôlement	Le principe d'enrôlement reste valable avec la nouvelle IGC-Santé.

Tableau 29 : IGC-Santé : principe d'enrôlement inchangé

Afin d'assurer la cohérence et la sécurité du système, l'enrôlement doit garantir pour chaque personne :

1	Association de la carte avec son titulaire	Exemple : le processus d'envoi de la CPS au Professionnel de Santé suivi par l'ASIP.
2	Association des autorisations avec la personne	Exemple : la définition des accès est demandée par le responsable hiérarchique au responsable du contrôle d'accès par l'intermédiaire des ressources humaines
3	Association de la carte avec le contrôle d'accès	Cf. Identification d'une carte CPx

Tableau 30 : Points garantis par l'enrôlement

Si une seule de ces relations n'est pas réalisée suivant des processus sous des conditions de confiance, les conséquences sont la baisse du niveau de sécurité de la zone concernée :

1	Une personne utilise les accès d'une autre
2	Une personne a plus d'autorisations que nécessaire
3	Le contrôleur autorise une carte invalide

Tableau 31 : Dégradation de la sécurité

9.3.2 Identification d'une carte CPx

Afin d'assurer correctement la phase d'enrôlement, il est nécessaire d'identifier de manière unique les cartes CPx qui seront utilisées en sans-contact afin de les associer sans ambiguïté à un ensemble de droits. Se rapporter aux Annexe – ISO 14443 et IAS-ECC pour la partie sans-contact de la carte CP et

Annexe – Numéros de série de la CPx.

9.4 Factorisation des enrôlements

L'objectif de l'enrôlement doit aussi être de centraliser les opérations de mises à jour des bases de données utilisées par les différents sous-systèmes utilisant le mode « sans-contact ».

Il sera ainsi difficile de demander à l'utilisateur de s'enrôler à l'accueil pour ses accès aux bâtiments, au service SI pour ses accès en Smartcard logon, aux services généraux pour les enrôlements liés aux impressions et aux accès parking.

Mieux : si toutes ces actions ne sont pas centralisées, il sera difficile de maintenir la cohérence des informations d'enrôlement si elles sont « copiées » dans différentes base de données utilisées par et pour différents services.

A défaut de pouvoir centraliser ces informations d'enrôlement, il sera nécessaire de prévoir des mécanismes de synchronisation des informations qui à leur tour imposeront que les différents formats de stockage de l'information soient connus et que des tâches régulières de mise à jour soient orchestrées au sein du SI.

Par exemple, pour les établissements qui font du Smartcard logon et du sans-contact, l'enrôlement sans-contact peut être factorisé avec un enrôlement « Smartcard logon »

1- lecture du SAN en mode contact / en parsant le certificat d'authentification
2- lecture de l'UID en mode sans-contact
3- alimentation des bases de données idoines avec ces informations

10Annexe – Documents institutionnels de référence

Les documents de référence pour la partie sans-contact de la carte CPx sont les suivants :

Cryptolib CPS v5	**[2]**	Le document **[Présentation de la carte CPS3]** en ligne sur le site « intégrateurs » (http://integrateurs-cps.asipsante.fr/) de l'ASIP Santé contient 5 pages dans un paragraphe « 6.4.2 Annexe 4 : les services d'identification et d'authentification par la CPx / sans-contact » dédiées à l'authentification sans-contact avec la carte CPx.
	[3]	Le document **[Manuel de programmation de la Cryptolib CPS v5]** accessible sous {login; mot de passe; captcha} (les conditions d'accès sont précisées sur la page d'accueil du site « intégrateurs ») dans la partie « **Téléchargement logiciels** » via « **Cryptolib CPx (Installeur MSI) + pack de programmation** » contient 2 chapitres 8 et 9 sur: 1. l'accès au volet sans-contact via le PKCS#11 2. la gestion du jeton d'établissement.
	[4]	Le document **[Documentation programme d'exemple de la Cryptolib CPS v5]** illustre l'implémentation technique de ce scénario (page 67).
Architecture et cadre réglementaire	**[12]**	**[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]** édité par l'ANSSI en novembre 2012
	[13]	**[APSAD D83 - Contrôle d'accès - Document technique pour la conception et l'installation]** édité par le CNPP en novembre 2012

Tableau 32 : Cryptolib CPS v5 : documents de référence pour la partie sans-contact

11Annexe – ISO 14443 et IAS-ECC pour la partie sans-contact de la carte CPx

11.1 Les protocoles

Les fonctionnements des cartes sans-contacts et des cartes contacts sont proches. Ainsi :

- Les principales normes des cartes contacts sont les ISO 7816-1 à 4.
- Les principales normes des cartes sans-contacts sont les ISO 14443-1 à 4 et ISO 15693-1 à 3.
- Les normes ISO 14443 1 à 4 des cartes sans-contacts correspondent aux normes ISO 7816-1 à 3 des cartes contacts.

Carte CPx et ISO 15693	Les cartes CPx ne sont pas compatibles avec les normes ISO 15693-1 à 3. Ces normes ne seront donc pas détaillées dans ce document bien qu'il existe des lecteurs supportant les normes ISO 14443 et ISO 15693[4].

Tableau 33 : CPx Sans contact et ISO 15693

L'intégration des normes des cartes contacts et sans-contacts entre elles peut être schématisée ainsi :

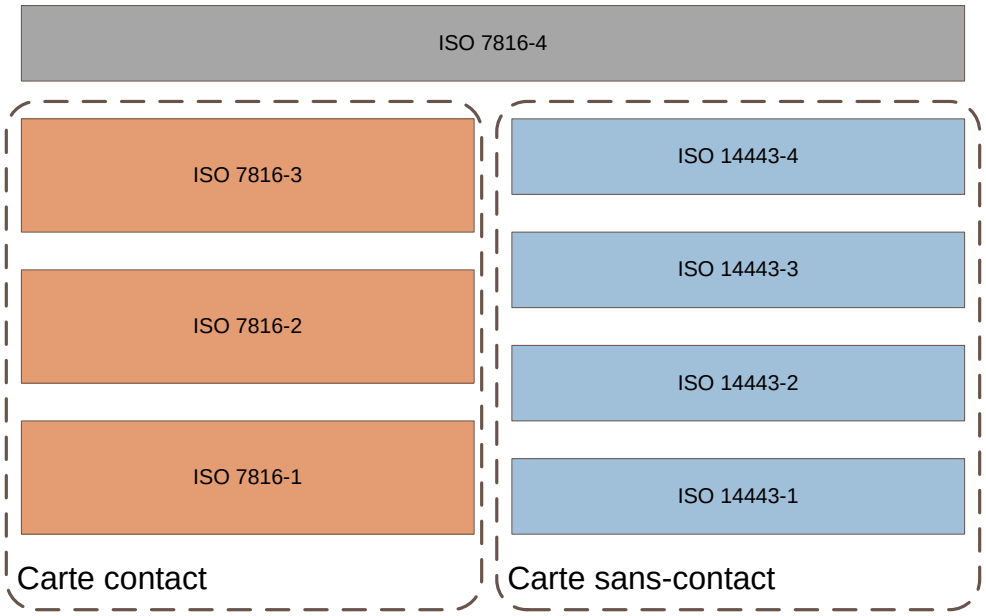


Figure 20 : normes contact / sans-contact

L'ISO 14443 est composé de 4 volets (ou « tirets »).

Les volets 1,2 et 3 de l'ISO 14443 correspondent à la **couche physique** (couche 1 de l'OSI). Il s'agit donc de la couche qui permet la communication entre la carte et le lecteur via des ondes électromagnétiques. En technologie sans-contact, l'« onde » correspond au « fil » en technologie contact.

[4] implicitement déconseillé par **[Guide sur la Sécurité des technologies sans-contact pour le contrôle des accès physiques]**

Plusieurs caractéristiques d'« onde » et de méthodes de mise en œuvre existent. Les normes ISO 14443 en décrivent deux, notées **type A** et **type B**. L'ISO 14443 type A et l'ISO 14443 type B marquent donc une différence de **couche physique**. La principale différence entre les types A et les types B, outre d'utiliser des supports physiques différents, est la gestion du début de la transmission. En effet, les cartes type B génèrent un numéro de série aléatoire à chaque début de transmission, le PUPI (Pseudo-Unique PICC (Proximity Integrated Circuit Card) Identifier). Le PUPI est :

- utilisé par l'anticollision ;
- unique en un endroit donné à un moment donné ;
- cf. ISO/IEC 14443-3, chapitre 7.9.2.

Au-dessus de la **couche physique** se trouve la **couche de transmission** (couche 2 de l'OSI) définie par l'ISO 14443-4. L'ISO 14443-4 permet la transmission, en mode sans-contact, de commandes conformes à l'ISO 7816-4 **[Standards "Identification cards — Integrated circuit(s) cards with contacts"]** identiques aux commandes échangées en mode contact. Elle permet à la carte et au lecteur de cartes de communiquer au moyen de messages de niveau applicatif, structurés et spécifiés indépendamment des formats des ondes électromagnétiques qui les véhiculent.

11.2 La technologie

La technologie sans-contact s'appuie sur les mêmes composants que les cartes « contact ». Les différences essentielles sont :

- L'alimentation électrique, par un principe d'induction.
- La communication « sans fil » sur une fréquence définie.

Ces deux aspects sont extrêmement liés l'un à l'autre puisqu'ils dépendent directement de l'élément physique spécifique à la carte sans-contact : l'antenne.

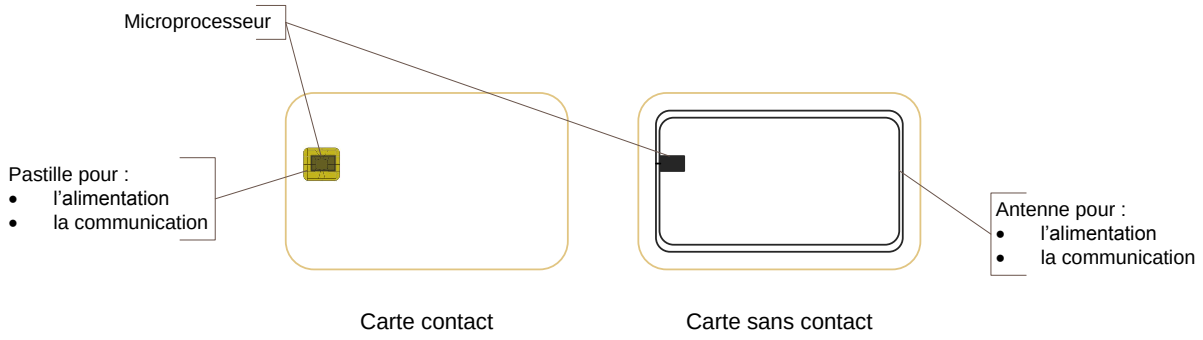


Figure 21 : technologie contact / sans-contact

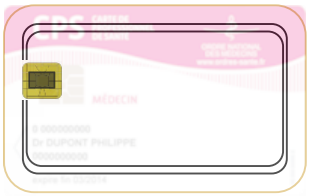
Voici des exemples d'imbrication des effets de l'une sur l'autre :

- une mauvaise alimentation génère des erreurs de transmission ;
- l'augmentation de la qualité de transmission augmente la consommation ;
- l'augmentation de consommation réduit la distance de lecture.

11.3 La carte CPx

Comme nombre de cartes à puces de nouvelle génération, la carte CPx offre la double technologie contact et sans-contact.

Comme tous les produits suivant les standards du marché, la carte CPx s'appuie sur l'ISO 14443 **[Standards "sans-contact"]** pour sa partie sans-contact.



CPS3

Figure 22 : Schéma de la carte CPx

La carte CPx s'appuie sur le standard IAS-ECC pour la couche **applicative** (couche 7 de l'OSI): les couches applicatives des 2 parties contact et sans-contact de la carte CPx sont conformes au standard IAS-ECC **[EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS [IAS ECC]]**.

L'offre de services diffère suivant la technologie :

- En contact, l'ensemble des services sont accessibles : authentification du porteur, authentification forte, signature, fichier d'information professionnelle, …
- En sans-contact, seules les fonctionnalités suivantes sont disponibles : authentification technique, lecture de fichiers spécifiques (voir matrice d'intégration du sans-contact ci-après).

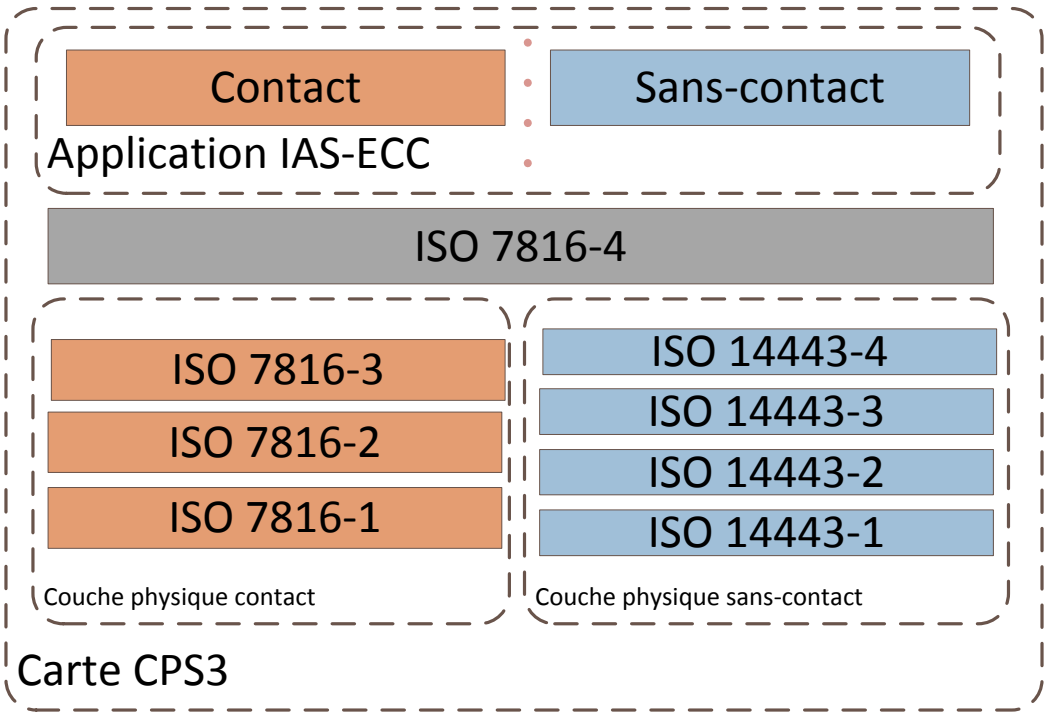


Figure 23 : normes contact / sans-contact rapportées à la CPx

12Annexe – Attaques de cartes sans-contact

Les considérations présentées ci-après ne sont pas exhaustives : les attaques de contrôle d'accès sont légion. Elles sont présentées pour sensibiliser le lecteur aux aspects de sécurité liés au sans-contact. Ces aspects sont généralement induits par le caractère diffusif des ondes électromagnétiques, par opposition aux fils ou aux contacts qui « confinent » les communications traditionnelles. L'importance à accorder à ses attaques reste à évaluer en rédigeant une **analyse de risque**.

12.1 Légende

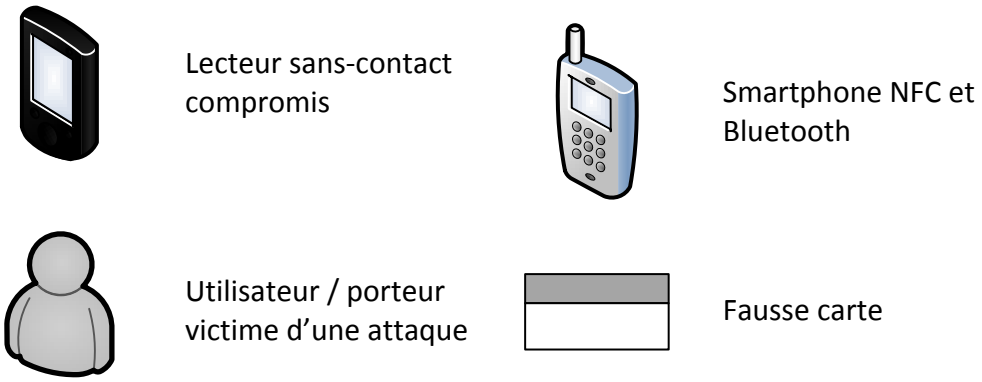


Figure 24 : Légende des schémas présentés dans la partie « attaques »

12.2 Attaques liés aux accès « UID / Type A »

12.2.1 Attaque par force brute

Cette attaque consiste à fabriquer ou à collecter un nombre suffisant de cartes en espérant que l'une d'entre elles expose un UID d'une carte réelle. Elle repose sur le fait que la taille de l'UID est généralement petite et donc que les collisions d'UID sont probables.

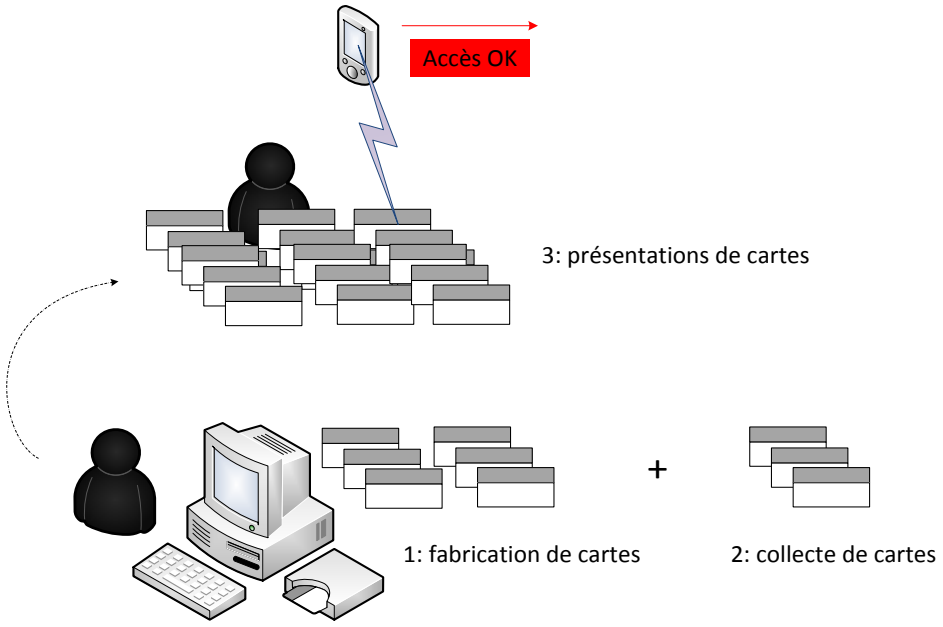


Figure 25 : Type A : attaque par force brute

Ce scénario couvre le cas de porteurs possédant plusieurs cartes sans-contact dont une au moins permet d'ouvrir des accès pour lesquels elle n'est pas destinée (cas d'ouverture d'accès avec un badge Navigo par exemple).

Conseils NXP	Pour pallier au problème des collisions d'UID, NXP recommande désormais l'usage d'UID de 7 bytes ou de NUID (non-unique ID) de 4 bytes (http://www.mifare.net/en/technology/4-7byte-uid/)

Tableau 34 : Contre-mesure à la l'attaque par force brute : conseils NXP sur les UID

Ce scénario pourrait être facilité par l'apparition de smartphones NFC permettant d'exposer des UID à la volée.

Monitoring	Les tentatives d'accès infructueuses peuvent être détectées par analyse des erreurs par traçabilité coté serveur.

Tableau 35 : Contre-mesure à la l'attaque par force brute : monitoring

12.2.2 Attaque par duplication de carte (« clone »)

12.2.2.1 Principe

Les attaques par duplication de carte reposent sur l'exploitation de failles cryptographiques identifiées sur le type de carte visé. Avec le temps, ce type d'attaque devient facilement implémentable (1 heure pour casser et cloner une carte avec 100€ de matériel **[OpenSilicium n°12 – Prise en main des technologies RFID / NFC]**).

Le principe est le suivant :

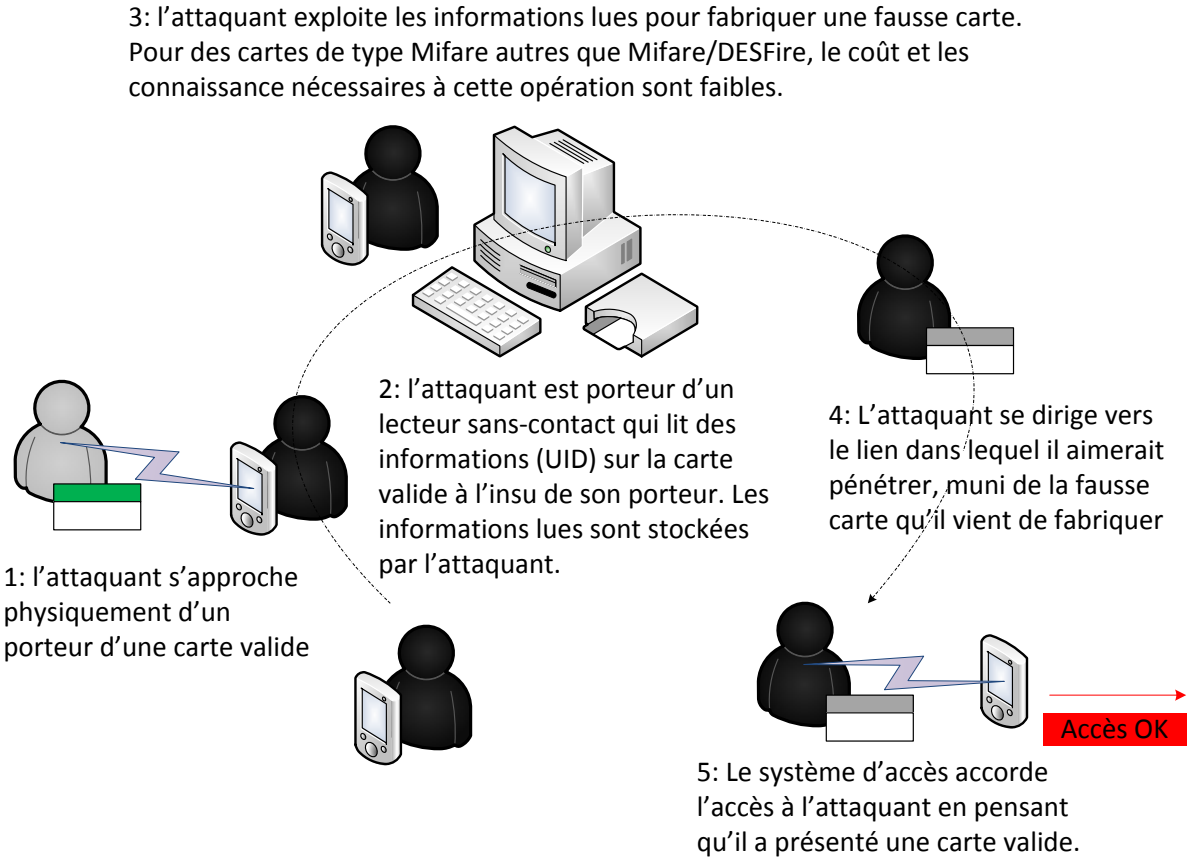


Figure 26 : Attaque par duplication de carte

Cette attaque nécessite cependant de collecter de l'information.

12.2.2.2 Collecte de données en itinérance

Afin de préparer son attaque, l'attaquant doit collecter des données de cartes réelles auprès de porteurs qui seront ses futures victimes. Il profite du lien sans-contact pour le faire :

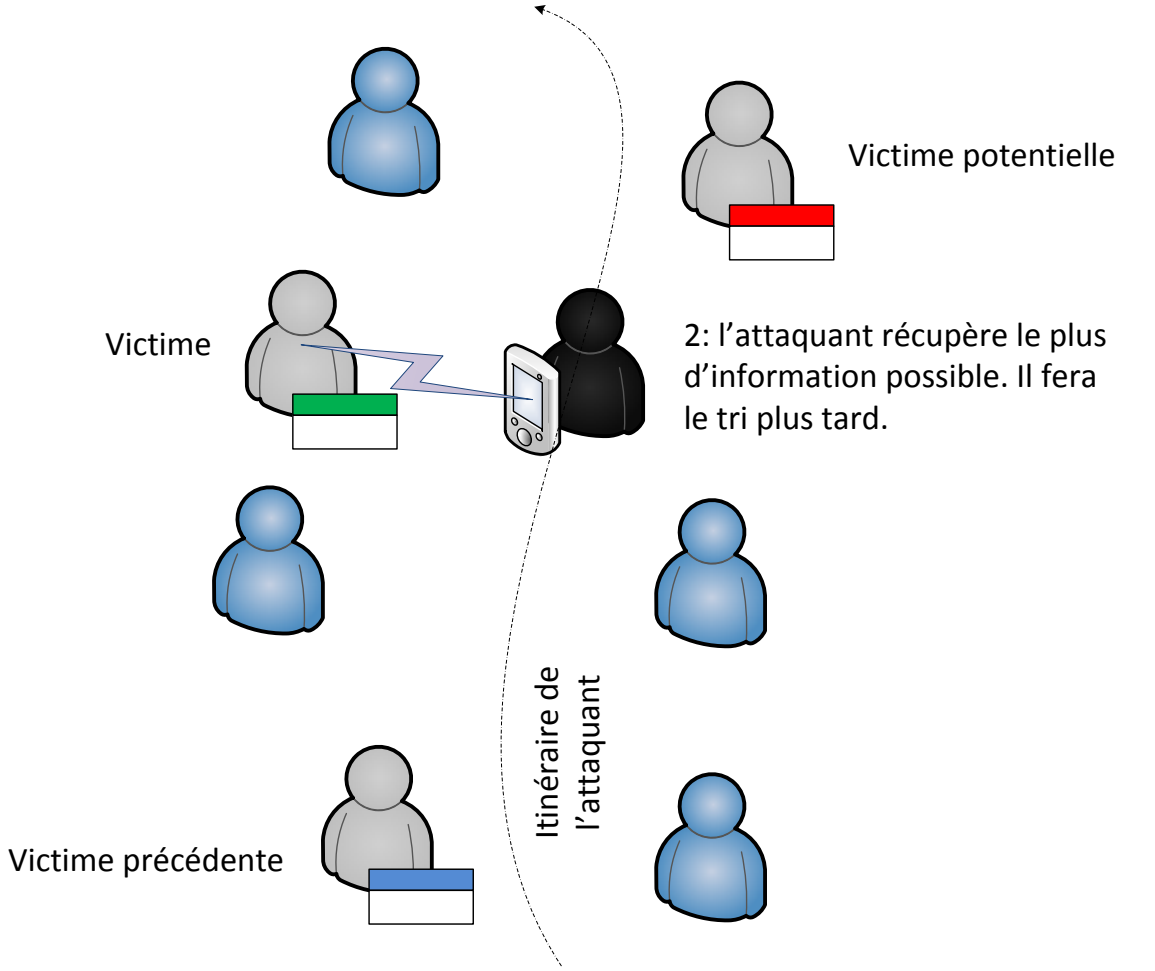


Figure 27 : Collecte de données carte en itinérance

Ce type de collecte est utilisé en attaque à la carte bleue sans-contact par exemple.

12.2.2.3 Collecte en itinérance ciblée

Le problème de la collecte itinérante précédente est qu'elle n'est finalement pas très adaptée à l'attaque en contrôle d'accès. L'attaquant va donc adapter sa collecte au site qui l'intéresse :

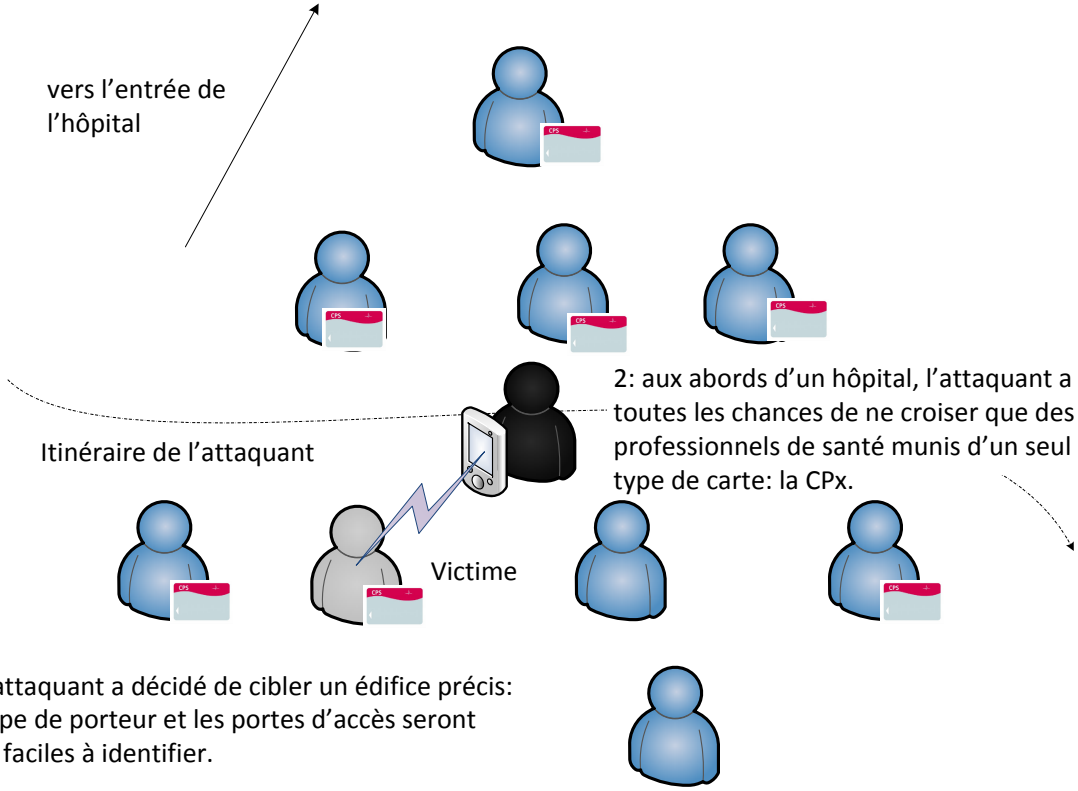


Figure 28 : Collecte en itinérance ciblée

	Collecte de données carte en itinérance ciblée	Ce type de comportement peut être découragé par de la vidéo-surveillance

Tableau 36 : Contre-mesure à la collecte de données carte en itinérance ciblée

12.2.2.4 Collecte sur le lecteur sans-contact (« skimmer »)

Le principe de cette collecte est de compromettre un lecteur sans-contact de sorte à ce qu'il récupère pour un attaquant des informations cartes. C'est une attaque classique sur les automates bancaires qui s'applique aussi au sans-contact et qui peut se rencontrer dans le domaine de la Santé sur des points d'intérêts (armoire à pharmacie) :

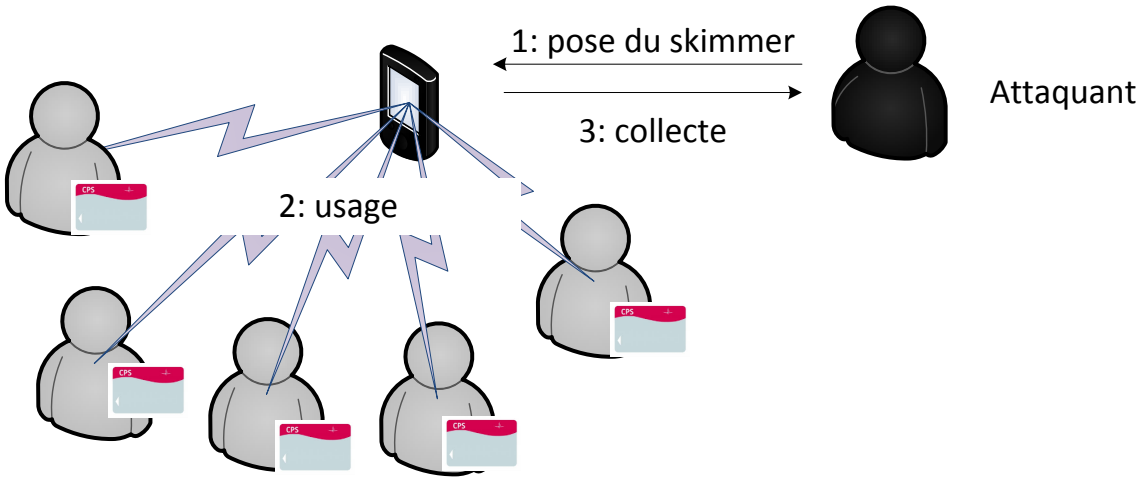


Figure 29 : Collecte avec skimmer

Collecte avec un skimmer	Le parc de lecteur doit être régulièrement inspecté. Les lecteurs munis de dispositifs empêchant leurs manipulations doivent être privilégiés.

Tableau 37 : Contre-mesure à la collecte de données carte avec un skimmer

12.3 Attaques Mifare

Mifare est sujet à une attaque par force brute cryptographique permettant de réaliser un clone complet de la carte. Voir « Attaque par duplication de carte (« clone ») » plus haut.
Voir aussi le bulletin de sécurité publié par l'ANSSI :

« Vulnérabilité exploitable des cartes sans contact Mifare Classic » du 29 octobre 2008

Des tags « spéciaux » appelés « Mifare with changeable UID » présentent un bloc 0, celui du fabriquant et contenant l'UID, réinscriptible. L'outil nfc-mfsetuid des NFC Tools permet de débloquer ce bloc et d'y inscrire l'UID voulu **[OpenSilicium n°12 – Prise en main des technologies RFID / NFC]**. Changer un UID revient en gros à changer l'adresse MAC de sa carte réseau : d'impossible au début, l'opération est devenue courante. Le délai de compromission sur ce type d'attaque est de l'ordre de la minute pour un individu ne disposant d'aucune connaissance technique particulière.

MFCUK « Mifare Classic Universal toolkit » implémente la « darkside attack » pour récupérer une des clés Mifare Classic dans des délais de l'ordre de 30 minutes. Les tags récents ne sont plus sensibles à cette attaque **[OpenSilicium n°12 – Prise en main des technologies RFID / NFC]**.

MFOC « Mifare Classic Offline Cracker » implémente la « nested authentication attack » pour récupérer toutes les clés du tag si un seul secteur du tag est accessible par une clé connue **[OpenSilicium n°12 – Prise en main des technologies RFID / NFC]**. Combinée à l'attaque précédente, le délai de compromission sur ce type d'attaque est de l'ordre de l'heure pour un individu ne disposant d'aucune connaissance technique particulière.

Mifare/DESfire n'est pas concerné par ce type attaque mais les composants MIFARE DESFire MF3ICD40 sont sensibles aux attaques par « Differential Power Analysis » (https://www.emsec.rub.de/media/crypto/veroeffentlichungen/2011/10/10/desfire_2011_1.pdf), ce qui a poussé NXP à sortir l'EV1, qualifié EAL4+ (http://www.mifare.net/en/technology/security/mifare-desfire-d40/). Le délai de compromission sur ce type d'attaque est de l'ordre de la semaine mais nécessite une connaissance pointue et des investissements élevés.

12.4 Attaque par routage des communications sans-contact (MITM)

L'attaque par routage des communications sans-contact concerne tous les types de cartes et tous les types de protocoles de sécurité sans-contact.

Elle est rendue possible par la concentration des technologies (NFC, Bluetooth…) au sein de dispositifs portables puissants (Smartphone) fonctionnant sous des OS libres, dont le code source est connu et modifiable à souhait.

Cette attaque est contrecarrée par la mise en place de sécurités dédiées dans les puces et/ou dans les lecteurs (contrôle des délais de réponse par exemple).

12.4.1 Principe

Le principe est le suivant :

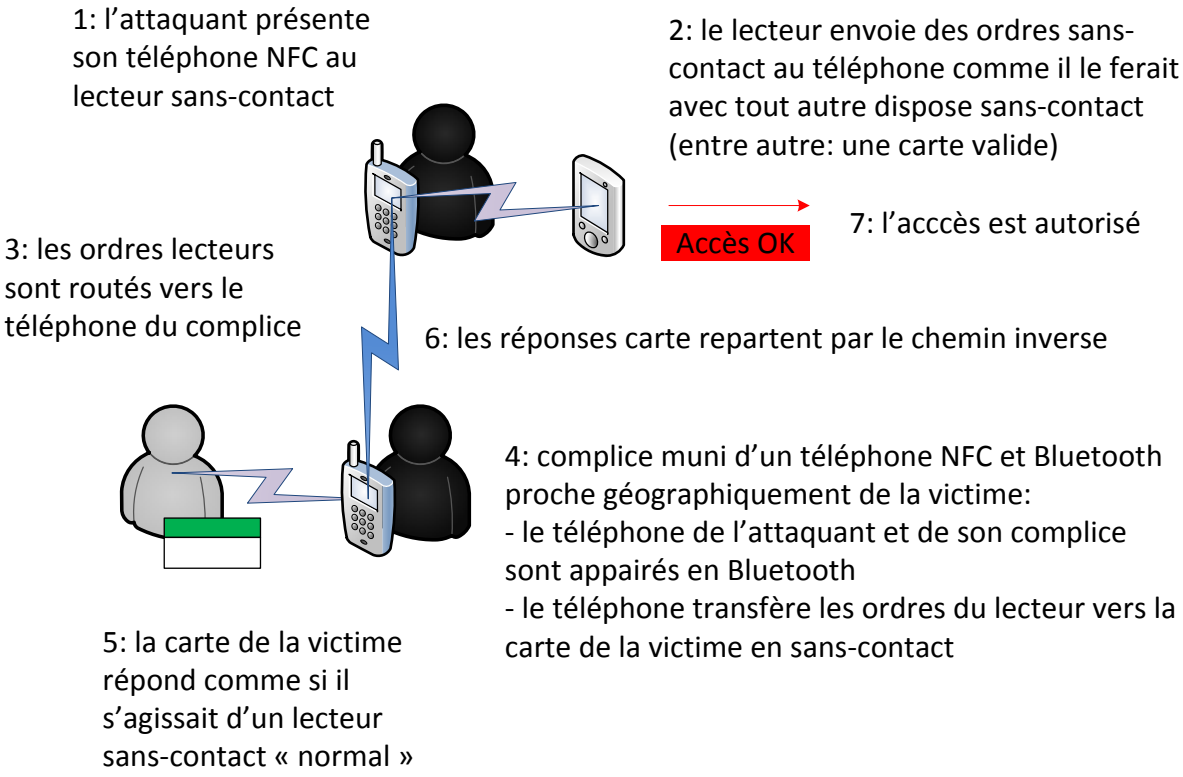


Figure 30 : Attaque par routage des communications sans-contact

12.4.2 Application à l'intrusion : début d'une attaque out-out

Dans cette attaque, l'attaquant et son complice sont tous les deux hors du périmètre sécurisé :

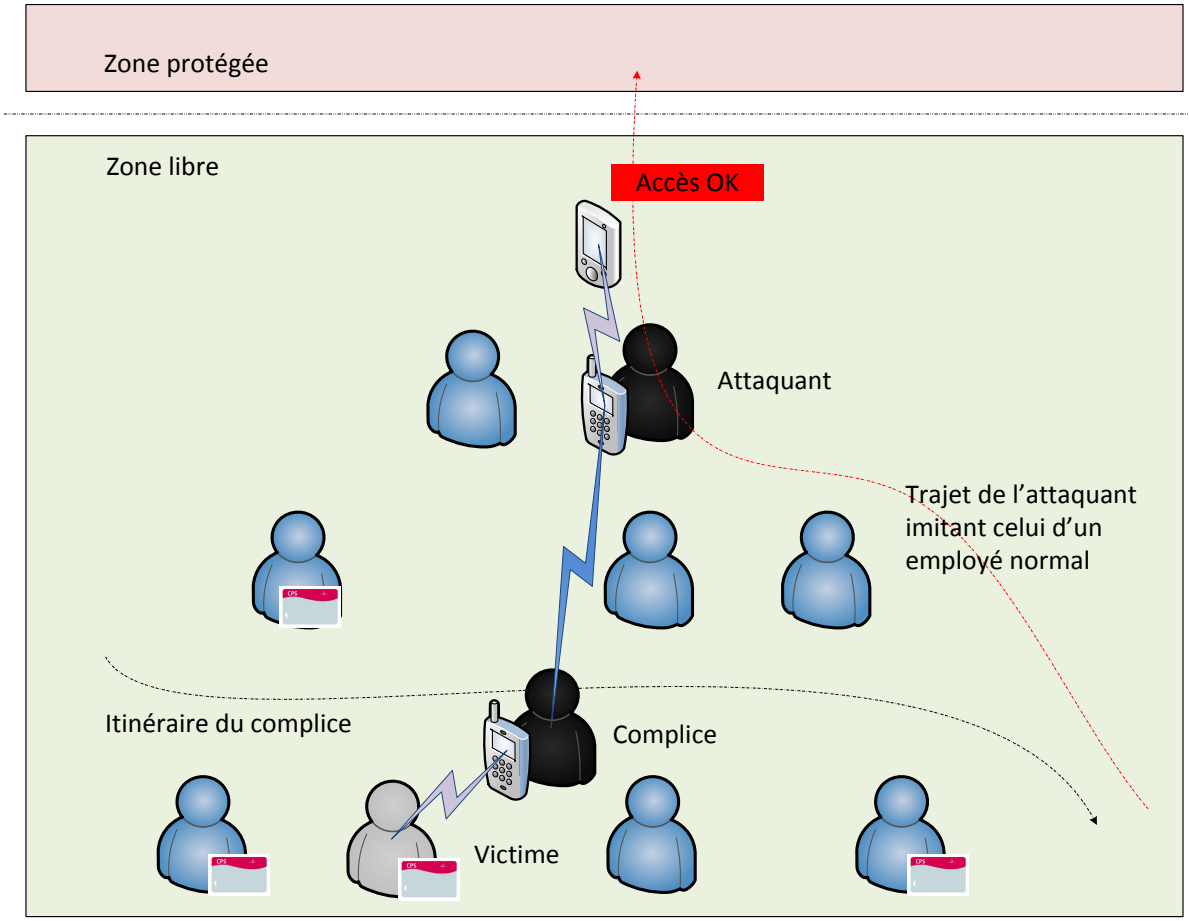


Figure 31 : Attaque out-out : début

12.4.3 Application à l'intrusion : suites d'une attaque out-out

Une fois que l'attaquant est entré dans la zone sécurisée, il est intéressant d'analyser la situation ultérieure où la victime se présente à son tour devant la porte d'accès protégée :

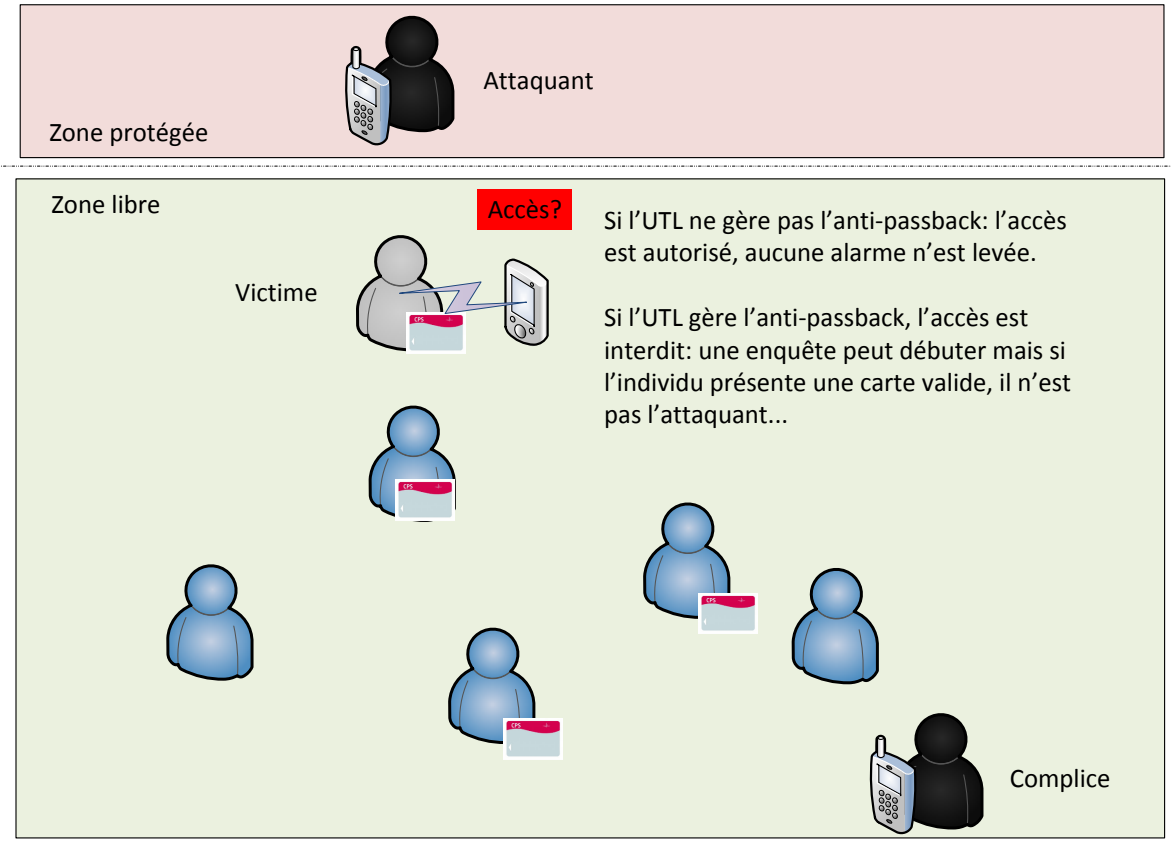


Figure 32 : Attaque out-out : suites

	Anti-passback	Les UTL gérant l'anti-passback doivent être privilégiés.

Tableau 38 : Contre-mesure à la l'attaque out-out : anti-passback

	Protocole d'enquête	En cas de problème d'accès, un protocole d'enquête précis et systématique doit être mis en place : - Demande de présentation du badge défectueux - Exploitation des traces du système d'accès 1. Récupération des données de la carte en erreur 2. Etablissement des liens carte-porteur - Recoupements d'information (quel est le service de la personne ?...) - vidéosurveillance

Tableau 39 : Contre-mesure à la l'attaque out-out : protocole d'enquête

12.4.4 Application à l'intrusion : début d'une attaque in-out

Dans cette attaque, initialement, l'attaquant est en zone libre alors que son complice est déjà dans le périmètre sécurisé, périmètre dans lequel il a pu entrer précédemment par d'autres moyens ou par attaque out-out :

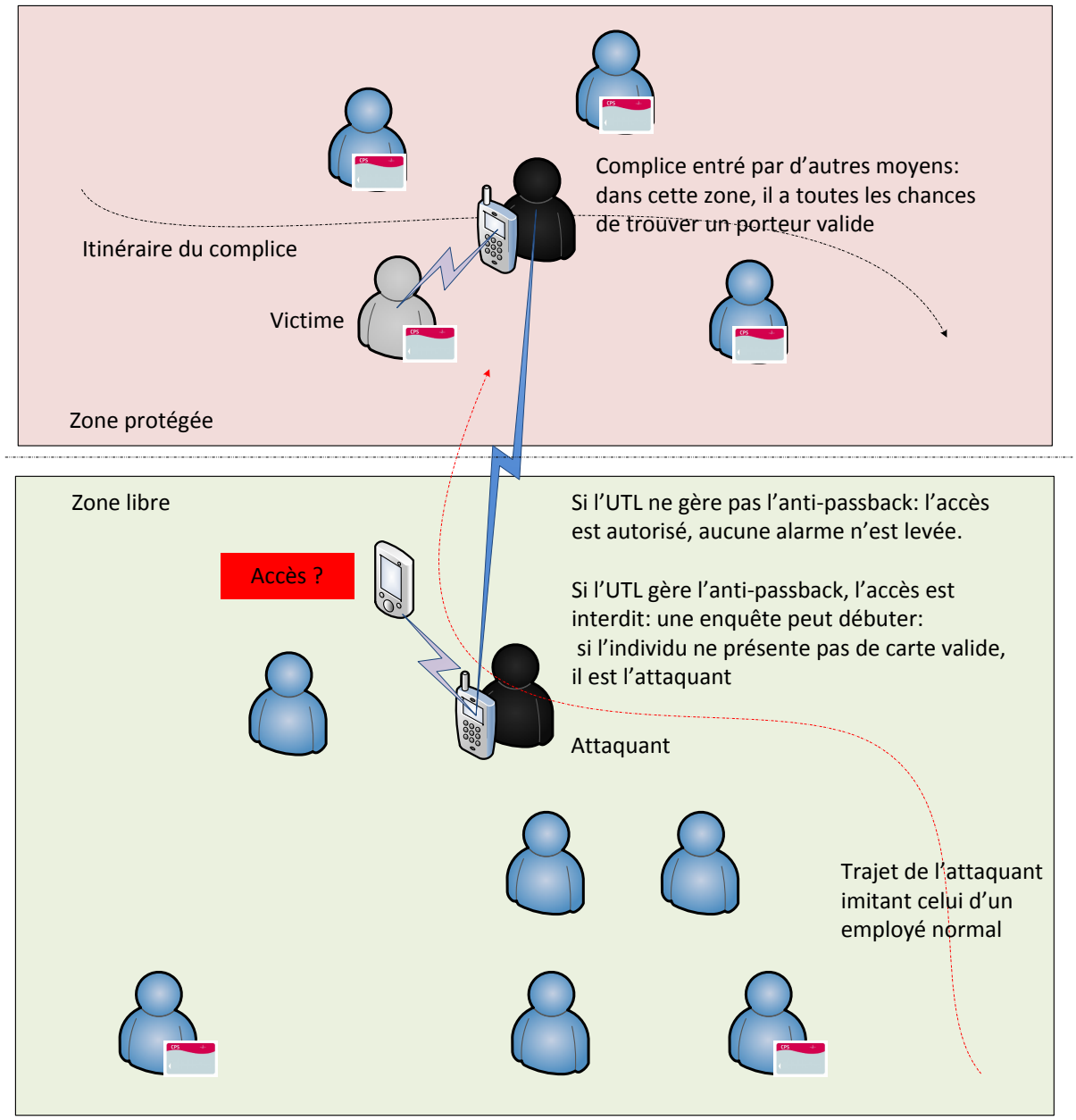


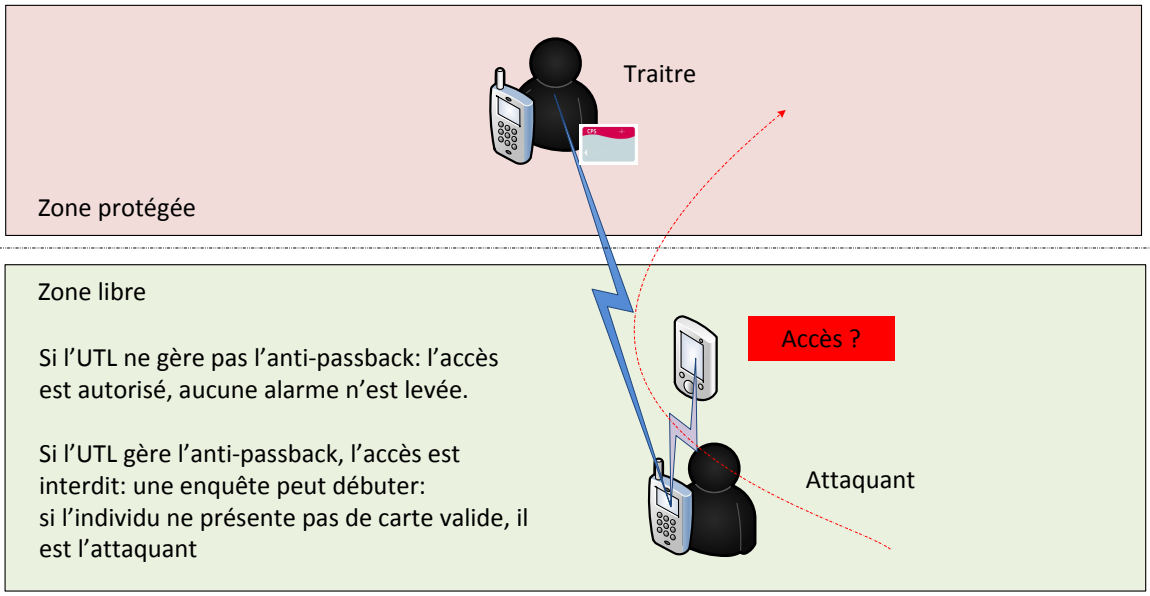
Figure 33 : Attaque in-out

Contre-mesures	Les contre-mesures sont les mêmes que pour le in-out

Tableau 40 : Contre-mesure à la l'attaque in-out : anti-passback et protocole d'enquête

12.4.5 Cas particulier du « traitre »

Le « traitre » est un complice qui est aussi un porteur de carte valide (soit il est membre de l'entreprise, soit c'est un complice qui s'est procuré une carte valide).



L'analyse des traces du système d'accès permet de récupérer les données de la carte utilisée pour l'attaque. Le porteur de cette carte est soit une victime soit un traitre. Une étude de l'historique des accès liés à cette carte est nécessaire. Les liens entre les deux individus doivent être analysés.

Figure 34 : Attaque x-out : cas du traitre

13Annexe – Exemples d'implémentation d'enrôlement sans-contact

13.1 Rappels

Le chapitre « Sécurité / Informations personnelles » du présent document rappelle les contraintes de sécurité imposées par la CNIL au sans-contact, contraintes adoptées par l'ASIP Santé pour sa carte CPx.

Chaque établissement ou organisme souhaitant mettre en œuvre la CPx en sans-contact doit dès lors implémenter un mécanisme « local » d'enrôlement de la partie sans-contact afin d'associer un volet sans-contact donné (via l'UID sans-contact par exemple) à un porteur en vue d'offrir une fonctionnalité précise via son SI (présentiel, badgeuse, cantine…) et ce, en restant alerté tout aussi bien sur les aspects « données personnelles » que sur les aspects « sécurité ».

Cette annexe décrit deux scénarios d'enrôlements « sans-contact » locaux envisageables.

13.2 Prérequis

<table>
<tr><th colspan="2">Prérequis</th></tr>
<tr><td colspan="2">OS Microsoft Windows</td></tr>
<tr><td colspan="2">Cryptolib CPS v5 installée</td></tr>
<tr><td colspan="2">CCM configuré en Mode de surveillance des lecteurs activé</td></tr>
<tr><td>1 Lecteur « contact »</td><td rowspan="2">Ou 1 lecteur « contact / sans-contact » PC/SC v2</td></tr>
<tr><td>1 Lecteur « sans-contact » PC/SC v2</td></tr>
<tr><td>1 lecteur code-barres USB</td><td>Si l'enrôlement à la réception de la carte CPx est retenu</td></tr>
<tr><td>Java JRE 1.6+</td><td rowspan="2">Si l'automatisation de l'enrôlement avec Java sous Windows est retenue (cf. ci-dessous).</td></tr>
<tr><td>Développeur Java, connaissances JCA / Smartcardio</td></tr>
<tr><td>Connaissance OpenSC</td><td></td></tr>
</table>

Tableau 41 : Enrôlement {contact ; sans-contact} : pré-requis

13.3 Enrôlement de cartes existantes

13.3.1 Enrôlement manuel sans-contact d'une carte CPx

Ce scénario permet de mesurer/d'appréhender visuellement ce qu'il est possible de faire pour mener à bien un enrôlement sans-contact :

<table>
<tr><th colspan="3">Scénario : enrôlement manuel {contact / sans-contact} d'une carte CPx</th></tr>
<tr><td rowspan="9">Transaction d'enrôlement d'une carte CPx en sans-contact</td><td colspan="2">Début de la transaction</td></tr>
<tr><td rowspan="5">Phase contact</td><td>S'assurer que le(s) lecteur(s) est(sont) branché(s)</td></tr>
<tr><td>Retirer toutes les cartes et s'assurer que le magasin de certificats personnels de Windows est vide</td></tr>
<tr><td>Insérer la carte CPx en mode contact</td></tr>
<tr><td>Consulter le magasin de certificats Microsoft : en déduire le numéro de série et/ou toute autre information intéressante relative à la carte CPx</td></tr>
<tr><td>Retirer la carte du lecteur</td></tr>
<tr><td rowspan="2">Phase sans-contact</td><td>Poser la carte sur le lecteur sans-contact</td></tr>
<tr><td>Utiliser des « outils lecteur » : en déduire l'UID sans-contact</td></tr>
<tr><td colspan="2">Déduire de la transaction l'association {numéro de carte logique ; numéro IAS ; SAN ; …; UID sans-contact}</td></tr>
<tr><td colspan="2">Fin de la transaction</td></tr>
</table>

Tableau 42 : Enrôlement {contact ; sans-contact} : Scénario manuel

Enrôlement sans-contact en mode {contact ; sans-contact}	Ce type d'enrôlement permet de récupérer des informations (numéro IAS, SAN…) qu'il n'est pas possible de récupérer en enrôlement « full sans-contact » (cf. ci-après). Il permet donc de mieux anticiper les évolutions des systèmes d'accès.

Tableau 43 : Avantage enrôlement sans-contact en mode {contact ; sans-contact}

13.3.2 Illustration de la phase « contact »

Si la carte CPx est insérée dans un lecteur « contact », le CCM affiche une fenêtre de ce type (clic-droit / « Lister l'état des lecteurs… ») :

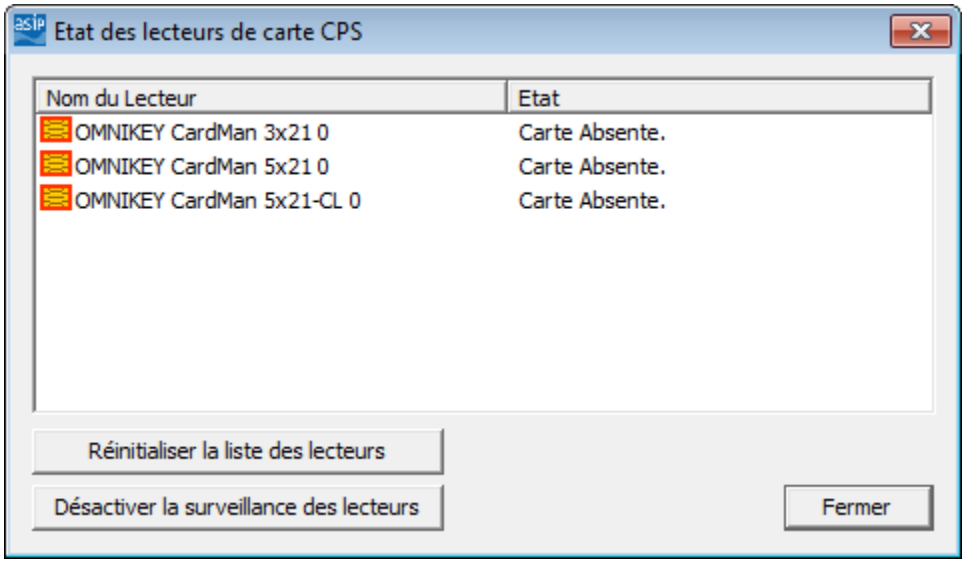


Figure 35 : Enrôlement {contact ; sans-contact} : Pas de carte dans le lecteur

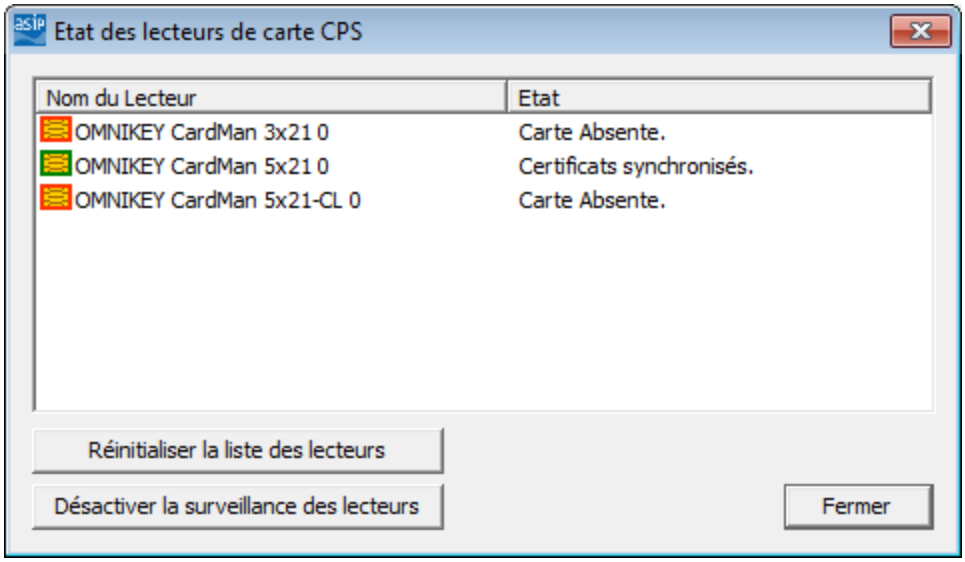


Figure 36 : Enrôlement {contact ; sans-contact} : Contact : CCM : Carte dans le lecteur

Et, sur ouverture du magasin de certificats Microsoft (« Touche Windows > inetcpl.cpl ») :

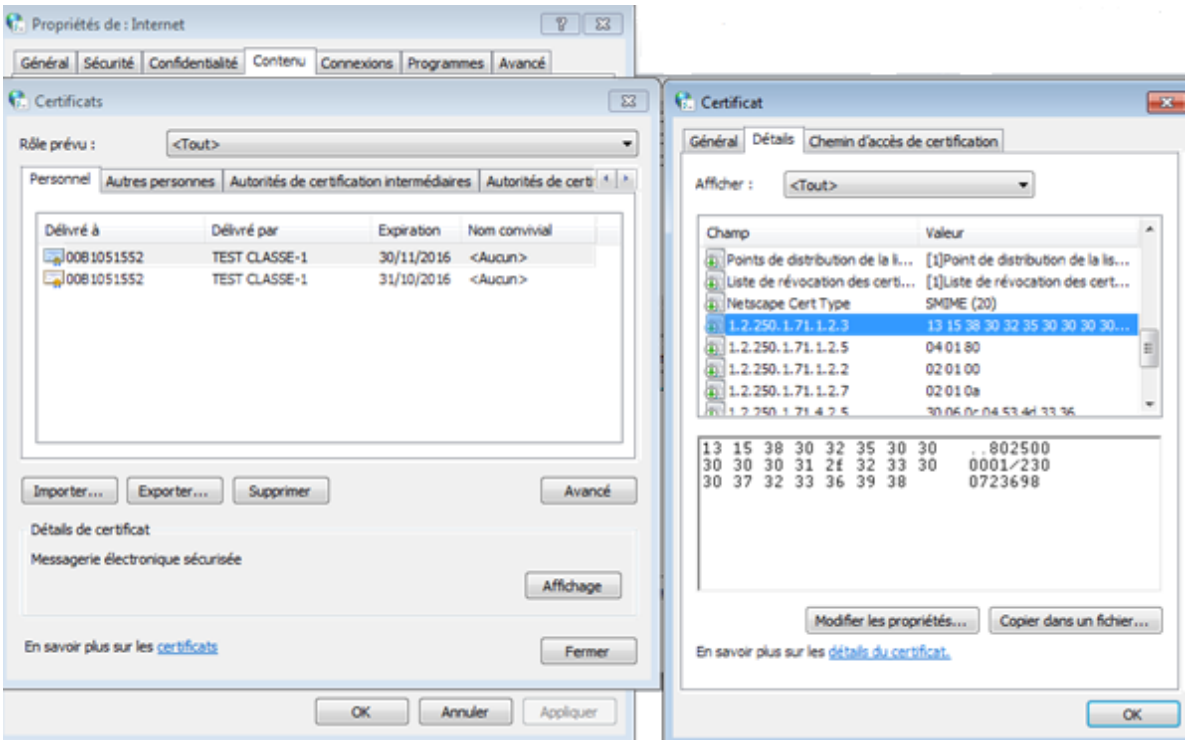


Figure 37 : Enrôlement {contact ; sans-contact} : Contact : magasin, certificat et numéro de série de la carte CPx

Le numéro de série de la carte CPx porteuse du certificat d'authentification ou de signature courant est présent dans le certificat (champ **gipCardID** décrit page 21 de la documentation **[26]** accessible depuis le site esante.gouv.fr : http://esante.gouv.fr/services/espace-cps/les-certificats-cps, lien « IGC cartes : détail des certificats X.509 CPS2ter et CPS3 »).

Cette information est accessible en consultant le magasin de certificats Windows et en analysant les certificats CPx présents dans le magasin.

13.3.3 Illustration de la phase « sans-contact »

Si la carte CPx est retirée du lecteur « contact » et posée sur le lecteur « sans-contact », le CCM affiche une fenêtre de ce type :

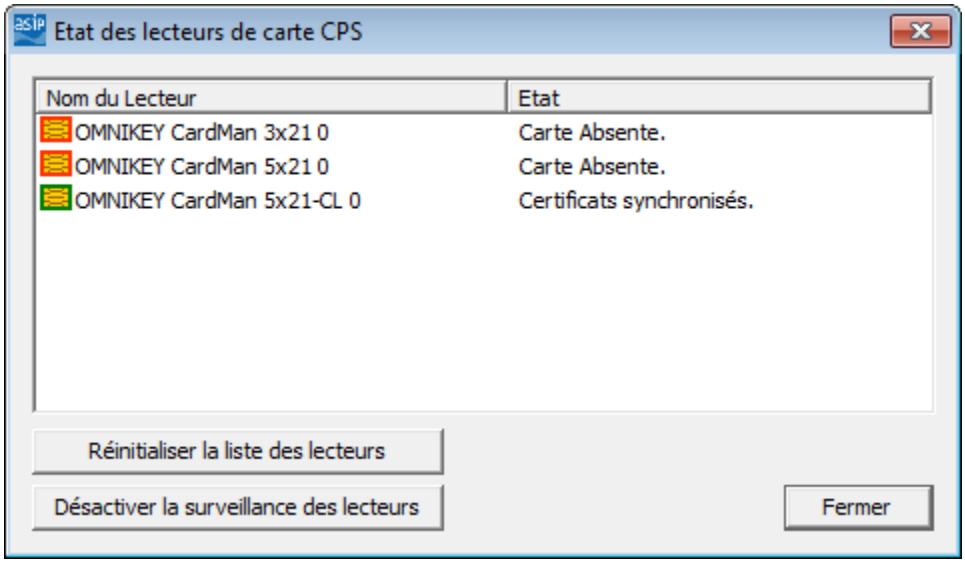


Figure 38 : Enrôlement {contact ; sans-contact} : Sans-Contact : CCM : Synchronisation du certificat sans-contact avec le CCM

Et, sur ouverture du magasin de certificats Microsoft (« Touche Windows > inetcpl.cpl ») :

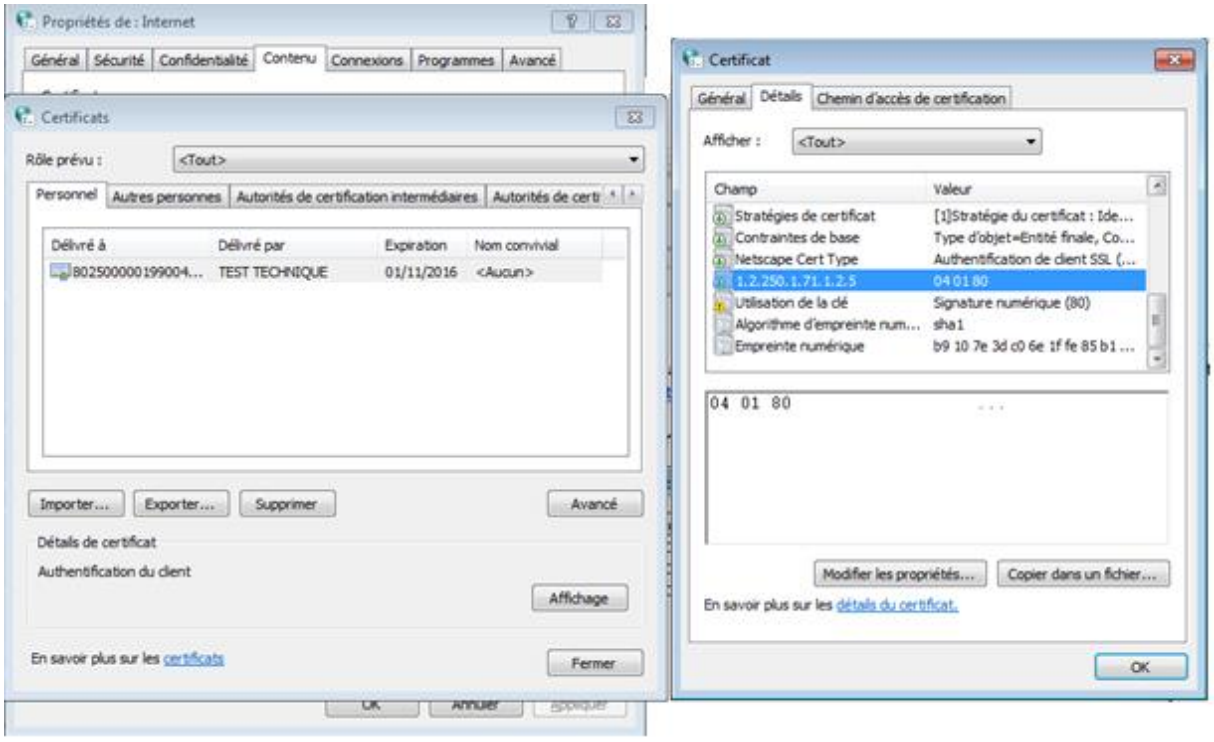


Figure 39 : Enrôlement {contact ; sans-contact} : Sans-Contact : magasin et certificat « technique » sans-contact

On retrouve le caractère « anonyme » de la partie CPx sans-contact : pas de numéro de série de carte, pas de nom de porteur, pas d'UID dans les certificats, ...

L'UID de la partie sans-contact de la carte est cependant accessible en le demandant au lecteur sans-contact :

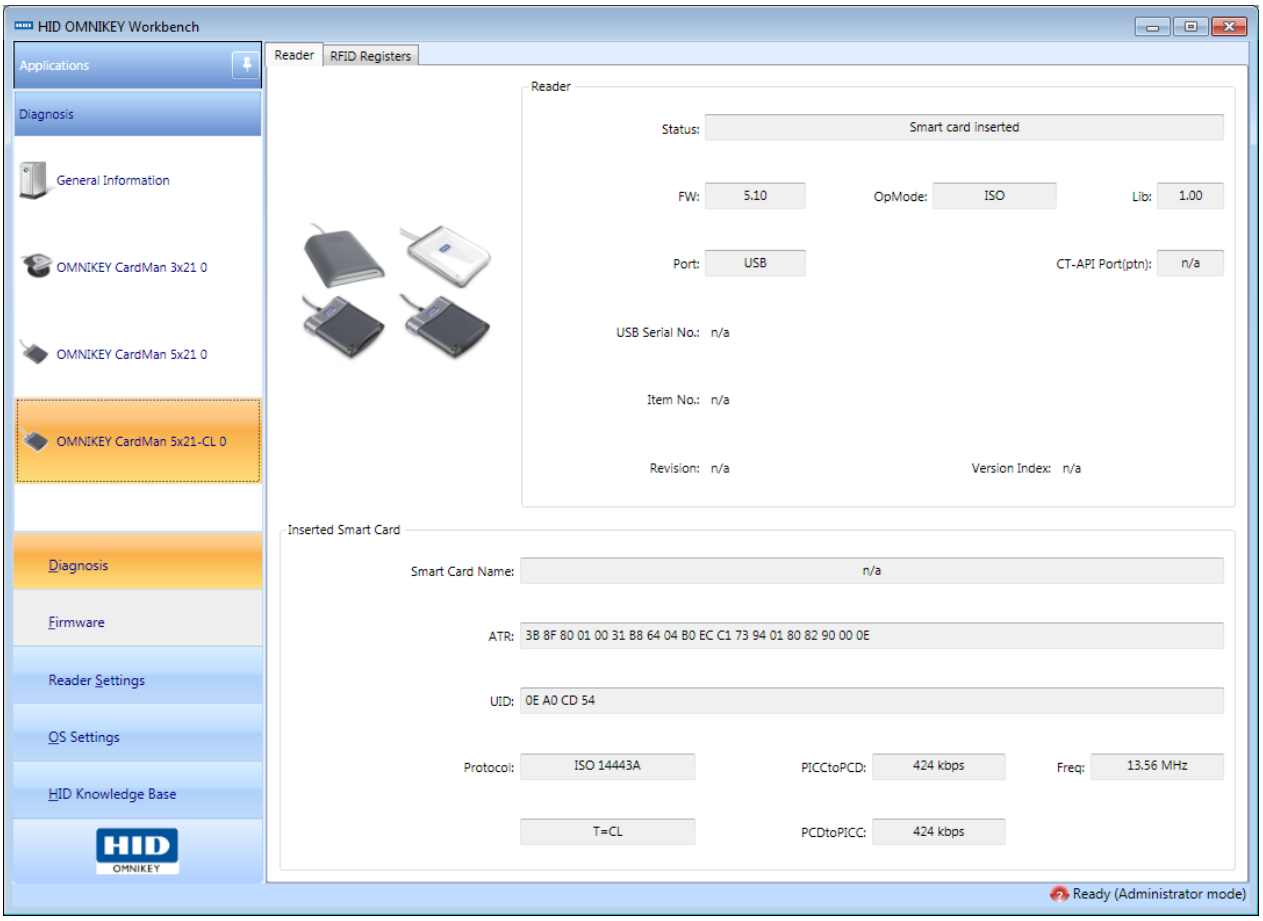


Figure 40 : Enrôlement {contact ; sans-contact} : Sans-Contact : Récupération de l'UID auprès du lecteur sans-contact en utilisant des outils lecteurs propriétaires

13.3.4 Automatisation de l'enrôlement sans-contact d'une carte CPx sous Microsoft Windows avec Java

L'enrôlement {contact ; sans-contact} est automatisable en effectuant les tâches suivantes :

<table>
<tr><th colspan="3">Scénario : Automatisation de l'enrôlement {contact / sans-contact} d'une carte CPx sous Windows</th></tr>
<tr><td rowspan="7">Transaction d'enrôlement d'une carte CPx en sans-contact avec Java</td><td colspan="2">Lancer un « utilitaire logiciel »</td></tr>
<tr><td colspan="2">Début de la transaction</td></tr>
<tr><td rowspan="3">Phase contact</td><td>S'assurer que le(s) lecteur(s) est(sont) branché(s)</td></tr>
<tr><td>Retirer toutes les cartes et s'assurer que le magasin de certificats personnels de Windows est vide</td></tr>
<tr><td>Insérer la carte CPx en mode contact</td></tr>
<tr><td>Phase sans-contact</td><td>Retirer la carte du lecteur quand le logiciel le demande</td></tr>
<tr><td colspan="2">L'« utilitaire logiciel » déduit l'association {numéro de série / SAN …; UID sans-contact}</td></tr>
<tr><td colspan="2">Fin de la transaction</td></tr>
</table>

Tableau 44 : Enrôlement {contact ; sans-contact} : Automatisation avec Java

L'automatisation de la phase d'enrôlement {contact / sans-contact} repose donc sur la conception d'un petit « utilitaire logiciel » (non fourni par l'ASIP Santé, à spécifier pour développement par des intégrateurs). Cet utilitaire sera certain de pouvoir récupérer les informations requises puisqu'elles sont disponibles auprès du système, comme illustré ci-dessus:

1. En consultant le magasin de certificats Microsoft :
    a. En suivant la documentation **[26]**
    b. Java permet d'appeler le CSP Microsoft par l'intermédiaire de JCA (cf. paragraphe « **Intégration via les APIs logicielles / CSP** » du manuel d'installation et d'utilisation de la Cryptolib CPS v5, en particulier le tableau « **Cryptolib CPS v5 : recommandations pour intégration CSP** »).
    c. Cette intégration est illustrée dans la partie « **Intégration de la Cryptolib CPS avec les langages managés / Java** »
        i. Voir en particulier le tableau « **Java/JCA: exemple de code de signature numérique avec la CPx et l'API de cryptographie du JRE** »
        ii. Comme indiqué, Java présente une sérieuse limitation au moment de consulter le magasin de certificats : le tableau **« Niveau d'intégration de la Cryptolib CPS avec Java** » pointe vers le correctif à appliquer

2. En demandant l'UID de la carte au lecteur
    a. Cette opération est normalisée par PC/SC v2
    b. Avec Java 1.6+, l'accès aux ressources PC/SC (lecteur, carte à puce et évènements) est possible via javax.smartcardio (cf. paragraghe « **Intégration via les APIs logicielles** » du manuel d'installation et d'utilisation de la Cryptolib CPS v5, en particulier le tableau « **Cryptolib CPS v5 : recommandations pour intégration PC/SC** »)
    c. L'APDU lecteur normalisé PC/SC v2 permettant de récupérer l'UID - "GetUID" - est :
        i. `final byte[] commandGetUID = {(byte) 0xFF, (byte) 0xCA, (byte) 0x00, (byte) 0x00, (byte) 0x00};`
        ii. À passer à la commande sendCommand :
            1. `sendCommand(currentCardChannel, commandGetUID)`

Ecrit en Java, l'« utilitaire logiciel » permettant de mêler les points 1 et 2 pourrait s'exécuter de la façon suivante :

```
# Insérer la carte dans le lecteur « contact ».
# Le CCM, placé en mode de surveillance automatique,
# passe au vert et alimente le magasin avec les certificats carte CPx
# -> Attendre que le CCM passe au « vert ».
# Lancer l'utilitaire.
# Choix du lecteur en mode contact :
# Utilisation de javax.smartcardio pour assurer l'introduction de la carte CPx dans le lecteur:

[1]             :PC/SC terminal OMNIKEY CardMan 3x21 0, card present: false [default terminal]
[2]             :PC/SC terminal OMNIKEY CardMan 5x21 0, card present: true
[3]             :PC/SC terminal OMNIKEY CardMan 5x21-CL 0, card present: false
Choose one of these card terminals (1-3):
2
Selected: OMNIKEY CardMan 5x21 0
Selected protocol       :*
Connected               :ATR:  3bac00402a00122500648000031000900, Historical: 00122500648000031000900, Protocol: T=0
TRANSMIT                :00a40004023f00, RESPONSE:621e82013883023f00840880250000001ff0100a1088c067affffffff458a01059000
TRANSMIT                :ffca000000, RESPONSE:6e00

# aucun UID car mode contact (normal) :
UID             :

# ouverture du magasin de certificat et parsing du certificat d'authentification par exemple:

IssuerDN                :CN=TEST CLASSE-1, OU=TEST PROFESSIONNEL, O=TEST, C=FR
SubjectDN               :CN=00B1051552 + SURNAME=MAXIMAXIMAXIMAXIMAXIMAX5155 +
GIVENNAME=MUMUMUMUMUMUMUMUMUMUMUMUM, OU=Médecin, O=TEST, C=FR
ASIP Santé Card SerialNumber:2300723698
Subject Alternative Name    :0.0B1051552@carte-cps.fr

# A ce stade de la transaction, le numéro de série ASIP Santé de la carte et le SAN sont récupérés.
# Toutes autres informations utiles contenues dans les certificats (ou les certificats eux-mêmes)
# peuvent être extraites et associées au résultat de la phase suivante (GetUID) :

# Retrait de la carte:
Swap cardreader, hit a key once ready:

# Utilisation de javax.smartcardio pour le choix du lecteur en mode sans-contact :

[1]             :PC/SC terminal OMNIKEY CardMan 3x21 0, card present: false [default terminal]
[2]             :PC/SC terminal OMNIKEY CardMan 5x21 0, card present: false
[3]             :PC/SC terminal OMNIKEY CardMan 5x21-CL 0, card present: true
Choose one of these card terminals (1-3):
3
Selected: OMNIKEY CardMan 5x21-CL 0
Selected protocol       :*
Connected               :ATR:  3b8f80010031b86404b0ecc1739401808290000e, Historical: 0031b86404b0ecc173940180829000, Protocol:
T=1

# Utilisation de javax.smartcardio pour envoi d'APDU:

TRANSMIT                :00a40004023f00, RESPONSE:621e82013883023f00840880250000001ff0100a1088c067affffffff458a01059000
TRANSMIT                :ffca000000, RESPONSE:0ea0cd549000

# Interprétation des réponses APDU:
UID             :0ea0cd54

# Utilisation de JCA pour récupérer le certificat sans-contact (peut être utile…):

IssuerDN                :OU=TEST TECHNIQUE, O=TEST, C=FR
SubjectDN               :CN=8025000001990047679F, O=TEST, C=FR

# A ce stade de la transaction, l'UID est récupéré (à comparer avec les outils logiciels lecteur
propriétaires) et peut être associé aux autres informations cartes récupérées plus tôt.
```

Tableau 45 : Enrôlement {contact ; sans-contact} : Déroulement possible d'un outil Java

13.3.5 Automatisation de l'enrôlement sans-contact d'une carte CPx avec OpenSC

L'enrôlement {contact ; sans-contact} est automatisable en effectuant les tâches suivantes et en se référant à **[Spécifications externes PKCS#11 de la Cryptolib CPS v5], [Les données métier de la CPS3 Volets CPS2ter et IAS]** et **[**Erreur ! Source du renvoi introuvable.**]**:

Scénario : Automatisation de l'enrôlement {contact / sans-contact} d'une carte CPx avec OpenSC		
Transaction d'enrôlement d'une carte CPx en sans-contact avec OpenSC	**Lancer un prompt**	
	Début de la transaction	
	Phase contact	S'assurer que le(s) lecteur(s) est(sont) branché(s)
		Insérer la carte CPx en mode contact
		pkcs11-tool.exe --module cps3_pkcs11_w64.dll --verbose --list-token-slots
		pkcs11-tool.exe --module cps3_pkcs11_w64.dll --verbose --list-objects
		Rem extraction certificat d'authentification : pkcs11-tool.exe --module cps3_pkcs11_w64.dll --type cert --label "**Certificat d'Authentification CPS**" -r --verbose --output-file 01-authent.cer Rem on peut en déduire le SAN, utile en Smartcard logon Rem voir annexe « IGC de santé » de ce manuel : interprétation de données décrite dans **[26]**
		certutil 01-authent.cer
		Rem lecture des informations liées au PS : pkcs11-tool.exe --module cps3_pkcs11_w64.dll --type data --label "**CPS_INFO_PS**" -r --verbose --output-file 02-cps_info_ps.bin Rem interprétation de données décrite dans **[Les données métier de la CPS3 Volets CPS2ter et IAS]**
		Rem lecture des caractéristiques du PS : pkcs11-tool.exe --module cps3_pkcs11_w64.dll --type data --label "**CPS_NAME_PS**" -r --verbose --output-file 03-cps_name_ps.bin
		Rem liste des données PKCS#11 non-protégées et protégées décrite dans **[Spécifications externes PKCS#11 de la Cryptolib CPS v5]** Rem voir tous les objets de la carte avec soumission du code porteur (changer le PIN !): pkcs11-tool.exe --module cps3_pkcs11_w64.dll --verbose --list-objects --login --pin 1234
		Rem lecture de l'activité (changer le PIN !): pkcs11-tool.exe --module cps3_pkcs11_w64.dll --type data --label "**CPS_ACTIVITY_01_PS**" -r --verbose --output-file 04-cps_activity_01_ps.bin --login --pin 1234 Rem interprétation de données décrite dans **[Les données métier de la CPS3 Volets CPS2ter et IAS]**
		Retirer la carte du lecteur
	Phase sans-contact	Poser la carte sur le lecteur sans-contact quand le logiciel le demande
		Rem récupération de l'UID Type A : opensc-tool.exe -s FFCA000000
	On en déduit l'association {numéro de série / SAN …; UID sans-contact} en analysant le contenu des fichiers 01-authent.cer, 02-cps_info_ps.bin, 03-cps_name_ps.bin, 04-cps_activity_01_ps.bin générés	
	Fin de la transaction	

Tableau 46 : Enrôlement {contact ; sans-contact} : Automatisation avec OpenSC

13.4 Enrôlement de cartes à la réception

Un code barre est présent sur le recto de l'enveloppe contenant la carte CPx. Ce code barre contient le **numéro de carte logique** de la carte CPx contenu dans l'enveloppe :

Numéro de carte logique (**idCardLog**), cf.

- Annexe – Numéros de série de la CPx
- **3ième ligne de texte**, en bas à gauche du visuel carte, sous la profession et au-dessus de « expire fin.. »

13.4.1 Principe

Voir **[**Erreur ! Source du renvoi introuvable.**]** pour un rappel sur les échanges de courrier CPx.

L'enveloppe d'envoi de carte CPx ressemble à :

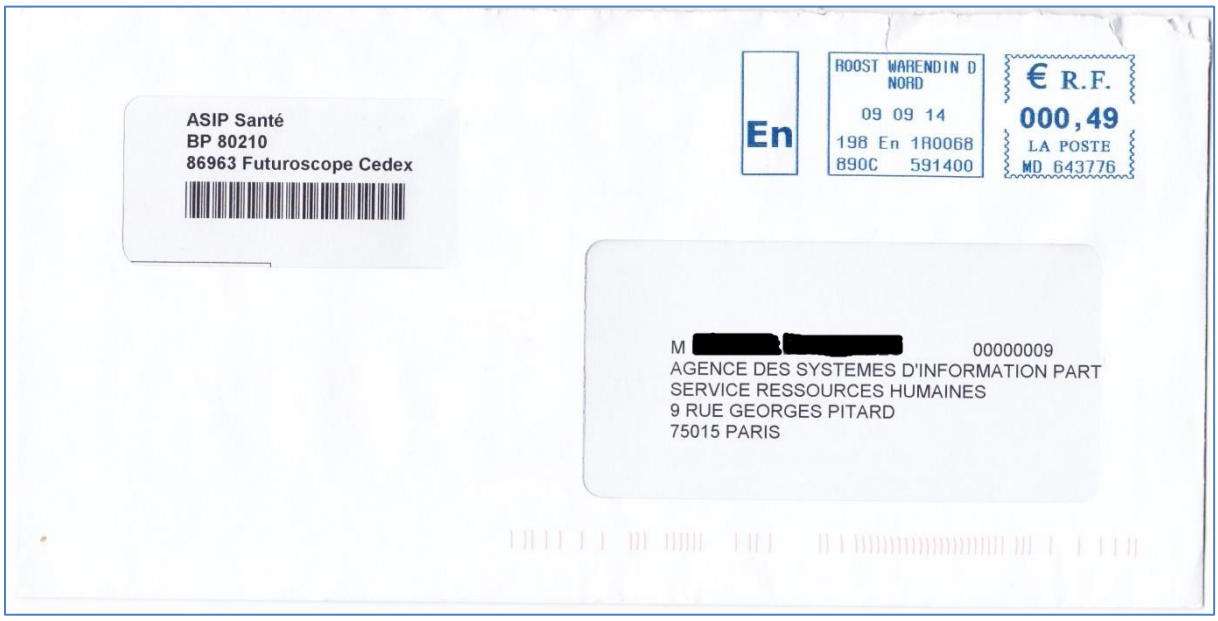


Figure 41 : Enveloppe d'envoi carte CPx

L'encart fenêtré suivant contient un code barre :

Figure 42 : Code barre fenêtré de l'enveloppe d'envoi carte CPx

Ce code barre est un code barre au format « **CODE_39** » qui contient, par exemple, la valeur « **2400140649** » :

Raw text	2400140649
Raw bytes	(Not applicable)
Barcode format	CODE_39
Parsed Result Type	TEXT
Parsed Result	2400140649

Figure 43 : Décodage du code barre fenêtré de l'enveloppe d'envoi carte CPx

Ce code correspond **au numéro logique** de la carte CPx contenue dans l'enveloppe (voir aussi Annexe – Numéros de série de la CPx).

13.4.2 Enrôlement sans-contact d'une carte CPx à la réception

Scénario : enrôlement {contact / sans-contact} d'une carte CPx à la réception		
Transaction	***Début de la transaction***	
	Phase Code barre	Lire **le code barre** présent sur le recto de l'enveloppe contenant la carte CPx **sans ouvrir** l'enveloppe.
		En déduire le **numéro de carte logique** de la carte CPx
	Phase sans-contact	S'assurer que le(s) lecteur(s) sans-contact est(sont) branché(s)
		Poser l'enveloppe, et donc la carte, sur le lecteur sans-contact
		Utiliser des « outils lecteur » : en déduire l'UID sans-contact
	Déduire de la transaction l'association {numéro de carte logique / SAN …; UID sans-contact}	
	Fin de la transaction	

Tableau 47 : Scénario enrôlement {contact / sans-contact} d'une carte CPx à la réception

13.4.3 Automatisation de l'enrôlement sans-contact d'une carte CPx à la réception

<table>
<tr><th colspan="3">Scénario : Automatisation de l'enrôlement {contact / sans-contact} d'une carte CPx à la réception</th></tr>
<tr><td rowspan="6">Transaction</td><td colspan="2">Lancer un « utilitaire logiciel »</td></tr>
<tr><td colspan="2">Début de la transaction</td></tr>
<tr><td rowspan="2">Phase Code barre</td><td>Lire le code barre présent sur le recto de l'enveloppe contenant la carte CPx sans ouvrir l'enveloppe
avec une « douchette » capable de lire du CODE_39
en scannant l'enveloppe et lisant logiciellement le code barre (OCR)</td></tr>
<tr><td>Retirer la carte du lecteur quand le logiciel le demande</td></tr>
<tr><td rowspan="2">Phase sans-contact</td><td>S'assurer que le(s) lecteur(s) sans-contact est(sont) branché(s)</td></tr>
<tr><td>Poser l'enveloppe, et donc la carte, sur le lecteur sans-contact quand le logiciel le demande</td></tr>
<tr><td colspan="2">L'« utilitaire logiciel » déduit l'association {numéro de carte logique / SAN …; UID sans-contact}</td></tr>
<tr><td colspan="2">Fin de la transaction</td></tr>
</table>

Tableau 48 : Automatisation de l'enrôlement {contact / sans-contact} d'une carte CPx à la réception

13.5 Déploiements possibles de l'outil

Cette problématique d'enrôlement se pose essentiellement en entreprise ou en établissement.

Un outil développé spécifiquement pour accomplir cette fonctionnalité peut être déployé :

- Si l'outil est en Java :
  - Soit dans une application légère sous forme d'une applet
    - Attention dans ce cas aux problématiques de compatibilité avec les navigateurs ciblés, aux « pop-ups » / à l'ergonomie utilisateur, aux mécanismes de type « Click-&-Play »
  - Soit dans une application lourde de type Swing
    - déployée par JNLP
    - déployée via les outils d'infrastructure du SI (scripts d'ouverture de sessions, disques en partage…)
- Si l'outil est natif :
  - Avec les technologies d'installeurs des plates-formes cible (MSI, PKG, RPM…)

14Annexe – Diagrammes de séquence

14.1 Annexe – Diagramme de séquence associé au contrôle d'accès physique en type A sur la base de l'UID Mifare

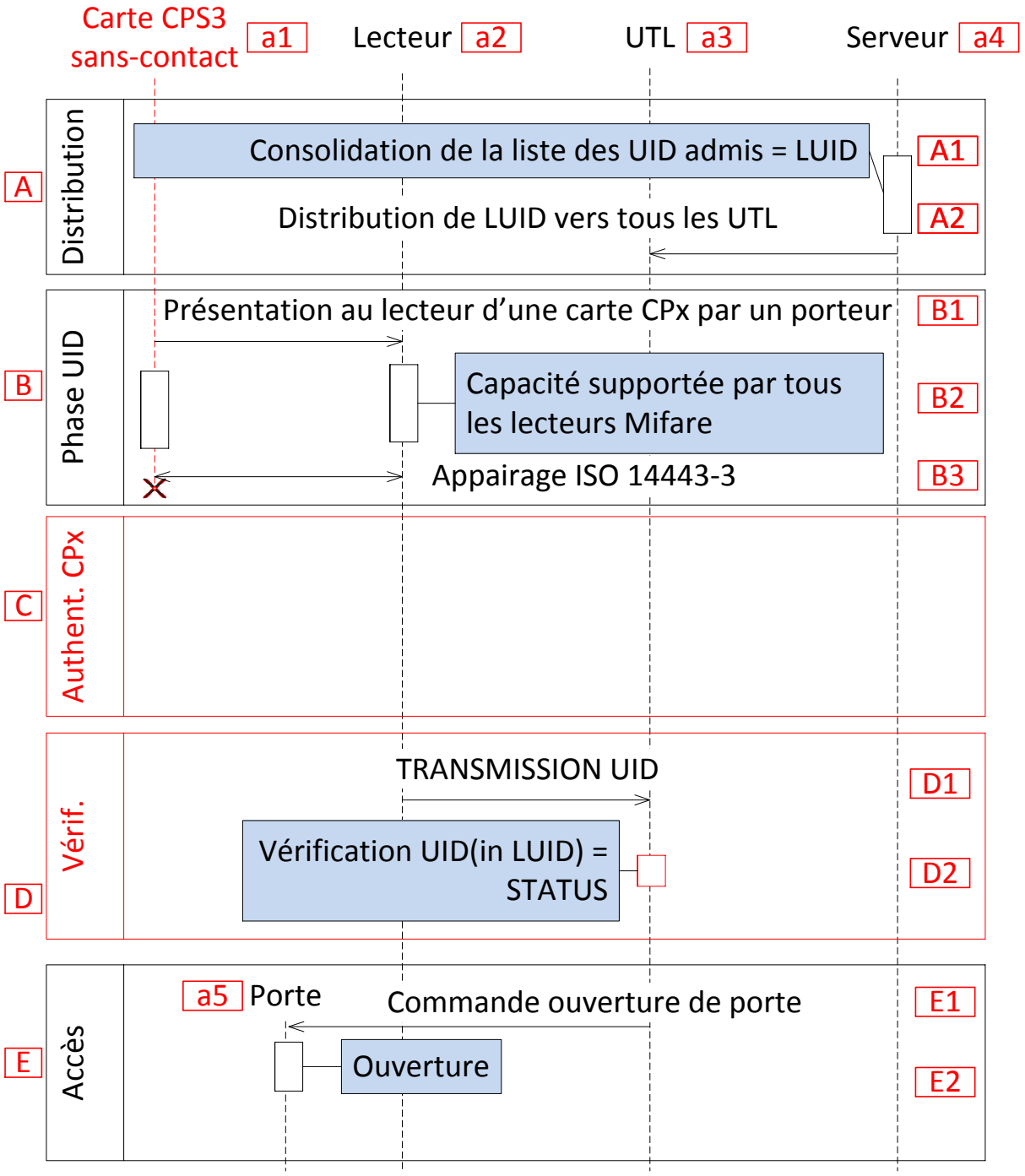


Figure 44 : Diagramme de séquence associé au contrôle d'accès physique en type A sur la base de l'UID Mifare

Les remarques sont :

#	Remarque
[a1]	La courte ligne de vie de la carte CPx dans les échanges carte-lecteur est due au fait que seul le niveau ISO 14443 est utilisé.
[C]	L'absence d'authentification CPx.
[D2]	Une simple vérification de présence de l'UID détecté dans une liste blanche en guise de vérification.

Tableau 49 : remarques liées au diagramme de séquence associé au contrôle d'accès physique en type A sur la base de l'UID Mifare

14.2 Annexe – Diagramme de séquence associé au cas du « lecteur générique IAS-ECC et autonome »

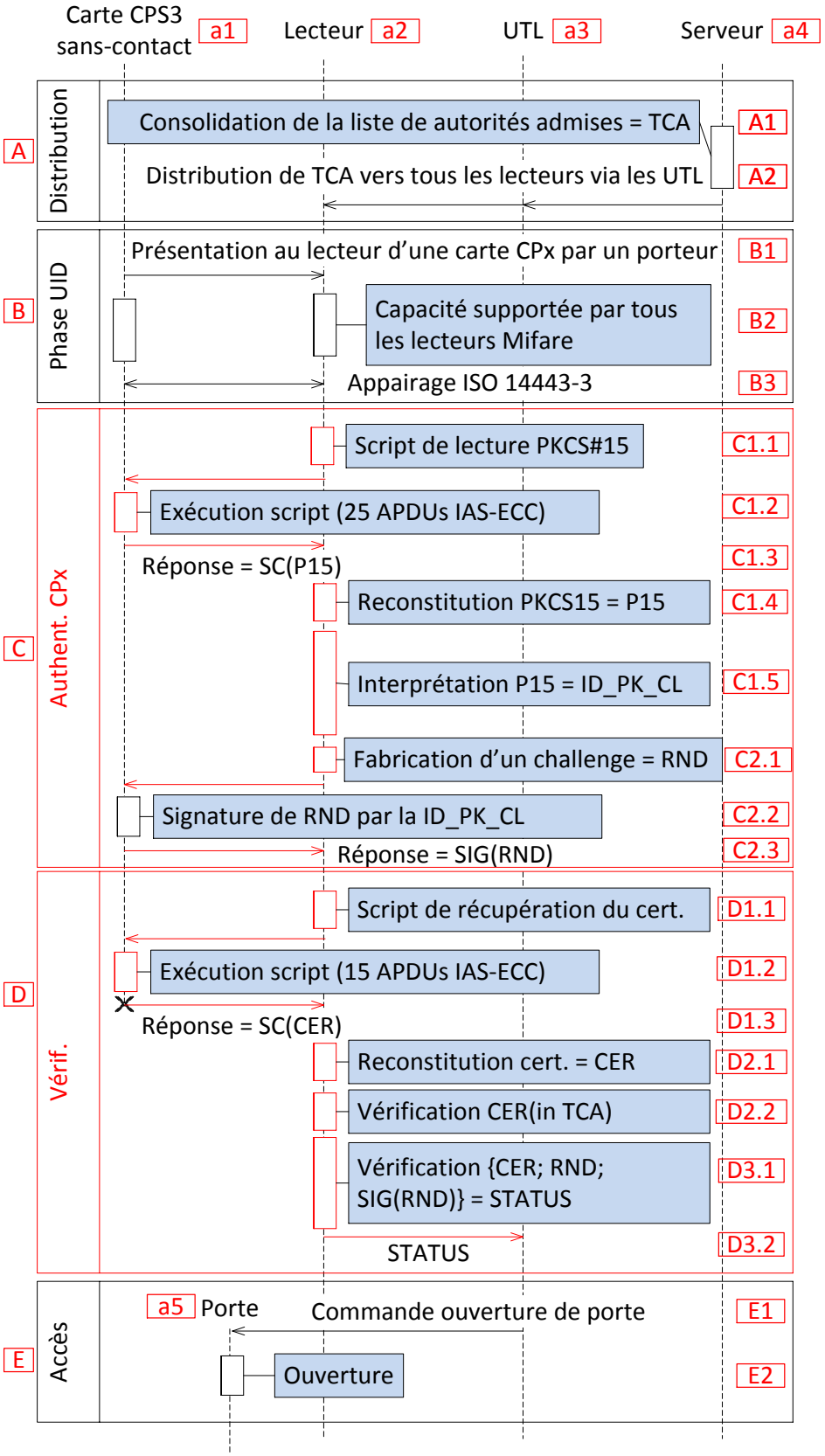


Figure 45 : Diagramme de séquence associé au cas du « lecteur générique IAS-ECC et autonome »

Les remarques particulières par rapport à la séquence présentée, plus haut :

#	Remarque
[A1]	De façon générique, seule la liste des autorités de certification de confiance est distribuée sur les lecteurs depuis un serveur de gestion centralisé. Mais, en pratique : • il faudrait aussi distribuer des CRLs • il vaudrait mieux constituer des listes blanches de certificats (pour ne pas accepter systématiquement les cartes de l'ES voisin par exemple)
[A2]	Les lecteurs doivent alors avoir les capacités mémoires (ROM et RAM) nécessaires afin d'exploiter les listes reçues.
[a1]	La ligne de vie de la carte CPx est plus longue que précédemment du fait que le lecteur demande à la carte de s'authentifier (échanges d'APDU supplémentaires après la récupération de l'UID).
[B]	La phase de récupération de l'UID est une brique de base, commune à tous les scénarios envisageables.
[C]	La phase générique d'authentification de la carte CPx impose la lecture et l'interprétation des structures PKCS#15 contenues dans la carte CPx. Ces structures assurent l'interopérabilité de la carte CPx et permettent ici de retrouver l'identifiant de clé sans-contact afin de lui demander d'effectuer l'opération d'authentification.
[D]	La phase de vérification est plus simple que la précédente mais reste coûteuse en temps.
[a3]	L'UTL ne porte aucune complexité dans ce scénario.

Tableau 50 : remarques liées au diagramme de séquence associé au cas du « lecteur générique IAS-ECC et autonome »

14.3 Annexe – Diagramme de séquence associé au cas du « lecteur transparent et UTL intelligent »

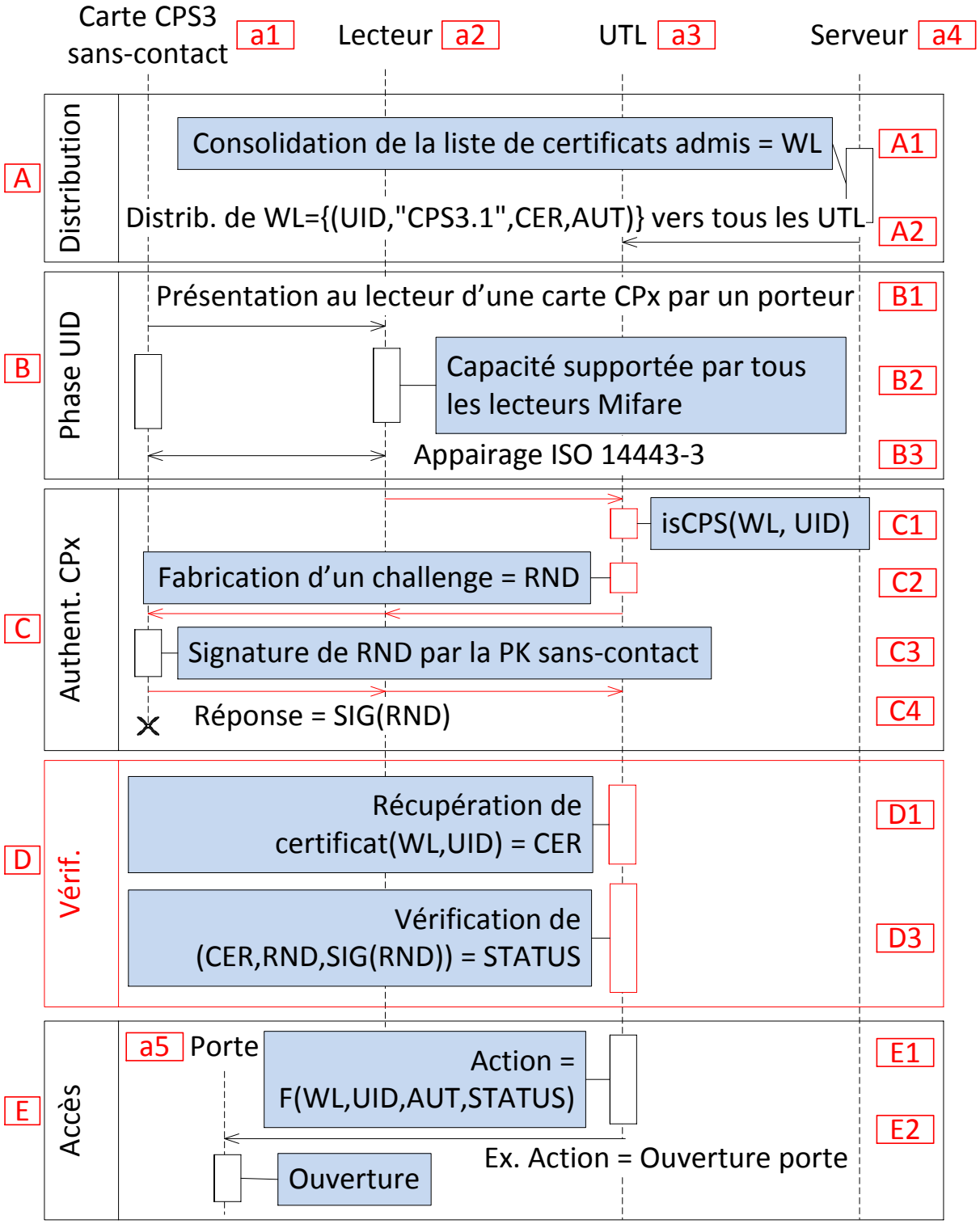


Figure 46 : Diagramme de séquence associé au cas du « lecteur générique IAS-ECC et autonome »

Les remarques sont :

#	Remarque
[A1]	La liste blanche (WL) à consolider nécessaire à ce scénario peut par exemple prendre la forme de quadruplets (UID, Type carte = "CPS3.1", Certificat d'authentification sans-contact de la carte CPx, autorisations). La mise en place d'un système d'enrôlement permet de construire quotidiennement une WL. Cette opération est l'occasion de vérifier le statut des certificats et d'en extraire les clés publiques. ⇨ L'inclusion du type de carte ("CPS3.1" seulement pour l'instant) permet d'anticiper les situations où plusieurs générations de carte CPx cohabitent, ce qui n'est pas exclu à moyen-long terme mais aussi de faire cohabiter le sans-contact CPx avec d'autres cartes sans-contact. ⇨ Compter 1600 octets par enregistrement (16 + 16 + 1024 + 512) ○ 300 cartes : 480 ko ○ 2000 cartes : 3 Mo ○ 20000 cartes : 30 Mo ○ 120000 cartes : 183 Mo ⇨ Pour les 2 derniers cas ○ La gestion d'un grand nombre de cartes est souvent liée à une dispersion sur plusieurs sites différents ▪ subdiviser la liste principale en listes nominales de cartes par site ▪ gérer les déplacements inter-site en « lazy-loading » ⇨ En lieu et place du certificat, seule la clé publique peut être distribuée (256 bytes au lieu de 1024) ce qui divise la taille des fichiers par 2.
[a2]	Pas de changement des lecteurs si ces derniers supportent le mode transparent. ⇨ D'où l'importance de retenir ce type de lecteur lors de tout nouveau projet. Le nombre total de lecteurs à installer dépend de la configuration des sites, de la stratégie sans-contact retenue (en conjonction avec d'autres moyens d'accès -sas, portiques…) et des fonctionnalités retenues (l'anti-passback requiert des lecteurs en sortie par exemple). A titre indicatif, compter : • 8 lecteurs par zone d'accueil + 1 UTL • 4 lecteurs par couloir (2 portes, 2 accès de secours) + 1 UTL • 2 lecteurs par niveau de parking + 1 UTL • 1 lecteur par zone spéciale (locaux informatiques, UTL factorisé avec celui de l'étage) • Y ajouter les lecteurs pour les postes de travail et les imprimantes si ces scénarios sont retenus
[a3]	Capacités des UTL plus en adéquation avec la cryptographie et les vérifications induites.
[C][D]	Bonne réactivité du système • **4 APDUs** IAS-ECC pour **300 bytes** transmis seulement et **50 ms** d'exécution, voir « Annexe – IAS-ECC avec la CPx en sans-contact » ○ attention à la compatibilité de ce volume de données avec Wiegand (mots de 64bits) • Pas d'APDU de lecture des structures PKCS#15 • Pas de temps d'analyse des structures PKCS#15 • Pas d'APDU de lecture du certificat
Point d'attention	UTL avec des capacités spécifiques liées à la carte CPx. ⇨ D'où l'importance de retenir des UTL susceptibles d'être facilement mis à jour.

Tableau 51 : remarques liées à l'utilisation en « lecteur transparent et UTL intelligent »

15Annexe – IAS-ECC avec la CPx en sans-contact

15.1 Concessions des spécifications de la carte CPx

Le détail des APDUs IAS-ECC permettant de communiquer avec la carte CPx est communiqué par l'ASIP Santé après signature de la convention de concessions des spécifications de la carte CPx **[Procédure de concessions des spécifications de la carte CPS3]**.

Cette spécification couvre toutes les fonctions de la carte :

- Volet contact et sans-contact
- Système de fichiers
- Opérations cryptographiques
- Accès aux objets métiers

Les informations suivantes sont fournies pour permettre au lecteur d'évaluer spécifiquement la complexité des APDUs à mettre en œuvre en sans-contact avec la carte CPx en renvoyant aux sections idoines de la spécification IAS-ECC, l'exhaustivité des informations, y compris pour le sans-contact ou pour la partie « conteneur de données », restant sous couvert de la concession **[Procédure de concessions des spécifications de la carte CPS3]**.

15.2 Signature de données à destination d'authentification

15.2.1 Calcul du condensat

Pour effectuer la signature d'une donnée en vue de réaliser une authentification, par exemple la signature d'un jeton, le système doit préalablement « condenser » (« hasher ») le jeton et soumettre à la carte le condensat (« hash ») obtenu pour signature.

Le standard à suivre pour cette opération est PKCS#1 (RFC3447, voir les sections relatives aux DigestInfo et les « notes » page 42 de http://tools.ietf.org/html/rfc3447 pour d'autres exemples d'encodage ASN.1 des DigestInfo).

Le résultat du hachage des données soumises ne peut pas dépasser 102 bytes.

Les 3 mécanismes de hachage supportés par la clé d'authentification technique sont :

- SHA-1
- SHA-256
- SHA-512

(Voir http://tools.ietf.org/html/rfc3447#appendix-B.1 pour les OIDs associés).

15.2.2 Signature du condensat par la carte CPx

Le « hash » est soumis à la carte en utilisant la commande INTERNAL AUTHENTICATE.

Les données soumises au format PKCS#1 sont signées, sans interprétation, par la clé privée d'authentification technique de la carte.

Avant d'exécuter la commande INTERNAL AUTHENTICATE, l'IFD (ici l'IFD est le lecteur sans-contact ou l'UTL) doit positionner le contexte de sécurité de la carte correctement. Dans le cas de la CPx, il s'agit de spécifier le CRT « Client/Server Authentification » (page 91, page 148 et page 200 de ias_ecc_v1_0_1_fr.pdf).

15.2.3 Résumé des échanges

#	Description
1	Génération des données à signer **HASH**: 1- Génération d'un aléa **DATA** de 20, 32 ou 64 bytes de long puis hachage de **DATA** donne **HASH** 2- Hachage de **DATA** = {jeton d'authentification} donne **HASH**
2	Soumission des données à signer **HASH** à la carte et récupération de la signature **SIG**. La réponse de la carte est une signature de longueur 256 bytes.
3	La signature est vérifiable avec la clé publique d'authentification technique de la carte **CER.PUB_KEY** contenue dans le certificat d'authentification technique de la carte accessible en lecture sans contrainte de sécurité. La vérification de la signature est effectuée par l'entité qui souhaite authentifier la carte (l'UTL par exemple). Si **CER.PUB_KEY**.Verify(**DATA**, **SIG**) retourne "**true**" la carte est bien celle que l'on pense être et l'accès est autorisé, sinon l'accès est refusé.

Figure 47 : Résumé des échanges carte

15.2.4 Vecteurs de test

Cas de test Ces vecteurs de test permettent de vérifier l'opération de vérification à embarquer dans l'UTL

Tableau 52 : Cas de test pour l'authentification de la carte CPx en sans-contact

Les 3 exemples qui suivent donnent les réponses cartes pour les 3 méthodes SHA-1, SHA-256 et SHA-512 et sont vérifiables avec la clé publique spécifiée dans la partie « données ».

15.2.4.1 Données

CER.PUB_KEY	PKCS#8	30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00		
		Affiché sous « Clé Publique » dans le viewer de certificats Windows	Séquence	30 82 01 0A
			Entier	02 82 01 01
			Modulus	00 CE 06 A1 1D AB 1A C9 AF 72 0C 7C 3E 7C 8F CA BD 4A 2D 94 EA 08 BA F4 75 5C A4 DB 7B 45 68 77 3B BA 8C 69 B8 38 41 75 04 A6 DD 31 05 19 14 F4 4A FE 1E 73 6D 16 26 41 6A 58 D7 E4 0F AF A9 87 12 FA 44 08 C9 0A 63 D5 CF CC 28 3E 3D CF 63 36 61 5E F9 3A 23 13 60 F9 FB 0B 40 A5 15 94 A4 63 8C F6 54 B3 73 DF 24 88 47 39 E3 8E 62 9B 3B DB DD 85 CD 53 D7 8A 3B 74 53 71 D2 E9 05 6A 43 48 CE 34 FD AC 7E F9 8B BD 08 D2 8B A1 15 6C 34 B9 3B 8F 0C 4E C4 27 16 83 FD 35 F2 D9 89 B1 C0 09 8F 8D 8E EC 9B F0 B5 DB F2 9A 23 67 52 A6 59 9D 2E 5E 81 EE 18 02 71 AF A9 C1 7A CF 93 1B 72 3E 92 F6 85 9E 4E 04 63 30 F9 C1 FC 5D B0 28 EE 1F 0C F2 D8 CB 5F 5A E4 B5 F1 DC 06 C6 A2 D0 37 99 BD C6 3F 87 52 B4 DA 84 90 1F DB 6F 8C 87 11 77 36 D9 D8 FE 7D 1C BC 5D 9F F9 BF 2F 32 F8 42 AC A3
			Entier	02 03
			Exponent	01 00 01

Tableau 53 : Vecteur de test: Clé publique

DATA	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Tableau 54 : Vecteur de test: Données

SHA1(DATA)	E1 29 F2 7C 51 03 BC 5C C4 4B CD F0 A1 5E 16 0D 44 50 66 FF
SHA256(DATA)	37 47 08 FF F7 71 9D D5 97 9E C8 75 D5 6C D2 28 6F 6D 3C F7 EC 31 7A 3B 25 63 2A AB 28 EC 37 BB
SHA512(DATA)	0B 6C BA C8 38 DF E7 F4 7E A1 BD 0D F0 0E C2 82 FD F4 55 10 C9 21 61 07 2C CF B8 40 35 39 0C 4D A7 43 D9 C3 B9 54 EA A1 B0 F8 6F C9 86 1B 23 CC 6C 86 67 AB 23 2C 11 C6 86 43 2E BB 5C 8C 3F 27

Tableau 55 : Vecteur de test: Hasches des données (SHA1, SHA256 et SHA512)

15.2.4.2 SHA1withRSA

15.2.4.2.1 Message envoyé à la carte

30	
21	
30	
09	
06 05 2B 0E 03 02 1A	OID SHA-1
05 00	
04	
14	20 bytes
E1 29 F2 7C 51 03 BC 5C C4 4B CD F0 A1 5E 16 0D 44 50 66 FF	Valeur du **SHA-1**(**DATA**)

Tableau 56 : Vecteur de test: Message vers la carte (SHA1)

15.2.4.2.2 Réponse carte

28	9C	A0	22	C2	7B	16	94	95	6A	D1	63	90	A4	D4	42
04	24	E2	AF	43	79	32	08	6F	B7	E7	39	EE	46	57	34
17	F0	AD	B1	E8	C5	9E	BD	99	E2	33	03	C6	33	16	F7
B4	DD	22	B6	D5	B0	DF	B2	96	A1	F5	26	1A	86	A1	15
68	AA	22	EF	02	E8	BD	73	77	78	62	F3	C6	DD	BB	B4
8E	55	D3	FF	C4	72	CF	66	FC	35	C2	3C	AE	08	18	53
77	81	E9	D6	78	CB	6F	30	39	02	73	AB	5E	5E	A7	7F
69	E0	48	3B	52	4B	46	AE	3E	72	96	FF	5E	A0	80	E3
D5	8E	37	D3	A3	95	C1	67	6A	74	91	EF	31	72	78	7F
F1	C6	60	65	A8	61	A8	FD	07	7C	DA	79	85	15	EE	1F
34	C5	C5	42	1B	2F	82	25	8A	20	21	01	70	27	4C	6A
3C	A6	F7	39	27	12	B8	A1	D0	2B	4E	88	63	0A	39	7E
04	C8	20	28	6B	AB	F5	A9	1A	58	19	1F	C5	23	F2	CB
9D	96	95	9B	A8	78	17	34	60	E3	22	85	DA	D1	93	FE
AC	22	A5	2F	77	E7	1D	DE	CB	7D	0D	11	29	94	5D	99
CA	DB	45	F8	CF	A0	BB	76	7A	74	1D	9B	F5	FE	9A	4B

Tableau 57 : Vecteur de test: Réponse de la carte (SHA1)

15.2.4.3 SHA256withRSA

15.2.4.3.1 Message envoyé à la carte

30	
31	
30	
0D	
06 09 60 86 48 01 65 03 04 02 01	OID SHA-256
05 00	
04	
20	32 bytes
37 47 08 FF F7 71 9D D5 97 9E C8 75 D5 6C D2 28 6F 6D 3C F7 EC 31 7A 3B 25 63 2A AB 28 EC 37 BB	Valeur du **SHA-256**(**DATA**)

Tableau 58 : Vecteur de test: Message vers la carte (SHA256)

15.2.4.3.2 Réponse carte

```
20 B5 39 F8 EC 57 83 5B EF 90 2A 30 5B D9 B7 C2
3E E4 69 A8 18 DF 32 45 4E 2A 11 A7 FF 03 3E 21
BA 5E 67 40 FF 84 72 57 61 70 8D 4E 26 80 20 A1
A5 70 75 CD BA 8D 9F FE E9 D2 91 C0 41 EE 7B BD
21 37 F8 D3 30 8A D9 7F F4 FB ED EF 0B 94 BB FB
6A 06 4A 4A B8 AE 8F 9A 4B EF 6D 34 64 F2 27 66
D9 45 96 15 8E C2 94 20 20 37 E5 AF A0 32 28 A8
FD B7 78 EF 38 11 1D 84 83 E8 11 E3 E1 1A DD B1
BD 85 84 51 D8 EF 1E 5E 3E DA 21 CC 1F AF 56 F0
98 BB 1F 49 C3 A7 E8 5D EE 1F 2B 8A 64 10 55 29
1E C8 72 F7 7E EC E7 91 35 4B AA 5D 92 53 06 44
F0 A2 4A C6 B0 36 E6 19 B5 F2 5E 79 60 F5 02 D1
68 3D 40 DB E0 4F 88 DC D7 EE E1 2C A3 53 F1 5F
F7 6B 2C 0C 80 93 71 71 67 57 31 F8 26 87 C5 3B
EE F4 11 D1 80 6D 3F 62 D7 0B 74 BD 8C C0 EB D9
94 DE 21 52 CE 5F E4 BC 81 65 EF 90 6E F8 60 21
```

Tableau 59 : Vecteur de test: Réponse de la carte (SHA256)

15.2.4.4 SHA512withRSA

15.2.4.4.1 Message envoyé à la carte

30	
51	
30	
0D	
06 09 60 86 48 01 65 03 04 02 03	OID SHA-512
05 00	
04	
40	64 bytes
0B 6C BA C8 38 DF E7 F4 7E A1 BD 0D F0 0E C2 82 FD F4 55 10 C9 21 61 07 2C CF B8 40 35 39 0C 4D A7 43 D9 C3 B9 54 EA A1 B0 F8 6F C9 86 1B 23 CC 6C 86 67 AB 23 2C 11 C6 86 43 2E BB 5C 8C 3F 27	Valeur du **SHA-512**(**DATA**)

Tableau 60 : Vecteur de test: Message vers la carte (SHA512)

15.2.4.4.2 Réponse carte

```
6D C1 1F 5C E1 72 0A FD 9A 21 4E CE 7A 91 19 4D
0D AD 16 5C E1 D4 A8 C7 C5 4B 44 A0 D2 B6 B5 34
1E AC 78 C5 45 DF 5A C4 15 63 28 72 8D 6D 86 75
94 07 73 E2 5A 2C D5 8E DB B6 52 E7 AC B5 EA FE
96 D1 94 95 0D 13 63 D0 4A DA 53 D8 68 DE E8 9F
E2 4C C8 61 53 52 3B C6 EC 31 61 E9 B1 53 9D 34
20 84 FB 70 86 B0 89 4A 54 3D 4A 22 A4 AD 9F E8
D5 BF A0 1F F6 A5 16 E0 DF C0 BD 38 51 11 A3 BA
48 BC 79 15 1E 7D F6 7F 84 93 5F FA 95 35 D9 D8
D3 8A 26 AE 29 03 48 03 C7 A8 8B 73 7D B4 74 98
C6 AA 98 9D 7F 92 5A 63 2C D1 18 F4 67 64 0E 0A
7E 9C 65 A6 1B 69 D5 D4 FE 74 71 0B AA 28 94 0C
5B 5C 3B EA 21 BF 47 FC DA B7 83 61 0C 70 DD 8B
37 B9 29 43 FE 49 8C A6 8B D4 71 EA B8 9E 0D 8D
39 D3 52 2C 00 8E 6A 2E 45 77 8A D4 90 F7 FD 4B
69 5F F7 BC B5 2A BF 9C B9 E6 4A 24 1F 60 36 F7
```

Tableau 61 : Vecteur de test: Réponse de la carte (SHA512)

15.2.5 Exemples de production de signature

15.2.5.1 Production de signature avec OpenSSL

Cf. **[22] OpenSSL et mod_ssl avec les produits de certification ASIP-Santé**

Chapitre 11 "Utilisation de la carte CPS avec le moteur PKCS#11 OpenSC pour OpenSSL"

Section 11.7 "Utilisation en sans-contact"

Et Section 11.5.5 "Hachage et signature d'un fichier"

15.2.5.2 Production de signature avec Java

Cf. **[1] Manuel d'installation et d'utilisation de la Cryptolib CPS**

Section 19.6.1 Intégration de la Cryptolib CPS avec les langages managés / Java

15.2.5.3 Production de signature avec C#

Cf. **[1] Manuel d'installation et d'utilisation de la Cryptolib CPS**

Section 19.6.2 Intégration de la Cryptolib CPS avec les langages managés / .NET

15.2.5.4 Production de signature via les APDUs IAS-ECC

Les APDUs IAS-ECC requis pour communiquer avec la carte CPS sont documentés via **[16] Procédure de concessions des spécifications de la carte CPS3**.

Il est cependant très facile d'appliquer IAS-ECC à la CPS3 en sans-contact et d'en déduire les APDUs de demande de signature d'un condensat à envoyer à la CPS3.

#	Commande	Réponse
1	**SELECT**	
1.1	00 A4 09 04 04 3F 00 00 01	62 23 82 01 38 83 02 00 01 84 0D E8 28 BD 08 0F 80 25 00 00 01 FF 00 10 A1 08 8C 06 7A FF FF FF FF 45 8A 01 05 [90 00]
2	**MSE SET**	
2.1	00 22 41 A4 06 80 01 02 84 01 83	[90 00]
3	**INTERNAL AUTHENTICATE (Exemple avec SHA1)**	
3.1	00 88 00 00 23 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 E1 29 F2 7C 51 03 BC 5C C4 4B CD F0 A1 5E 16 0D 44 50 66 FF	28 9C A0 22 C2 7B 16 94 95 6A D1 63 90 A4 D4 42 04 24 E2 AF 43 79 32 08 6F B7 E7 39 EE 46 57 34 17 F0 AD B1 E8 C5 9E BD 99 E2 33 03 C6 33 16 F7 B4 DD 22 B6 D5 B0 DF B2 96 A1 F5 26 1A 86 A1 15 68 AA 22 EF 02 E8 BD 73 77 78 62 F3 C6 DD BB B4 8E 55 D3 FF C4 72 CF 66 FC 35 C2 3C AE 08 18 53 77 81 E9 D6 78 CB 6F 30 39 02 73 AB 5E 5E A7 7F 69 E0 48 3B 52 4B 46 AE 3E 72 96 FF 5E A0 80 E3 D5 8E 37 D3 A3 95 C1 67 6A 74 91 EF 31 72 78 7F F1 C6 60 65 A8 61 A8 FD 07 7C DA 79 85 15 EE 1F 34 C5 C5 42 1B 2F 82 25 8A 20 21 01 70 27 4C 6A 3C A6 F7 39 27 12 B8 A1 D0 2B 4E 88 63 0A 39 7E 04 C8 20 28 6B AB F5 A9 1A 58 19 1F C5 23 F2 CB 9D 96 95 9B A8 78 17 34 60 E3 22 85 DA D1 93 FE AC 22 A5 2F 77 E7 1D DE CB 7D 0D 11 29 94 5D 99 CA DB 45 F8 CF A0 BB 76 7A 74 1D 9B F5 FE 9A 4B [90 00]

Tableau 62 : Production de signature CPx via les APDUs IAS-ECC (SHA1)

15.2.6 Exemples de vérification de signature

Vérification de signature CPx : un bon exemple d'interopérabilité	La vérification de la signature produite par la carte CPx est l'occasion d'illustrer l'interopérabilité induite par l'utilisation systématique de standards reconnus.

Tableau 63 : Vérification de signature CPx : un bon exemple d'interopérabilité

15.2.6.1 Vérification de signature avec OpenSSL

Commande	Description
%OPENSSL_EXE%	
x509	https://www.openssl.org/docs/apps/x509.html
-inform DER	
-in **%1**	**%1** est le fichier contenant le certificat sans-contact au format DER (**CER**)
-pubkey	
-noout	
| %OPENSSL_EXE% enc -base64 -d > **%2**	Redirection vers le fichier **%2** contenant la clé publique au format DER (**CER.PUB_KEY**)

Figure 48 : Extraction de la clé publique du certificat sans-contact

Commande	Description
openssl rsautl -in %1 -verify -asn1parse -inkey %2 -pubin	
%OPENSSL_EXE%	
rsautl	https://www.openssl.org/docs/man1.0.1/apps/rsautl.html
-in **%1**	**%1** est le fichier contenant la **signature (SIG)** (binaire)
-verify	
-asn1parse	**[optionnel]** Dans nos cas, les données obtenues par le déchiffrement de la signature sont des données ASN1.
-**inkey %2**	**%2** est le fichier contenant la clé publique au format **PEM.** Avec OpenSSL, le PEM d'une clé publique au format PKCS#8 doit commencer par -----BEGIN PUBLIC KEY----- et finir par -----END PUBLIC KEY-----
-pubin	

Le résultat de la vérification peut être (cas du vecteur de test SHA256 ici) :

```
Loading 'screen' into random state - done
   0:d=0  hl=2 l=  49 cons: SEQUENCE
   2:d=1  hl=2 l=  13 cons:  SEQUENCE
   4:d=2  hl=2 l=   9 prim:   OBJECT         :sha256
  15:d=2  hl=2 l=   0 prim:   NULL
  17:d=1  hl=2 l=  32 prim:  OCTET STRING
    0000 - 37 47 08 ff f7 71 9d d5-97 9e c8 75 d5 6c d2 28   7G...q.....u.l.(
    0010 - 6f 6d 3c f7 ec 31 7a 3b-25 63 2a ab 28 ec 37 bb   om<..1z;%c*.(.7.
```

Figure 49 : Déchiffrement de la signature RSA avec la clé publique et la commande rsautl

Si le résultat du déchiffrement correspond au message envoyé à la signature (**PADDING(SHA-X, SHA-X(DATA))**), la signature est correcte (c'est le cas ici).

Ce test de correspondance est automatisé par la commande "**dgst**":

Commande	**Description**
%OPENSSL_EXE%	
dgst	https://www.openssl.org/docs/apps/dgst.html
-**%1**	**%1** vaut sha1, sha256 ou sha512
-keyform **DER**	
-verify **%2**	**%2** est le fichier contenant la **clé publique** au format **DER**
-signature **%3**	**%3** est le fichier contenant la **signature** (**SIG**) (binaire)
%4	**%4** est le fichier contenant les données à signer (**DATA**)
Le résultat de la vérification peut être : « **Verification Failure** » ou « **Verified OK** »	

Figure 50 : Vérification de la signature avec la commande dgst

15.2.6.2 Vérification de signature avec Java

Le code Java suivant vérifie les 3 signatures présentées plus haut (noter que les valeurs sont en dur et le code répété 3 fois par souci pédagogique, cette pratique n'étant pas à reproduire en production) :

```
// ASIP Santé: key:
final PublicKey pubKey = KeyFactory.getInstance("RSA").generatePublic(
        new RSAPublicKeySpec(
                new BigInteger(ToolsImpl.fromHexString(
                        "00"
                      + "CE06A11DAB1AC9AF720C7C3E7C8FCABD4A2D94EA08BAF4755CA4DB7B4568773B"
                      + "BA8C69B838417504A6DD31051914F44AFE1E736D1626416A58D7E40FAFA98712"
                      + "FA4408C90A63D5CFCC283E3DCF6336615EF93A231360F9FB0B40A51594A4638C"
                      + "F654B373DF24884739E38E629B3BDBDD85CD53D78A3B745371D2E9056A4348CE"
                      + "34FDAC7EF98BBD08D28BA1156C34B93B8F0C4EC4271683FD35F2D989B1C0098F"
                      + "8D8EEC9BF0B5DBF29A236752A6599D2E5E81EE180271AFA9C17ACF931B723E92"
                      + "F6859E4E046330F9C1FC5DB028EE1F0CF2D8CB5F5AE4B5F1DC06C6A2D03799BD"
                      + "C63F8752B4DA84901FDB6F8C87117736D9D8FE7D1CBC5D9FF9BF2F32F842ACA3")),
                new BigInteger(ToolsImpl.fromHexString("010001"))
                )
        );


// ASIP Santé: data:
final byte[] data = ToolsImpl.fromHexString("00000000000000000000000000000000");



// ASIP Santé: BEGIN OF SHA1
// ASIP Santé: signature:
byte[] sigSha1ToVerify = ToolsImpl.fromHexString(
          "289CA022C27B1694956AD16390A4D4420424E2AF437932086FB7E739EE465734"
        + "17F0ADB1E8C59EBD99E23303C63316F7B4DD22B6D5B0DFB296A1F5261A86A115"
        + "68AA22EF02E8BD73777862F3C6DDBBB48E55D3FFC472CF66FC35C23CAE081853"
        + "7781E9D678CB6F30390273AB5E5EA77F69E0483B524B46AE3E7296FF5EA080E3"
        + "D58E37D3A395C1676A7491EF3172787FF1C66065A861A8FD077CDA798515EE1F"
        + "34C5C5421B2F82258A20210170274C6A3CA6F7392712B8A1D02B4E88630A397E"
        + "04C820286BABF5A91A58191FC523F2CB9D96959BA878173460E32285DAD193FE"
        + "AC22A52F77E71DDECB7D0D1129945D99CADB45F8CFA0BB767A741D9BF5FE9A4B");

Signature sig1 = Signature.getInstance("SHA1withRSA");
sig1.initVerify(pubKey);

// ASIP Santé: verify:
sig1.update(data);
// ASIP Santé: PKCS#1 stuff is done internally by the Java API.
boolean verif = sig1.verify(sigSha1ToVerify);
System.out.println("ASIP Santé: SHA1withRSA   signature status is " + verif + ".");
// ASIP Santé: display result should be: "ASIP Santé:   SHA1withRSA signature status is true."
// ASIP Santé: END OF SHA1
```

```
// ASIP Santé: BEGIN OF SHA256
// ASIP Santé: signature:
byte[] sigSha256ToVerify = ToolsImpl.fromHexString(
            "20B539F8EC57835BEF902A305BD9B7C23EE469A818DF32454E2A11A7FF033E21"
          + "BA5E6740FF84725761708D4E268020A1A57075CDBA8D9FFEE9D291C041EE7BBD"
          + "2137F8D3308AD97FF4FBEDEF0B94BBFB6A064A4AB8AE8F9A4BEF6D3464F22766"
          + "D94596158EC294202037E5AFA03228A8FDB778EF38111D8483E811E3E11ADDB1"
          + "BD858451D8EF1E5E3EDA21CC1FAF56F098BB1F49C3A7E85DEE1F2B8A64105529"
          + "1EC872F77EECE791354BAA5D92530644F0A24AC6B036E619B5F25E7960F502D1"
          + "683D40DBE04F88DCD7EEE12CA353F15FF76B2C0C80937171675731F82687C53B"
          + "EEF411D1806D3F62D70B74BD8CC0EBD994DE2152CE5FE4BC8165EF906EF86021");

Signature sig256 = Signature.getInstance("SHA256withRSA");
sig256.initVerify(pubKey);

// ASIP Santé: verify:
sig256.update(data);
// ASIP Santé: PKCS#1 stuff is done internally by the Java API.
verif = sig256.verify(sigSha256ToVerify);
System.out.println("ASIP Santé: SHA256withRSA signature status is " + verif + ".");
// ASIP Santé: display result should be: "ASIP Santé: SHA256withRSA signature status is true."
// ASIP Santé: END OF SHA256
```

```
// ASIP Santé: BEGIN OF SHA512
// ASIP Santé: signature:
byte[] sigSha512ToVerify = ToolsImpl.fromHexString(
             "6DC11F5CE1720AFD9A214ECE7A91194D0DAD165CE1D4A8C7C54B44A0D2B6B534"
           + "1EAC78C545DF5AC4156328728D6D8675940773E25A2CD58EDBB652E7ACB5EAFE"
           + "96D194950D1363D04ADA53D868DEE89FE24CC86153523BC6EC3161E9B1539D34"
           + "2084FB7086B0894A543D4A22A4AD9FE8D5BFA01FF6A516E0DFC0BD385111A3BA"
           + "48BC79151E7DF67F84935FFA9535D9D8D38A26AE29034803C7A88B737DB47498"
           + "C6AA989D7F925A632CD118F467640E0A7E9C65A61B69D5D4FE74710BAA28940C"
           + "5B5C3BEA21BF47FCDAB783610C70DD8B37B92943FE498CA68BD471EAB89E0D8D"
           + "39D3522C008E6A2E45778AD490F7FD4B695FF7BCB52ABF9CB9E64A241F6036F7");

Signature sig512 = Signature.getInstance("SHA512withRSA");
sig512.initVerify(pubKey);

// ASIP Santé: verify:
sig512.update(data);
// ASIP Santé: PKCS#1 stuff is done internally by the Java API.
verif = sig512.verify(sigSha512ToVerify);
System.out.println("ASIP Santé: SHA512withRSA signature status is " + verif + ".");
// ASIP Santé: display result should be: "ASIP Santé: SHA512withRSA signature status is true."
// ASIP Santé: END OF SHA512
```

Ce code sort le résultat suivant:

```
ASIP Santé: SHA1withRSA   signature status is true.
ASIP Santé: SHA256withRSA signature status is true.
ASIP Santé: SHA512withRSA signature status is true.
```

15.2.6.3 Vérification de signature avec C#

C# impose de déclarer explicitement l'utilisation de PKCS#1 et la longueur du tableau de bytes permettant de construire le modulus doit être exactement 0x100 (le préfixe 0x00 ne doit pas être précisé).

Passée cette difficulté, la logique du code est similaire à Java :

```
// ASIP Santé: data:
byte[] data = fromHexString("00000000000000000000000000000000");

// ASIP Santé: key:
// ASIP Santé: remove the leading "00" from the modulus!
byte[] Modulus = fromHexString(
          "CE06A11DAB1AC9AF720C7C3E7C8FCABD4A2D94EA08BAF4755CA4DB7B4568773B"
        + "BA8C69B838417504A6DD31051914F44AFE1E736D1626416A58D7E40FAFA98712"
        + "FA4408C90A63D5CFCC283E3DCF6336615EF93A231360F9FB0B40A51594A4638C"
        + "F654B373DF24884739E38E629B3BDBDD85CD53D78A3B745371D2E9056A4348CE"
        + "34FDAC7EF98BBD08D28BA1156C34B93B8F0C4EC4271683FD35F2D989B1C0098F"
        + "8D8EEC9BF0B5DBF29A236752A6599D2E5E81EE180271AFA9C17ACF931B723E92"
        + "F6859E4E046330F9C1FC5DB028EE1F0CF2D8CB5F5AE4B5F1DC06C6A2D03799BD"
        + "C63F8752B4DA84901FDB6F8C87117736D9D8FE7D1CBC5D9FF9BF2F32F842ACA3"
    );
byte[] Exponent = fromHexString("010001");

RSACryptoServiceProvider key = (RSACryptoServiceProvider)AsymmetricAlgorithm.Create("RSA");
RSAParameters RSAKeyInfo = new RSAParameters();
RSAKeyInfo.Modulus = Modulus;
RSAKeyInfo.Exponent = Exponent;
key.ImportParameters(RSAKeyInfo);
// ASIP Santé: end of key.

// ASIP Santé: begin of SHA1
string hashAlgStr = "SHA1";
HashAlgorithm hashAlg = HashAlgorithm.Create(hashAlgStr);
byte[] hash = hashAlg.ComputeHash(data);

RSAPKCS1SignatureFormatter RSAFormatter = new RSAPKCS1SignatureFormatter(key);
RSAFormatter.SetHashAlgorithm(hashAlgStr);

byte[] signedHash = fromHexString(
          "289CA022C27B1694956AD16390A4D4420424E2AF437932086FB7E739EE465734"
        + "17F0ADB1E8C59EBD99E23303C63316F7B4DD22B6D5B0DFB296A1F5261A86A115"
        + "68AA22EF02E8BD73777862F3C6DDBBB48E55D3FFC472CF66FC35C23CAE081853"
        + "7781E9D678CB6F30390273AB5E5EA77F69E0483B524B46AE3E7296FF5EA080E3"
        + "D58E37D3A395C1676A7491EF3172787FF1C66065A861A8FD077CDA798515EE1F"
        + "34C5C5421B2F82258A20210170274C6A3CA6F7392712B8A1D02B4E88630A397E"
        + "04C820286BABF5A91A58191FC523F2CB9D96959BA878173460E32285DAD193FE"
        + "AC22A52F77E71DDECB7D0D1129945D99CADB45F8CFA0BB767A741D9BF5FE9A4B"
    );
RSAPKCS1SignatureDeformatter RSADeformatter = new RSAPKCS1SignatureDeformatter(key);
RSADeformatter.SetHashAlgorithm(hashAlgStr);

bool verif = RSADeformatter.VerifySignature(hash, signedHash);
Console.WriteLine("ASIP Santé: " + hashAlgStr + "withRSA   signature status is " + verif);
// ASIP Santé: display result should be: "ASIP Santé:   SHA1withRSA signature status is True."
// ASIP Santé: END OF SHA1
```

```
// ASIP Santé: begin of SHA256
hashAlgStr = "SHA256";
hashAlg = HashAlgorithm.Create(hashAlgStr);
hash = hashAlg.ComputeHash(data);

RSAFormatter = new RSAPKCS1SignatureFormatter(key);
RSAFormatter.SetHashAlgorithm(hashAlgStr);

signedHash = fromHexString(
          "20B539F8EC57835BEF902A305BD9B7C23EE469A818DF32454E2A11A7FF033E21"
        + "BA5E6740FF84725761708D4E268020A1A57075CDBA8D9FFEE9D291C041EE7BBD"
        + "2137F8D3308AD97FF4FBEDEF0B94BBFB6A064A4AB8AE8F9A4BEF6D3464F22766"
        + "D94596158EC294202037E5AFA03228A8FDB778EF38111D8483E811E3E11ADDB1"
        + "BD858451D8EF1E5E3EDA21CC1FAF56F098BB1F49C3A7E85DEE1F2B8A64105529"
        + "1EC872F77EECE791354BAA5D92530644F0A24AC6B036E619B5F25E7960F502D1"
        + "683D40DBE04F88DCD7EEE12CA353F15FF76B2C0C80937171675731F82687C53B"
        + "EEF411D1806D3F62D70B74BD8CC0EBD994DE2152CE5FE4BC8165EF906EF86021"
    );
RSADeformatter = new RSAPKCS1SignatureDeformatter(key);
RSADeformatter.SetHashAlgorithm(hashAlgStr);

verif = RSADeformatter.VerifySignature(hash, signedHash);
Console.WriteLine("ASIP Santé: " + hashAlgStr + "withRSA   signature status is " + verif);
// ASIP Santé: display result should be: "ASIP Santé:   SHA256withRSA signature status is True."
// ASIP Santé: END OF SHA256
```

```
// ASIP Santé: begin of SHA512
hashAlgStr = "SHA512";
hashAlg = HashAlgorithm.Create(hashAlgStr);
hash = hashAlg.ComputeHash(data);

RSAFormatter = new RSAPKCS1SignatureFormatter(key);
RSAFormatter.SetHashAlgorithm(hashAlgStr);

signedHash = fromHexString(
          "6DC11F5CE1720AFD9A214ECE7A91194D0DAD165CE1D4A8C7C54B44A0D2B6B534"
        + "1EAC78C545DF5AC4156328728D6D8675940773E25A2CD58EDBB652E7ACB5EAFE"
        + "96D194950D1363D04ADA53D868DEE89FE24CC86153523BC6EC3161E9B1539D34"
        + "2084FB7086B0894A543D4A22A4AD9FE8D5BFA01FF6A516E0DFC0BD385111A3BA"
        + "48BC79151E7DF67F84935FFA9535D9D8D38A26AE29034803C7A88B737DB47498"
        + "C6AA989D7F925A632CD118F467640E0A7E9C65A61B69D5D4FE74710BAA28940C"
        + "5B5C3BEA21BF47FCDAB783610C70DD8B37B92943FE498CA68BD471EAB89E0D8D"
        + "39D3522C008E6A2E45778AD490F7FD4B695FF7BCB52ABF9CB9E64A241F6036F7"
    );
RSADeformatter = new RSAPKCS1SignatureDeformatter(key);
RSADeformatter.SetHashAlgorithm(hashAlgStr);

verif = RSADeformatter.VerifySignature(hash, signedHash);
Console.WriteLine("ASIP Santé: " + hashAlgStr + "withRSA   signature status is " + verif);
// ASIP Santé: display result should be: "ASIP Santé:   SHA512withRSA signature status is True."
// ASIP Santé: END OF SHA512
```

Ce code sort le résultat suivant:

```
ASIP Santé: SHA1withRSA     signature status is True
ASIP Santé: SHA256withRSA   signature status is True
ASIP Santé: SHA512withRSA   signature status is True
```

16Annexe – Vérification des statuts des certificats techniques sans-contact de l'ASIP Santé

Comme expliqué dans le chapitre Protection des données personnelles, l'ASIP Santé ne possède pas de liste de correspondance entre carte et certificat sans-contact.

Lors de la mise en opposition d'une carte CPx, l'ASIP Santé révoque les 2 certificats d'authentification et de signature de la carte CPx concernée. Ces 2 certificats sont effacés de l'annuaire et leurs numéros de série sont publiés via les listes de révocation (CRL) ASIP Santé, ces dernières – et uniquement elles d'ailleurs – faisant foi pour la vérification par un tiers des statuts de certificats.

Par contre, l'ASIP Santé n'est pas en mesure de révoquer le certificat technique sans-contact correspondant à la carte opposée, puisque l'ASIP Santé ne gère aucune correspondance {carte ; certificat technique} et n'est donc pas en mesure de retrouver le numéro de série du certificat technique correspondant.

L'ASIP Santé ne publie donc aucune CRL relative aux certificats techniques sans-contact (autorités OU=ASIP-SANTE TECHNIQUE, O=ASIP-SANTE, C=FR pour la production ou OU=TEST TECHNIQUE, O=TEST, C=FR pour les tests).

Si elle devait être effectuée – et elle doit l'être dans tous les scénarios basés sur PKIX – la vérification des statuts des certificats techniques ASIP Santé doit donc se faire localement via l'émission d'une liste de certificats révoqués construite (éventuellement signée, en tout cas sécurisée) et maintenue localement en lien avec les processus d'enrôlement et les procédures de gestion des pertes et des vols mis en place dans le SI considéré.

IGC-Santé : vérification des CRLs en sans-contact	Le gabarit des certificats techniques ne change pas avec l'arrivée de la nouvelle IGC-Santé: la considération ci-dessus reste valable.

Tableau 64 : IGC-Santé : vérification des CRL en sans-contact inchangée

17Annexe – Numéros de série de la CPx

La carte CPx possède trois « numéros de série » :

#	Identifiant	Accès	Description
1	numéro RFID : « **UID** » en type A « **PUPI** » en type B	En sans-contact uniquement via une commande lecteur PC/SC v2	identifiant en mode sans-contact En type B, le « PUPI » est une donnée aléatoire temporaire à l'échange en cours avec le lecteur.
			non publié
2	identifiant logique ou numéro de carte : « **IdCarteLog** »	En **contact uniquement** (pas en sans-contact) ou par **lecture optique du code barre sur l'enveloppe postale contenant la CPx**	numéro à 10 chiffres
			unique pour chaque carte CPx
			inscrit sur le visuel, juste sous le nom du porteur
			public
			publié dans notre annuaire
			présent dans les certificats des cartes CPx
			2nde partie de l'extension privée gipCardID cf. http://integrateurs-cps.asipsante.fr/documents/IGC-CPS2ter-2020-Certificats-X.509-et-CRL-V1.0.pdf
			présent dans toutes les générations de cartes CPx
			retourné par les deux librairies cps_pkcs11_w32 (**v4**) et cps3_pkcs11_wxx (**v5**) dans le champ **Label** de la structure **TOKEN_INFO** (voir tableau ci-après)
3	identifiant IAS-ECC : « **IdCarteIAS** »	1 seul identifiant IAS-ECC accessible en contact et en sans-contact via des APDUs IAS-ECC non spécifiques à la carte CPx (cf. **[EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS [IAS ECC]]**)	numéro sur 8 chiffres
			unique pour chaque carte CPx
			identifiant interne de la puce IAS
			n'apparaît ni sur le visuel ni dans les certificats
			non publié
			n'est présent que depuis la carte CPS3, il n'existait pas dans la carte CPS2ter
			retourné seulement par la librairie PKCS#11 de la Cryptolib CPS v5 (cps3_pkcs11_wxx) dans le champ **SerialNumber** de la structure **TOKEN_INFO** (voir tableau ci-après)

Tableau 65 : identifiants CPx

Carte	Cryptolib CPS	SerialNumber (TOKEN_INFO)	Label (TOKEN_INFO)
CPS2ter	Cryptolib CPS v4	IdCarteLog	CPS-IdCarteLog
CPS3	Cryptolib CPS v4	IdCarteLog	CPS-IdCarteLog
CPS2ter	Cryptolib CPS v5	IdCarteLog	CPS2ter-IdCarteLog
CPS3	Cryptolib CPS v5	IdCarteIAS	CPS3v1-IdCarteLog

Tableau 66 : Gestion des identifiants CPx via C_GetTokenInfo et TOKEN_INFO

18Annexe – Carte CPS 3.3 et support de Mifare Classic 1K

18.1 Configuration de transport

La carte CPS3 dans sa version "3.3" intègre la fonctionnalité sans contact "Mifare Classic 1K" introduite par NXP (pour rappel, la fonction Mifare de la carte CPS3.1 est comparable Mifare Ultralight seulement).

Les cartes CPS3.3 sont disponibles à des fins de test depuis février 2017 et entreront en production en octobre 2017.

Par défaut, les valeurs des clés Mifare KEY A et KEY B des CPS3.3 sont positionnées à FF, en cohérence avec ce qui est décrit en page 10 du document **[19]** en ce qui concerne l'état d'une puce Mifare à la livraison (chip delivery).

Les "Access Conditions" ("Sector trailer", octets 6, 7 et 8) sont positionnées à 7F 07 88, plutôt qu'à FF 07 80. Ces conditions sont conformes à la procédure d'identification spécifiée par NXP en **[20]** §2.3 (voir en particulier le diagramme de la page 13).

La différence entre les deux configurations de transport possibles se situe au niveau des conditions d'accès du « sector trailer » (block 3) :
- Dans la configuration de transport CPS3.3, le block 3 vaut: C1|C2|C3 = 011
- Dans l'autre configuration de transport indiquée par la documentation NXP, le block 3 vaut : C1|C2|C3 = 001

En prenant le tableau de la page 13 du document **[19]**:
- La configuration appliquée sur la CPS3.3 est celle entourée en bleu ci-dessous
- L'autre configuration de transport indiquée par NXP est celle entourée en vert

Table 7. Access conditions for the sector trailer

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read[1]
0	1	0	never	never	key A	never	key A	never	Key B may be read[1]
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never	key A|B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration[1]
0	1	1	never	key B	key A|B	key B	never	key B	
1	0	1	never	never	key A|B	key B	never	never	
1	1	1	never	never	key A|B	never	never	never	

Figure 51: CPS3.3: Mifare Classic 1k: Access Conditions en configuration de transport

La configuration de transport préconisée par NXP et reprise par la CPS3.3 (7F 07 8**8**) ne pose pas donc de problème particulier:
- Key A et Key B sont modifiables (sous contrôle de KEY B)
- Les "Access bits" sont modifiables (sous contrôle de KEY B)
- L'authentification lors du formatage se fait sur la KEY B avec la valeur FF par défaut.

Mifare Classic 1K: rappels de sécurité	La technologie Mifare Classic 1K fait toujours l'objet d'un bulletin de sécurité de la part de l'ANSSI. La Carte CPS3.3 active cette fonctionnalité par souci de compatibilité avec des fonctions sans-contact sans enjeu de sécurité (cantine). Les clés par défaut doivent être immédiatement remplacées dès réception. Un projet sans-contact à base de CPS3.3 Mifare Classic 1K doit prévoir une phase de définition des différents secteurs à utiliser (mapping).

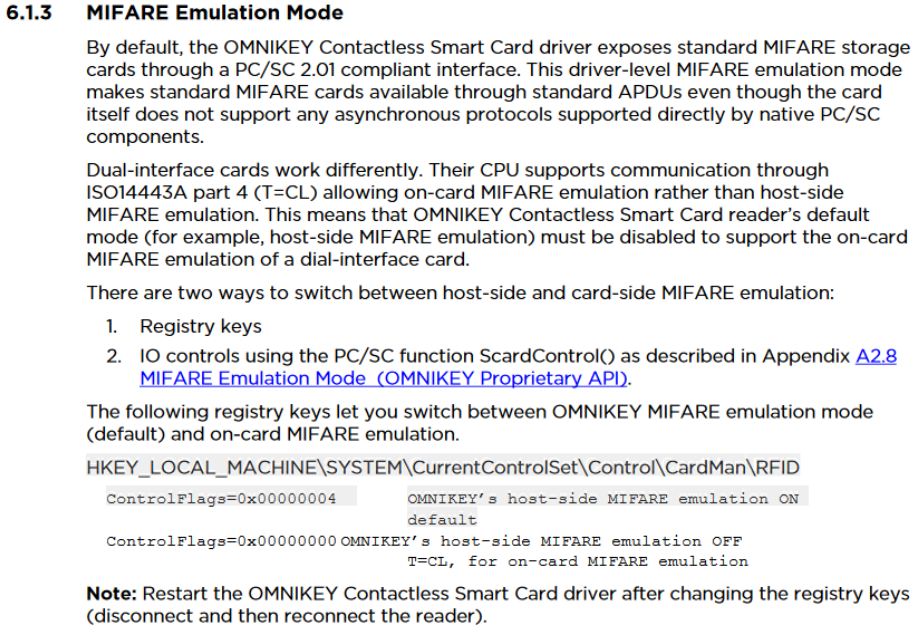
Tableau 67 : Mifare Classic 1K: rappels de sécurité

18.2 Utilisation avec le lecteur HID 5321 CL

Pour utiliser les cartes CPS3.3 en Mifare Classic 1K et un lecteur HID 5321 CL sous Microsoft Windows, il est nécessaire de suivre **[21]** page 25 en configurant la clé de registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CardMan\RFID
ControlFlags=0x00000004
```

Tableau 68 : CPS3.3: Mifare Classic 1k et HID 5321 CL: Extrait de la documentation "developers guide"



6.1.3 MIFARE Emulation Mode

By default, the OMNIKEY Contactless Smart Card driver exposes standard MIFARE storage cards through a PC/SC 2.01 compliant interface. This driver-level MIFARE emulation mode makes standard MIFARE cards available through standard APDUs even though the card itself does not support any asynchronous protocols supported directly by native PC/SC components.

Dual-interface cards work differently. Their CPU supports communication through ISO14443A part 4 (T=CL) allowing on-card MIFARE emulation rather than host-side MIFARE emulation. This means that OMNIKEY Contactless Smart Card reader's default mode (for example, host-side MIFARE emulation) must be disabled to support the on-card MIFARE emulation of a dial-interface card.

There are two ways to switch between host-side and card-side MIFARE emulation:

1. Registry keys
2. IO controls using the PC/SC function ScardControl() as described in Appendix A2.8 MIFARE Emulation Mode (OMNIKEY Proprietary API).

The following registry keys let you switch between OMNIKEY MIFARE emulation mode (default) and on-card MIFARE emulation.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CardMan\RFID

ControlFlags=0x00000004	OMNIKEY's host-side MIFARE emulation ON default
ControlFlags=0x00000000	OMNIKEY's host-side MIFARE emulation OFF T=CL, for on-card MIFARE emulation

Note: Restart the OMNIKEY Contactless Smart Card driver after changing the registry keys (disconnect and then reconnect the reader).

Figure 52: CPS3.3: Mifare Classic 1k et HID 5321 CL: Extrait de la documentation "developers guide"

Ce paramétrage n'est pas compatible avec l'envoi d'APDU IAS-ECC sans-contact

19Annexe – Points d'attention et contournements

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0010	1196	Win7 Win8	x86 x64	Le Smartcard logon sans-contact ne fonctionne pas.	Installer une Cryptolib CPS v5 plus récente que la v5.0.13	Confirmé	Confirmé
AT_0020	1098	Win7 Win8	x86 x64	Le Smartcard logon sans-contact ne fonctionne pas en TSE.	Installer une Cryptolib CPS v5 plus récente que la v5.0.13	Confirmé	Confirmé
AT_0030	1208	Tout OS	x86 x64	Le moteur PKCS#11 pour OpenSSL ne fonctionne pas en sans-contact avec la Cryptolib CPS v5.	Adapter le code du moteur PKCS#11 en changeant la logique de la fonction PKCS11_find_token du fichier p11_slot.c	Confirmé	Confirmé
AT_0040	1196	Win7 Win8	x86 x64	Le Smartcard logon sans-contact fonctionne à condition de faire entrer un « hint » à l'utilisateur, ce qui pénalise l'ergonomie des solutions sans-contact.	- Implémenter un « Custom Credential Provider » - Attendre le Minidriver CPS	Confirmé	Confirmé

#	Ticket	OS	Archi	Limitation	Alternative	Statut problème	Statut alternative
AT_0050		Tout OS	x86 x64	Des problèmes fréquents de lecture du jeton sans-contact (SCARD_E_COMM_DATA_LOST au niveau PC/SC ou CKR_GENERAL_ERROR au niveau PKCS#11) sont constatés avec le lecteur Xiring DITEO en mode sans-contact.	- Implémenter un mécanisme de reprise au niveau applicatif sur occurrence des erreurs SCARD_E_COMM_DATA_LOST ou CKR_GENERAL_ERROR - Vérifier le badge (pas de partie métallique, pas de présentation de clé en plus de la carte) - Raccourcir le jeton et le formater le jeton sous la forme d'un TLV et ne lire que les données utiles en analysant la longueur des données comme préconisé plus haut - Accoler la carte au lecteur (les erreurs sont moins fréquentes) - changer de lecteur	Confirmé	Confirmé

Tableau 69 : Points d'attentions et contournements

20Annexe – Liste des figures

21Annexe – Liste des tableaux

22Notes

[fin du document]

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
Tel : 01 58 45 32 50
esante.gouv.fr