AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

LA CARTE CPS3

– Présentation générale –

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard – 75015 Paris
T. + 33 (0)1 58 45 32 50
www.asipsante.fr

Sommaire

Figures et Tableaux

1 Objet du document

Ce document est une présentation générale de la nouvelle carte CPS3 qui remplace la carte CPS2ter à partir de février 2011.

Il décrit les nouvelles fonctionnalités de la carte CPS et souligne les différences fonctionnelles et techniques entre la CPS3 et la CPS2ter.

2 Synthèse du document

La carte de professionnel de santé, ou carte CPS, est la carte d'identité professionnelle électronique du secteur de la santé. Elle constitue le maillon final d'une chaîne de confiance qui permet à son titulaire d'attester son identité professionnelle et ses qualifications.

Elle est délivrée par l'ASIP Santé qui est le tiers de confiance reconnu et l'autorité de certification désignée du secteur de la santé.

Elle contient principalement l'identité du porteur, sa qualification professionnelle, et son (ou ses) activité(s) et des certificats électroniques permettant de garantir ces informations.

Une nouvelle version de la carte CPS, la CPS3.1, est déployée à partir de février 2011en remplacement de la carte CPS2ter.

Pourquoi une nouvelle carte ?

L'environnement réglementaire et industriel ayant évolué depuis l'émission de la carte CPS2ter en décembre 2004, l'ASIP Santé a décidé de développer une nouvelle carte, la CPS3. Cette carte est basée sur un produit standard et disponible chez la plupart des industriels de la carte à microprocesseur. Elle s'appuie sur un standard national en passe de devenir un standard européen : le standard IAS ECC (pour Authentication, Identification, Signature for the European Citizen Card).

Le standard IAS ECC a été spécifié par le GIXEL, groupement des industriels de la carte, à l'initiative de la DGME et a été depuis repris par l'ANTS notamment pour la eAdministration.

Afin de maintenir la compatibilité des cartes CPS avec le terrain, la carte CPS3 embarque deux volets distincts : un volet qui se comporte à l'identique de la CPS2ter, et un nouveau volet basé sur le standard IAS pour toutes nouvelles fonctionnalités.

Tout en conservant la compatibilité avec les applications déployées sur le terrain, la CPS3 permet de nouveaux usages en lien avec ses nouveautés techniques :

- Un mode standard IAS
- Un fonctionnement en mode sans-contact ;
- Une sécurité renforcée ;
- Une meilleure conformité avec les standards internationaux ;
- De meilleures performances ;
- De nouvelles fonctions cryptographiques ;

La CPS3, une carte multiple

La CPS3 se présente en fait comme trois cartes en une : une carte CPS2ter, une carte IAS et une carte sans contact :

- Une carte CPS2ter pour assurer la compatibilité avec les applications déployées sur le terrain ;
- Une nouvelle carte conforme à un standard industriel (IAS ECC) et qui est proposée par plusieurs fabricants de carte à puce. Cette carte représente la cible vers laquelle toutes les applications terrain doivent migrer à terme.
- Une carte sans contact destinée à améliorer l'ergonomie d'usage de la carte CPS dans certaines situations, notamment dans les établissements de santé.

Une compatibilité avec la CPS2ter

A la mise sous tension de la carte CPS3 dans le lecteur, celle-ci se comporte rigoureusement comme une CPS2ter. Ceci est un gage de compatibilité avec toutes les applications existantes et notamment avec les applications Sesam-Vitale.

Les applications utilisant les API Sesam-Vitale, l'API CPS et/ou la Cryptolib CPS seront toujours en mesure, sans évolutions, de fonctionner avec la CPS3.

Seules les nouvelles applications, utilisant le nouveau middleware ASIP Santé seront en mesure d'activer les nouvelles fonctionnalités (contact ou sans contact).

Le mode standard IAS pour la CPS

La carte au standard IAS (Identification, Authentification, Signature) constitue le standard choisi en France pour la eAdministration. Ce standard prend en compte le standard européen ECC (European Citizen Card) et représente donc le socle de développement de l'ensemble de l'identité et donc de l'économie numérique en europe. Ce standard encore récent doit permettre de disposer d'une offre industrielle interopérable ainsi que la normalisation des échanges entre la carte et le terminal (qu'il s'agisse d'un poste de travail personnel ou professionnel). En d'autres termes, un utilisateur doit pouvoir utiliser indifféremment n'importe qu'elle carte IAS avec un lecteur de carte équipant en standard son poste et des éléments logiciels uniques de dialogue entre ses applications et le lecteur.

Ainsi toutes les cartes de la sphère publique (Carte Vitale 2, Carte Nationale d'Identité, Carte de Vie Quotidienne, Carte d'Agent de l'Administration et désormais Carte de Professionnel de Santé) pourront servir de support à l'identité numérique.

Ces cartes permettent l'usage de lecteurs dits transparents PC/SC (Personal Computer / Smart Card) qui équipent en standard certains poste de travail tant sous windows que sous Mac ou Linux ou qui sont disponibles sur le marché sous la forme de périphériques bon marché.

Un nouveau mode de communication sans contact

Dans un souci d'ergonomie et pour ouvrir la carte CPS à de nouveaux usages, un nouveau mode de communication a été ajouté aux fonctionnalités de la CPS3 : le mode sans contact.

Ce mode 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. Cela nécessite bien entendu 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 par rapport au lecteur.

Un niveau de sécurité adapté

Les référentiels applicables aux systèmes d'information de santé en termes de sécurité sont en cours de constitution.

Toutefois, le Référentiel Général de Sécurité, établissant le cadre des échanges dématérialisés entre les usagers et l'administration et défini conjointement par l'ANSSI et la DGME, est un élément d'entrée essentiel puisqu'il fixe les règles à respecter en fonction du niveau de sécurité visé.

S'agissant des données de santé, le niveau visé pour la CPS3 est le niveau « renforcé » tel que défini dans le référentiel de l'ANSSI. En conséquence, le niveau d'évaluation retenu pour la carte CPS3 est le niveau EAL4+.

Une meilleure conformité aux standards internationaux

La CPS3 s'appuie sur le standard IAS ECC qui a été spécifié par le GIXEL, le groupement des industriels de la carte, à l'initiative de la DGME et qui a été depuis repris par l'ANTS pour la eAdministration.

Avant d'être présenté aux instances de normalisation européennes, ce standard a été consolidé avec les organismes allemands homologues.

De ce fait, ce standard national est en passe de devenir un standard européen : le standard IAS ECC (pour Authentication, Identification, Signature for the European Citizen Card).

De meilleures performances

La carte CPS3 utilise un composant dont la technologie plus récente offre de meilleures performances notamment en termes de temps de calcul cryptographique.

Un nouveau graphisme pour une meilleure identification visuelle

Les graphismes et impressions utilisés pour la personnalisation visuelle des différents types de carte sont modifiés afin de permettre une meilleure identification des cartes CPS3. Ces cartes qui attestent, via le Répertoire Permanent des Professionnels de Santé, de la qualité du titulaire et de son droit à exercer, comportent désormais le logo de l'autorité d'enregistrement responsable de cette attestation et notamment celui des ordres professionnels pour les professions concernées, ainsi que celui de l'autorité administrative émettrice de la carte, l'ASIP Santé.

Des nouveaux usages possibles

La carte CPS, grâce à ses capacités cryptographiques, permet la mise en œuvre de mécanismes de sécurité indispensable pour la eSanté :

- Identification unique de tout professionnel de santé de manière fiable et certifiée au niveau national ;
- Authentification des utilisateurs distants : permet de garantir l'identité des professionnels de santé connectés grâce à la saisie de leur code confidentiel et la possession de la carte ;
- Signature électronique des transactions et des messages échangés entre professionnels de santé ou avec les patients ;
- Chiffrement des messages lors des transmissions sur des réseaux non sûrs.

<u>De nouvelles modalités d'authentification du porteur</u>

- L'authentification forte avec contact et saisie du code confidentiel reste l'usage classique de la carte
- Afin d'améliorer l'ergonomie d'usage dans un contexte de mobilité, une authentification simple sans contact est proposée par la carte CPS3. Combinée avec une authentification forte initiale en mode contact, ce mode d'utilisation apporte la simplicité recherchée tout en garantissant un niveau de sécurité acceptable.
- Pour les applications requérant un niveau de sécurité moins exigeant, par exemple le contrôle d'accès aux locaux, au parking ou la restauration d'entreprise, l'identification simple sans contact par la lecture d'un numéro de série de composant répond au besoin.

<u>La possibilité d'écrire des données applicatives</u>

Dans certains nouveaux usages, et notamment en établissement de santé, il peut être nécessaire de disposer d'une zone mémoire capable de recevoir des données applicatives comme par exemple un jeton de droits, des horaires d'accès, des habilitations…

La CPS3 offre une zone mémoire en lecture libre sans contact, mais qui toutefois, pour des raisons de sécurité, ne peut être écrite que sous contrôle du code confidentiel(en mode contact).

<u>Des évolutions sur les données métier stockées dans la CPS</u>

La CPS3 dispose de 2 zones distinctes de stockage des données métier CPS :

⇒ Le **Volet CPS2ter** qui contient les données métier telles que présentes actuellement dans la CPS2ter. Le contenu et la structure sont conservés de manière à assurer une compatibilité totale avec l'existant et notamment la production des FSE ;

⇒ Le **Volet IAS** qui contient les données métier CPS mises à jour. **Le format de ces données métier est modifié** pour se mettre en conformité avec le RPPS.

Toutefois, certaines modifications dans les 2 volets ont été apportées aux données métier afin de se mettre en conformité avec les besoins des utilisateurs :

- Les données sur la carte elle-même restent inchangées : numéro logique carte, type de carte,… (sauf la date de fin de validité de la carte qui est avancée de 2 heures par rapport à ce qui était fait précédemment pour tenir compte des changements d'horaires annuels) ;
- Les données sur le professionnel de santé en tant que personne physique ne changent pas : civilité, Nom patronymique, prénoms… ;
- Les données du porteur en tant que professionnel de santé sont modifiées comme suit :
    - Informations modifiées :
        - de nouveaux codes confidentiel et de déblocage par porteur sont définis,
        - les codes « profession » et « future profession » restent identiques mais sont maintenant enregistrés dans 2 champs distincts au lieu d'un seul,
        - le numéro d'identification national ADELI est remplacé par le numéro RPPS,
        - la spécialité ordinale est codifiée en savoir-faire RPPS (exclusivement dans le volet IAS) ;
    - Informations qui ne sont plus gérées et qui sont donc supprimées de la carte (absentes dans les 2 volets de données) :
        - code métier,
        - situation professionnelle,
        - forme juridique,
        - Orientations Particulières,
        - Spécialisation,
        - Attribution(s) Complémentaire(s) ADELI,
        - Autres Compétences ADELI,
        - spécialité d'exercice,
        - dates de début et de fin des situations d'exercice ;
    - La structure des données contenues dans le volet IAS est différente de celle du volet CPS2ter. Elle devient conforme au standard IAS. **Les applications qui migrent pour utiliser le volet IAS doivent tenir compte de ce changement de structure**.
    - certaines de ces informations continuent toutefois à être publiées dans l'annuaire soit pour maintenir la compatibilité ascendante, soit parce qu'elles sont nécessaires aux applications, notamment pour gérer des droits d'accès ; il appartient alors à l'application qui lit la carte d'obtenir ces informations complémentaires en interrogeant l'annuaire
- Les Données d'Assurance maladie sont maintenues dans le volet CPS2ter.

<u>De nouvelles fonctions cryptographiques</u>

Les fonctions cryptographiques de la CPS2ter sont conservées grâce au volet CPS2ter de la CPS3. Toutefois, l'ASIP Santé conseille aux développeurs et promoteurs d'application de migrer vers le volet IAS afin de pérenniser leurs investissements.

Grâce à la conformité au standard IAS, des évolutions futures de la CPS3 pourront être envisagées pour inclure de nouvelles fonctions cryptographiques telles que la signature qualifiée, la génération de clés sur site par exemple ou la mise en œuvre d'algorithmes cryptographiques (SHA-2…). Le profil de personnalisation de la CPS3 devra évoluer pour permettre ces fonctionnalités (nouvelles versions de CPS3).

Un nouveau middleware sur le poste de travail du PS

L'accès à la carte sur le poste de travail est réalisé au moyen d'un composant logiciel d'interface appelé « middleware ».

Pour l'accès aux fonctionnalités CPS2ter, le middleware utilisé avec les cartes et qui est actuellement déployé sur le terrain pourra continuer à être utilisé. Il s'agit des Cryptolib-CPS

et des API-CPS. Ces composants et les manuels associés sont disponibles sur le site Editeurs de l’ASIP Santé.

En revanche, l’accès aux données et nouvelles fonctions IAS de la carte CPS3, en mode contact et sans contact, n’est possible qu'au moyen du nouveau middleware ASIP Santé.

Ce logiciel a pour vocation de remplacer, à terme, la Cryptolib-CPS (et les API-CPS associées) pour permettre l’accès aussi bien aux CPS2ter qu’aux CPS3.

3 Contexte

La carte de professionnel de santé, ou carte CPS, est la carte d'identité professionnelle électronique du secteur de la santé. Elle constitue le maillon final d'une chaîne de confiance qui permet à son titulaire d'attester son identité professionnelle et ses qualifications.

Elle est délivrée par l'ASIP Santé qui est le tiers de confiance reconnu et l'autorité de certification désignée du secteur de la santé après validation de la qualité du titulaire par une autorité d'enregistrement désigné par ordonnance. Les ordres professionnels sont des autorités d'enregistrement pour toutes les professions de santé qui en sont dotées.

La carte CPS contient principalement l'identité du porteur, sa qualification professionnelle, et son (ou ses) activité(s) et des certificats électroniques permettant de garantir ces informations.

Cette carte permet de connaître l'identité professionnelle du porteur pour, par exemple, déduire ses droits d'accès à des applications, à des informations du système d'information de son établissement ou du système d'information de santé national. Elle permet aussi de signer électroniquement des documents (fichier, mail) ou de les chiffrer.

3.1 L'état du parc actuel

La famille de cartes CPS se compose de cartes destinées aux professions de santé réglementées (les CPS), les cartes attribuées aux personnels d'établissements de santé et à leur directeur (CPE/CDE) et les cartes distribuées aux organismes ayant une activité reconnue dans le secteur de la santé mais ne dispensant pas de soins (CPA)

Les cartes CPS sont actuellement distribuées aux professions de santé suivantes :

- médecin, pharmacien, chirurgien-dentiste, sage-femme, infirmier(e), masseur-kinésithérapeute, pédicure-podologue ;
- orthoptiste, audioprothésiste, podo-orthésiste, épithésiste, orthopédiste-orthésiste, ergothérapeute, orthoprothésiste, orthophoniste, orthoptiste, manipulateur d'électroradiologie, psychomotricien, ocularistе, opticien-lunetier.

3.2 Le besoin de développer une nouvelle version de la CPS

L'environnement réglementaire a évolué depuis l'émission de la CPS2ter en décembre 2004 avec la parution le 17 mai 2007 au Journal Officiel du décret n°2007-960 signé le 15 mai 2007 dit décret « Confidentialité » : l'usage de la carte CPS par les professionnels de santé est devenu obligatoire pour tout accès à des données de santé électroniques, ou tout échange de ces données.

Par ailleurs, face au développement des applications communicantes (applications internet, messagerie électronique…), la CPS devient un outil indispensable du processus de soins, et est amenée à être utilisée par tous les professionnels de santé dans leur pratique quotidienne, en ville comme à l'hôpital. Elle est notamment appelée à se déployer dans les établissements de soins.

Les grandes applications nationales du secteur de la santé nécessitent la mise en œuvre de dispositifs de sécurité garantissant un haut niveau de confiance :

- Dossier Médical Personnel (DMP) : afin de garantir un haut niveau de protection des données médicales, le DMP requiert la carte CPS pour la consultation des données des patients ;
- Dossier Pharmaceutique (DP) : le contrôle d'accès et la traçabilité des opérations lors de la délivrance des médicaments repose sur la carte CPS ;
- Développement des services en ligne de l'Assurance Maladie : historique des remboursements, consultation des droits en ligne, espace pro…

Ces nouveaux besoins ont permis d'identifier un certain nombre d'évolutions nécessaires de la carte aussi bien en termes fonctionnels que techniques et ont justifié le développement de la carte CPS3 par l'ASIP santé.

3.3 Les objectifs fixés pour développer la CPS3

Les objectifs fixés pour cette nouvelle version de carte CPS sont les suivants :

1. Assurer la continuité de service.

Le composant électronique utilisé actuellement pour les cartes CPS2ter est en fin de vie. L'ensemble des fonctionnalités assurées par la carte CPS2ter ont été portées sur le nouveau composant. La mise en service de ce nouveau composant doit être effective avant épuisement du stock d'anciens composants.

2. Garantir la compatibilité avec les applications existantes.

La carte CPS3 remplace la carte CPS2ter. A ce titre, elle se doit de garantir la compatibilité avec les solutions actuellement déployées sur le terrain. C'est le cas par exemple des applications du domaine de l'Assurance Maladie et des logiciels de messagerie sécurisée qui s'appuient sur la carte CPS2ter. Ces solutions continueront à fonctionner à l'identique avec la CPS3.

3. Améliorer l'ergonomie.

Pour tenir compte des contextes métier, la CPS3 intègre de nouvelles fonctionnalités :

- Une interface de communication sans contact pour faciliter les opérations manuelles de l'utilisateur.
- De nouveaux services applicatifs qui seront détaillés plus loin (lecture/écriture de données applicatives sur la carte, authentification simple du support, …) et qui permettront d'adapter le niveau de sécurité mis en œuvre en fonction de l'utilisation.

4. Etre conforme aux référentiels de sécurité applicables et aux standards internationaux.

La constante augmentation des besoins et des attentes en termes de sécurité numérique a conduit les industriels du secteur de la carte à puce à définir une spécification commune standardisée qui couvre l'ensemble des besoins relatifs à l'Identification, l'Authentification et la Signature électronique (rassemblés sous le sigle IAS). La dernière version de cette spécification est IAS ECC v1.

Ce contour fonctionnel coïncide avec l'utilisation de la carte CPS au sein des systèmes d'information de santé.

La maturité de la spécification IAS, la mise en place du schéma d'homologation associé, des cartes et des logiciels d'interface, sous l'égide de l'Agence Nationale des Titres Sécurisés (ANTS) dépendant du Ministère de l'Intérieur, pour garantir l'interopérabilité entre les différentes briques du système indépendamment du fournisseur de cartes, sont autant d'éléments qui ont amené l'ASIP Santé à choisir IAS ECC comme standard industriel pour la CPS3.

Par ailleurs, ce standard IAS ECC est en cours de normalisation au niveau européen après avoir été consolidé avec les organismes de normalisation allemands homologues.

5. Migrer vers une offre industrielle plus standard.

Comme indiqué précédemment, le standard cible choisi est IAS ECC. Cette migration va permettre de :

- Sécuriser l'approvisionnement en composants : l'offre IAS ECC est présente chez les principaux fournisseurs de cartes à puce. De ce fait, elle est maintenue par

l’ensemble des industriels indépendamment du cycle de vie propre du composant électronique.

- Faciliter l’intégration de la carte CPS dans les solutions disponibles auprès des éditeurs : IAS ECC n’est pas uniquement utilisé dans le secteur de la santé, il commence à être intégré dans des solutions généralistes du monde des infrastructures à clés publique d’entreprise (PKI).

4 Caractéristiques générales de la CPS3

4.1 Une carte multiple

Pour une application donnée, la CPS3 se présente en réalité comme trois cartes en une : une carte CPS2ter, une carte IAS et une carte sans contact. Le fonctionnement de ces 3 cartes est assuré grâce à une puce unique embarquée sur le plastique de la CPS3.

Pour les deux premières cartes, le composant de la CPS3 contient 2 volets applicatifs pouvant être adressés simultanément : un volet CPS2ter qui simule à l'identique une carte CPS2ter et un volet IAS conforme au standard industriel IAS ECC.

Pour la carte sans contact, la CPS3 embarque une antenne noyée dans le plastique et un module de communication conforme au protocole normalisé ISO 14443.

Les nouvelles fonctionnalités, principalement liées à l'amélioration de l'ergonomie de la carte CPS, sont disponibles uniquement dans le volet IAS ECC de manière à préparer la migration des applications terrain utilisant cette partie propriétaire qui est appelée à disparaître dans le futur.
Tout en conservant la compatibilité avec les applications déployées sur le terrain, la CPS3 permet de nouveaux usages en lien avec ses nouveautés techniques :

- Un fonctionnement en mode sans-contact notamment pour certains usages en établissements de santé ;
- Une sécurité renforcée ;
- De meilleures performances.
- De nouvelles fonctions cryptographiques basées sur le standard IAS ;
- Une meilleure conformité avec les standards internationaux ;
- De nouvelles données ;

4.2 Caractéristiques fonctionnelles

La carte CPS, grâce à ses capacités cryptographiques, permet la mise en œuvre de mécanismes de sécurité indispensable pour la eSanté :

- Identification unique de tout professionnel de santé de manière fiable et certifiée au niveau national ;
- Authentification des utilisateurs distants : permet de garantir l'identité des professionnels de santé connectés grâce à la saisie de leur code confidentiel et la possession de la carte ;
- Signature électronique des transactions et des messages échangés entre professionnels de santé ou avec les patients ;
- Chiffrement des messages lors des transmissions sur des réseaux non sûrs.

Pour cela, la carte CPS embarque dans sa mémoire, des données d'identification et de qualification professionnelles ainsi qu'un certain nombre de clés cryptographiques associées à des certificats de clés publiques émis par l'ASIP Santé pour garantir toutes ces données.

4.2.1 De nouvelles modalités d'authentification du porteur

Concernant l'usage le la CPS3 dans les processus d'authentification de son porteur, les cinq cas d'usages suivants ont été identifiés. Ils seront ensuite décrits en détail en *« Annexe 4 : les services d'identification et d'authentification par la CPS3 »*.

1. Authentification forte avec contact :
    - C'est le mécanisme standard d'authentification combinant une double authentification d'une part du support carte, et d'autre part du porteur via la présentation de son code confidentiel ;
    - Ce cas d'usage permet de se protéger du risque de clonage du support.

2. Authentification forte sans contact sécurisé :

   Cette solution, qui nécessite des lecteurs sécurisés spécifiques, n'est pas mise en œuvre avec la première version de CPS3 mais pourra le cas échéant être implémentée dans les versions ultérieures :

   - Identique à l'authentification avec contact, mais avec l'obligation d'utiliser des lecteurs spéciaux, ayant une capacité cryptographique et d'embarquement sécurisé de clés secrètes ;
   - Ce mécanisme permet de chiffrer les échanges entre la carte et le lecteur et ainsi de se prémunir des écoutes de communication plus facile en mode sans contact ;
   - Ce cas d'usage permet de se protéger du risque de clonage du support.

3. Authentification simple sans contact :
   - Il s'agit ici de simplifier le processus d'authentification en permettant le mode sans contact sans imposer de saisie du code confidentiel (usage de type « badgeage à la volée ») ;
   - Cet usage doit être combiné avec le cas 1 afin d'améliorer la couverture de risque sécurité en cas de perte ou de vol.
   - Ce cas d'usage permet de se protéger du risque de clonage du support.
4. Identification sans contact avec lecture de données :
   - Certaines applications ne requièrent pas un haut niveau de sécurité mais principalement l'identification de manière sûre du porteur du support carte. C'est le cas par exemple des systèmes de contrôle d'accès au parking ou aux locaux.
   - Il n'y a pas de protection contre le risque de clonage du support dans ce mode d'utilisation de la CPS3
   - Mais la protection peut être renforcée par la lecture d'un jeton applicatif qui aura été écrit lors d'une première authentification forte en mode contact, par exemple en début de session journalière de travail ou lors d'un rafraichissement périodique des droits.
5. Identification simple sans contact :
   - Il s'agit d'identifier la carte en lisant simplement son numéro de série ;
   - Ce cas d'usage est adapté aux solutions déployées sur le terrain pour le contrôle d'accès physique par exemple (accès aux locaux, …) ou l'accès à la restauration d'entreprise ;
   - Il n'y a pas de protection contre le risque de clonage du support dans ce mode d'utilisation de la CPS3 ;
   - Le niveau de sécurité peut également être légèrement amélioré en conjuguant une authentification forte.

4.2.2 La possibilité d'écrire des données applicatives

Afin de permettre de nouveaux usages à la carte CPS, et notamment en établissement de santé, la CPS3 dispose d'une zone mémoire capable de recevoir des données applicatives comme par exemple un jeton de droits, des horaires d'accès, des habilitations…

Pour des raisons de sécurité, cette zone mémoire ne peut être écrite que sous contrôle du code confidentiel, et par conséquent seulement en mode contact.

En revanche, la lecture de ces données applicatives peut être effectuée aussi bien en contact qu'en sans contact.

4.2.3 Des évolutions sur les données métier stockées dans la CPS

La CPS3 dispose de 2 zones distinctes de stockage des données métier CPS :

⇒ Le **Volet CPS2ter** qui contient les données métier telles que présentes actuellement dans la CPS2ter. Ce volet permet de garantir la compatibilité ascendante avec toutes les applications sur le terrain. Le contenu et la structure sont conservés de manière à assurer une compatibilité totale avec l'existant. Cette zone n'est accessible que via le jeu de commande CPS2ter ;

⇒ Le **Volet IAS** qui contient les données métier CPS mises à jour et modifiées pour se mettre en conformité avec le RPPS et pour lesquelles une nouvelle répartition est mise en place entre les données carte et les données publiées dans l'annuaire CPS, notamment pour tenir compte des données réellement utiles et utilisées par les applications déployées sur le terrain. La structuration des données métiers dans ce volet respecte les spécifications IAS. Cette zone n'est accessible que via le jeu de commande IAS ;

Les données métier comprennent :

- Les données liées aux activités du professionnel de santé ;
- Les données accessibles en mode sans contact ;
- Les données du Domaine Assurance Maladie (DAM)

Le tableau ci-après liste des données métier stockées dans la mémoire de la CPS3 :

Les données liées aux activités du professionnel de santé ;
- Les données concernant la carte elle-même ;
Identifiant de l'émetteur de la carte = ASIP Santé
Identifiant IAS : numéro unique de la carte
Catégorie de carte
Début de validité
Fin de validité
Code porteur
Code de déblocage
- Les données sur le porteur en tant que personne physique ;
Code civilité
Nom patronymique
Nom marital
Prénoms (jusqu'à 3 prénoms)
Prénom usuel
Codes langues (jusqu'à 4 langues)
- Les données sur le porteur en tant que professionnel de santé ;
Caractéristiques nationales
Type de carte de professionnel de santé
Identification nationale du porteur de la carte
Code profession
Code future profession (professionnels en formation)
Nom d'exercice
Qualifications nationales
Spécialité ordinale ADELI (volet CPS2ter)
Spécialité ordinale RPPS (volet IAS)
- Les données liées aux situations d'exercice du porteur.
Mode d'exercice
Code statut – Niveau de responsabilité
Tableau de pharmacien
Identification nationale ADELI modifiée (volet CPS2ter pour application Sesam-Vitale)
Identification nationale de la structure
Raison sociale de la structure
Secteur d'activité ADELI (volet CPS2ter)
Secteur d'activité RPPS (volet IAS)

Les données accessibles en mode sans contact ;	
	Numéro de série sans contact
	Identifiant technique : numéro unique de la carte en sans contact
	Certificat technique d'authentification
	Zone de données applicatives
Les données du Domaine Assurance Maladie (DAM)	
	Idem CPS2ter

Tableau 1 – Liste détaillée des données métier de la CPS3

4.2.3.1 Les données liées aux activités du professionnel de santé

Les données stockées dans la mémoire de la CPS3 sont les suivantes :

- Les données concernant la carte elle-même ;
- Les données sur le porteur en tant que personne physique ;
- Les données sur le porteur en tant que professionnel de santé ;
- Les données liées aux situations d'exercice du porteur.

4.2.3.2 Données relatives à la carte

Les données concernant la carte elle-même sont les suivantes :

- Identifiant de l'émetteur de la carte — Identifiant de l'ASIP Santé ; mentionné sur la première ligne de la face avant de la carte ;10 caractères décimaux ;
- Identifiant IAS — Identifiant logique attribué par l'ASIP Santé (19 caractères décimaux) ;
- Catégorie de carte — PS, patient/assuré,…, + indicateur Exploit/Test ;
- Début de validité — Premier jour de validité de la carte et du certificat ;
- Fin de validité — Dernier jour de validité de la carte et du certificat, mentionné également sur la face avant de la carte ;
- Code porteur
- Code de déblocage.

4.2.3.3 Données PS en tant que personne physique (PS ou PE)

La liste des informations relatives à la personne physique enregistrées dans la carte sont les suivantes :

- Code civilité ;
- Nom patronymique ;
- Nom marital ;
- Prénoms (jusqu'à 3 prénoms) ;
- Prénom usuel ;
- Codes langues (jusqu'à 4 langues).

4.2.3.4 Données porteur en tant que professionnel de santé

Les données sur le porteur en tant que professionnel de santé comprennent les caractéristiques nationales et les qualifications nationales.

➔Les informations dans la carte relatives aux caractéristiques nationales sont les suivantes :

-	Type de carte de professionnel de santé	CPS, CPF, CDE, CPE, CPA,…
-	Identification nationale du porteur	Numéro national unique du porteur
-	Code profession	Code profession pour les PS
-	Code future profession	Code future profession pour les professionnels en formation (PF)
-	Nom d'exercice	

➔Les informations dans la carte relatives aux qualifications nationales du PS sont les suivantes :

-	Spécialité ordinale ADELI	codifiée en format ADELI (Couple : Spécialité + Nature de Qualification) : ne concerne que les Médecins, Chirurgiens-Dentistes et Pharmaciens (obligatoire pour médecins). Cette information n'est enregistrée que dans le volet CPS2ter.
-	Spécialité ordinale RPPS	codifiée en format RPPS (issue des savoir-faire RPPS) : ne concerne que les Médecins, et Pharmaciens (obligatoire pour médecins). Cette information n'est enregistrée que dans le volet IAS ECC.

4.2.3.5 Données liées aux situations d'exercice du porteur :

Les données relatives aux activités professionnelles pour les porteurs d'une CPS (professions réglementées) peuvent concerner jusqu'à 16 situations d'exercice.

Une carte CPS contient jusqu'à 8 situations d'exercice. Les PS ayant plus de 8 activités sont dotés d'une seconde carte appelée carte « suite ».

Les personnels d'établissement sont dotés d'une carte CPE ne contenant qu'une seule situation d'exercice.

Les informations enregistrées dans la carte pour chaque situation d'exercice sont les suivantes :

-	Mode d'exercice	libéral, salarié, remplaçant
-	Code statut et Niveau de responsabilité	responsable, adjoint, sans responsabilités
-	Tableau de pharmacien	ne concerne pas les pharmaciens du Service de Santé des Armées (SSA)
-	Identification nationale ADELI	N°ADELI du PS (légèrement modifié pour tenir compte de lettres dans le n° de département), Réservée à l'application S-V et maintenue dans le volet CPS2ter uniquement
-	Identification nationale de la structure	Numéro national unique de la structure
-	Raison sociale de la structure	Libellé en clair de la raison sociale (absent pour les situations de remplacement)

- Secteur d'activité ADELI — Secteur d'activité de la structure codifié selon la nomenclature ADELI.
  Information présente uniquement dans le volet CPS2ter
- Secteur d'activité RPPS — Secteur d'activité de la structure codifié selon la nomenclature RPPS
  Information présente uniquement dans le volet IAS ECC

4.2.3.6 Les données accessibles en mode sans contact

En mode sans contact, afin de se conformer aux exigences de la CNIL, seules des données non nominatives peuvent être échangées via le protocole ISO 14443.

Ceci implique que les applications ayant besoin de relier ces informations avec des informations d'identification nationale, doivent effectuer un enrôlement préalable.

C'est à cette fin que la CPS3 contient un identifiant technique attribué à la fabrication de la carte et non publié au niveau national.

Les données accessibles en mode sans contact sont les suivantes :

1- Identifiant protocolaire :

Cet identifiant est utilisé au niveau du protocole de communication pour éliminer les risques de collision si plusieurs cartes se présentent dans le champ électromagnétique du lecteur.

La carte CPS3 émet un identifiant protocolaire composé du numéro de série du composant défini et inscrit par le fabricant de la puce

Ce numéro est fixe et propre à chaque carte. Il peut donc être utilisé pour identifier de manière unique une carte CPS3.

Son format est de 4 octets hexadécimaux (– par exemple : '1A 45 9F BD'-). : il correspond au champ UID ou PUPI respectivement pour les protocoles type A et type B.

2- Identifiant Technique CPS3 (N°de série IAS) :

Cet identifiant technique est constitué par un numéro unique attribué par l'ASIP Santé lors de la fabrication de la carte. Cet identifiant représente le numéro logique « IAS ».

Le numéro logique IAS se compose de 19 caractères décimaux constitués comme suit : [id ASIP(10)][n°unique support(8)] [clé(1)] – (par ex : 8025000001123456783)

L'identifiant technique est accessible via le jeu de commandes IAS aussi bien en mode sans-contact qu'en mode contact.

3- Certificat Technique d'authentification :

Le certificat de clé publique d'authentification technique est raccroché à une Autorité de Certification CPS.

Les caractéristiques de ce certificat technique sont les suivantes :

- Il ne contient pas de données nominatives sur le porteur, comme toute information échangée en mode sans contact ;
- Il respecte le format standard X.509 ;
- Il n'est pas publié dans l'annuaire CPS ;
- Il certifie la validité et l'unicité de l'identifiant technique CPS3 (numéro IAS) ;
- Il nécessite un enrôlement initial dans le SIH ;

Le certificat technique est accessible via le jeu de commandes IAS aussi bien en mode sans-contact qu'en mode contact.

4- Zone de données applicatives (jeton) :

La zone réservée pour le stockage de données applicatives est de 4096 octets au maximum. Les données dans cette zone doivent être considérées comme temporaires par les applications puisqu'un professionnel de santé multi-activités ne dispose qu'une d'une carte CPS et que par conséquent, la carte peut potentiellement être utilisée par plusieurs systèmes d'information.

La zone de données applicatives est accessible uniquement via le jeu de commandes IAS, aussi bien en mode sans-contact qu'en mode contact.

L'écriture de données dans cette zone se fait uniquement en mode contact, après saisie du code confidentiel.

La lecture est libre aussi bien en contact qu'en sans-contact

4.2.3.7 Les données du Domaine Assurance Maladie (DAM)

Les données du domaine d'assurance maladie sont maintenues dans le volet CPS2ter pour assurer la compatibilité avec les applications terrain existantes. Elles sont accessibles uniquement avec le jeu de commandes CPS2ter.

En revanche, elles ne sont pas disponibles dans le volet IAS afin de simplifier la migration des applications vers un usage plus standard de la carte CPS3 comme carte d'identité professionnelle.

4.2.4 De nouvelles fonctions cryptographiques

Les fonctions cryptographiques de la CPS2ter sont conservées grâce au volet CPS2ter de la CPS3. Toutefois, l'ASIP Santé conseille aux développeurs et promoteurs d'application de migrer vers le volet IAS afin de pérenniser leurs investissements.

Il faut noter que la bi-clé RSA d'accréditation et sa valeur d'accréditation associée, initialement utilisées pour l'accès au réseau RSS, sont supprimées dans les 2 volets CPS2ter et IAS ECC.

La configuration des fichiers du volet IAS ECC permet la mise en œuvre des fonctionnalités cryptographiques de la carte CPS3 suivantes:

- Authentification RSA ;
- Signature RSA ;
- Génération de nombre aléatoire.

A cet effet, la première version de la CPS3 contient les bi-clés RSA suivants, ainsi que les certificats associés :

- Une clé RSA dédiée à l'authentification : taille de 1024 bits pour compatibilité avec la CPS2ter
- Une clé RSA dédiée à la signature : taille de 2048 bits
- Une nouvelle bi-clé RSA pour l'authentification du support en mode sans contact. Le certificat associé à cette nouvelle bi-clé (appelé « certificat technique »).

A terme, 3 emplacements de clés RSA supplémentaires sont prévus et sont réservés à un usage futur.

Grâce à la conformité au standard IAS, des évolutions futures de la CPS3 pourront être envisagées pour inclure de nouvelles fonctions cryptographiques telles que la signature qualifiée, la génération de clés sur site par exemple ou la mise en œuvre d'algorithmes cryptographiques (SHA2…).

Le profil de personnalisation de la carte devra évoluer pour permettre ces fonctionnalités (nouvelles versions de CPS3).

4.2.5 De meilleures performances

La carte CPS3 utilise un composant dont la technologie plus récente offre de meilleures performances grâce notamment à un coprocesseur cryptographique offrant de meilleurs temps de calcul.

Globalement, la CPS3 apporte une réduction du temps d'authentification ou de signature d'environ 40%.

4.3 Caractéristiques techniques

4.3.1 Une compatibilité avec la CPS2ter

A la mise sous tension de la carte CPS3 dans le lecteur, celle-ci se comporte rigoureusement comme une CPS2ter. Ceci est un gage de compatibilité avec toutes les applications existantes et notamment avec les applications Sesam-Vitale.

Les applications utilisant les API Sesam-Vitale, l'API CPS et/ou la Cryptolib CPS seront toujours en mesure, sans évolutions, de fonctionner avec la CPS3.

Seules les nouvelles applications, utilisant le nouveau middleware ASIP seront en mesure d'activer les nouvelles fonctionnalités (contact ou sans contact).

4.3.2 Un nouveau mode de communication sans contact

Dans un souci d'ergonomie et pour ouvrir la carte CPS à de nouveaux usages, un nouveau mode de communication a été ajouté aux fonctionnalités de la CPS3 : le mode sans contact.

Ce mode 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 l'usure du support. Cela nécessite bien entendu l'utilisation d'un lecteur disposant de la fonctionnalité sans contact.

La carte CPS3 embarque un composant unique permettant le mode dual, c'est-à-dire offrant les deux modes de communication « contact » et « sans contact ». Elle embarque une antenne noyée dans le plastique. Le module de transmission conforme au protocole normalisé ISO 14443 A ou B, selon le composant embarqué, est activé dès que la carte se trouve dans le champ électromagnétique d'un lecteur sans contact.

Cette technologie permet, selon le lecteur utilisé, un fonctionnement jusqu'à une distance maximale d'environ 10 cm par rapport au lecteur.

Compte tenu de la politique d'approvisionnement retenue par l'ASIP, la CPS3 peut être indifféremment conforme à la norme ISO 14443 A ou B. Cela implique donc que les lecteurs destinés à accepter des cartes CPS3 doivent être compatibles simultanément avec les 2 normes ISO14443A **et** 14443B, le parc de cartes pouvant potentiellement être réparti entre les 2 types.

Une présentation plus détaillée des usages de la CPS3 en sans contact est donnée en annexe de ce document (cf. « Annexe 5 : synthèse des usages de la CPS3 »).

4.3.3 Un niveau de sécurité adapté

Les référentiels applicables aux systèmes d'information de santé en termes de sécurité sont en cours de constitution.

Sans présumer des décisions qui seront prises à ce sujet, le Référentiel Général de Sécurité établi conjointement par l'ANSSI et la DGME, dans le cadre des échanges entre les usagers et l'administration, est un élément d'entrée essentiel puisqu'il fixe les règles à respecter en fonction du niveau de sécurité visé.

Le niveau le plus élevé défini par le RGS est le niveau « renforcé » qui impose, pour les produits de sécurité (dont fait partie la carte à puce), une évaluation sécuritaire selon le référentiel international « Critères Commun » au niveau EAL4+.

S’agissant de données de santé, c’est en particulier ce niveau applicable qui est en cours de définition.

Le fait d’appliquer les exigences liées au niveau « renforcé » du RGS pour la carte CPS3 permet d’avoir l’assurance de conformité vis-à-vis des référentiels applicables aux données de santé. Il est également à noter que l’offre industrielle standard IAS intègre d’emblée ce niveau d’évaluation.

En conséquence, le niveau d’évaluation qui a été retenu pour la carte CPS3 est le niveau EAL4+.

4.3.4 Une meilleure conformité aux standards internationaux

La CPS3 s’appuie sur le standard IAS ECC qui a été spécifié par le GIXEL, le groupement des industriels de la carte, à l’initiative de la DGME et qui a été depuis repris par l’ANTS pour la carte d’identité nationale électronique.

Avant d’être présenté aux instances de normalisation européennes, ce standard a été consolidé avec les organismes allemands homologues.

De ce fait, ce standard national est en passe de devenir un standard européen : le standard IAS ECC (pour Authentication, Identification, Signature for the European Citizen Card).

4.3.5 Un nouveau graphisme pour une meilleure identification visuelle

Les graphismes et impressions utilisés pour la personnalisation visuelle des différents types de carte de la famille sont modifiés afin de permettre une meilleure identification des cartes CPS3.

Le visuel de la carte intègre les codes graphiques de l’ASIP Santé.

Ces cartes qui attestent, via le Répertoire Permanent des Professionnels de Santé, de la qualité du titulaire et de son droit à exercer, comportent désormais le logo de l’autorité d’enregistrement responsable de cette attestation et notamment celui des ordres professionnels pour les professions concernées, ainsi que celui de l’autorité administrative émettrice de la carte, l’ASIP Santé.

4.4 Logiciel d’interfaçage de la carte CPS3 avec les applications (Middleware ASIP)

L’accès à la carte sur le poste de travail est réalisé au moyen de composants logiciels d’interface appelés « middleware ». Ces logiciels permettent aux applications la prise en charge de la carte via le lecteur de carte (PC/SC ou Sesam-vitale).

L’impact sur les architectures des postes de travail est décrit plus en détail dans le chapitre « Annexe 2 : impacts sur les architectures de poste de travail ».

En règle générale, les applications doivent savoir adresser plusieurs interfaces avec les dispositifs de sécurité via le standard PKCS#11 ou d’autres (CSP, Tokend). Ils pourront donc indifféremment opérer soit avec le middleware CPS soit avec le middleware ASIP.

4.4.1 Accès aux fonctionnalités et données CPS2ter

4.4.1.1 Avec une carte CPS2ter

Pour l’accès au travers du canal CPS2ter, le middleware utilisé avec les cartes, et actuellement déployé, pourra continuer à être utilisé. Il s’agit des Cryptolib-CPS et des API-CPS. Ces composants et les manuels associés sont disponibles sur le site Editeurs de l’ASIP Santé.

4.4.1.2 Avec une carte CPS3 – volet CPS2ter

De manière identique aux cartes CPS2ter, l'accès aux données et fonctions CPS2ter d'une carte CPS3 se fait identiquement à partir des Cryptolib-CPS ou des API-CPS.

4.4.2 Accès aux fonctionnalités IAS

4.4.2.1 En mode contact

L'accès aux données et fonctions IAS de la carte CPS3, en mode contact, n'est possible qu'au moyen du middleware ASIP.

4.4.2.2 En mode sans contact

L'accès aux données et fonctions IAS de la carte CPS3, en mode sans contact, n'est possible qu'au moyen du middleware ASIP.

En revanche, la lecture simple en sans contact du numéro de série du composant ne nécessite pas l'utilisation du middleware ASIP mais seulement du pilote du lecteur attaché au système d'information.

5 Synthèse des évolutions par rapport à la CPS2ter

Le tableau, ci-dessous, présente les différences principales entre la CPS2ter en termes de caractéristiques générales et d'usages :

Caractéristiques & usages	Carte CPS3		Carte CPS2ter
	Volet IAS ECC	Volet CPS2ter	
Carte à microprocesseur cryptographique	☑		☑
Compatible avec les lecteurs PC/SC du marché	☑		☑
Utilisation avec le Middleware ASIP « IAS ECC »	☑		☑
Module de communication sans contact	☑		☒
Compatible avec les lecteurs sans contact ISO 14443 type A et B	☑		☒
Nouveau visuel	☑		☒
Données métier CPS2ter	☒	☑	☑
Jeu de commandes CPS2ter	☒	☑	☑
Compatibilité avec les lecteurs homologués SESAM-VITALE (fonctions et données CPS2ter)	☒	☑	☑
Utilisation avec les Cryptolib et API CPS	☒	☑	☑
Données métier IAS ECC (nouvelles fonctionnalités)	☑	☒	☒
Jeu de commandes IAS	☑	☒	☒
Usages			
Authentification forte d'accès sur des systèmes d'information	☑		☑
Signature de document et de message électroniques	☑		☑
Capacité de télé mise-à-jour (évolution future)	☑		☑
Contrôle d'accès physique et multi-services « avec contact »	☑		☑
Authentification simple (sans PIN)	☑	☒	☒
Contrôle d'accès physique et multi-services « sans contact »	☑	☒	☒
Contrôle d'accès logique « sans contact »	☑	☒	☒
Lecture / écriture de données applicatives	☑	☒	☒

Caractéristiques & usages	Carte CPS3		Carte CPS2ter
	Volet IAS ECC	Volet CPS2ter	
Nouvelle cryptographie IAS ECC			
Signature qualifiée (évolution future)	☑	☒	☒
Clé d'authentification RSA 2048 bits (évolution future)	☑	☒	☒
Nouvel algorithme de hachage SHA-2 (évolution future)	☑	☒	☒
Nouvelle IGC ASIP (évolution future CPS3.2)	☑	☒	☒

Tableau 2 - Comparaison des fonctions CPS3 / CPS2ter

Ce tableau fait apparaître :

- Les caractéristiques de la carte CPS actuellement déployée sur le terrain (colonne « Carte CPS2ter »).
- Les caractéristiques de la carte CPS3 en précisant quel est le volet impliqué lorsque nécessaire.

Le tableau ci-dessous liste les différences entre la CPS2ter et la CPS3 en termes de données métier stockées dans la mémoire de la carte :

- ☑ = information présente
- M = information présente mais modifiée par rapport à la CPS2ter
- ☒ = information supprimée

Les données liées aux activités du professionnel de santé ;	**CPS3**		**Annuaire CPS**
	Volet CPSP3	**Volet CPS2ter**	
- Les données concernant la carte elle-même ;	-	-	-
Identifiant de l'émetteur de la carte = ASIP Santé	☑	☑	
Numéro logique carte ou Identifiant IAS	☑	☑	☑
Catégorie de carte	☑	☑	
Début de validité (carte et certificats)	☑	☑	
Fin de validité (carte et certificats)	M	☑	
Code porteur	M	☑	
Code de déblocage	M	☑	
- Les données sur le porteur en tant que personne physique ;	-	-	-
Code civilité	☑	☑	☑
Nom patronymique	☑	☑	
Nom marital	☑	☑	
Prénoms (jusqu'à 3 prénoms)	☑	☑	
Prénom usuel	☑	☑	☑
Codes langues (jusqu'à 4 langues)	☑	☑	
- Les données sur le porteur en tant que professionnel de santé ;	-	-	-
Caractéristiques nationales			
Type de carte de professionnel de santé	☑	☑	☑
Identification nationale du porteur de la carte	☑	☑	☑
Ancienne identification nationale ADELI du porteur de la carte (pour les cartes RPPS)			☑
Code profession	M	☑	☑
Code future profession (professionnels en formation)	M	☑	☑
Code métier		☒	
Situation professionnelle		☒	☑
Nom d'exercice	☑	☑	☑
Remplacement exclusif			☑
N'exerce pas			☒
Qualifications nationales			

Les données liées aux activités du professionnel de santé ;	CPS3		Annuaire CPS
	Volet CPSP3	Volet CPS2ter	
Spécialité ordinale ADELI (volet CPS2ter)	☑	☑	☒
Spécialité ordinale RPPS (volet IAS)	☑		☑
Orientations Particulières		☒	☑
Spécialisation		☒	☑
Attribution(s) Complémentaire(s) ADELI		☒	☒
Attribution(s) Complémentaire(s) RPPS			☑
Autres Compétences ADELI (Couples : Spécialité + Nature de Qualification)		☒	
Autres Compétences (Savoir-faire) RPPS			☑
- Les données liées aux situations d'exercice du porteur.	-	-	-
Mode d'exercice	☑	☑	☑
Code statut – Niveau de responsabilité	☑	☑	☑
Titre			☑
Spécialité d'exercice ADELI		☒	☒
Spécialité d'exercice RPPS			
Tableau de pharmacien	☑	☑	☑
Filière étude pharmacie			☒
Situation professionnelle			☒
Spécialisation			☒
Orientations Particulières			☒
Attributions complémentaires			☒
Identification nationale ADELI (volet CPS2ter)		☑	
Identification nationale de la structure	☑	☑	☑
Raison sociale de la structure	☑	☑	☑
Secteur d'activité ADELI (volet CPS2ter)		☑	☒
Date de début et de fin des situations d'exercice		☒	
Les données accessibles en mode sans contact ;			
Numéro de série sans contact	☑		
Identifiant technique	☑		
Certificat technique d'authentification	☑		
Zone de données applicatives	☑		
Les données du Domaine Assurance Maladie (DAM)			
Inchangées	☑	☑	

Tableau 3 – Différences entre les données métier CPS3 / CPS2ter

Les données sur la carte elle-même :

Elles restent identiques dans les 2 volets CPS2ter et IAS ECC sauf une petite modification de la date de fin de validité qui est avancée de 2 heures afin de tenir compte des changements d'heure annuels. Par ailleurs, les codes confidentiels et de déblocage changent avec les CPS3.

Les données PS en tant que personne physique :

Elles restent identiques dans les 2 volets CPS2ter et IAS ECC ;

Les données « porteur » en tant que professionnel de santé :

- Les Codes Profession pour les PS et Future Profession pour les professionnels en formation, toujours présents à l'identique dans le volet CPS2ter sont codés dans 2 champs distincts dans le volet IAS ECC ;
- Le Code Métier supprimé du volet IAS ECC et n'est plus renseigné dans le volet CPS2ter ;
- L'information « Situation professionnelle » qui existe uniquement et obligatoirement pour les PS qui n'exercent pas, comme par exemple les retraités, n'est plus stockée dans la carte mais reste publiée dans l'annuaire.

Les informations suivantes ne sont plus renseignées dans le volet CPS2ter ou remplacées par d'autres :

- Orientations Particulières	. ne concerne que les Médecins ; . reste publié dans l'annuaire ;
- Spécialisation	. ne concerne que les Sages-femmes, Masseurs-Kinésithérapeutes et les Auxiliaires de santé ; . reste publié dans l'annuaire ;
- Attribution(s) Complémentaire(s) ADELI	. ne concerne que les Médecins et les Chirurgiens-Dentistes. . ne seront plus publiées dans l'annuaire
- Attribution(s) Complémentaire(s) RPPS	. ne concerne que les Médecins et les Chirurgiens-Dentistes (remplacent les Autres Compétences ADELI)
- Autres Compétences ADELI	. (Couples : Spécialité + Nature de Qualification) : . ne concerne que les Médecins, Chirurgiens-Dentistes et Pharmaciens. . non publiées dans l'annuaire)
- Autres Compétences RPPS	. Savoir-faire RPPS . ne concerne que les Médecins et Chirurgiens-Dentistes (remplacent les Autres Compétences ADELI).

Les données liées aux situations d'exercice :

Les informations suivantes ne sont plus renseignées ni dans le volet CPS2ter ni le volet IAS ECC et ne sont plus publiées dans l'annuaire :

- Spécialité d'exercice ADELI
- Filière étude pharmacie
- Situation professionnelle
- Spécialisation
- Orientations Particulières
- Attributions complémentaires
- Forme juridique de la structure
- Dates début et fin de validité des situations d'exercice

6 ANNEXES

6.1 Annexe 1 : compléments techniques

6.1.1 L'architecture matérielle

La carte CPS3 embarque un microprocesseur associé à un coprocesseur cryptographique. L'ensemble est évalué sécuritairement selon les Critères Communs au niveau EAL4+ (au minimum).

Le schéma qui suit est une représentation générique du composant électronique de la CPS3 :

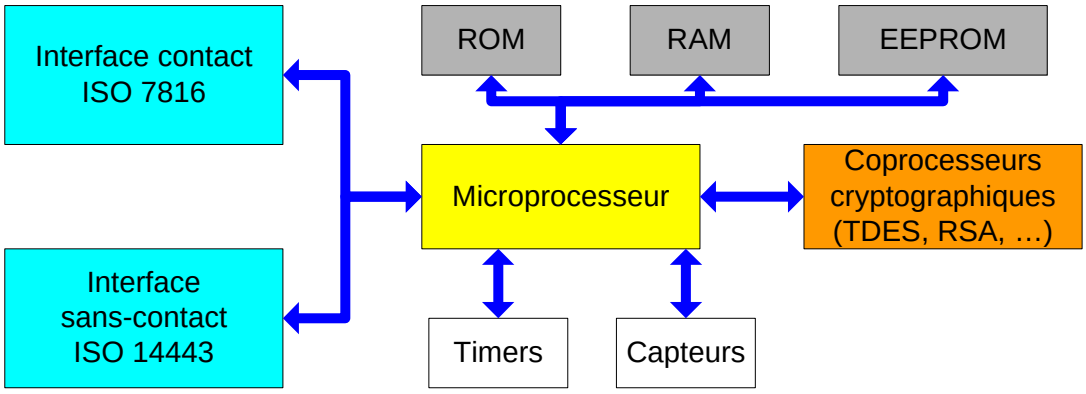

Figure 1 – Représentation générique du composant électronique de la CPS3

Le but n'est pas ici de rentrer dans le détail du fonctionnement de chaque élément mais de bien faire apparaître le lien existant entre les interfaces de communication et les fonctionnalités applicatives accessibles. La carte CPS3 est une carte dite « Dual Interface » ce qui signifie que :

- elle comporte un seul composant.
- ce composant intègre deux interfaces de communication : l'une pour le mode contact et l'autre pour le mode sans contact.

En théorie, les fonctionnalités accessibles dans les modes contact et sans contact sont potentiellement les mêmes : ce sont celles des applications CPS2ter et IAS ECC. Toutefois, la stratégie de migration et les contraintes liées à l'utilisation du sans contact impliquent des limitations qui seront exposées au §6.4.2 – Le mode sans contact.

En termes de conformité aux standards applicables dans ce domaine, la carte CPS3 assure :

- le mode contact en conformité avec la norme ISO 7816-3 selon le protocole T=0.
- le mode sans contact de proximité (distance <10cm) en conformité avec la norme ISO 14443 en type A ou B en fonction des différentes sources de composant du fournisseur de l'ASIP Santé.

6.1.2 L'architecture logicielle

La carte CPS3 repose sur une plateforme Javacard.

Comme indiqué précédemment, elle est multi-applicative et contient :

- Une application CPS2ter pour assurer la continuité de service et la compatibilité terrain.
- Une application IAS ECC qui est le standard retenu pour la carte CPS en phase cible.

Le schéma qui suit présente l'architecture logicielle générale de la CPS3 :

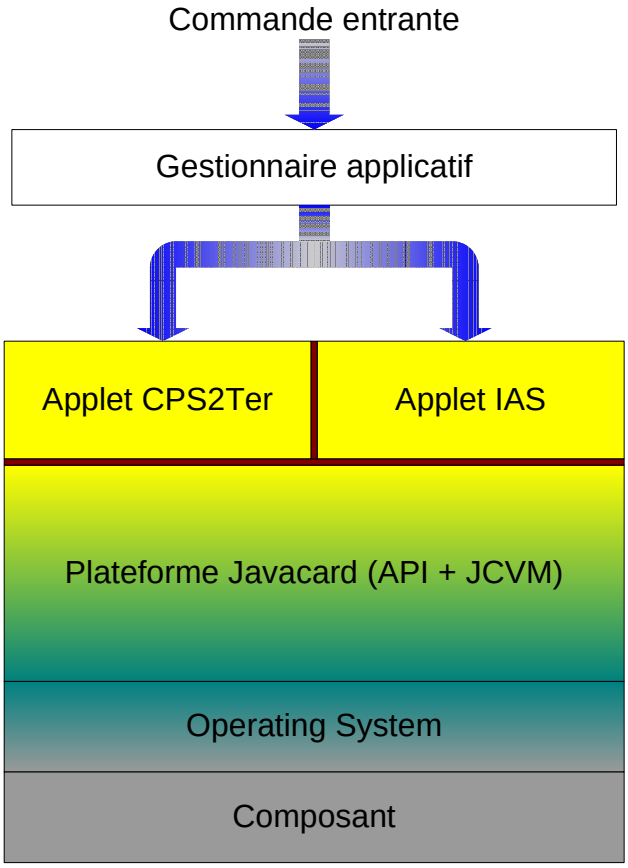

Figure 2 – Architecture logicielle générale de la CPS3

Ce schéma montre que le mode de compatibilité CPS2ter est géré au niveau le plus bas possible, c'est-à-dire au niveau de la carte. L'orientation vers l'applet CPS2ter des commandes qui lui sont destinées est faite en interne ce qui rend le passage de la carte CPS2ter vers la carte CPS3 transparent pour les solutions existantes.

6.2 Annexe 2 : impacts sur les architectures de poste de travail

Les paragraphes qui suivent présentent l'architecture logicielle du poste de travail pour l'accès à la carte CPS3 en fonction des différentes configurations terrain possibles.

Les modalités d'accès à la carte CPS2ter actuelle sont également représentées de manière à faire apparaître :

- La compatibilité de la CPS3 avec les modes d'accès existants.
- Les éléments impactés par la migration vers IAS ECC.

Nota : dans les différents schémas, la carte CPS3 apparaît avec un visuel vierge (corps de carte blanc) pour faciliter la compréhension. Dans la réalité, le visuel CPS3 sera celui qui a décrit au paragraphe *« Annexe 3 : nouveau visuel pour la carte CPS3 »*.

Les conventions utilisées dans les schémas qui vont suivre sont les suivantes :

- Les flèches en orange représentent les accès aux fonctionnalités CPS2ter au travers des Cryptolib-CPS et API CPS.
- Les flèches en vert représentent les accès aux fonctionnalités CPS2ter au travers des composants d'interface liés à l'environnement SESAM VITALE.
- Les flèches en bleu représentent les accès aux fonctionnalités IAS ECC au travers du Middleware IAS.

Les combinatoires impactant l'architecture du poste de travail dépendent d'une part du type de carte considéré et d'autre part des types de lecteurs qui équipent le poste de travail.

Différentes configurations nominales sont décrites ci-après, sachant qu'elles peuvent potentiellement cohabiter sur le même poste de travail :

- Fonctionnalités CPS2ter en mode contact hors domaine assurance maladie ;
- Fonctionnalités CPS2ter en mode contact dans le domaine assurance maladie ;
- Nouvelles fonctionnalités CPS3 en mode contact via un lecteur PC/SC ;
- Nouvelles fonctionnalités CPS3 en mode sans-contact via un lecteur PC/SC
- Nouvelles fonctionnalités CPS3 en mode sans-contact via d'autres lecteurs non PC/SC

6.2.1 *Fonctionnalités CPS2ter en mode contact hors domaine assurance maladie*

Dans cette configuration, le poste de travail comprend des applications accédant à la ressource carte via un lecteur unique standard de type PC/SC. Aucune des applications ne requiert de lecteur Sesam-Vitale.

Ces applications utilisent les données CPS2ter mais pas les données d'assurance maladie.

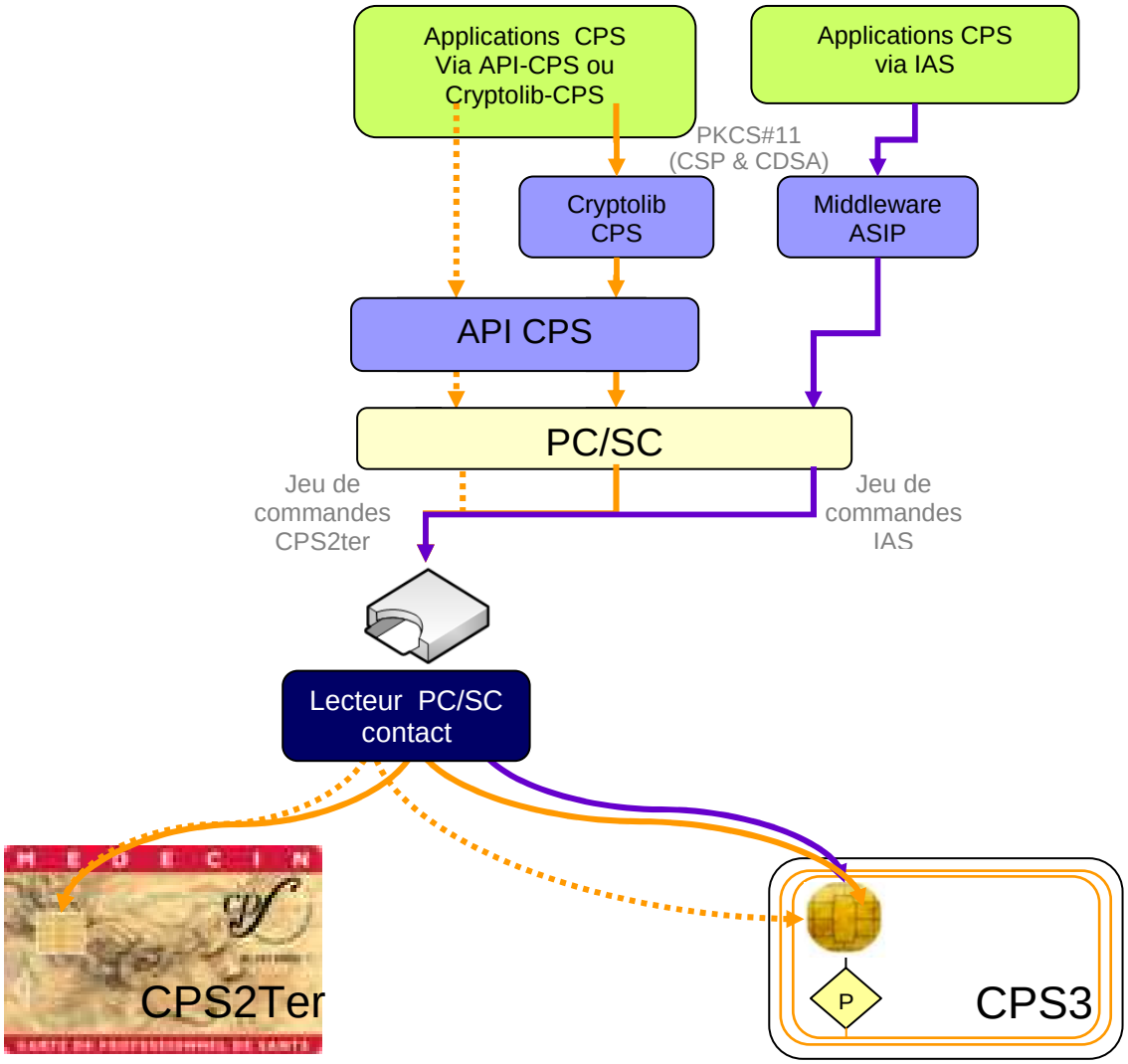

Figure 3 – Accès carte en mode CPS2ter contact (hors Assurance Maladie)

On voit sur cette figure que les modes d'accès actuels aux fonctionnalités CPS2ter sont conservés à l'identique. Pour garantir le fonctionnement des solutions actuelles lors de la migration de la carte CPS2ter vers la carte CPS3, il n'y a pas de mise à jour à faire au niveau des composants CPS (Cryptolib-CPS et API) ni de nouveau Middleware à installer.

A terme, ces solutions devront toutefois évoluer en intégrant le Middleware IAS notamment pour faire migrer les fonctionnalités CPS2ter vers les fonctionnalités équivalentes offertes par l'IAS ECC.
Le comportement du poste à l'insertion d'une carte devient alors le suivant :

- Insertion d'une carte CPS2ter :
  - Seule l'application utilisant le middleware CPS (ou les API-CPS) sera en mesure d'exploiter la carte ;
  - Si l'application IAS tente d'accéder à la carte, un code d'erreur du type « carte inconnue » sera remonté par le middleware IAS

- Insertion d'une carte CPS3 :
  - Les 2 types d'applications pourront accéder à la carte, chacune d'elles utilisant le middleware pour lequel elles sont paramétrées et qui utilisera le jeu de commandes correspondant vers la carte

6.2.2 Fonctionnalités CPS2ter en contact et dans le domaine assurance maladie

Cette configuration comprend au moins un lecteur Sesam-Vitale attaché au poste et d'autres applications peuvent potentiellement utiliser un autre type PC/SC.

Les applications ne traitent que des CPS2ter.

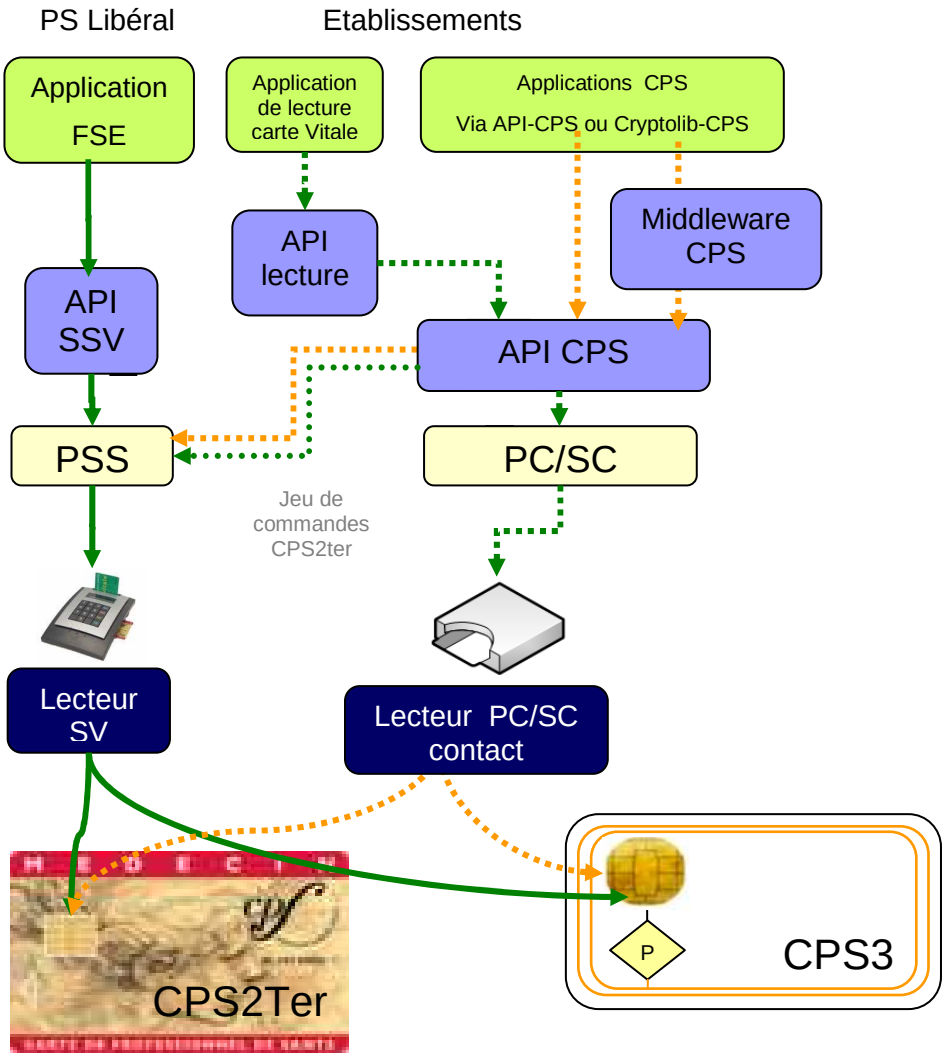

Figure 4 – Accès carte en mode CPS2ter contact (domaine Assurance Maladie)

Comme précédemment, on voit que la migration de la carte CPS2ter vers la carte CPS3 n'implique pas de mise à jour ou d'évolutions au niveau des éléments d'interface. Seules les fonctionnalités CPS2ter sont accessibles sur la CPS3.

L'utilisation des lecteurs bi-fentes homologués par le GIE Sesam-Vitale n'est pas non plus impactée.

6.2.3 Nouvelles fonctionnalités CPS3 en mode contact via un lecteur PC/SC

Il s'agit ici d'une configuration permettant à une application d'accéder aux nouvelles fonctionnalités apportées par la carte CPS3 et accessibles exclusivement via le jeu de commandes IAS ECC. Un lecteur PC/SC est utilisé à cet effet.

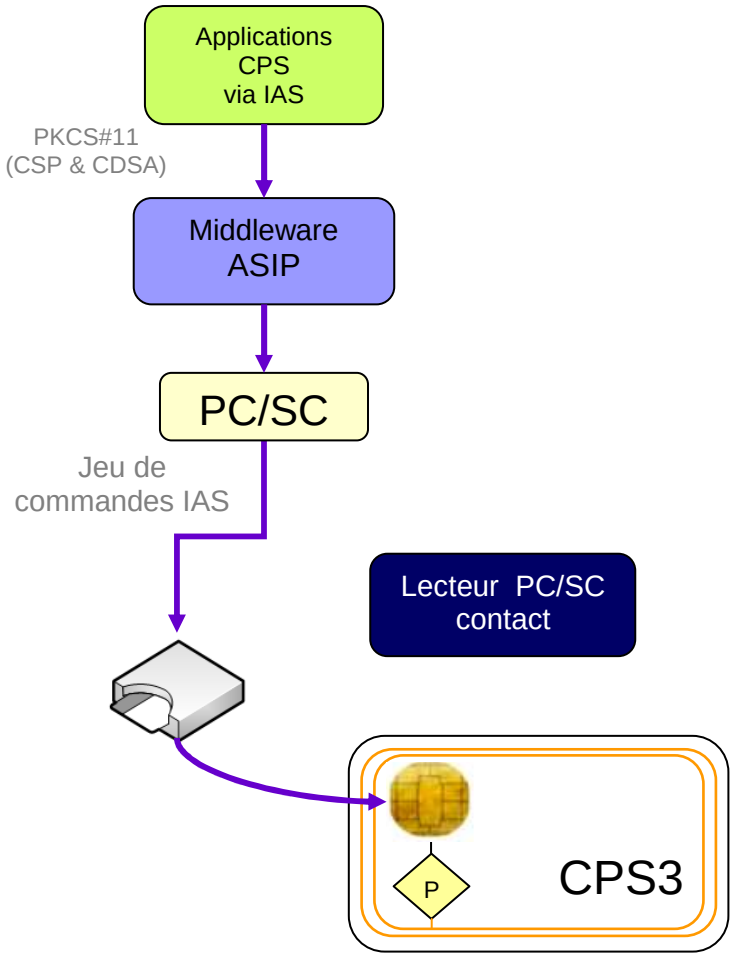

Figure 5 – Accès carte en mode contact pour les nouvelles fonctionnalités IAS

Les nouvelles fonctionnalités offertes par la CPS3 sont ajoutées uniquement du côté de l'application IAS ECC (logique de migration).En utilisant le middleware IAS, l'application pourra aussi bien accéder aux données métier et fonctionnalités CPS2ter qu'aux nouvelles fonctionnalités de la CPS3.
Le comportement du poste à l'insertion d'une carte devient alors le suivant :

- Insertion d'une carte CPS2ter :
  - Si l'application IAS tente d'accéder à la carte, un code d'erreur du type « carte inconnue » sera remonté par le middleware IAS
- Insertion d'une carte CPS3 :
  - L'application IAS détecte la présence d'une CPS3. Elle est alors en mesure d'activer ses nouvelles fonctionnalités (écriture/lecture de données, authentification simple sans saisie du PIN…)

6.2.4 *Nouvelles fonctionnalités CPS3 en mode sans contact via un lecteur PC/SC*

Cette configuration permet à une application d'accéder aux fonctionnalités sans contact apportées par la CPS3 en utilisant un lecteur sans contact conforme au standard PC/SC.

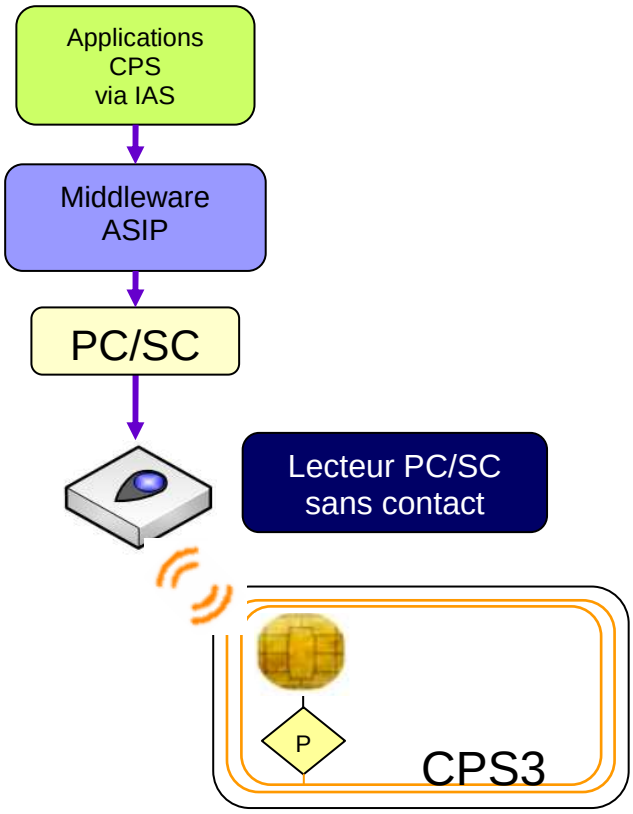

Figure 6 – Accès carte en mode sans contact pour les nouvelles fonctionnalités

Comme pour le mode contact, les nouvelles fonctionnalités offertes en mode sans contact ne sont accessibles que du côté IAS ECC et nécessiteront donc l'utilisation du Middleware IAS.

Les lecteurs à utiliser doivent être des lecteurs PC/SC compatibles ISO 14443 en types A et B.

Du fait des contraintes propres au mode sans contact (cf. §6.4.2.1), les données nominatives ne sont pas accessibles librement en mode sans contact.

Si ce besoin était confirmé, alors l'accès à ces données doit être conditionné par la mise en place d'un canal sécurisé entre la carte et le lecteur, ce dernier devant être équipé d'un module de sécurité.

En l'état actuel de l'offre industrielle, cette solution impose des contraintes techniques et organisationnelles qui restent à étudier, telles que la diffusion des clés lecteurs.

6.2.5 *Nouvelles fonctionnalités CPS3 en mode sans-contact via d'autres lecteurs*

Il s'agit ici de configurations basées sur des lecteurs qui ne sont pas au standard PC/SC. Cela pourrait par exemple être le cas de lecteurs de contrôle d'accès physique embarquant ou non la capacité de gérer le jeu de commandes IAS de la CPS3.

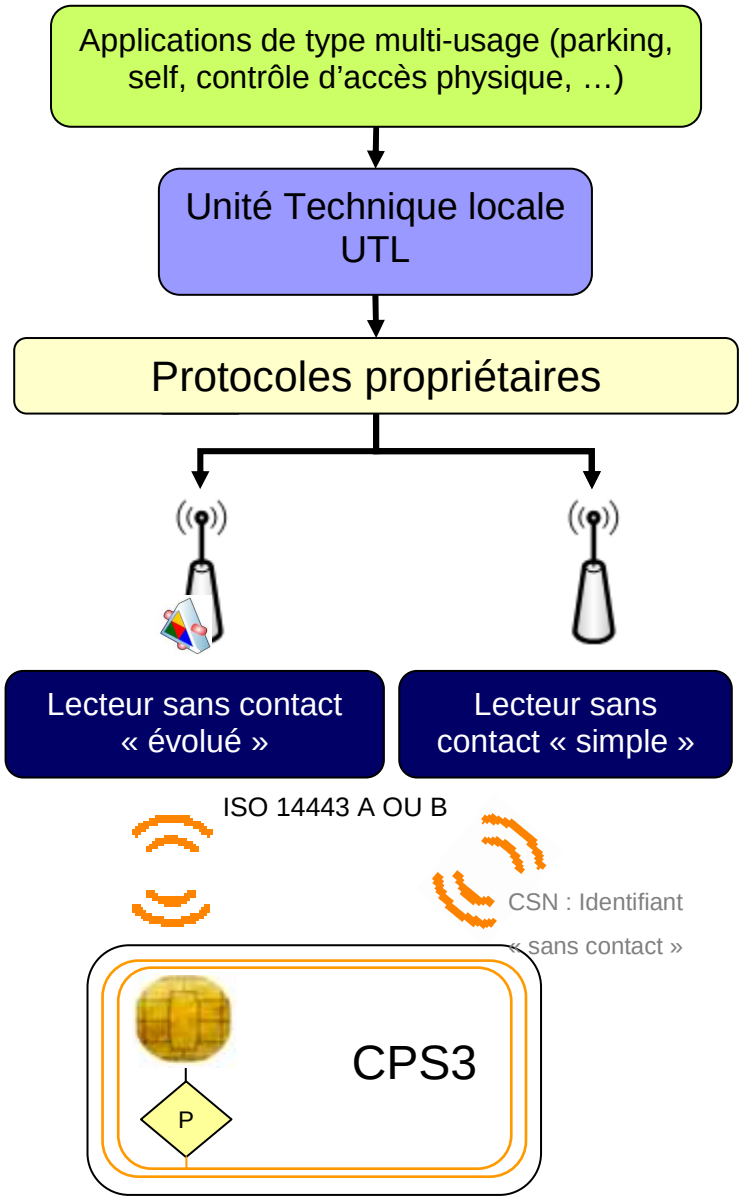

Figure 7 – Accès carte complémentaire en mode sans contact

Certaines applications de type multi-usage reposent sur l'utilisation de lecteurs spécifiques qui embarquent un logiciel dédié pour permettre l'accès à différents types de cartes.

Ces lecteurs peuvent être de 2 types :

- « simple » lorsqu'ils n'utilisent que les couches basses du protocole ISO14443 pour récupérer uniquement une donnée d'identification au niveau de la carte. Cet identifiant est un paramètre lié au protocole sans contact mis en œuvre : il s'agit de l'identifiant utilisé au cours de la phase dite d'anti-collision : l'UID pour le protocole de type A et le PUPI pour le protocole de type B.

  S'agissant d'un paramètre de protocole, sa récupération n'implique pas le niveau applicatif de la carte. En d'autres termes, l'applet IAS ECC (seule accessible en sans contact) n'est pas appelée pour la récupération de cet identifiant.

- « évolué » lorsque des fonctionnalités de niveau applicatif sont mises en œuvre (par exemple une authentification du support). Le lecteur doit alors embarquer un code exécutable permettant d'utiliser le jeu de commandes de l'applet présente dans la carte. Pour utiliser la carte CPS3 dans ce type d'environnement, le lecteur devra embarquer le jeu de commande et les mécanismes IAS ECC.

Dans tous les cas, les lecteurs utilisés doivent également être compatibles ISO 14443 en types A et B.

6.3 Annexe 3 : nouveau visuel pour la carte CPS3

Le visuel des cartes CPS2ter est rappelé ci-dessous à titre indicatif (cas d'une carte CPS médecin).

Figure 8 – Visuel de la carte CPS

Concernant les informations imprimées sur la carte, une légère modification du champ « identification du porteur » a été portée sur la CPS3 : le premier caractère est remplacé par une lettre afin de se mettre en conformité avec la nomenclature relative aux types d'identifiants. Ainsi, la lettre A correspondant aux identifiants ADELI est remplacée sur la carte par un « 0 ».

6.4 Annexe 4 : les services d'identification et d'authentification par la CPS3

6.4.1 Le mode avec contact

Dans ce mode, qui est le cas actuel d'utilisation de la carte CPS, l'ensemble des fonctions de la carte est accessible après son insertion dans un lecteur.

Les données CPS et fonctions cryptographiques sont accessibles aussi bien à partir des Cryptolib-CPS (CPS2ter) que du Middleware ASIP (CPS3 IAS).

Dans ce mode contact, le professionnel de santé peut s'authentifier « fortement » auprès d'applications locales ou distantes grâce à son code confidentiel et la mise en œuvre des fonctions cryptographiques d'authentification X.509 de la carte.

Il peut également signer électroniquement des documents et des messages en mettant en œuvre la clé de signature.

Ces services déjà mis en œuvre avec la carte CPS2ter sont reconduits avec la CPS3. Leur description n'est donc pas reprise ici.

Il est à noter que les services d'identification (cf. §6.4.2.3 et §6.4.2.4) et d'authentification simple (cf. §6.4.2.5) proposés en mode sans contact sont également disponibles en mode contact.

6.4.2 Le mode sans contact

6.4.2.1 Présentation

Le mode sans contact a été ajouté sur la CPS3 pour améliorer l'ergonomie lors de l'utilisation de la carte et pour développer de nouveaux usages.

Comme indiqué au §6.1.1, ce mode n'est qu'une nouvelle interface de communication entre la carte et son environnement extérieur. Techniquement, les services accessibles pourraient être en théorie les mêmes qu'en mode contact. Toutefois, d'autres éléments à prendre en compte impliquent des limitations ou des contraintes supplémentaires :

- La logique de migration implique un ajout des nouvelles fonctionnalités du côté du standard cible uniquement, c'est-à-dire du côté IAS ECC. Les fonctionnalités de l'applet CPS2ter ne sont donc pas accessibles en sans contact.
- Le mode sans contact est sujet à des risques qui n'existent pas en mode contact : la consultation des données de la carte à l'insu du porteur et la possibilité d'espionner les échanges entre la carte et le lecteur. Des mécanismes particuliers doivent alors être mis en œuvre pour garantir le respect de la vie privée de l'utilisateur et également empêcher sa traçabilité.

Pour tenir compte de ce dernier point sans utiliser une solution trop lourde, les règles suivantes sont appliquées aux données IAS ECC de la CPS3 :

- Les données nominatives ou d'identification nationale ne sont pas accessibles librement en mode sans-contact.
- Ajout d'un nouvel identifiant technique non lié au porteur accessible à la fois en mode contact et en mode sans contact.
- Ajout d'une nouvelle bi-clé RSA et du certificat technique associé (intégrant l'identifiant technique) d'authentification associé pour l'authentification du support en mode sans contact.

D'autre part, une zone de stockage d'informations applicatives, librement gérée par la solution exploitant la carte CPS3, est également ajoutée. Cette zone est en lecture libre contact et sans-contact et en écriture protégée par code confidentiel, en mode contact exclusivement.

En termes de services accessibles en sans contact, la CPS3 permet :

- L'identification simple de niveau protocolaire ISO 14443-3.
- L'identification simple de niveau applicatif.
- L'identification simple avec transport de données.
- L'authentification simple du support.

Ces différents services peuvent être combinés.

6.4.2.2 L'identification simple de niveau protocolaire ISO 14443-3

6.4.2.2.1 Présentation

C'est une utilisation qu'on retrouve principalement dans le domaine du multi-services (parking, self, contrôle d'accès physique) où une identification simple basée sur le numéro de série du support permet d'identifier le porteur. Un enrôlement est nécessaire initialement afin d'intégrer le porteur dans le parc des utilisateurs.

Dans ce mode, le numéro de série retourné est le numéro du composant sans contact inscrit à la fabrication par le fabricant de la puce. Techniquement, c'est en fait l'identifiant utilisé pour gérer les risques de collision de protocole, dans le cas où plusieurs cartes se trouveraient dans le champ du lecteur, conformément à la norme ISO14443-3.

La carte CPS3 utilise un identifiant d'anticollision non aléatoire.

L'échange de cet identifiant se fait dans le cadre du protocole ISO14443-3.

Ce service est présent sur la CPS3 pour des raisons de compatibilité avec les solutions terrain existantes basées sur d'autres types de support.

6.4.2.2.2 Mise en œuvre

La mise en œuvre de ce service s'effectue selon les étapes suivantes :

- Récupération de l'identifiant technique qui est l'identifiant d'anti-collision. Cet identifiant est un paramètre lié au protocole sans contact mis en œuvre, il s'agit de l'identifiant utilisé au cours de la phase dite d'anti-collision : l'UID pour le protocole de type A et le PUPI pour le protocole de type B.
- Réconciliation au niveau applicatif / SI de ce numéro de série du support avec l'identité nationale du porteur.
- Transmission de ce numéro de série aux niveaux supérieurs pour traitements et contrôles.

6.4.2.2.3 Avantages

- Utilisation avec n'importe quel lecteur sans contact compatible avec la norme ISO14443 (A et B).
- Simplicité.
- Intégration plus simple dans les systèmes de contrôle d'accès physique ou certaines solutions de type multi-services ne nécessitant pas un haut niveau de sécurité.

6.4.2.2.4 Inconvénients

- Pas de protection contre le clonage.
- Le cas échéant, cette fonctionnalité doit être combinée à une authentification forte afin de renforcer le niveau global de sécurité

6.4.2.3 L'identification simple de niveau applicatif

6.4.2.3.1 Présentation

A l'instar du cas précédent, le but est également d'identifier le porteur dans un contexte multi-services. L'application utilisatrice fait le lien entre un numéro identifiant et une personne ou un compte utilisateur défini lors de l'enrôlement.

Les données carte impliquées pour ce service sont :

- L'identifiant technique non lié au porteur (intégré aux données de l'applet IAS ECC).

6.4.2.3.2 Mise en œuvre

La mise en œuvre de ce service s'effectue selon les étapes suivantes :

- Récupération au travers du Middleware IAS de l'identifiant technique via un lecteur PC/SC.
- Réconciliation au niveau applicatif / SI de cet identifiant technique avec l'identité nationale du porteur.
- Transmission de cet identifiant aux niveaux supérieurs pour traitements et contrôles.

6.4.2.3.3 Avantages

- Simplicité.

6.4.2.3.4 Inconvénients

- Pas de protection contre le clonage.
- Un peu plus compliqué que le cas précédent mais offre une fonctionnalité simple d'identification utilisable dans une architecture IAS
- Le cas échéant, cette fonctionnalité doit être combinée à une authentification forte afin de renforcer le niveau global de sécurité

6.4.2.4 L'identification simple avec transport de données

6.4.2.4.1 Présentation

Le but est ici d'identifier le porteur et de partager des informations entre applications et dans un contexte multi-services. L'application utilisatrice fait le lien entre un numéro identifiant et une personne ou un compte utilisateur défini lors de l'enrôlement.

Elle récupère sur le support des informations applicatives (jeton de session par exemple) initialisées soit par elle-même (lors d'une ouverture de session antérieure par exemple) soit par une autre application afin de gérer la mobilité du porteur.

Les données carte (intégrées aux données de l'applet IAS ECC) impliquées pour ce service sont :

- L'identifiant technique non lié au porteur.
- La zone de stockage d'informations applicatives en lecture libre.

Les paramètres liés à cette zone de stockage (taille, conditions et modalités d'accès, …) seront définis dans un document consacré à la description détaillée de l'ensemble des données associées à l'applet IAS ECC de la CPS3.

6.4.2.4.2 Mise en œuvre

- Récupération au travers du Middleware IAS de l'identifiant technique via un lecteur PC/SC.

- Réconciliation au niveau applicatif / SI de cet identifiant technique avec l'identité nationale du porteur.
- Transmission de cet identifiant aux niveaux supérieurs pour traitements et contrôles.
- Lecture des informations applicatives transmises pour interprétation au niveau applicatif / SI.

Ce mode de fonctionnement suppose l'initialisation préalable de la zone de données avec des informations valides et exploitables. Cette initialisation est faite en mode contact suite à une authentification forte réussie. L'applicatif exploitant la CPS3 peut alors par exemple y inscrire un jeton de session qui sera valide pendant une durée limitée pour des réouvertures de sessions ultérieures en mode sans contact.

6.4.2.4.3 Avantages

- Meilleure ergonomie pour les situations de mobilité en architecture décentralisée (écriture de jetons de session, jetons de droits…).

6.4.2.4.4 Inconvénients

- Sécurité passive (pas de mise en œuvre de cryptographie par la carte) mais un peu plus renforcée par rapport aux deux autres cas d'identification simple.
- Pas de protection contre le clonage.
- Le cas échéant, cette fonctionnalité doit être combinée à une authentification forte afin de renforcer le niveau global de sécurité

6.4.2.5 L'authentification simple

6.4.2.5.1 Présentation

Le but est ici d'effectuer l'authentification du support, pour assurer la protection contre le clonage. En d'autres termes, l'applicatif vérifie au travers de ce service que le support présenté a bien été émis par l'ASIP Santé et que, par conséquent, les informations qu'il contient sont dignes de confiance.

Les données carte (intégrées aux données de l'applet IAS ECC) impliquées pour ce service sont :

- L'identifiant technique non lié au porteur.
- Le certificat technique associé non publié dans l'annuaire de l'ASIP Santé.
- La bi-clé RSA correspondant dans la carte (seule la clé privée est impliquée).

L'application utilisatrice fait le lien entre l'identifiant technique et une personne ou un compte utilisateur défini lors de l'enrôlement

6.4.2.5.2 Mise en œuvre

- Lecture du certificat technique via le lecteur pC/SC.
- Vérification de la validité du certificat technique (basé sur l'identifiant technique).
- Échange de type « défi– réponse » et vérification du cryptogramme généré par la carte pour vérifier que la carte contient bien la clé privée correspondant au certificat technique.
- Transmission de cet identifiant aux niveaux supérieurs pour traitements et contrôles.
- Lien entre identifiant technique et identifiant national à établir lors de l'enrôlement par l'applicatif.

6.4.2.5.3 Avantages

- Authentification du support.
- Protection contre le clonage.

6.4.2.5.4 Inconvénients

- Pas d’authentification du porteur, seulement du support carte. Cette authentification du porteur peut être effectuée par l’application si nécessaire.
- Pas de liste de révocation.
- Le cas échéant, cette fonctionnalité doit être combinée à une authentification forte afin de renforcer le niveau global de sécurité

6.5 Annexe 5 : synthèse des usages de la CPS3

	MODE DE LECTURE	DONNEE CARTE UTILISEE
Usages sans contact		
Contrôle d'accès physique		
o Identification du support en sans contact		
Identification du support physique	ISO 14443 A ou B	numéro de série du support (1) - pas de protection contre le clonage du support
Identification du support logique	IAS	identifiant technique CPS3 (2) - pas de protection contre le clonage du support
o Lecture du jeton applicatif	IAS	Zone de données applicatives (6)
o Authentification simple du support	IAS	Utilisation de la bi-clé technique et du certificat technique (4). Pas de saisie du code porteur. Protection contre le clonage du support
Contrôle d'accès logique		
o Identification du support en sans contact		
Identification du support physique	ISO 14443 A ou B	numéro de série du support (1) - mode déconseillé en contrôle d'accès logique, le numéro de série n'étant pas attribué par l'ASIP - pas de protection contre le clonage du support
Identification du support logique	IAS	identifiant technique CPS3 (2) - solution légère d'identification mais n'empêchant pas le clonage du support
o Lecture du jeton applicatif	IAS	Zone de données applicatives (6)
o Authentification simple du support	IAS	Utilisation de la bi-clé technique et du certificat technique (4). Pas de saisie du code porteur. Protection contre le clonage du support
Usages avec contact		
Contrôle d'accès physique		
o Identification du support en contact		
Identification du support logique	IAS	identifiant technique CPS3 (2) - pas de protection contre le clonage du support
o Lecture du jeton applicatif	IAS	Zone de données applicatives (6)
Contrôle d'accès logique		
o Identification du support		

	MODE DE LECTURE	DONNEE CARTE UTILISEE
en contact		
Identification du support physique	ISO 14443 A ou B	numéro de série du support (1) - mode déconseillé en contrôle d'accès logique, le numéro de série n'étant pas attribué par l'ASIP - pas de protection contre le clonage du support
Identification du support logique	IAS	identifiant technique CPS3 (2) - solution légère d'identification mais n'empêchant pas le clonage du support
o Ecriture du jeton applicatif	IAS	Zone de données applicatives (6)
o Lecture du jeton applicatif	IAS	Zone de données applicatives (6)
o Saisie PIN	IAS ou API-CPS (*)	Saisie du code confidentiel
o Authentification forte	IAS ou API-CPS (*)	avec certificat national
o Signature	IAS ou API-CPS (*)	avec certificat national
o Lecture données métier CPS2ter (ex : situations d'exercice)	IAS ou API-CPS (*)	ancien format ADELI
o Lecture données métier CPS3 (ex : situations d'exercice)	IAS ou API-CPS (*)	nouveau format RPPS
o Lecture certificat CPS2ter	IAS ou API-CPS (*)	IGC-CPS

(*) Compatibilité avec la CPS2ter de la CPS3

Certaines fonctions sont également accessibles en mode API CPS (cf. colonne mode de lecture)

Notes relatives au tableau des usages de la CPS3 :

1 - numéro de série du support	numéro anti-collision du protocole ISO 14443 (UID ou PUPI respectivement pour le type A et le type B) - 4 octets hexadécimaux - exemple : '1A 45 9F BD'-	Accessible exclusivement en sans contact et en protocole ISO 14443
2 - Identifiant technique CPS3	Identifiant technique constitué par un numéro unique attribué lors de la perso. de la carte (id. logique IAS). 19 caractères décimaux : [id ASIP(10)][n°unique support(8)] [clé(1)] - ex : 8025000001**12345678**3	Accessible via le jeu de commandes IAS aussi bien en mode sans-contact qu'en mode contact
3 - Identifiant national PS	Identifiant unique du porteur de la carte constitué par le numéro unique du professionnel de santé. Le format de cet identifiant dépend du type de porteur (cf. doc "données de la carte CPS")	Accessible via le jeu de commandes IAS aussi bien en mode sans-contact qu'en mode contact
4 - Certificat technique	Certificat de clé publique d'authentification raccroché à une Autorité de Certification CPS. - Pas de donnée nominative sur le porteur (pas publié dans l'annuaire CPS) - Certifie la validité et l'unicité de l'identifiant technique CPS3. - Nécessite un enrôlement initial dans le SIH	Accessible via le jeu de commandes IAS aussi bien en mode sans-contact qu'en mode contact
5 - Certificat national	Certificat de clé publique d'authentification, de signature ou de chiffrement Ils sont raccrochés à l'Autorité de Certification CPS. Ils certifient la validité et l'unicité de l'identifiant national PS. Ils sont publiés dans l'annuaire CPS	Accessible via le jeu de commandes IAS uniquement en mode contact
6 - Jeton applicatif	Zone de données de 4096 octets max.	Accessible via le jeu de commandes IAS uniquement Ecriture uniquement en mode contact protégée par le code confidentiel. Lecture libre en contact et sans-contact