WEBINAIRE

Mise en œuvre de l'identification électronique des acteurs de santé

(PARTIE 2)

Maîtriser la chaîne de gestion des identités

ARS Ile-de-France / DCGDR / SESAN

31 mars 2026

Intervenants

Halimata NIANG

Charline AUZOU

ars Agence Régionale de Santé Île-de-France

Lucie MATHIEUX

Thierry DUBREU

Souhil ZEBBOUDJ

sesan SERVICE NUMÉRIQUE DE SANTÉ

Ordre du jour

1h45

Introduction	5 mn
Rappel des objectifs et document de cadrage	15 mn
Les différents moyens d'identification électronique (MIE)	15 mn
Processus de délivrance du MIE / Association au compte local	15 mn
Exemples d'architecture	15 mn
La fédération d'identités en lien avec ProSantéConnect	10 mn
La gestion de l'authentification unique (SSO)	10 mn
Questions / Réponses et échanges	20 mn

Introduction

Rappel des objectifs et Document de cadrage

Rappel des objectifs du programme HOP'EN 2/HospiConnect

Le programme HOP'EN2 fixe des objectifs à atteindre qui s'inscrivent dans une trajectoire plus globale d'HospiConnect qui doit couvrir l'ensemble des services numériques en santé.

Catégorie de l'objectif	Libellé de l'objectif	Objectifs HospiConnect 2026	Objectifs HospiConnect 2027	Objectifs HospiConnect 2028
Objectif obligatoire	1.0 – Mise en conformité PGSSI-S	Note de cadrage du projet & remplissage des indicateurs de maturité	PV de décision de la commission d'homologation des MIE (PGSSI-S) **(avec ou sans réserve)** Mise à jour des indicateurs de maturité	PV de décision de la commission d'homologation des MIE (PGSSI-S) **sans réserve** Mise à jour des indicateurs de maturité
Maîtriser la chaine de gestion des identités et des accès au SIH	1.1 – Gestion des identités : l'identifiant RPPS des utilisateurs est connu du DPI		L'identifiant RPPS **des professions à Ordre** et enregistrées par l'ARS est connu du DPI pour l'ensemble des utilisateurs concernés (dès la création du compte utilisateur)	L'identifiant RPPS est associé **à tous les utilisateurs du DPI**, y compris les utilisateurs devant faire l'objet d'un enregistrement au RPPS par l'employeur (ES)
	1.2 – Gestion des comptes : les permissions d'accès au DPI sont mises à jour lors des mouvements de personnel		La procédure de mise à jour des comptes utilisateurs **est décrite et opérationnelle (automatique ou manuelle),** notamment pour la gestion des habilitations lors des arrivées, départs et changement de services. Une revue manuelle ou automatique des comptes et des habilitations est effectuée au minimum chaque année.	La procédure de mise à jour des comptes est **automatique** lors des arrivées/départs et changements de services (GRH), à partir d'une base de compte centralisée pour le SIH. Les activités du RPPS sont mises à jour au sein du SIH. Une revue automatique des comptes et des habilitations est effectuée au minimum chaque année.
	1.3 – Utilisation d'un MIE 2FA pour l'accès au DPI (homologué RIE)		**Les médecins et IDE** sont équipés d'un MIE 2FA utilisable pour l'authentification au DPI (directement ou via SSO)	**Tous les utilisateurs du DPI** s'authentifient avec un MIE 2FA en mode nominal. La prise en charge des modes dégradés est à décrire
	1.4 – Accès possible des utilisateurs du DPI au DMP en mode intégré : ES homologué AIR simplifié (***ou API PSC)***		**Les médecins et IDE** peuvent accéder à la consultation du DMP des patients ayant consenti depuis le DPI en intégré en mode AIR Simplifié ou par API PSC.	**Tous les utilisateurs du DPI** disposant d'une habilitation à la consultation du DMP accèdent au DMP de leurs patients depuis le DPI.
Rendre effectif l'accès automatique au DMP pour les professionnels autorisés	2.1 – Le consentement à la consultation du DMP des patients est recueilli		L'organisation mise en place permet de recueillir le consentement ou l'opposition du patient, en amont ou lors de la prise en charge, pour 75% du flux mensuel de patients	L'organisation mise en place permet de recueillir le consentement ou opposition du patent pour 90% du flux mensuel de patients
	2.2 – La consultation du DMP est 'effective' pour les patients ayant donné leur consentement dont l'INS est qualifiée, pour le PS habilité		40% des utilisateurs habilités du DPI a consulté le DMP d'un patient par une transaction automatique (TD3.1) au DMP dans le mois	60% des utilisateurs habilités du DPI a consulté le DMP d'un patient par une transaction automatique (TD3.1) au DMP dans le mois

HospiConnect/HOP'EN 2 – Échéance 2026

1. Note de cadrage

3 templates proposés :

- GHT
- Entité juridique (EJ) avec plusieurs établissements géographiques (EG)
- EJ mono EG

Templates au format Word disponible sur la page du programme HOP'EN2 d'ici le 30 mars

2. Evaluation de la maturité identification électronique

Outil d'auto-évaluation à renseigner à la maille EJ

Autoévaluation à réaliser dans Convergence
Les indicateurs de maturité pourront être consultés partir du 30 mars depuis le guide HospiConnect en ligne

3. Déclaration sur l'honneur des dépenses engagées

- Ressources RH
- Dépenses externes
- Dépenses éditeurs

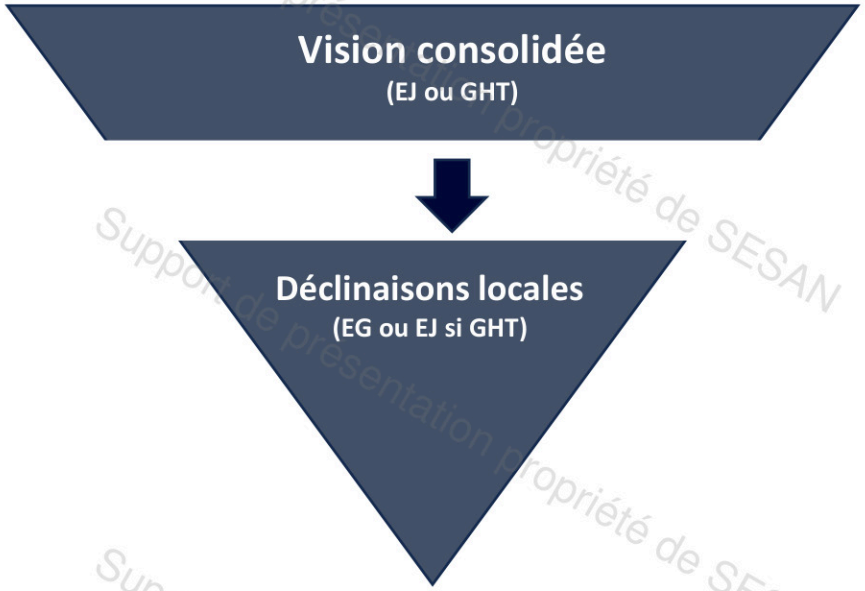
A renseigner dans Convergence

Le guichet HospiConnect/HOP'EN2 permettant le dépôt des livrables ouvrira sur Convergence le 4 mai 2026 (https://convergence.esante.gouv.fr/)

HospiConnect/HOP'EN 2 – Note de cadrage

Une note de cadrage pour construire la trajectoire permettant d'atteindre les cibles 27/28

La note de cadrage doit permettre de poser la gouvernance, les principes et la trajectoire nécessaires à la maîtrise des identités et des accès au SIH et à la consultation du DMP via le DPI, dans une logique de projet d'établissement.



Du commun au spécifique

- **Présentation générale et périmètre du projet**
  Organisation générale, périmètre fonctionnel et applicatif
- **Contexte, objectifs opérationnels et trajectoire 2026–2028**
  Situation actuelle, trajectoire objectifs HOP'EN2, arbitrage à prendre, risques et facteurs de réussite
- **Calendrier prévisionnel et jalons clés**
  Phases du projets et jalon structurant 2026-2028
- **Organisation et gouvernance du projet**
- **Suivi des indicateurs du projet**
- 6 **Communication et accompagnement des professionnels**

- Tout le cadrage du programme peut ne pas être finalisé. L'objectif est de partager un état à date de la réflexion mettant en avant le reste à faire et les actions prévues;
- Vous pouvez utiliser une mise en page propre à votre établissement dans la mesure où le plan du template fourni est conservé.

Publication des templates de la note de cadrage

Disponible depuis le 31 mars 2026 sur la page HOP'EN 2 – Trois formats adaptés à votre configuration

GHT — Template GHT

Groupement Hospitalier de Territoire

Pour les GHT avec déclinaison par Entité Juridique. Permet une vision consolidée au niveau GHT + spécificités par EJ.

Pour : Vision GHT + détail par EJ

EJ Mono — Template EJ mono-établissement

Entité Juridique mono-établissement

Pour les établissements simples : une seule entité juridique sur un seul site. Format le plus concis.

Pour : ES public ou privé mono-site

EJ Multi — Template EJ multi-EG

Entité Juridique multi-établissements géographiques

Pour les EJ privées couvrant plusieurs sites géographiques. Comprend des sections Niveau EJ et des déclinaisons par Établissement Géographique.

Pour : EJ privée multi-sites

HospiConnect/HOP'EN 2 – templates de la note de cadrage

GHT ou EJ multi-établissements

✓ Deux niveaux de complétion : vision GHT/EJ + déclinaison par site

✓ Mettre en évidence les spécificités de chaque ES si trajectoires différentes

✓ Ou indiquer que les éléments s'appliquent uniformément à tous les ES

✓ Sections « Niveau GHT » : 1-2 pages max par grande section

✓ Expliciter l'hétérogénéité SI/maturité/ressources entre EJ

EJ mono-établissement

✓ Format simplifié : une seule déclinaison sans niveau intermédiaire

✓ Aller droit au but : concision recommandée

✓ Tableaux fournis dans le template (optionnels, mais conseillés)

✓ Renvoyer les détails complexes en annexe

✓ Matrice de risques et facteurs de réussite à compléter

HospiConnect/HOP'EN 2 – Note de cadrage : contenu

Section	Éléments à fournir	Points de vigilance
1. Présentation générale et périmètre	• ES couverts par la note • Organisation SI/métiers (DSI, RH, soins, affaires médicales) • Périmètre applicatif : DPI, SIH, autres briques (nom, éditeur, hébergement, rôle dans HospiConnect)	*Préciser les interfaces clés liées aux identités et accès (entrant/sortant)*
2. Contexte, objectifs et trajectoire 2026–2028	• Situation actuelle : source de vérité, gestion des identités (RPPS), mouvements de personnel, populations spécifiques • Trajectoire par objectif (1,0→1,4/2,1→2,2) : SI concernés, populations cibles, situation actuelle, arbitrages, actions • Points restant à arbitrer + hypothèses/risques/dépendances	*C'est la section la plus structurante : détailler les 7 objectifs HospiConnect un par un*
3. Calendrier et jalons clés	• Grandes phases : cadrage, pilote, déploiement, accompagnement • Jalons structurants 2026/2027/2028 • Planning macro en annexe (obligatoire)	*Vision macro uniquement ici — renvoyer le détail en annexe*
4. Organisation et gouvernance	• Instances de pilotage : composition, rôle, fréquence • Articulation avec les instances existantes (CME, comité stratégique, directions) • Équipe projet : chef de projet, référents métiers/techniques, temps dédié	*Mentionner le portage au niveau direction (DG, DSI, Direction des soins)*
5. Suivi et évaluation	• Fréquence de suivi des indicateurs • Responsables du suivi • Outils mobilisés (tableaux de bord, extractions SI, Convergence)	*Les indicateurs de maturité seront à renseigner sur Convergence*
6. Communication et accompagnement	• Publics cibles (médecins, soignants, administratifs…) • Messages clés et supports envisagés • Actions de sensibilisation/formation • Modalités d'accompagnement au changement	*Montrer comment le projet sera rendu concret pour les équipes terrain*

HospiConnect/HOP'EN 2 –Annexe « questions structurantes pour le cadrage

01 Cycle de vie des identités

› Quelle est notre source de vérité sur les identités ?

› Tous les professionnels accédant au SIH sont-ils référencés ?

› Comment gère-t-on les mobilités et les départs ?

› Où subsistent des comptes non maîtrisés ?

02 Droits & accès numériques

› Sommes-nous capables de dire qui a accès à quoi aujourd'hui ?

› Les habilitations sont-elles structurées par rôles/profils ?

› Les droits suivent-ils automatiquement les mobilités ?

› Un SSO est-il justifié par les usages ? Comment gérer les accès distants ?

03 Services numériques

› Avons-nous une cartographie des services numériques ?

› Quels services sont les plus critiques pour la continuité des soins ?

› Lesquels sont les plus utilisés et donc les plus exposés ?

› Quels services traiter en priorité dans la trajectoire ?

04 Moyens d'identification électronique (MIE)

› Quel MIE pour quel usage et quelle population ?

› Quelle cible selon les niveaux d'assurance requis ?

› Quel secours en cas de perte, oubli, vol ou dysfonctionnement ?

› Comment organiser le support, le renouvellement et la logistique ?

05 Gouvernance & sensibilisation

› Qui porte le sujet au niveau de la direction ?

› Qui arbitre les décisions structurantes et les exceptions ?

› Comment suit-on les écarts, risques et déviations ?

› Comment embarquer les métiers, le support et les utilisateurs ?

HospiConnect/HOP'EN 2 –Annexe « questions structurantes pour le cadrage

06 Contractualisation AIR simplifié (accès DMP)

- L'ES a-t-il mesuré sa maturité vis-à-vis du référentiel de sécurité DMP ?
- Les professionnels habilités sont-ils dotés de MIE 2FA ?
- La commission d'auto-homologation a-t-elle été constituée ? Le PV rédigé ?
- Un rendez-vous de contractualisation avec la CPAM a-t-il été planifié ?

07 DPI et consultation intégrée du DMP

- L'ES dispose-t-il d'un DPI référencé Ségur vague 2 (ou en cours) ?
- Le planning de déploiement des fonctionnalités DMP a-t-il été cadré avec l'éditeur ?
- Un bon de commande sera-t-il signé avant septembre 2026 ?
- Le certificat DMP est-il valide ? Son renouvellement anticipé si besoin ?

08 Recueil du consentement patient

- Quand et par qui le consentement est-il recueilli (admission, prise en charge…) ?
- Comment est-il tracé et intégré dans les logiciels (GAM, DPI) ?
- Les notions d'équipe et d'épisode de soins ont-elles été définies et paramétrées ?
- Les équipes ont-elles été sensibilisées aux droits patients sur Mon Espace Santé ?

09 Matrice d'habilitation du DPI

- Une matrice d'habilitation a-t-elle été définie pour le DPI ?
- Est-elle actualisée et déployée à l'échelle de l'ensemble de l'établissement ?
- L'ES a-t-il pris connaissance du projet de recommandation CNIL sur le DPI ?
- L'impact du téléchargement de documents DMP vers le DPI a-t-il été intégré ?

HospiConnect/HOP'EN 2 –Questionnaire maturité SIH

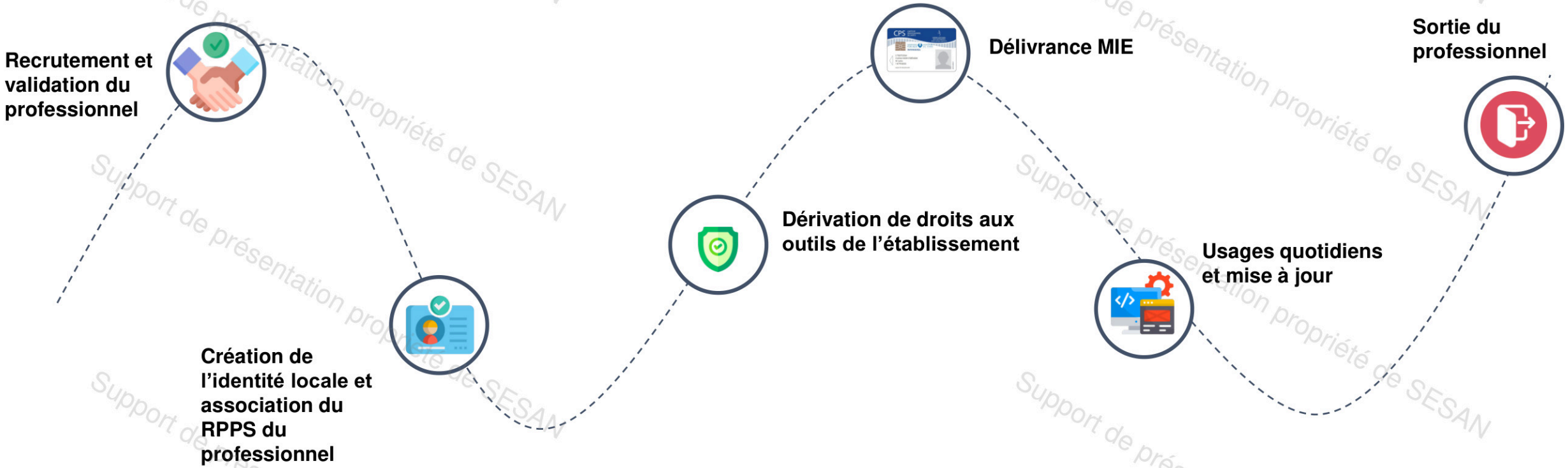
Le questionnaire de maturité prend en compte tout le SIH. Les établissements auront la possibilité de préciser le périmètre de couverture applicative de leurs réponses.

- Sur Convergence la maille de réponse sera à l'EJ pour être en cohérence avec le programme de financement.
- Par contre les ES auront la possibilité de répondre à la maille EG (cas d'un EJ multi EG) de leur côté non pas sur convergence, mais sur la base du fichier Excel qui sera mis à disposition sur le guide HOSPICONNECT de l'ANS.

En synthèse, pour le programme de financement, on reste à l'EJ, pour les réalités opérationnelles des ES ils peuvent affiner la vision pour construire leur trajectoire par EG.

Focus sur l'ordre du jour

- Sécuriser la chaîne d'identification des professionnels dans sa structure revient à repenser chacune des étapes ci-dessous.
- Plusieurs chantiers sont à mettre en place, en parallèle, pour déployer cette chaîne de bout en bout



Focus sur les objectifs Hospiconnect 1.3 et 1.4

1 - Maîtriser la chaîne de gestion des identités et des accès au SIH et permettre la consultation du DMP

1.3 – Utilisation d'un Moyen d'identification électronique Double facteurs 2FA pour l'accès au DPI (conformité Référentiel d'Identification Electronique)

2027 **Les médecins et IDE** sont équipés d'un MIE 2FA utilisable pour l'authentification au DPI (directement ou via SSO)

2028 **Tous les utilisateurs du DPI** s'authentifient avec un MIE 2FA en mode nominal. La prise en charge des modes dégradés est à décrire

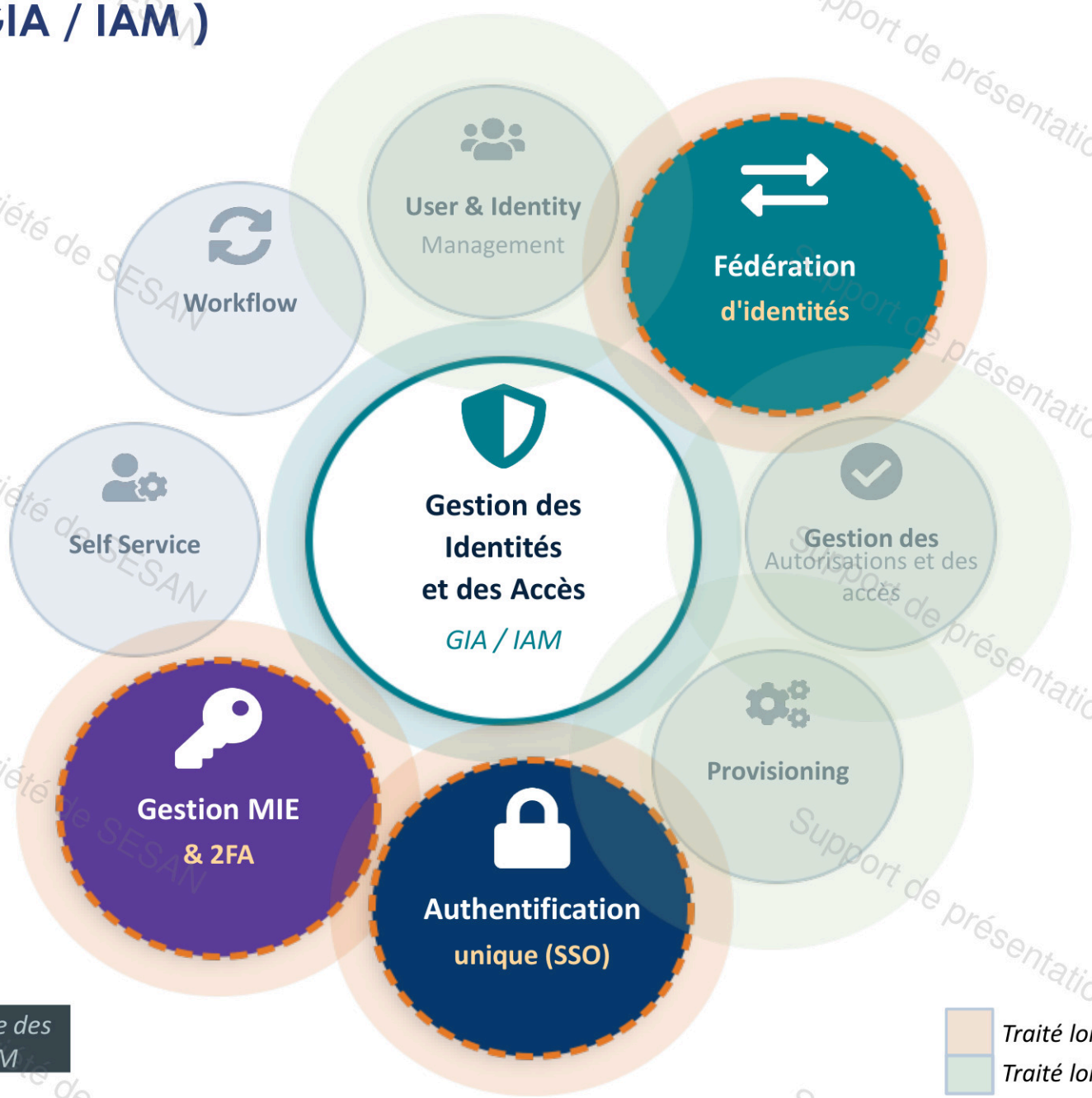
1.4 – Accès possible des utilisateurs du DPI au DMP en mode intégré : ES homologué AIR simplifié (ou API PSC)

2027 Les médecins et IDE peuvent accéder à la **consultation du DMP** des patients ayant consenti **depuis le DPI en intégré en mode AIR Simplifié** ou par API PSC.

2028 Tous les utilisateurs du DPI disposant d'une habilitation à la consultation du DMP accèdent au DMP de leurs patients depuis le DPI.

Sera traité lors d'un prochain webinaire

Rappel des composants structurants d'une Gestion des Identités et des accès (GIA / IAM)

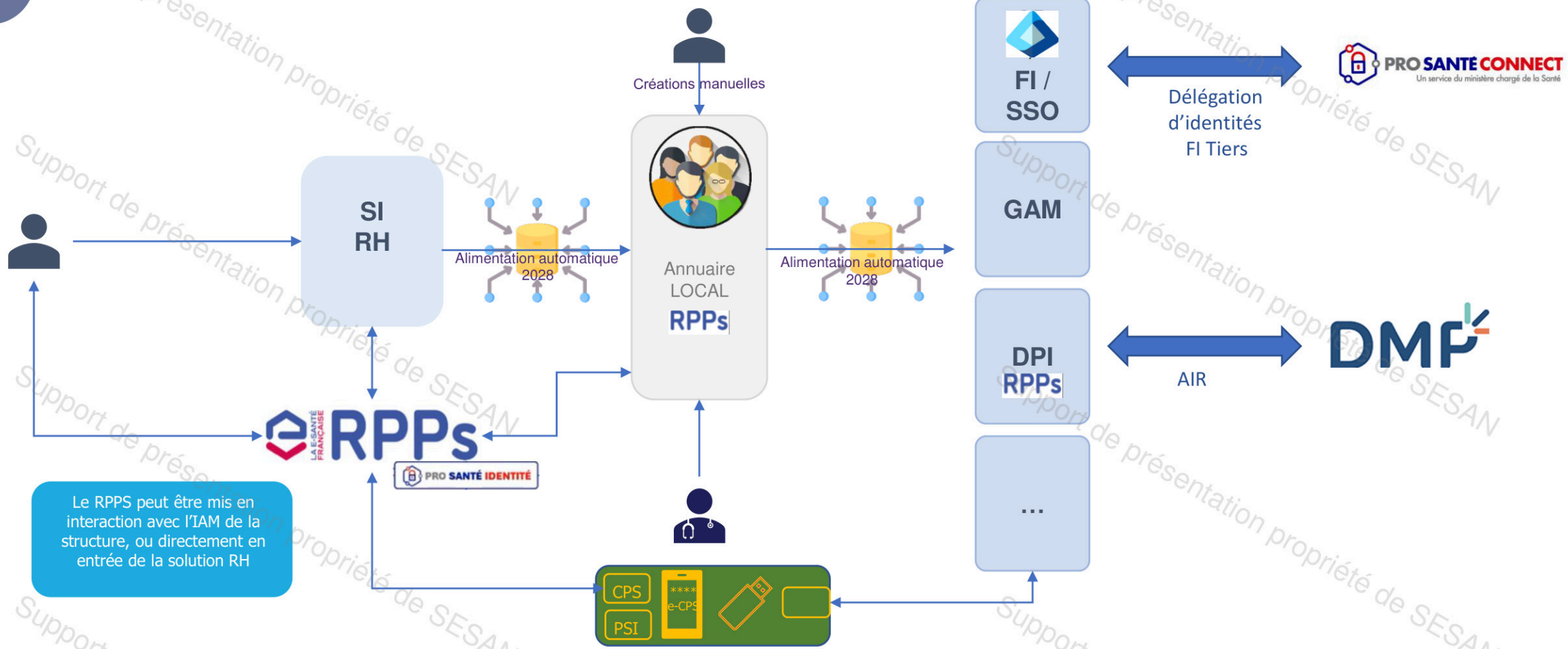


AUDIT — *transversal à l'ensemble des composants de la GIA / IAM*

Traité lors de ce webinaire

Traité lors du webinaire du 17/02

Rappels préalable : Constitution d'un annuaire local d'identités



Processus d'enrôlement et de délivrance du MIE doit tendre vers EIDAS substantiel

L'identité du professionnel est créée dans le système de l'établissement (RH ou directement Annuaire Local).
L'identité locale est associée systématiquement à l'identité RPPS du professionnel (création ou récupération), l'exercice est vérifié/mis à jour.
L'identifiant RPPS est connu a minima du DPI pour chaque utilisateur
Chaque utilisateur dispose d'un MIE (personnel ou ES) associé à son compte local et au RPPS
L'utilisateur dispose du profil / habilitations adéquats dans les applications du SI

Les différents moyens d'identification électronique (MIE)

Rappel concernant les facteurs d'authentification

Ce que je SAIS
Facteur de connaissance

Secret mémorisé par l'utilisateur, connu de lui seul. C'est le facteur le plus répandu mais le plus vulnérable aux attaques.

Exemples

- **Mot de passe** — Long + complexe + unique ✓
- **Code PIN** — Chiffres ou alphanum., 4-8 car. ✓
- **Question secrète** — Déconseillé — faible entropie ✗
- **Phrase de passe** — Recommandé ANSSI : 4 mots ✓

eIDAS : Faible seul — Substantiel si couplé avec PIN MIE

Ce que je POSSÈDE
Facteur de possession

Objet physique ou logique dont seul l'utilisateur dispose.

Exemples

- **Carte CPS / PSI** — eIDAS Élevé — PKI X.509 ✓
- **e-CPS (appli mobile)** — eIDAS Substantiel — TOTP/Push ✓
- **Clé FIDO2** — eIDAS Substantiel — résiste phishing ✓
- **OTP SMS / Email** — Niveau bas — SIM swap possible ✗

eIDAS : Substantiel à Élevé selon MIE

Ce que je SUIS
Facteur d'inhérence (biométrie)

Caractéristique physique ou comportementale unique et permanente de l'utilisateur. Pratique mais pose des problèmes CNIL et RGPD.

Exemples

- **Empreinte digitale** ✓
- **Reconnaissance faciale** ✓
- **Iris / rétine** ✓
- **Reconnaissance vocale** — Déconseillé seul ✗

eIDAS : Élevé potentiel — selon impl.

Combinaisons MFA recommandées en établissement de santé

			Niveau faible
Carte CPS (possession)	e-CPS (possession)	Clé FIDO2 (possession)	MDP (connaissance)
+	+	+	+
PIN CPS (connaissance)	PIN + biométrie mobile (conn./inhérence)	PIN local (connaissance)	OTP SMS (possession faible)

L'authentification multi-facteurs (MFA) impose d'utiliser au moins 2 facteurs appartenant à 2 catégories différentes.

Santé : eIDAS substantiel minimum (2FA) — DMP, MSSanté, DPI

Les différents moyens d'identification électronique (MIE)

Cartes CPx / PSI

- CPx délivrées automatiquement (ARS/ordre) / PSI sur commande
- Multi-usage (contact / sans contact), y compris en mobilité : accès, badgeuse, wallet
- Compatible MIFARE DESFIRE
- Conformité aux Exigences nationales/européennes

- Dépendance organisme externe pour la délivrance (délai)
- Lecteur fixe ou sans contact requis
- Coût 12 €/carte déduit de la subvention Care

Enrôlement du MIE au SI requis

eCPS (appli mobile)

- Disponible pour tous les inscrits au RPPS/PSI
- Recommandée sécurisation accès externes
- Disponible sans lecteur

- Nécessite téléphone personnel ou pro (et du réseau …). Peut être interdit dans certains contextes
- Usage complexe en mobilité interne
- Ne convient pas aux postes partagés

Enrôlement du MIE au SI requis

Clés FIDO2

- Gestion et maitrise 100% internalisée. Charge de gestion à prévoir.
- Compatible PSC
- Multi-usage limité

- Niveau sécurité minimal conforme aux exigences du RIE
- Coût 30–60 €/clé
- Ré-enrôlement **annuel** avec PSC
- Certification ANSSI requise (liste)
- Attestation conformité RIE requise

Enrôlement du MIE au SI requis
+ Appairage PSC : via eCPS

Cartes Neutres

- Gestion et maitrise 100% internalisée. Charge de gestion à prévoir. (Couvre le cas interimaires)
- Flexibilité quotidien importante
- Multi-usage (contact / sans contact), y compris en mobilité : accès, badgeuse, wallet

- Niveau sécurité minimal conforme aux exigences du RIE
- Coût 2 à 3 €/carte
- Ré-enrôlement **annuel** avec PSC
- Certification ANSSI requise (liste)
- Attestation conformité RIE requise

Enrôlement du MIE au SI requis
+ Appairage PSC : via eCPS

Les cartes CPE ne sont pas conformes eIDAS substantiel et ont vocation à disparaître au profit des nouvelles cartes PSI.
NE PAS COMMANDER MASSIVEMENT DE CPE

Focus attestation de conformité au RIE en fonction du MIE

CAS 1 — Délégation via ProSantéConnect

Conformité IMPLICITE

- Lorsque le service délègue l'authentification à ProSantéConnect, la conformité au RIE est implicite
- MIE proposés par l'ANS : e-CPS, CPS, PSI (selon éligibilité)
- MIE compatibles activables par e-CPS : clés FIDO2 ou cartes FIDO
- Les cartes CPE/CPA actuelles ne reposant pas sur un répertoire national ne seront plus compatibles avec PSC

CAS 2 — MIE utilisé hors ProSantéConnect

Attestation OBLIGATOIRE

- L'utilisation de MIE hors PSC doit être encadrée par une attestation de conformité au référentiel du schéma d'identification associé
- L'attestation est délivrée par la personne morale qui délivre le MIE (établissement, fournisseur de solution)
- Un guide de conformité sera fourni par l'ANS pour préparer le dossier. La conformité à certaines exigences sera facilitée par l'usage de dispositifs compatibles PSC

MIE mis en œuvre par des Fournisseurs d'Identité habilités PSC

Etablissements avec une solution IAM / SSO

https://esante.gouv.fr/ens/offre/pro-sante-connect/liste-solutions-identite-compatibles-delegation-psc

Échéance : attestation de conformité obligatoire avant le 31/12/2026

Jusqu'au 31/12/2026, la commission de conformité peut émettre des réserves sur certaines exigences, sans toutefois permettre l'usage de MIE dont le niveau de sécurité serait inférieur à la notion actuelle de MIE de transition

CAS 3 — Cartes CPx hors PSC (authentification directe avec PIN, sur base de l'enrôlement ANS) :

Reste possible notamment pour les téléservices AM. L'enrôlement des cartes CPx dans un SI local doit faire l'objet d'une attestation de conformité.

Focus attestation de conformité au RIE en fonction du MIE

Qui délivre l'attestation ?

La personne morale qui délivre le MIE

Établissement de santé

Pour ses propres cartes neutres, clés FIDO2 ou MIE locaux

Fournisseur de solution IAM/SSO

Pour les MIE qu'il délivre dans le cadre d'un service externalisé

Groupement / GCS / GHT

Pour un schéma MIE mutualisé entre établissements

Un guide de conformité ANS sera publié pour aider à la constitution du dossier

Contenu de l'attestation & Calendrier

Contenu de l'attestation :

- Identification du schéma d'identification électronique associé au MIE (*)
- Description du MIE et du processus de délivrance
- Analyse de risque du MIE et du système d'information associé
- Référence au niveau de garantie eIDAS visé (substantiel ou équivalent RIE)
- Évaluation technique de la sécurité du dispositif
- Plan d'action en cas de réserves de la commission

Arrêté 28/03/2022	Entrée en vigueur 01/06/2022	Attestation obligatoire 31/12/2026	RIE v2 T2 2026

(*) Le schéma d'identification est le document décrivant les procédures et exigences techniques garantissant un niveau de sécurité donné pour le MIE concerné.

Processus de délivrance du MIE / Association au compte local

Processus de délivrance du moyen d'identification électronique National

CPS — Professionnels à Ordre

- Envoi automatique à chaque modification d'exercice (sauf infirmiers)
- Envoi à l'adresse renseignée auprès de l'Ordre
- Nouvelle carte à chaque changement d'exercice
- Adresse de correspondance obligatoirement à jour

Ordre Pro

maCPS

CPS — Professionnels ARS (ex-ADELI désormais au RPPS)

- CPS accessible selon profession et mode d'exercice
- Commande via portail maCPS (auth. RPPS + OTP ou e-CPS)
- Envoi à l'adresse validée par l'ARS dans le dossier d'inscription

ma-cps.esante.gouv.fr

CPS/PSI — Professionnels à rôle

- Commande via portail maCPS / PSI
- Enregistrement préalable via RPPS+ ou PSI
- Carte PSI envoyée à l'adresse établissement (FINESS) OU du pro
- Nécessite un contrat d'adhésion ANS (FINESS EJ), designation d'un gestionnaire PSI

RPPS+

maCPS (PSI à venir)

e-CPS (appli mobile)

- Disponible automatiquement pour tous les inscrits RPPS / PSI
- Activation via l'appli e-CPS (iOS / Android) — sans démarche établissement
- Nécessite un téléphone personnel ou professionnel
- Peut être interdit dans certains contextes

e-CPS App (App Store Google Play)

Les cartes CPS sont envoyées directement au professionnel —> elles ne sont pas maîtrisées par l'établissement.
Les cartes PSI sont délivrées sur commande auprès de l'ANS à l'adresse de la structure demandeuse OU du professionnel

Nouveauté : CPS4 déployée depuis juillet 2025 — technologie DESFIRE, validité 6 ans. Les CPS3 restent valables jusqu'à expiration.

Processus de délivrance du moyen d'identification électronique Local

Contrairement aux MIE nationaux (ANS), les MIE locaux sont entièrement gérés par l'établissement : création, distribution, renouvellement, révocation — sous attestation de conformité RIE.

Clés FIDO2

- Achat sur liste produits certifiés ANSSI (publication ANS à venir)
- Personnalisation et association au compte professionnel local
- Appairage PSC obligatoire via e-CPS (au moins 1 fois)
- Ré-enrôlement régulier requis avec PSC

Cartes Neutres

- Support physique DESFIRE EV3 obligatoire (exigence RIE)
- Personnalisation interne par l'équipe en charge des badges de l'établissement et association au compte professionnel local
- Appairage PSC obligatoire via e-CPS (au moins 1 fois)
- Attestation de conformité RIE à produire (avant 31/12/2026)

✔ MIE local (établissement) : délivrance ET enrôlement à charge de l'établissement — attestation RIE obligatoire

Remise & enrôlement des MIE nationaux ou locaux dans le SI

Prérequis : la déclaration du professionnel au RPPS / PSI doit avoir été faite au préalable (identifiant national attribué)

Remise du MIE au professionnel

Objectif : s'assurer que le MIE (PSI / local) est remis au bon professionnel (identité = RPPS) — remise en main propre

Réception du MIE (PSI / MIE Local)

Rendez-vous de remise

RDV individuel — remise contre présentation d'un document d'identité

Vérification d'identité

Contrôle de concordance CNI ↔ identité RPPS ↔ MIE reçu, avant activation

Activation & remise

Remise avec le code PIN initial

Enrôlement dans le SI local d'un MIE existant

Phase intégrée à la délivrance — le MIE doit être connu et associé au SI local avant le premier usage

Vérification annuaire local

Existence du professionnel dans le SI / AD vérifiée ou creation du compte

Association MIE ↔ identité

Liaison identifiant RPPS-PSI avec le compte local dans l'annuaire d'Identités *

Test d'authentification

Validation du bon fonctionnement MIE sur lecteur ou application SSO / IdP

Accès aux applications

Le professionnel peut accéder aux applis via son MIE (SIH, DMP, PSC…)

*** Sans lien entre le MIE et un compte local, le professionnel ne peut pas et ne doit pas pouvoir utiliser son MIE sur les applications de l'établissement.**

Architecture : rôles respectifs des différents composants logiques entrant en jeu dans la phase d'authentification

1. Annuaire d'authentification

Référentiel des comptes d'authentification

- Stocke les comptes utilisateurs
- Attribut RPPS/PSI associé
- Groupes, rôles, politiques
- Alimenté par l'IAM en lien avec le logiciel RH
- Vérifie l'authentification MDP

2. Fournisseur d'Identités (FI / IDP)

Vérifie le MIE présenté et émet un jeton de session

- Vérification MIE (CPS / FIDO2 / e-CPS)
- Émission token
- Gestion session utilisateur
- Délégation vers PSC (OIDC)
- Consulte l'annuaire d'authentification

3. SSO Broker

Permet aux applications raccordées d'accepter le jeton sans re-demander de credentials

- Applications raccordées (SAML / OIDC)
- Portail de connexion unique
- Gestion des sessions inter-apps
- Transmission attributs aux apps
- Relaie vers le bon IDP
- Evite la ré authentification

4. ProSantéConnect (Fédérateur national)

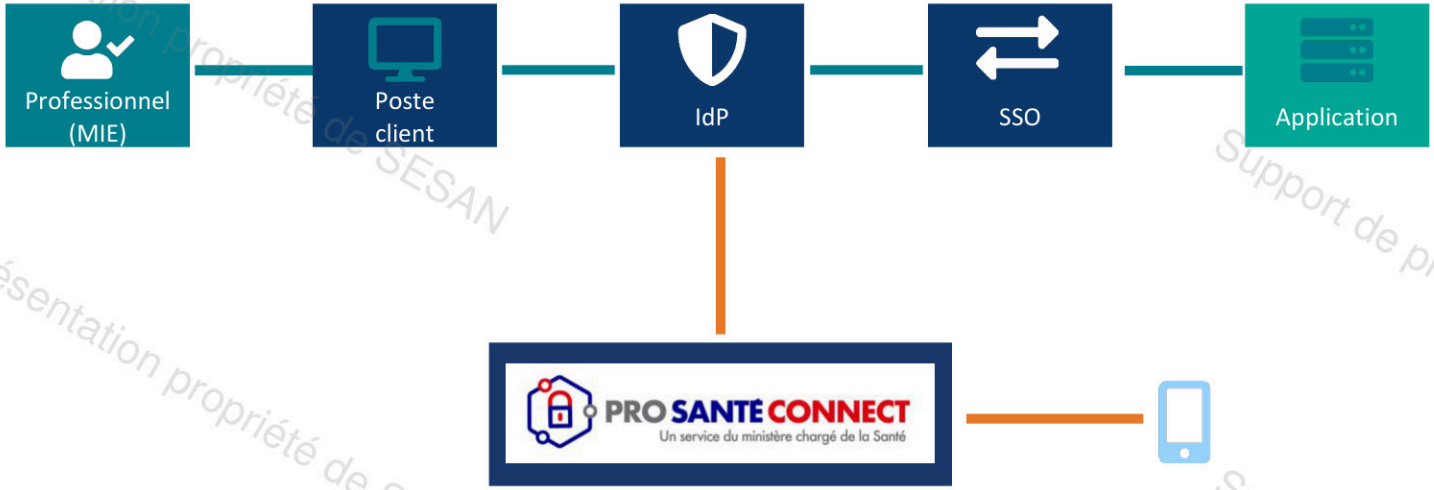
Lie identité locale ↔ identité nationale RPPS et transmet attributs sectoriels aux FS

- raccordé au SSO broker ou IdP
- Transmission attributs RPPS au FS
- Certification niveau de garantie MIE

En pratique plusieurs de ces composants (y compris l'annuaire local d'Identités et la partie IAM) peuvent être combinés dans un seul outil

Une application qui n'est pas raccordée au SSO broker (SP SAML ou RP OIDC) n'obtient aucun bénéfice du SSO, même si l'IdP authentifie le MIE et continuera de demander des credentials propres — même si l'IdP a authentifié le MIE -> L'impact est une ré authentification de l'utilisateur
Le raccordement de chaque application est un chantier d'intégration à part entière.

Enrôlement du MIE avec ProSantéConnect



Je m'authentifie au poste de travail avec mon MIE.

Mon MIE est reconnu car pré déclaré dans mon IDP/SSO.

Lors de la 1ere connexion, je saisis mes identifiants/mdp habituels.

L'association de mon MIE avec mon compte local est validée.

L'IDP / SSO vérifie que l'enrolement du MIE a déjà été effectué avec PSC, sinon je suis redirigé auprès de PSC.

Je dois m'authentifier une seule fois via une eCPS.

Si j'utilise un MIE local, l'association de mon MIE avec l'annuaire national est validée

Je peux accéder aux applications raccordées à l'IDP/SSO via OIDC sans ré-authentification, y compris aux services nationaux ou régionaux "sans couture"

L'appairage entre l'identité locale et l'identité Pro Santé Connect est **limité dans le temps**

Exemples d'architectures

Exemples d'architectures postes partagés — 4 scénarios opérationnels

1 Auth. directe via PSC (sans SSO local)

Cabinet, petit ES, structure sans infrastructure SSO

⚠ *DPI entièrement derrière PSC — sans PSC, aucun accès possible – Toutes les applications doivent être compatibles OIDC/PSC*

Simple · Dépendance PSC totale

2 Session poste générique + SSO + PSC

ES avec infrastructure SSO — poste non sécurisé au niveau OS

⚠ *session Windows générique accessible sans MIE — MIE intervient uniquement au niveau applicatif*

SSO opérationnel · Session OS générique

3 MIE conditionne l'ouverture de session + SSO + PSC

Poste partagé sécurisé — le MIE est la clé d'accès Windows

✔ *1 seul geste MIE pour tout (OS + apps) — mais perte du contexte de travail à chaque rotation*

Traçabilité nominative dès l'OS · Poste partagé

4 MIE conditionne la session + SSO + VDI / Session nomade

Poste partagé + virtualisation — le contexte de travail suit le professionnel

✔ *Contexte de travail maintenu à chaque rotation — le PS retrouve sa session sur n'importe quel poste*

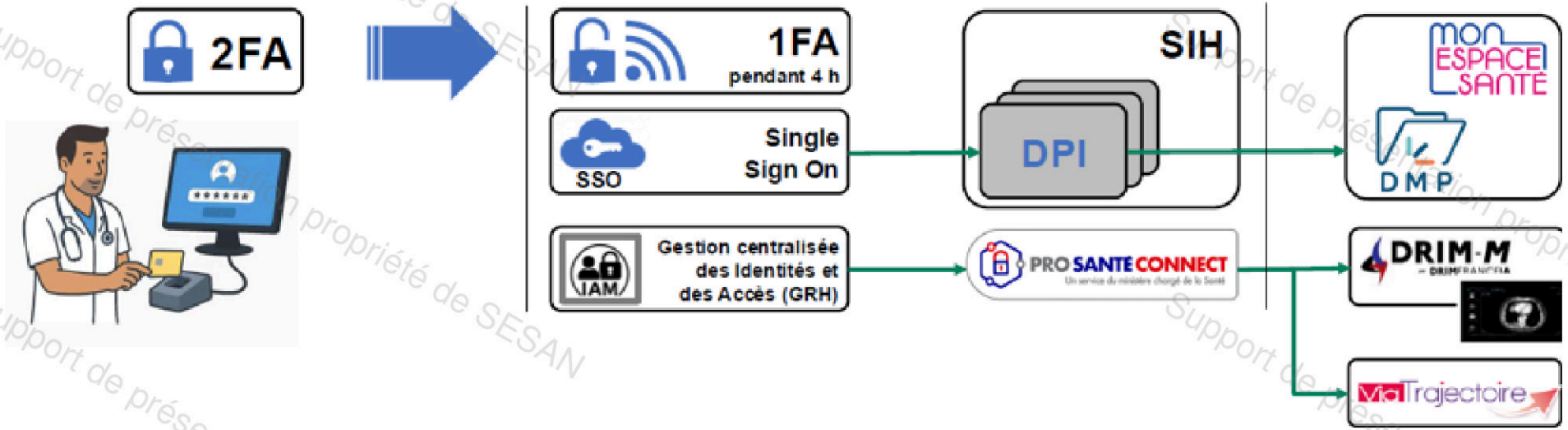
Sécurité max · Mobilité · Complexité élevée

Complexité et sécurité croissantes : 1 → 4 | Le SSO ne bénéficie qu'aux applications raccordées au broker | **Toutes les architectures nécessitent un mode dégradé en cas d'indisponibilité PSC**

Exemples d'architectures postes partagés — Tableau comparatif

	Architecture	Protection du poste	Auth. multi-applications (SSO)	Mode dégradé (sans PSC)	Gestion nomadisme	Complexité mise en œuvre	Dépendance à PSC	Simplic. usages
1	**Auth. directe via PSC (sans SSO local)**	✗ Session poste générique	✗ Multi-app via PSC uniquement (mutualisée)	✗ Dépendance totale à PSC	✗ Rotation complexe Perte contexte	✓ Simple à déployer	✗ Totale (DPI derrière PSC)	✗ Re-auth PSC à chaque app
2	**Session poste générique + SSO + PSC**	✗ Session poste générique	✓ SSO broker pour toutes les apps raccordées	✓ Mode local possible si non raccordé PSC	✗ Rotation complexe Perte contexte de travail	⚠ SSO à déployer + raccordement des apps	⚠ Partielle (SSO local en secours)	✓ 1 auth MIE pour toutes les apps
3	**MIE = accès au poste + SSO + PSC**	✓ MIE obligatoire pour ouvrir la session	✓ SSO broker pour toutes les apps raccordées	✓ Mode local possible si non raccordé PSC	✗ Rotation complexe Perte contexte de travail	⚠ MIE OS + SSO + PSC à déployer	⚠ Partielle (SSO local en secours)	✓ 1 auth MIE pour tout (OS + apps)
4	**MIE = accès au poste + SSO + VDI/Session nomade**	✓ MIE obligatoire pour ouvrir la session	✓ SSO broker pour toutes les apps raccordées	✓ Mode local possible si non raccordé PSC	✓ Session maintenue Gain utilisateur +++	✗ MIE OS + SSO + PSC + VDI à déployer	⚠ Partielle (SSO local en secours)	✓ Contexte de travail repris partout

Exemple de cas d'usage Hospiconnect ALPHA - Architecture n°4



Je m'authentifie en 2FA toutes les 4 heures (CPS, FIDO2, carte neutre).

J'accède ensuite à tout le SIH en 1FA sans contact — dont le DMP via mon DPI.

Je peux changer de poste et récupérer mon environnement de travail instantanément (session nomade).

Exemple de cas d'usages Hospiconnect ALPHA

Connexion au poste de travail

La connexion au poste de travail représente la première étape du parcours d'authentification et constitue un point critique pour sécuriser l'accès aux environnements numériques.

Selon les choix effectués par les lauréats, deux approches principales coexistent :

Option 1 : Authentification 2FA primaire (connexion au poste)

Cas général

- L'utilisateur s'authentifie dès la connexion au poste en 2FA (par exemple via carte CPS ou une autre méthode). Dans ce cas, le jeton de connexion est automatiquement reporté au webSSO, permettant un accès fluide aux services numériques de santé sans authentification supplémentaire.
- Cette méthode suppose l'ouverture d'une **session nominative** sur le poste de travail (car l'utilisateur est authentifié à titre personnel).
  - En pratique, les sessions non nominatives, notamment dans le cas de postes kiosques sont très déployés dans les services de soins des structures.

Option 2 : Authentification 2FA secondaire (après ouverture de la session en 1FA)

Cas général

- Il est également possible de maintenir un niveau d'authentification 1FA au système d'exploitation du terminal pour la connexion initiale.
- Dans ce scénario, une étape supplémentaire est ensuite requise pour se connecter manuellement au fournisseur d'identité local afin d'accéder aux services numériques de santé.

Exemple de cas d'usages Hospiconnect ALPHA

Connexion au poste de travail

Cas d'usage particuliers	Option 1 : Authentification 2FA primaire	Option 2 : Authentification 2FA secondaire
Postes kiosques : postes partagés entre plusieurs utilisateurs au sein d'un service.	**Problématique rencontrée** Les postes kiosques sont généralement associés à des sessions communes, permettant à un grand nombre d'utilisateurs de se connecter. La configuration d'un grand nombre de sessions individuelles sur un même poste n'est pas supportée par la plupart des ordinateurs. Par conséquent, ces postes kiosques ne permettent généralement pas l'authentification 2FA primaire. **Exemple de solution mise en place** Mettre en place un 2FA « partiel » sur le poste de travail : l'utilisateur s'authentifie en 2FA sur le poste, créant un jeton d'authentification au sein de la session générique qui va être ouverte.	Dans ce cas, les utilisateurs peuvent se connecter à une session générique, et s'authentifier ensuite en 2FA au fournisseur d'identité déployé dans la structure. Il faut alors veiller à mettre au point un mécanisme de déconnexion du SSO lors de la fermeture de la session.
Sessions virtualisées	Dans le cas de postes virtualisés, les sessions utilisateurs sont actives sur un serveur distant des postes utilisés. Lorsqu'un PS ouvre un poste partagé utilisant cette virtualisation, il se connecte nominativement au poste. Ce poste récupère la session correspondante auprès du serveur afin que le PS retrouve son bureau et ses applications habituelles. En cas de changement de poste, le PS ferme sa session sur le poste 1. En se connectant au poste 2, il retrouvera son environnement de travail (bureau, paramètres, etc.). **Inconvénients** - Implémentation lourde - Temps de synchronisation entre le poste et le serveur distant	

La fédération d'identités en lien avec ProSantéConnect

Délégation de l'authentification PSC à un fournisseur d'identité local

ProSantéConnect permet de déléguer l'authentification au fournisseur d'identité de l'établissement

Le MIE local peut ainsi être utilisé pour accéder aux services numériques nationaux ou régionaux après appairage avec l'identité nationale.

Simplification de l'expérience utilisateur

tout en garantissant les exigences de sécurité

Conditions :

- Nécessite un Fournisseur d'identités référencé auprès de l'ANS *
- Nécessite une déclaration de l'établissement auprès de l'ANS et une configuration technique du FI local **

https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/delegation-un-fournisseur-d-identite-local

* https://esante.gouv.fr/ens/offre/pro-sante-connect/liste-solutions-identite-compatibles-delegation-psc

** https://esante.gouv.fr/ens/offre/pro-sante-connect/ressources-techniques-fi-tiers

La gestion de l’authentification unique (SSO)

Types de SSO — Synthèse comparative

Le SSO n'est pas une solution unique : 3 approches coexistent, complémentaires, selon le type d'applications et le contexte d'usage.
La brique SSO compatible OIDC est obligatoire dans la PGSSI-S depuis le 01/01/2025 pour les structures ayant >5 services sensibles ou >5000 PS.

1 eSSO
Enterprise SSO

Poste de travail + apps client lourd

Kerberos / NTLM / injection d'écran

MIE = ouverture session Windows (carte, FIDO2, badge…)

Avantages
- Couvre TOUT type d'appli sans modifier le code
- Postes partagés / nomades (session itinérante)
- Compatible apps non OIDC/SAML sans modification

Contraintes
- Agent à déployer sur chaque poste
- Moins sécurisé (injection credentials sur les écrans de connexion)

PSC : Via webSSO/IdP intermédiaire

2 WebSSO
Web Access Management

Applications web — navigateur

SAML 2.0 / OIDC / Kerberos web

MIE → IdP → token → apps raccordées

Avantages
- Pas d'agent sur les postes
- Contrôle d'accès avancé
- Traçabilité centralisée
- Compatible PSC (OIDC)

Contraintes
- Ne couvre que les apps web
- Raccordement de chaque app requis avec le SSO

PSC : Raccordement OIDC direct possible

3 Fédération d'identités
IdP local + PSC

Services internes + services nationaux

OpenID Connect (OIDC) — obligatoire PSC

MIE → IdP local → PSC → FS national

Avantages
- Navigation sans couture inter-établissements
- Identité nationale RPPS transmise
- Conformité RIE implicite (PSC)
- SSO entre services locaux ET nationaux

Contraintes
- Raccordement OIDC obligatoire des apps
- Appairage e-CPS (1 fois + renouvellement)
- Dépendance disponibilité PSC

PSC : C'est le cœur du dispositif

Questions / Réponses et échanges