



HospiConnect

Vers "Une identité numérique fiable et maîtrisée qui accède aux services numériques en santé"

Webinaire #2 - HospiConnect#ServicesSocles IE

24/03/2026

Agence du numérique en santé

Les Intervenants du jour



Florian Catteau
Directeur de Programme
ANS



Joachim Metzger
Directeur de Domaine
ANS

Webinaire, les bonnes pratiques



Je coupe mon micro
(sauf si je suis autorisé à
prendre la parole)



Je lève la main
avant de prendre
la parole



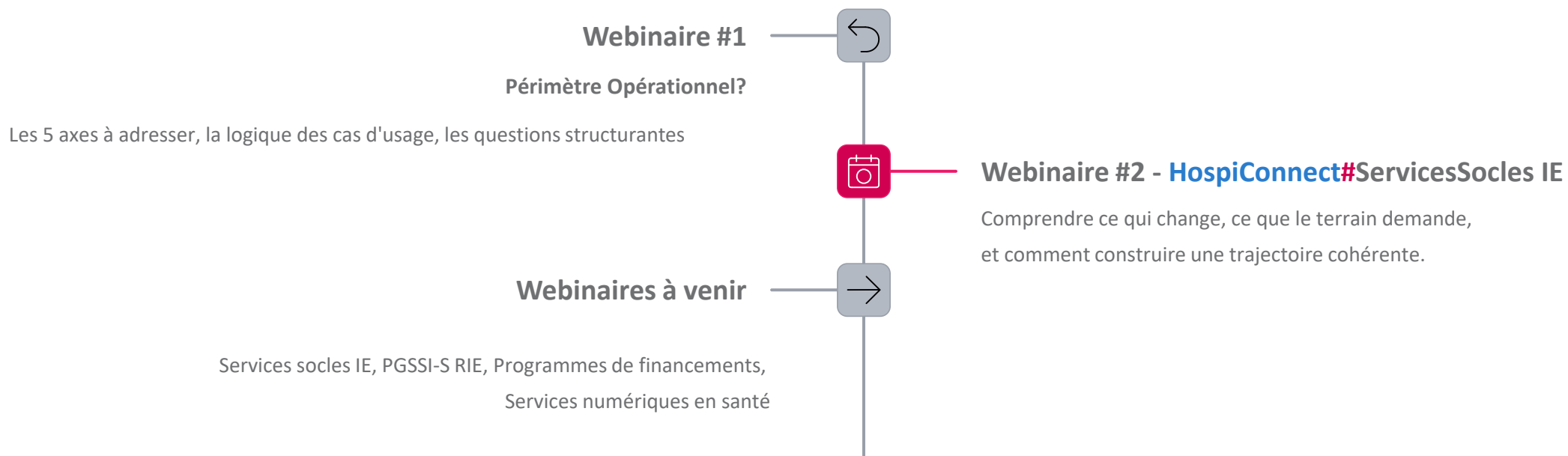
Activer la caméra **n'est pas nécessaire** pour le bon déroulé du webinaire



Je pose mes **questions** dans
l'**espace conversation**

Où se situe ce webinaire dans la série HospiConnect ?

Le webinaire #0 a posé les fondamentaux : le contexte, les enjeux, la trajectoire de l'identification électronique et la logique de la bannière unifiée HospiConnect. Le webinaire #1 a permis d'explicitier le périmètre opérationnel et rendre plus concrets les sujets que les établissements doivent adresser pour structurer leur démarche. Le webinaire #3 explicite l'articulation avec les services socles proposés par l'ANS.



 **Message clé** : Ce webinaire constitue le zoom sur les services socles proposés par la puissance publique relatifs à l'identification électroniques des professionnels.

PARCOURS WEBINAIRES

La série de webinaires HospiConnect : un parcours progressif

Cette série de six webinaires a été conçue comme un **parcours structuré et progressif**, permettant aux établissements de santé et à leurs partenaires de monter en compétence étape par étape. Chaque session aborde une facette complémentaire de la démarche HospiConnect. L'objectif est de construire une compréhension solide et actionnable, session après session.

Webinaire #0 - HospiConnect#BannièreUnifiée

[13/03] · Pourquoi HospiConnect ? Comprendre le cadre européen et national, la trajectoire Identification Électronique et la raison d'être de la démarche.

Webinaire #1 - HospiConnect#PérimètreOpérationnel

[19/03] · Faites le tour des sujets essentiels à prendre en compte pour comprendre la couverture complète du projet de transformation en établissement et engager votre démarche HospiConnect.

Webinaire #2 - HospiConnect#ServicesSocles IE

AUJOURD'HUI · Découvrez les évolutions récentes, les points clés à connaître et l'articulation entre les services socles et l'identification électronique pour mener votre projet et définir votre trajectoire.

Webinaire #3 - HospiConnect#ProgrammesDeFinancement

[26/03] · Focus sur le premier jalon à juin 2026 des programmes de financement HospiConnect/HOP'EN2 et HospiConnect/CaRE, point sur les dépenses éligibles et les livrables attendus.

Webinaire #4 - HospiConnect#RIE

[à venir] · Tout savoir sur la version 2 du Référentiel d'Identification Électronique de la PGSSI-S : exigences applicables aux moyens d'identification électronique et mise en œuvre concrète dans l'établissement.

Webinaire #5 - HospiConnect#SNS-DMP-mode AIR Simplifié

[à venir] · Focus sur le Dossier Médical Partagé (DMP) et le mode AIR Simplifié : comprendre les exigences d'accès aux Services Numériques de Santé, les conditions d'alimentation du DMP et la mise en œuvre du mode d'authentification AIR Simplifié en établissement.

 **Conseil** : suivez l'intégralité du parcours pour disposer d'une vision complète du contexte stratégique jusqu'aux leviers opérationnels et financiers.

PARCOURS WEBINAIRES

La série de webinaires du Ségur : prochaines sessions

En complément des webinaires HospiConnect, des sessions dédiées aux usages Ségur sont programmées. Elles permettent d'approfondir les cas d'usage concrets liés aux services numériques de santé.

Webinaire Ségur#Consentement à la Consultation du DMP

[Fin mai] · Consentement à la consultation du DMP : comprendre les règles applicables, les modalités de recueil du consentement patient et les impacts sur les pratiques des professionnels de santé en établissement.

Webinaire Ségur#MSS Fonction Réception

[Début juin] · MSS — Fonction réception : maîtriser les exigences liées à la messagerie sécurisée de santé, la fonction réception des documents et son articulation avec le DMP et les services numériques de santé.

 **Conseil** : Ces webinaires Ségur sont complémentaires au parcours HospiConnect. Ils approfondissent les cas d'usage concrets des services numériques de santé en établissement..

WEBINAIRE #2

Agenda du jour

- Contexte et Cadre Réglementaire

Comprendre la trajectoire imposée et les attentes européennes en matière d'identification.

- Retours Terrain et Réponses de l'ANS

Les défis rencontrés par les établissements et les solutions apportées par l'ANS.

- Pro Santé Connect et l'Espace de Confiance

Découverte des services socles et du concept d'espace de confiance numérique.

- Impact et Cas d'Usage Concrets

Ce que cela change pour vos établissements et des exemples d'implémentation.

- Conclusion et Perspectives

Synthèse des points clés et aperçu des prochaines étapes de déploiement.

 **Message clé** : Ce webinaire constitue le zoom sur les services socles proposés par la puissance publique relatifs à l'identification électroniques des professionnels.

CONTEXTE

Le cap sur une trajectoire imposée

La destination est fixée : converger vers un niveau de garantie substantiel et intégrer Pro Santé Connect dans la trajectoire cible. Les établissements conservent de la liberté sur les modalités de mise en œuvre, pas sur l'objectif à atteindre.

1

Cadre eIDAS / EHDS

Exigence de convergence vers un niveau de garantie substantiel pour l'accès aux services numériques en santé.

2

Trajectoire nationale IE

L'identification électronique doit converger vers un niveau de garantie équivalent au substantiel, avec une identité fiable, unique et suffisamment robuste pour les usages visés.

3

Pro Santé Connect dans le cadre

Pro Santé Connect est intégré par tous les services numériques en santé nationaux/régionaux. Il peut être utilisé comme moyen principal ou comme moyen alternatif en local.

 **Message clé** : La cible est claire : converger vers le substantiel et intégrer PSC

ANALYSE TERRAIN

Ce que le terrain a exprimé

HospiConnect ne traite pas un sujet isolé, mais une chaîne complète, de l'identité professionnelle jusqu'à l'accès aux services numériques. Les retours terrain confirment la nécessité d'une approche globale et cohérente.

Industrialisation de la création d'identité

Industrialiser les parcours de gestion d'identité, aujourd'hui encore trop dépendants d'actions manuelles ou autonomes du professionnel.

Synchronisation des activités local / national

Éviter les ruptures entre SI local et système national, en particulier pour la gestion des activités et la mise à jour des données.

Gestion opérationnelle des cartes physiques

Simplifier la gestion opérationnelle des MIE physiques de l'ANS, en tenant compte des situations réelles rencontrées dans les établissements.

Qualité et interopérabilité du répertoire d'identité

Renforcer l'interopérabilité entre outils locaux et référentiel national sectoriel, notamment pour le rapprochement des identités et la diffusion d'un identifiant fiable.



Message clé : Le vrai enjeu n'est pas un dispositif isolé, mais la cohérence d'ensemble de la chaîne d'identification électronique.

REPONSE ANS

La réponse de l'ANS : entre le cadre réglementaire et l'analyse des retours terrain

La réponse ANS articule cadre réglementaire et analyse des retours terrain. Elle ne consiste pas à imposer un outil unique, mais à structurer un espace de confiance dans lequel chaque établissement peut s'inscrire selon sa maturité.

Mieux gérer l'identité sectorielle

Via ProSanté Identité (PSI) : outiller l'enrôlement.

Ouvrir à des MIE adaptés

Le cadre reconnaît plusieurs types de moyens d'identification (ANS ou tiers) dès lors qu'ils répondent aux exigences de niveau substantiel et d'interopérabilité avec PSC.

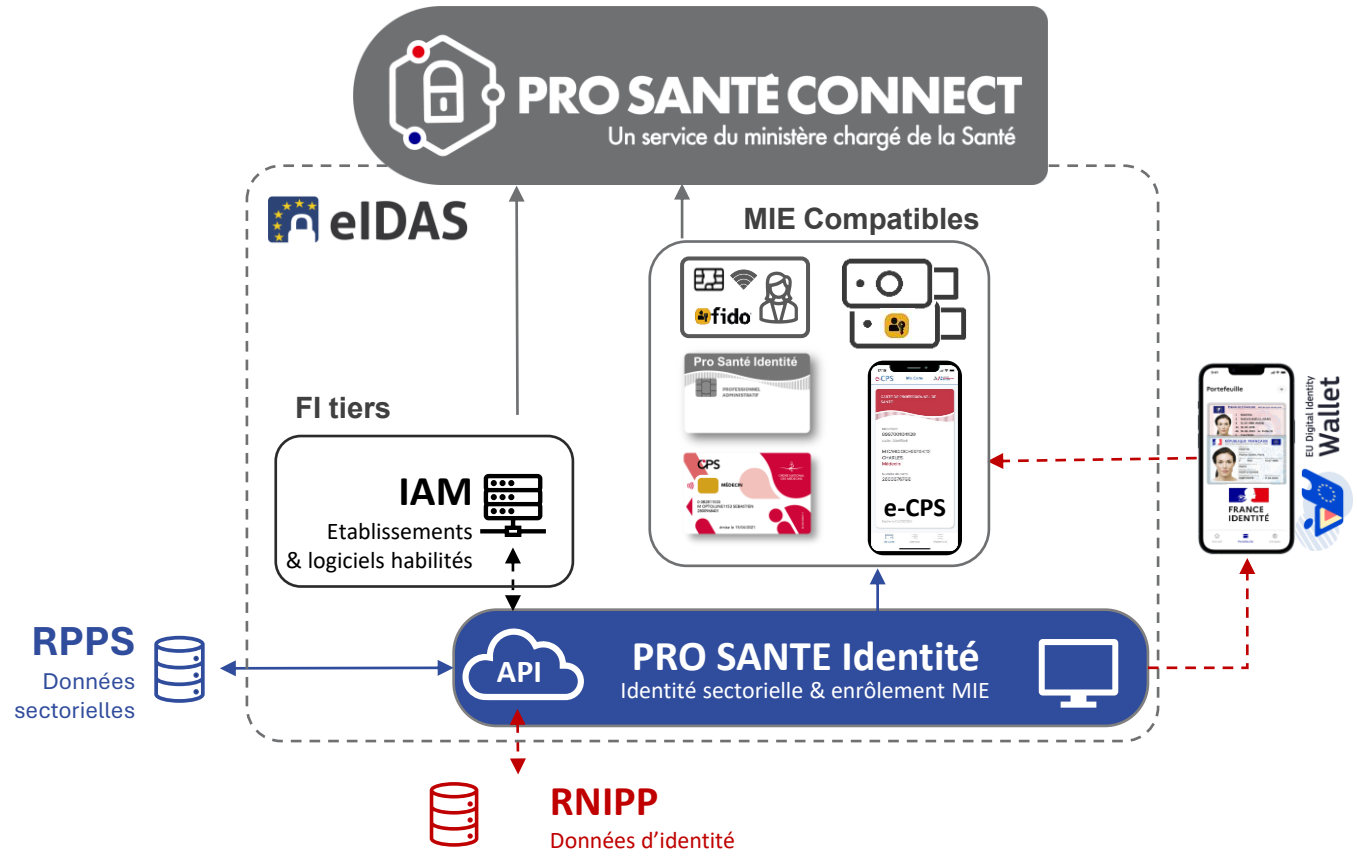
Mieux articuler RPPS / IAM / PSC

Le rapprochement entre identité locale, RPPS / RNIPP et Pro Santé Connect devient central, avec des mécanismes industrialisés de libre-service et de synchronisation RPPS accessibles via API.

 **Message clé** : L'enjeu n'est plus seulement d'identifier, mais de relier durablement identité locale, référentiels nationaux et accès via Pro Santé Connect.

REPONSE ANS – L'ESPACE DE CONFIANCE

La réponse de l'ANS : l'espace de confiance



- Synchro **RNIPP** (notifications)
- Avec RPPS** : services numériques en santé
- Hors RPPS** : services administratifs
- Accès **Web** ou **API** pour les établissements (IAM)
- Gestion des **MIE compatibles**: enrôlement avec e-CPS, commande de cartes ANS (CPS, PSI)
- Utilisation du **EUDI Wallet** (France Identité) : niveau de garantie substantiel

Message clé : L'enjeu n'est plus seulement d'identifier, mais de relier durablement identité locale, référentiels nationaux et accès via Pro Santé Connect.

REPONSE ANS – L'ESPACE DE CONFIANCE

La réponse de l'ANS : l'espace de confiance



Pro Santé Connect (PSC)

Fédérer la confiance. Pivot national de l'espace de confiance, FI notifié eIDAS niveau substantiel.



Pro Santé Identité (PSI)

Industrialiser l'identité. Portail libre-service, API : structure le cycle de vie de l'identité sectorielle.



MIE conformes

Ouvrir les supports. Carte, badge, clé logicielle : tout MIE reconnu conforme PSC peut entrer dans le cadre.



FI Tiers

Raccorder le local au national. Permet à un établissement disposant d'un schéma local conforme de se connecter à PSC.

 **Message clé** : L'enjeu n'est plus seulement d'identifier, mais de relier durablement identité locale, référentiels nationaux et accès via Pro Santé Connect.

EDC – PRO SANTE CONNECT

Pro Santé Connect (PSC) : le service socle à l'état de l'art conforme au RIE

“ Dans l'espace de confiance, Pro Santé Connect est la porte d'accès proposée pour une identification vérifiée et une authentification garantie à tous les services numériques en santé. ”

PSC en tant que Fédérateur de Fournisseurs d'Identité
est le garant de son Espace De Confiance

Imposé pour les accès nationaux et régionaux

Quel que soit le MIE retenu par l'établissement, PSC doit rester accessible aux Professionnels.
C'est une exigence, pas une recommandation.

Principal ou alternatif

PSC peut être la voie d'authentification principale, ou une voie de secours. Les deux configurations sont valides dans le RIE.

Solution de secours obligatoire si nominal

Si PSC est la solution nominale, une alternative doit être disponible. L'établissement doit anticiper la continuité d'accès à ses services locaux en cas d'indisponibilité.

 **Message clé** : Le sujet n'est pas de choisir entre PSC et une architecture locale : le sujet est de garantir que PSC reste toujours accessible

Pro Santé Identité : une identité vérifiée

Pro Santé Identité (PSI) est l'intermédiaire opérationnel qui permet aux établissements de prendre en main la gestion industrialisée des identités sectorielles vérifiées. Il s'appuie sur le RPPS et expose des interfaces adaptées à tous les niveaux de maturité technique.

PSI en tant que sas d'enregistrement
est le garant de la gestion des identités de l'Espace De Confiance PSC

Portail libre-service

Interface web permettant aux professionnels de gérer eux-mêmes leur identité sectorielle : création, mise à jour, rattachement à une activité RPPS.

API pour les établissements

Des API permettent aux structures d'automatiser l'enrôlement, la synchronisation et la gestion du cycle de vie des identités directement depuis l'IAM local.

Lien identité / RPPS / MIE

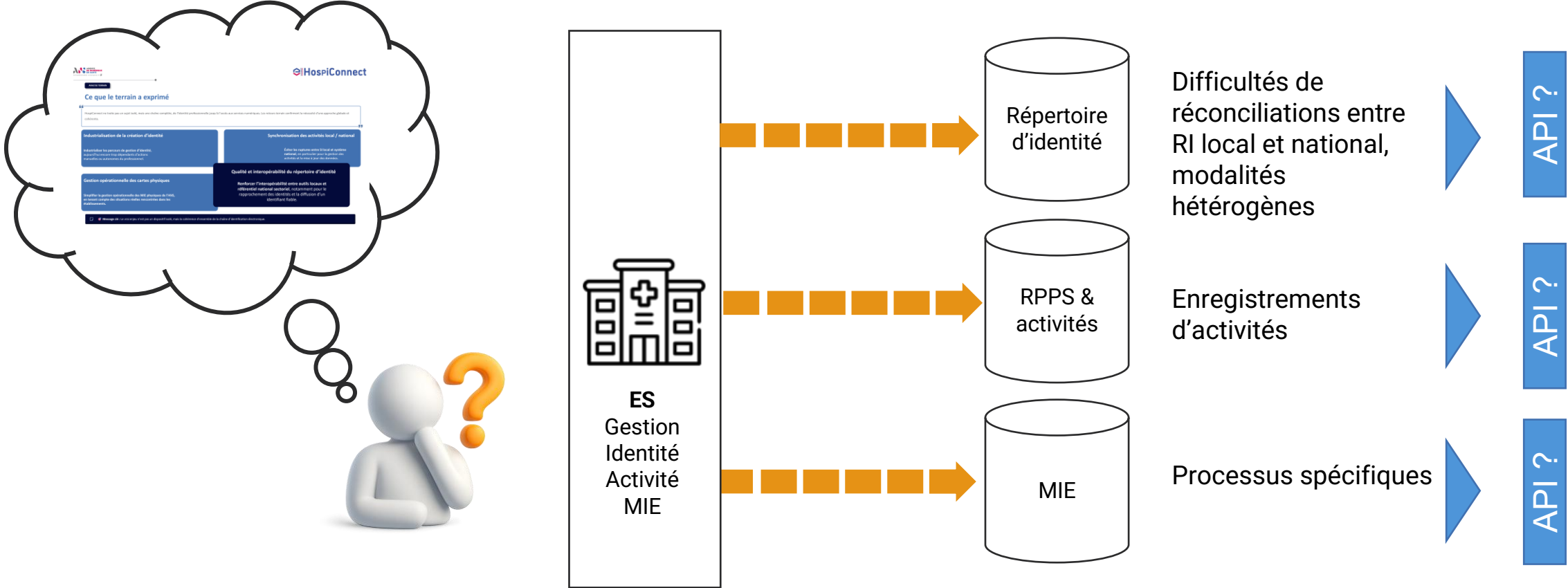
Pro Santé Identité assure la cohérence entre l'identité nationale, le référentiel RPPS, les MIE associés et l'identité locale.

 **Message clé :** Le sujet n'est pas de choisir entre PSI et gestion d'identité locale : le sujet est de garantir que l'identité locale est toujours vérifiée pour des accès aux données santé.

EDC – PRO SANTE IDENTITE

Pro Santé identité : un SAS d'enregistrement

Pro Santé Identité (PSI) est l'intermédiaire opérationnel qui permet aux établissements de prendre en main la gestion industrialisée des identités sectorielles vérifiées. Il s'appuie sur le RPPS et expose des interfaces adaptées à tous les niveaux de maturité technique.

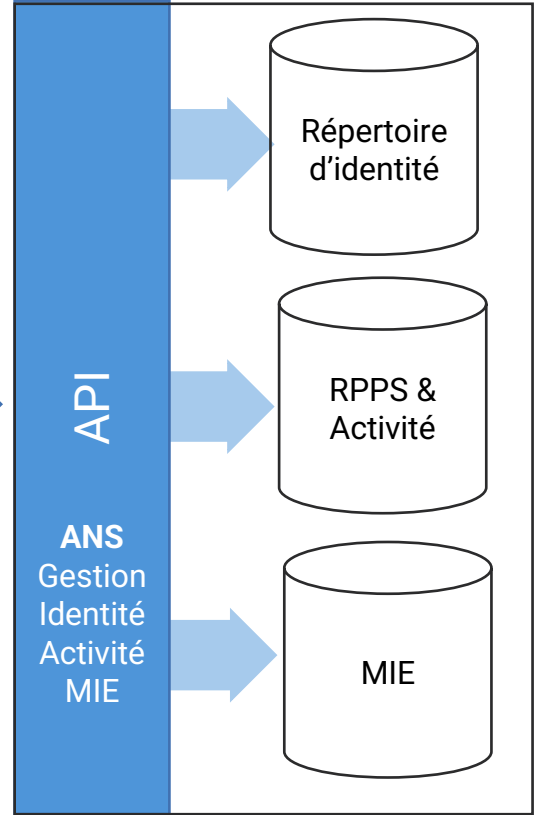
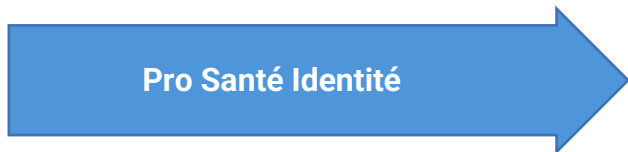


Pro Santé identité : un point d'entrée unique

Pro Santé Identité (PSI) est l'intermédiaire opérationnel qui permet aux établissements de prendre en main la gestion industrialisée des identités sectorielles vérifiées. Il s'appuie sur le RPPS et expose des interfaces adaptées à tous les niveaux de maturité technique.

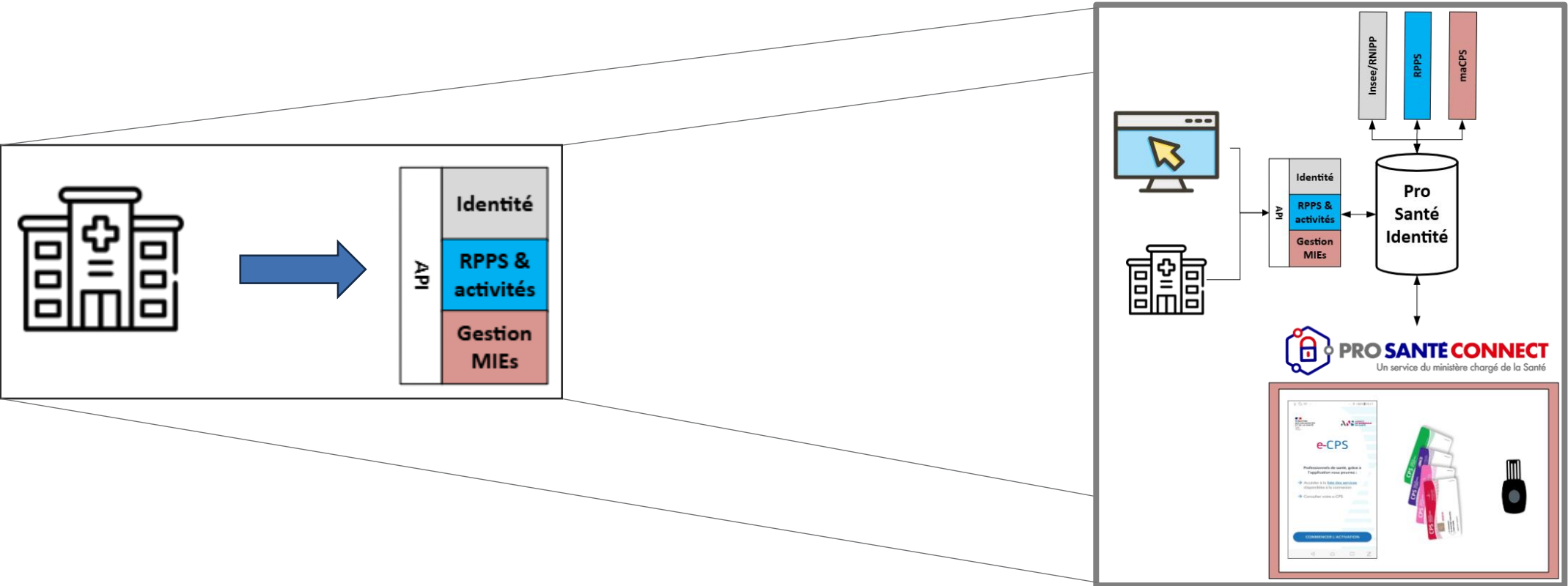
Pro Santé Identité

Mise à disposition d'un **flux unique pour les ES** permettant de répondre aux besoins de gestion des accès et des identités de manière centralisée et industrialisée



Pro Santé identité : une complexité masquée

Pro Santé Identité (PSI) est l'intermédiaire opérationnel qui permet aux établissements de prendre en main la gestion industrialisée des identités sectorielles vérifiées. Il s'appuie sur le RPPS et expose des interfaces adaptées à tous les niveaux de maturité technique.



EDC – PRO SANTE IDENTITE

Pro Santé identité : impact sur l'offre historique

“ Le modèle historique de la CPE est incompatible avec une trajectoire eIDAS Substantiel. ”

La CPS est construite pour une identité nationale sectorielle vérifiée, ce qui inclut : l'identifiant national sectoriel RPPS, l'ensemble des activités du professionnel et le visuel spécifique à sa profession.

La CPS inclut des certificats issus d'une Autorité de Certification (AC) particulière dite AC Racine « FORT ».

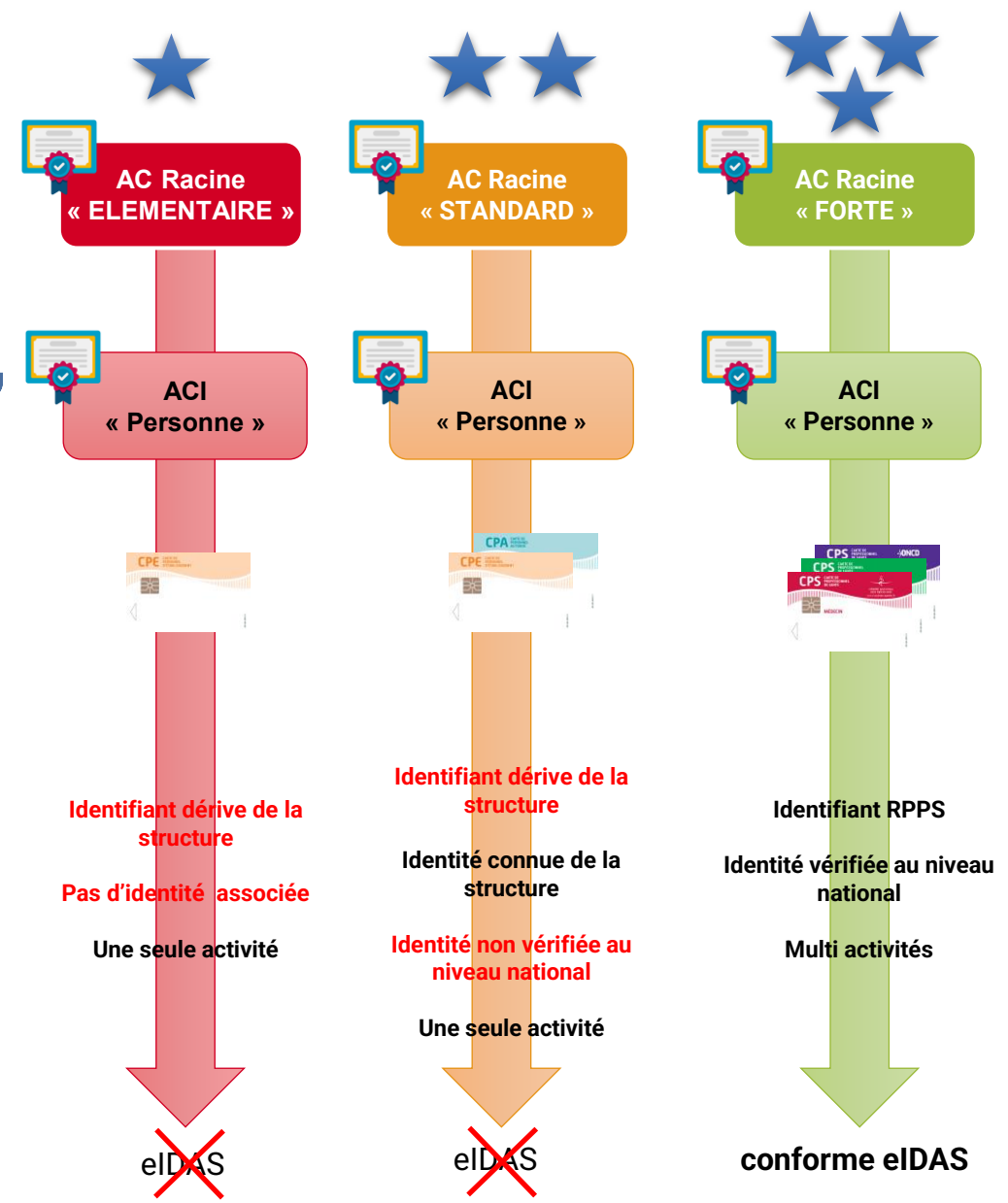
L'identifiant national sectoriel RPPS est un identifiant unique à 11 chiffres : [12345678901].

La CPE est construite pour une identité spécifiée ou non avec un identifiant local lié à la structure dont elle hérite l'activité.

La CPE inclut des certificats issus d'une des deux AC dites AC Racine « ELEMENTAIRE » et AC Racine « STANDARD ».

L'identifiant d'une CPE est un identifiant construit par l'identifiant de la structure [X...X] et un identifiant local [Y...Y] à la discrétion de cette dernière : [X...X]/[Y...Y].

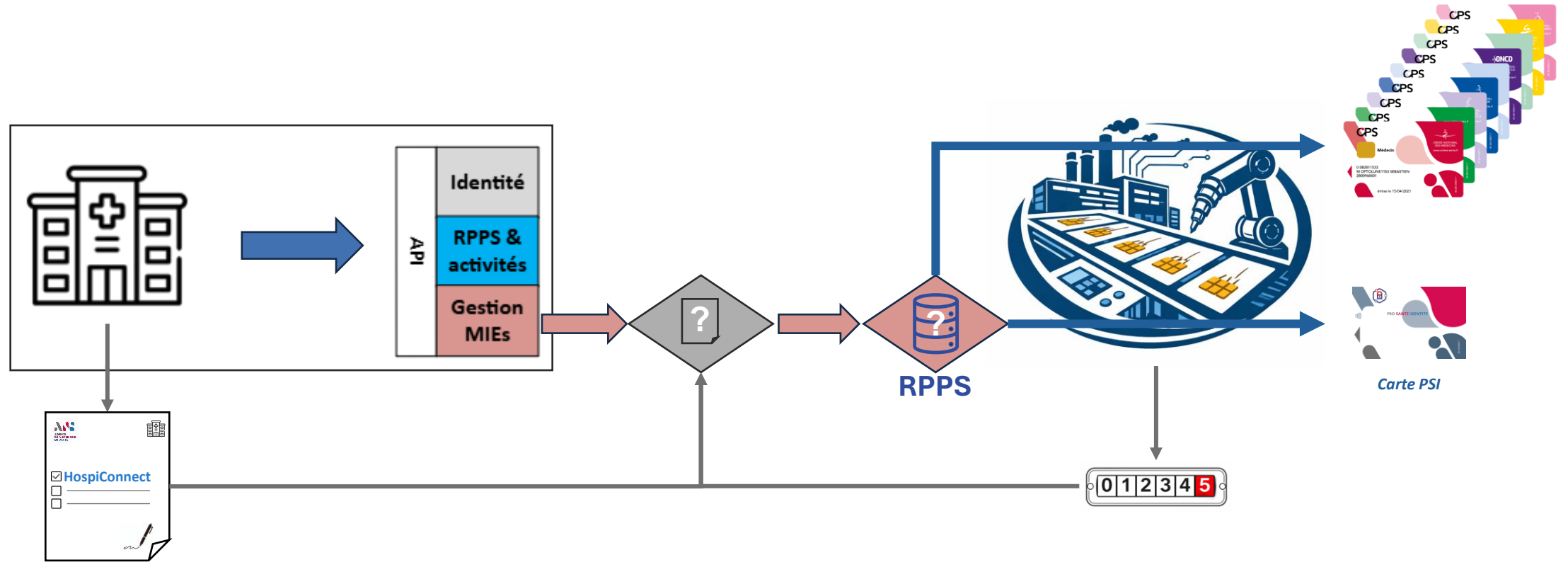
Cependant, la CPE reste disponible dans le cadre d'usage en lien avec les téléservices de l'Assurance Maladie.



EDC – PRO SANTE IDENTITE

Pro Santé identité : une nouvelle offre carte sous contractualisation

“ Pro Santé Identité (PSI) garantit une identité nationale vérifiée avec un identifiant national unique. Une offre MIE adossée à cette identification peut prétendre à intégrer un périmètre eIDAS Substantiel, cible de l’EDC PSC. La carte PSI sera construite à partir d’une identité de Pro Santé Identité vérifiée avec l’identifiant national [UUID] sur l’AC Racine « Forte » ”



EDC – FI TIERS

FI Tiers : fédérer le local au national

FI Tiers est l'élément qui permet à un établissement disposant d'un schéma d'identité locale robuste de le raccorder à PSC et de faire bénéficier ses Professionnels d'une authentification intégrée et fluide entre ses services locaux, régionaux et nationaux avec son identité sectorielle.

Le fournisseur d'identité local en tant que FI Tiers de PSC est fédéré par PSC lui-même pour le niveau national

Schéma local conforme

L'établissement doit disposer d'un répertoire d'identité local de qualité, avec des processus d'enrôlement et de vérification documentés et auditables.

Conditions du FI Tiers de l'EDC PSC applicables

Pour devenir FI tiers, l'éditeur et la structure doivent obtenir une habilitation ANS issue de leur conformité aux exigences du Référentiel PSC.

MIE conformes FI Tiers PSC

L'usage de MIE tiers (ex. badge DESFire, clé de sécurité) est conforme à PSC s'il répond aux exigences tant du MIE lui-même que de sa gestion locale : flexibilité pour les établissements.



Message clé : Les exigences du Référentiel EDC PSC relatives aux FI Tiers garantissent une conformité aux attendus du RIE

EDC – MIE COMPATIBLES

MIE Compatibles PSC : une gestion locale compatible avec le national.

Le Référentiel PSC n'impose pas un support unique. Il impose des exigences de niveau de sécurité. Tout MIE satisfaisant à ces exigences peut intégrer l'espace de confiance qu'il soit édité par l'ANS ou par un tiers.
L'ANS reconnaît un ensemble de MIE comme directement compatibles de PSC

Le MIE en tant que clef du porteur
est le garant de son identification et son authentification

MIE offre ANS


La CPS, la carte PSI et la e-CPS de l'ANS sont compatibles PSC, niveau substantiel, reconnues dans tous les services nationaux.

MIE compatibles PSC

En plus, de l'offre ANS, une liste de clefs de sécurité FIDO2 compatibles directement de PSC est publiées et maintenues par l'ANS.

Usage local hors PSC = conformité RIE

Un établissement peut utiliser un schéma local d'accès basé sur un MIE compatibles PSC. La conformité au RIE reste obligatoire mais est simplifiée.

 **Message clé :** un MIE compatible PSC peut devenir un badge local MIE conforme au RIE dès lors que le schéma d'enrôlement, de délivrance et d'authentification local répond aux exigences du RIE

EDC – ROADMAP

Prochaines échéances 2026

Avril	Mai	Juin	Juillet	Août	Septembre
EDC - PRO SANTE CONNECT NIVEAU 2					
EDC – MIE COMPATIBLES PSC					
		PSI – Libre-service			
		PSI – API IAM- ES			
		PSI – Portail ES			
					GUICHET FI TIERS
EXIGENCES FI TIERS					


Message clé : Le sujet n'est pas de choisir entre PSI et gestion d'identité locale : le sujet est de garantir que l'identité locale est toujours vérifiée pour des accès aux données santé.

CONSEQUENCES EN ETABLISSEMENT

Ce que cela change pour les établissements

Le changement de paradigme est profond : on ne raisonne plus « quel type de facteur d'authentification choisir ? » mais « quelle chaîne d'identification construire ? ». Chaque brique compte, et leur articulation est au cœur de la démarche.



Répertoire d'identité local de qualité

Fondation de la chaîne. Sans identité locale fiable, aucune brique en aval ne peut fonctionner correctement. Enrôlement, cycle de vie, synchronisation RPPS.



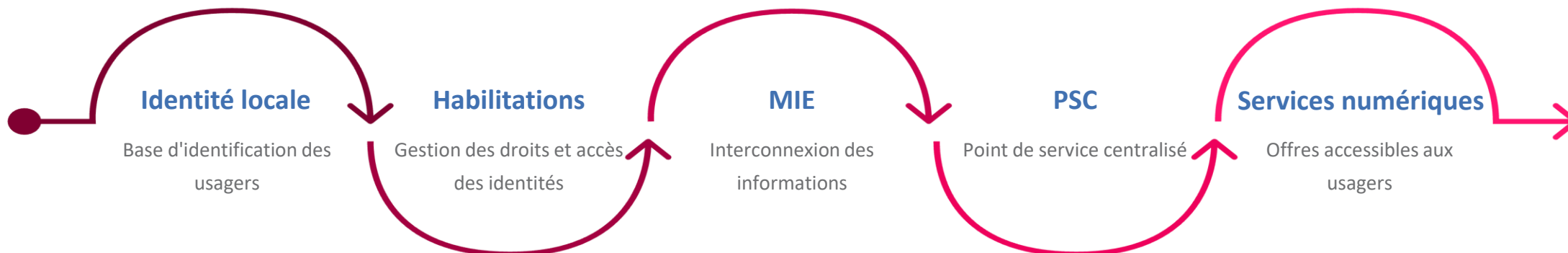
MIE + IAM + PSC articulés

Les trois couches doivent fonctionner ensemble : le MIE porte l'authentification, l'IAM gère les droits et les sessions, PSC assure l'interopérabilité nationale.



Parcours d'identité industrialisés

L'enrôlement, le renouvellement, la révocation et l'accès doivent être des processus automatisés, traçables et maintenables sans effort manuel excessif.

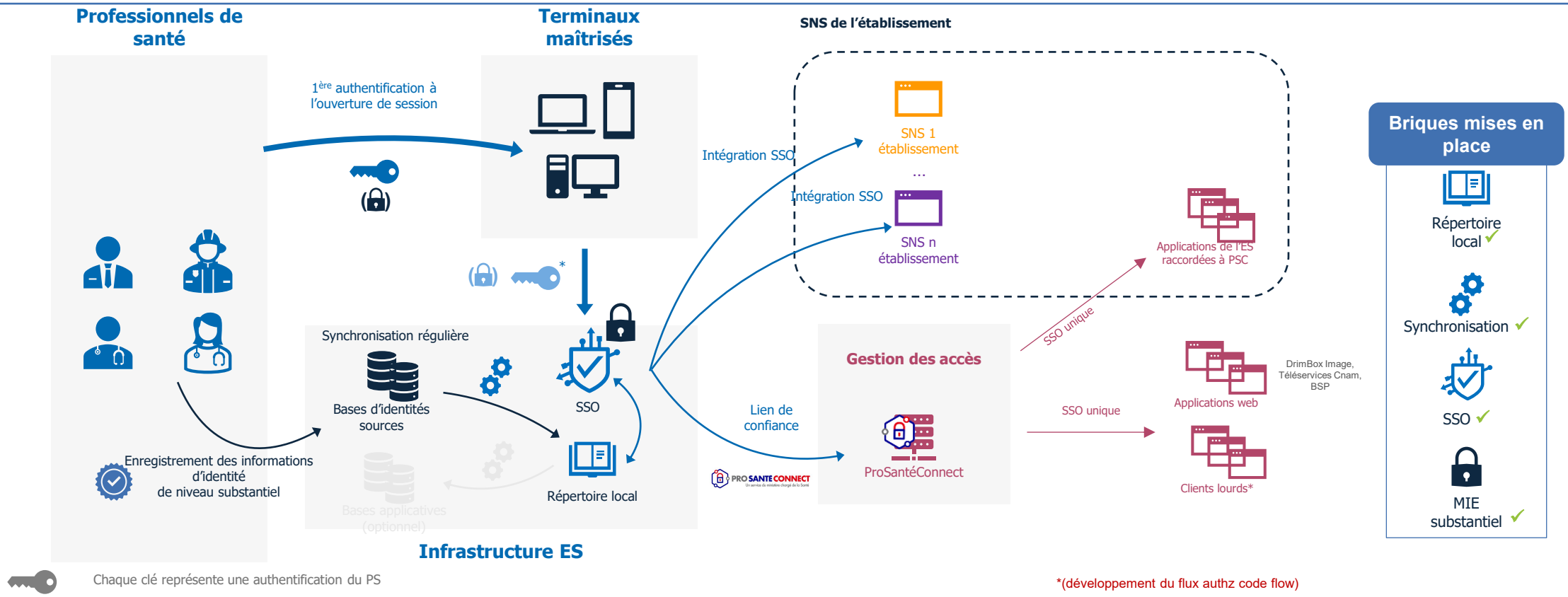


Message clé : Le changement pour les établissements est d'abord un changement de logique : passer d'une approche par outils à une approche par chaîne d'identification électronique.

CONSEQUENCES EN ETABLISSEMENTS

Ce que cela change pour les établissements

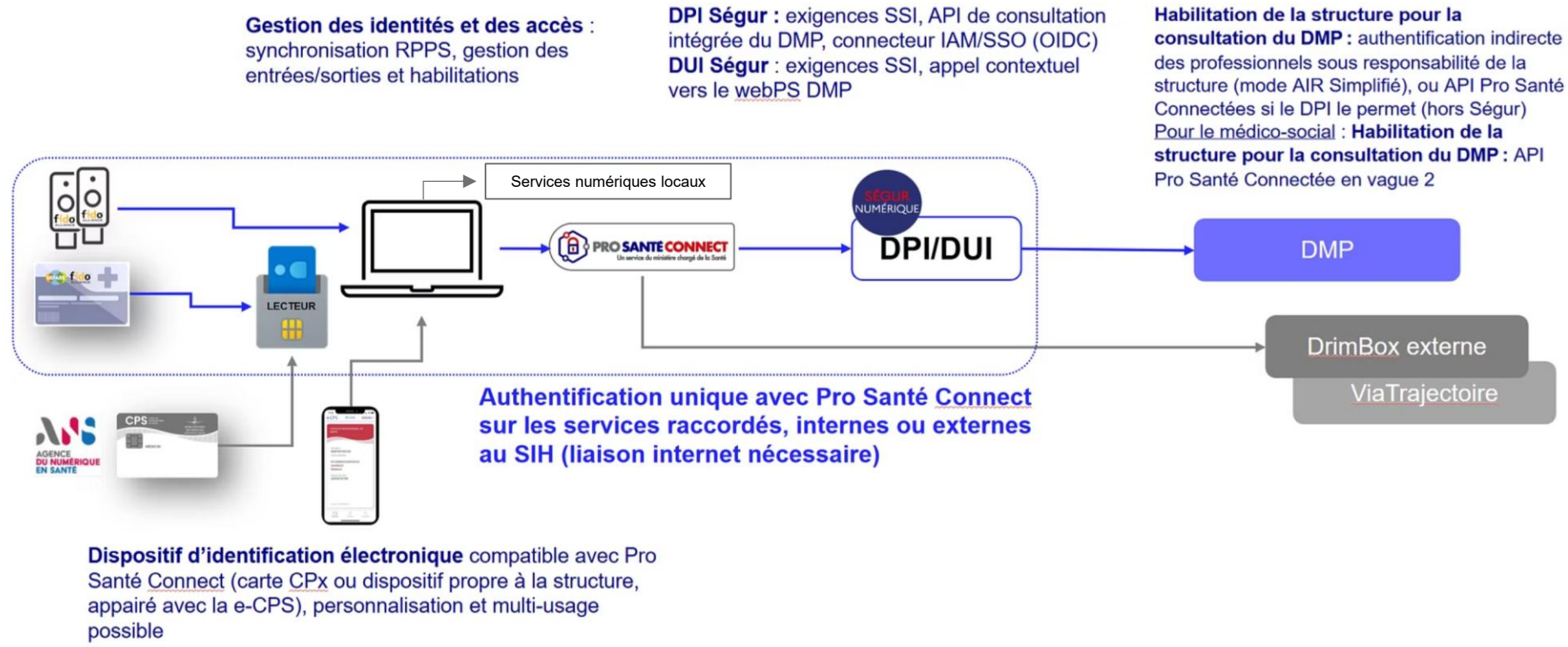
La situation cible pour les établissements de santé passe par l'intégration à leur SI de différentes briques leur permettant de sécuriser et de fluidifier les accès aux applications. Les travaux en cours visent aussi à offrir la possibilité aux établissements de permettre à leurs utilisateurs d'évoluer dans un écosystème unifié, sans frontière entre les applications raccordées à PSC et les SN de l'établissement.



OBJECTIFS – PREMIER NIVEAU

Premier niveau atteignable

Un premier niveau d'entrée dans l'espace de confiance est accessible dès aujourd'hui. Il constitue un socle réaliste et conforme, qui permet à l'établissement d'engager sa trajectoire sans attendre une urbanisation complète.



Message clé : Ce 1^{er} niveau est atteignable pour la grande majorité des établissements sans refonte complète du SI. Il constitue une base solide pour tendre vers la cible de la trajectoire.

OBJECTIFS – ETAT DE L'ART

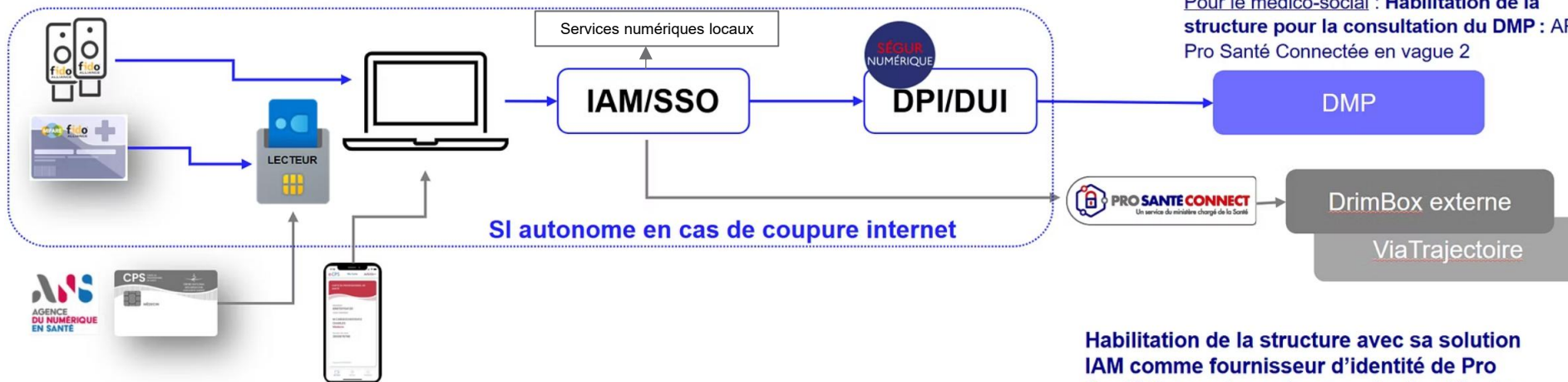
Etat de l'art

Ce schéma cible s'adresse prioritairement aux structures ayant recours à une large galaxie de services numériques, un volume significatif d'identités à gérer et une organisation capable d'industrialiser la gestion des accès et des moyens d'identification. Il ne constitue pas nécessairement la cible la plus adaptée pour les structures dont le parc applicatif est limité et concerne moins d'utilisateurs.

Gestion des identités et des accès (IAM): enregistrement et synchronisation RPPS, gestion des entrées/sorties (SI-RH), enrôlement des dispositifs d'identification, habilitations, authentification unique au sein du système d'information (SSO)

DPI Ségur : exigences SSI, API de consultation intégrée du DMP, connecteur IAM/SSO (OIDC)
DUI Ségur : exigences SSI, appel contextuel vers le [webPS DMP](#)

Habilitation de la structure pour la consultation du DMP : authentification indirecte des professionnels sous responsabilité de la structure (mode AIR Simplifié pour le sanitaire), ou API Pro Santé Connectée si le DPI le permet (hors Ségur)
 Pour le médico-social : **Habilitation de la structure pour la consultation du DMP :** API Pro Santé Connectée en vague 2



Dispositif d'identification électronique compatible avec Pro Santé Connect (carte CPx ou dispositif propre à la structure : liste de critères à publier par l'ANS), personnalisation et multi-usage possible

Habilitation de la structure avec sa solution IAM comme fournisseur d'identité de Pro Santé Connect : accès sans réauthentification aux services numériques externes


Message clé : Au-delà de la conformité minimale, une cible d'urbanisation plus ambitieuse est possible. Elle transforme l'identification électronique en actif numérique stratégique pour l'établissement, et non plus en simple contrainte réglementaire.

EXEMPLES DE CAS D'USAGE

1.1 – MIE local (attestation de conformité exhaustive mais guidée et simplifiée)

Exemple : Un badge MIFARE DESFire déployé en établissement peut être utilisé comme MIE local, en s'appuyant sur le guide dédié au MIFARE DESFire de l'ANS, à condition que le schéma local d'enrôlement et d'authentification réponde aux exigences du RIE

→ Répondre aux usages terrain

Le badge local est déjà utilisé pour l'accès physique. Capitaliser sur l'existant pour l'accès logique local réduit la charge de déploiement pour les équipes DSI.

L'accès aux services numériques de santé nationaux et régionaux est réalisé via PSC par exemple via la e-CPS

→ Garder la maîtrise locale

L'établissement reste maître de son infrastructure d'accès. Le MIE local est géré en interne, avec des processus adaptés à l'organisation.



→ Rester dans le bon cadre

L'attestation de conformité est assurée par la description et la qualification du schéma local avec un MIE local conforme au RIE.



 **Message clé :** Le changement pour les établissements est d'abord un changement de logique : passer d'une approche par outils à une approche par chaîne d'identification électronique.

EXEMPLES DE CAS D'USAGE

1.2 – MIE local (attestation de conformité exhaustive mais guidée et simplifiée)

Exemple : Une clé FIDO2 compatible PSC déployée en établissement peut être utilisée comme MIE local à condition que le schéma local d'enrôlement et d'authentification réponde aux exigences du RIE

→ Répondre aux usages terrain

La clé de sécurité est utilisée pour tous les accès logiques locaux nativement dans les postes de travail. Capitaliser sur l'ensemble des accès réduit la charge de déploiement pour les équipes DSI. L'accès aux services numériques de santé nationaux est réalisé via PSC grâce à la clef FIDO2 compatible PSC.

→ Garder la maîtrise locale

L'établissement reste maître de son infrastructure d'accès. Le MIE local est géré en interne, avec des processus adaptés à l'organisation. Son déploiement s'appuie sur les mécanismes natifs aux infrastructures réseaux

→ Rester dans le bon cadre

L'attestation de conformité est assurée par la description et la qualification du schéma local avec un MIE compatible PSC.



Message clé : Le changement pour les établissements est d'abord un changement de logique : passer d'une approche par outils à une approche par chaîne d'identification électronique.

EXEMPLES DE CAS D'USAGE

2.1 – FI tiers avec MIE local (attestation de conformité simplifiée et garantie)

Exemple : une solution d'IAM/SSO et sa structure peut répondre à l'ensemble des exigences de l'EDC PSC option FI Tiers avec un badge MIFARE DESFire déployé comme MIE accepté par PSC, en s'appuyant sur le guide dédié au MIFARE DESFire de l'ANS.

Ce cas illustre une trajectoire complète : un établissement qui a structuré son identité locale peut se raccorder directement au national via FI Tiers, et offrir à ses professionnels un accès fluide à l'ensemble des services PSC.

→ Répondre aux usages terrain

Le même badge local est déjà utilisé pour l'accès physique. Capitaliser sur l'existant pour l'accès logique local **et national** réduit la charge de déploiement pour les équipes DSI.

→ Garder la maîtrise locale

L'IAM gère les sessions et les droits. Le FI Tiers, habilité ANS, traduit l'identité locale en assertion de confiance reconnue par PSC.

→ Rester dans le bon cadre

Le professionnel accède de façon transparente aux services nationaux (DMP, messagerie sécurisée, DRIMbox, ...) avec son identité locale synchronisée nationale et son badge local.



Message clé : Le changement pour les établissements est d'abord un changement de logique : passer d'une approche par outils à une approche par chaîne d'identification électronique.

EXEMPLES DE CAS D'USAGE

2.2 – FI tiers avec MIE local (attestation de conformité simplifiée et garantie)

Exemple : Une clé de sécurité FIDO2 déployée en établissement est un MIE acceptée ou compatible par PSC à condition que la solution d'IAM/SSO et la structure répondent à l'ensemble des exigences de l' EDC PSC option FI Tiers.

Ce cas illustre une trajectoire complète : un établissement qui a structuré son identité locale peut se raccorder directement au national via FI Tiers, et offrir à ses professionnels un accès fluide à l'ensemble des services PSC.

→ Répondre aux usages terrain

La clé de sécurité est utilisée pour tous les accès logiques locaux et nationaux. Capitaliser sur l'ensemble des accès réduit la charge de déploiement pour les équipes DSI.

→ Garder la maîtrise locale

L'IAM gère les sessions et les droits. Le FI Tiers, habilité ANS, traduit l'identité locale en assertion de confiance reconnue par PSC. Son déploiement s'appuie sur les mécanismes natifs aux infrastructures réseaux

→ Rester dans le bon cadre

Le professionnel accède de façon transparente aux services nationaux (DMP, messagerie sécurisée, DRIMbox, ...) avec son identité locale synchronisée nationale et son badge local.



Message clé : Le changement pour les établissements est d'abord un changement de logique : passer d'une approche par outils à une approche par chaîne d'identification électronique.

SYNTHESE DES CAS D'USAGES PRESENTES

Exemples de cas d'usage – Récapitulatif

	MIE local	Schéma Enrôlement et Identification RIE	Accès aux services numériques nationaux	Avantage(s)	Inconvénient(s)	Attestation de conformité
.1	Divers	A documenter par la structure	PSC avec la e-CPS	Adaptation maximale aux usages locaux	Conformité au RIE à couvrir intégralement par la structure	Exhaustive mais guidée
.2	Carte ANS	A documenter par la structure <i>Prévoir une solution alternative en cas de PVD et d'arrivée non programmée</i>	PSC avec la carte ANS	Carte ANS compatible contrôle d'accès physique	<ul style="list-style-type: none"> Délai de délivrance incompressible Contrôle d'accès logique dépendant d'un middleware dédié 	Exhaustive mais guidée
1.1	MIFARE DESFire <i>guide dédié au MIFARE DESFire de l'ANS</i>	A documenter par la structure	PSC avec la e-CPS	MIE local Contrôle d'accès physique	Contrôle d'accès logique dépendant d'un middleware dédié	Exhaustive mais guidée et simplifiée pour le MIE
1.2	FIDO compatible PSC	A documenter par la structure	PSC avec le MIE local	Support accès logique natif aux systèmes d'exploitation	Contrôle d'accès physique encore émergeant	Exhaustive mais guidé et simplifiée pour le MIE
2.1	MIFARE DESFire <i>guide dédié au MIFARE DESFire de l'ANS</i>	Accompagné et garantie par le Guichet EDC PSC FI tiers	PSC via FI tiers	MIE local Contrôle d'accès physique		Simplifiée et garantie
2.2	FIDO accepté PSC	Accompagné et garantie par le Guichet EDC PSC FI tiers	PSC via FI tiers	Support accès logique natif aux systèmes d'exploitation	Contrôle d'accès physique encore émergeant	Simplifiée et garantie

SYNTHÈSE

Synthèse & prochaines étapes

“ On ne pilote plus un projet de carte. On construit une trajectoire d'identification électronique. Le MIE n'est qu'un composant de la cible : la vraie transformation porte sur l'ensemble de la chaîne, de l'identité jusqu'à l'accès aux services. ”

Le cap est imposé

Le cap est fixé : convergence vers une identification de niveau substantiel et intégration de Pro Santé Connect.
Ce cadre s'impose aux établissements. Il doit être anticipé dès maintenant dans les trajectoires locales.

Une trajectoire nationale - une mise en œuvre locale

Les établissements gardent de la marge sur la manière d'atteindre la cible. MIE, IAM, articulation avec PSC, recours à PSI ou à FI Tiers : plusieurs chemins sont possibles selon le contexte local.

Des exigences pour entrer dans l'espace de confiance

L'interopérabilité avec le national repose sur des exigences à respecter. Entrer dans l'espace de confiance suppose de répondre à un cadre de conformité, de sécurité et de gouvernance partagé.

Le facteur d'authentification n'est qu'une partie de la chaîne

Le MIE compte, mais il ne suffit pas : la cible repose aussi sur la qualité de l'identité, la gestion des droits, l'IAM, les parcours et l'interopérabilité avec le national.

Prochaines étapes

Webinaire #3

[HospiConnect#ProgrammesDeFinancement](#)
[26/03]

Ressources en ligne

Accédez aux guides et outils HospiConnect



https://sante.gouv-9827.slite.page/p/sVKcP-ZTcd2_vH/Guide-pour-la-securisation-et-la-simplification-de-l-identification-electronique-des-professionnels-en-structure

Lien Communication E-Santé

<https://esante.gouv.fr/actualites/hospiconnect-une-identite-numerique-fiable-et-maitrisee-dans-les-services-numeriques-en-sante-du-secteur-hospitalier>

Contact & questions

Mise en place FAQ [à venir]



esante.gouv.fr

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

 **@esante_gouv_fr**

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