ANS – Cadre d’urbanisation du secteur médico-social

Version 2024 du cadre d’urbanisation - Identification électronique des professionnels exerçant en ESMS et des usagers

Février 2024

Statut : Validé | *Classification : Public* | *Version :*

LA E-SANTÉ FRANÇAISE — AGENCE DU NUMÉRIQUE EN SANTÉ — MINISTÈRE DES SOLIDARITÉS, DE L’AUTONOMIE ET DES PERSONNES HANDICAPÉES — GOUVERNEMENT Liberté Égalité Fraternité — Délégation au numérique en santé — cnsa Caisse nationale de solidarité pour l’autonomie — service public de l’autonomie

Sommaire

1. Domaine d'étude 7 - Identification électronique des professionnels exerçant en ESMS et des usagers

1.1. Présentation des enjeux, besoins et axes de travail

1.1.1. Périmètre et enjeux

L'identification électronique des acteurs (structures, professionnels, usagers) est un des piliers fondamentaux pour garantir la sécurité de l'accès, des échanges et du partage de données personnelles dont des données de santé, en toute confiance. L'État rend opposable les référentiels prioritaires dans le cadre prévu par la loi, comme par exemple, le référentiel d'identification électronique (opposable par arrêté du 28 mars 2022) qui définit les Moyens d'Identification Electronique (MIE) autorisés pour l'accès à des services numériques en santé contenant des données à caractère personnel. On peut également citer le référentiel de sécurité et d'interopérabilité pour l'accès des professionnels au DMP (prépublié en concertation publique, pour une publication prévue à partir de septembre 2023). Ces référentiels permettent de protéger les données personnelles, dont les données de santé, des usagers, tout en construisant un cadre de confiance urbanisé propice à un développement fort du numérique en santé en France.

La phase d'analyse de l'existant et de définition des orientations stratégiques a permis de mettre en avant les enjeux suivants pour l'écosystème :

Faciliter les parcours	Garantir la confiance en proposant des dispositifs simples et sécurisés d'accès des professionnels et des usagers aux services numériques (DUI, Portails, etc.).
Faciliter les parcours	Clarifier les modalités d'identification électronique des aidants / représentants légaux / famille aux documents et données de l'usager (données DUI, MES[1], etc.).
Optimiser la coordination et pratiques professionnelles	Simplifier la saisie par les ESMS, de la description de leur offre et activités et réaffirmer le positionnement du ROR[1].
Favoriser l'auto-détermination	Définir les modalités de collecte du consentement des usagers concernant le traitement primaire et/ou secondaire de leurs données.
Garantir l'équité de traitement	Définir les exigences applicables à la déclaration d'un aidant numérique et les droits qui peuvent lui être délégués par un usager.

1.1.2. Contexte

L'accès et le partage sécurisé des données relatives à une personne accompagnée et la traçabilité de ces échanges reposent sur une identification unique des usagers et des acteurs de l'accompagnement, ainsi que sur une authentification sécurisée de ces acteurs. La Politique Générale de Sécurité des Systèmes d'Information de Santé

[1] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire

(PGSSI-S)[2] a rendu opposable à l'ensemble des solutions du secteur la mise en œuvre de niveaux minimaux d'authentification au travers de l'utilisation de services et référentiels socles du numérique en santé.

Par ailleurs, en complément des référentiels FINESS et RPPS qui constituent LA référence en matière d'identification respectivement des personnes morales et des personnes physiques pour l'offre en santé et médico-social, la mise en place d'un ROR[3] national constitue aujourd'hui un levier pour rationaliser la saisie de la description de l'offre par les ESMS[3], fluidifier son accès par les services consommateurs, et favoriser la mise à jour et la qualité des données.

En complément, la confiance dans les services numériques ne peut être maintenue que si les usagers sont informés et consentent aux usages qui sont faits de leurs données. Le consentement – qu'il concerne des usages primaires ou secondaires des données – est donc un enjeu clef au-delà d'une exigence réglementaire introduite par le RGPD[3].

Enfin, l'accès aux services numériques de santé peut représenter une difficulté pour près de 1/6ème de la population qui est en situation d'illectronisme[4]. L'identification d'un « aidant », en charge de conduire les démarches en ligne pour le compte de la personne accompagnée, constitue donc une nécessite pour de nombreux usagers.

1.1.3. Besoins et questionnements identifiés

Les entretiens et ateliers réalisés auprès des acteurs de l'écosystème du médico-social ont permis d'identifier les besoins et questionnements suivants :

Métier	▸ Est-ce que les professionnels du médico-social peuvent bénéficier d'une identité nationale pérenne de la même façon que les professionnels de santé ? Pourquoi les professionnels du médico-social doivent s'enregistrer dans le RPPS étendu aux acteurs du médico-social ?	Axes 7.3
	▸ Comment faciliter la mise à jour du référentiel national RPPS depuis le DUI ou la GRH ?	Axes 7.3
Urbanisation	▸ En tant que fournisseur de services, que puis-je proposer pour une identification unique des utilisateurs, commune à tous les services, qu'ils soient professionnels ou usagers ?	Axe 7.1, 7.2 et 7.3
	▸ Quand est-ce que l'authentification à double facteurs pour l'accès au DUI sera rendue obligatoire ?	Axe 7.1, 7.2 et 7.3
	▸ Les DUI devront-ils être interopérables avec l'application carte Vitale pour proposer un accès usager au DUI ? L'application carte Vitale certifiera-t-elle le porteur en plus de pouvoir véhiculer son INS (ex. utilisation du téléphone d'un tiers) ?	Axe 7.1
	▸ France Connect sera-t-il la porte d'entrée de tous les services socles dont le DUI ?	Axe 7.2
	▸ Les modalités d'authentification des professionnels offertes par Pro Santé Connect (CPS et e-CPS) vont-elles évoluer ? Est-il par exemple prévu d'intégrer un dispositif de type clé FIDO aux modalités d'authentification proposées par Pro Santé Connect ?	Axe 7.3
	▸ Quels sont les avantages de l'utilisation des clés FIDO2 ?	Axe 7.3
	▸ Une date est-elle fixée pour l'accès aux services socles DMP (via Web PS DMP) via Pro Santé Connect ?	Axe 7.3
	▸ Quel est l'avenir des cartes CPE et CPS ?	

[2] Corpus documentaire de la PGSSI-S publié le 01/04/2022
[3] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire
[4] INSEE- Etude sur l'illectronisme et la fracture numérique (2019)

	▸ Comment peut-on activer les carte e-CPS de notre personnel paramédical en attendant la fin de EPARS dans le cas où l'ARS n'a pas renseigné le mail et le numéro de téléphone du professionnel dans l'annuaire ADELI ?	Axe 7.3
	▸ Comment accéder aux différents services tels que le DMP ou MSSanté dans le cas où le professionnel n'est pas équipé d'un téléphone ?	Axe 7.3
	▸ Est-ce que la traçabilité des actes, prestations, etc. des professionnels des ESMS dans le DUI de l'établissement se fera par son identification ?	Axe 7.3
	▸ Des API sont-elles prévues pour pouvoir réaliser des enregistrements au RPPS ?	Axe 7.3
Règlementation	▸ Quels sont les niveaux d'identification requis pour le secteur médico-social, qu'il s'agisse des professionnels ou des usagers ?	Axe 7.1, 7.2 et 7.3
	▸ Est-il prévu une évolution du code du travail pour les salariés des ESMS pour permettre au professionnel de s'opposer à l'inscription de ses éléments personnels dans Pro Santé Connect ?	Axe 7.3
	▸ Le référentiel DMP a-t-il été officiellement publié ?	Axe 7.3
Sécurité	▸ Est-ce qu'un professionnel ou un usager peuvent se connecter avec identifiant et mot de passe à un service numérique en santé, en particulier au DUI ? Si non, quelles sont les alternatives ?	Axe 7.1, 7.2 et 7.3
	▸ Quels sont les services avec lesquels le DUI pourrait échanger des données par identification indirecte ? Dans quels cas d'usages ?	Axe 7.2
	▸ Quelles sont les opportunités de capitalisation sur l'expérimentation « AIR » pour mettre en œuvre une authentification indirecte renforcée pour le secteur médico-social ? Quels seraient les services concernés ?	Axe 7.2
	▸ Est-il nécessaire d'enregistrer les professionnels dans le RPPS avec des coordonnées personnelles ?	Axe 7.3

Les réponses à ces besoins et questionnements sont structurées selon les 6 axes suivants :

Ref.	Axe de travail
Axe 7.1	Identification et authentification des utilisateurs de service : Usagers
Axe 7.2	Identification et authentification des utilisateurs de service : Personnes morales
Axe 7.3	Identification et authentification des utilisateurs de service : Personnes physiques

Au titre de cette V1 du cadre d'urbanisation sectoriel pour le médico-social, nous proposons d'apporter des éléments de réponse, dans la suite de ce document, pour les axes 7.1, 7.2, 7.3[5] en réaffirmant et précisant les modalités d'identification et d'authentification des usagers et des professionnels de santé, conformément à la doctrine du numérique en santé et aux cadres réglementaires.

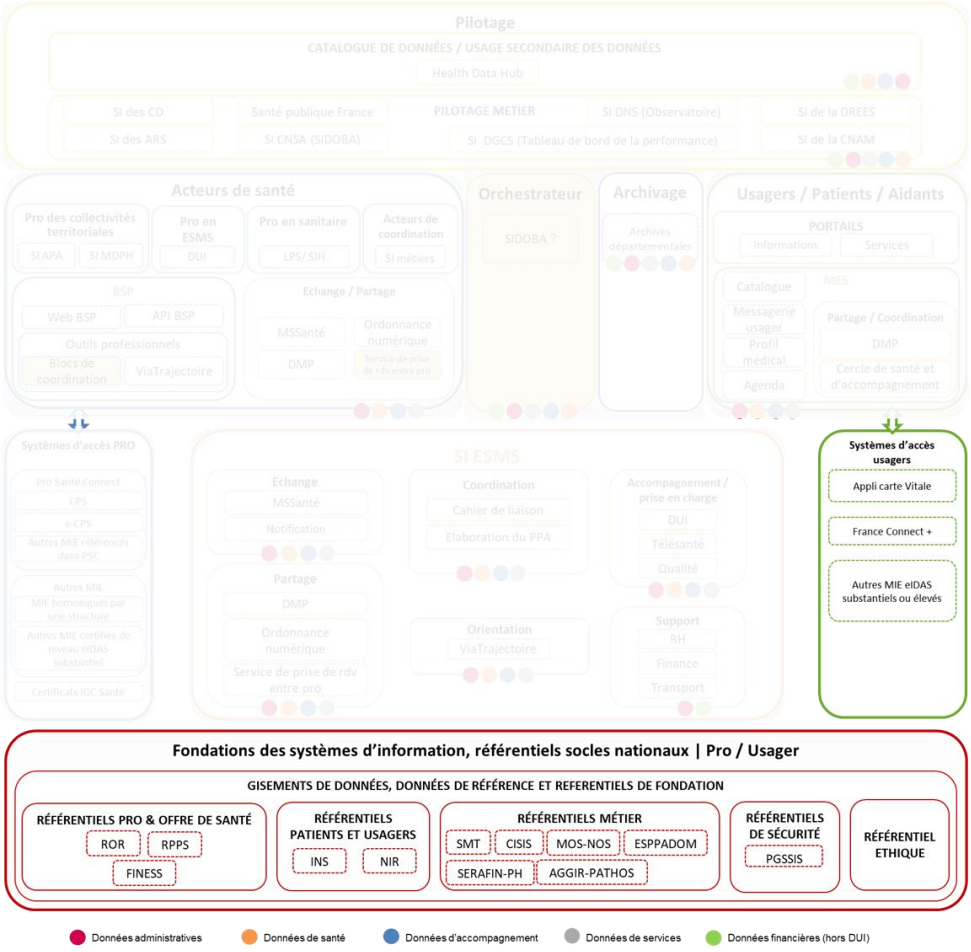
[5] Domaine d'étude 7 (partiel) - Optimisation de la saisie, par les ESMS, de la description de leur offre et activités

1.2. Axe 7.1 – IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS DE SERVICE : USAGERS

1.2.1. Services concernés en cible

L'axe de travail 7.1 concerne plus spécifiquement les sections fonctionnelles[6] suivantes, introduites dans la schématisation de l'architecture fonctionnelle :

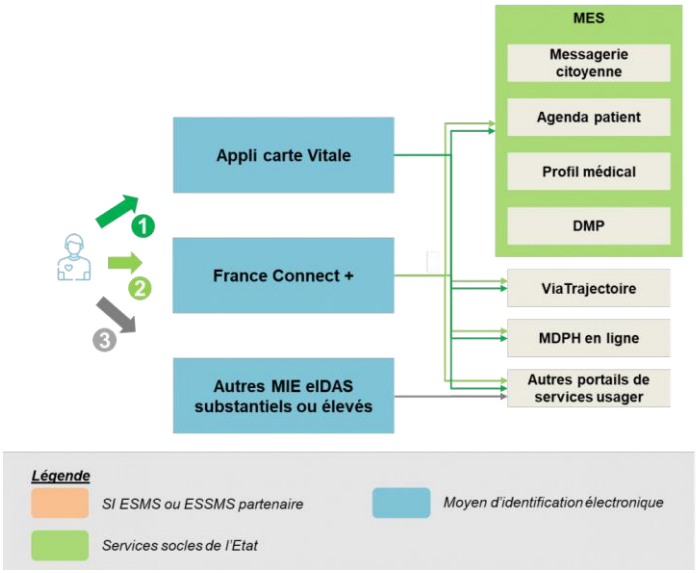
- Systèmes d'accès usager, et notamment les services appli carte Vitale (ou ApCV) et France Connect
- Fondations des systèmes d'information, référentiels socles nationaux | Pro / Usager et notamment les référentiels patients et usager – INS et NIR



1.2.2. Orchestration des services

Le schéma ci-dessous présente l'orchestration des services d'identification et d'authentification des utilisateurs de services (usagers).

[6] Voir chapitre Présentation des concepts et services du " document cœur : démarche, principes, schémas et glossaire »



1.2.3. Déclinaison des cas d'usage

Les niveaux de sécurité relatifs à l'authentification de l'usager dépendent des données collectées et/ou échangées par le service concerné (i.e. s'il s'agit de données de santé ou non). Les exigences associées à chaque niveau de sécurité sont rappelées dans le Référentiel d'Identification Electronique[7] porté par la Politique Générale de Sécurité des Systèmes d'Information (PGSSI-S).

Ces exigences spécifient que l'authentification à un service collectant, traitant ou hébergeant des données de santé, doit dès à présent respecter les exigences associées aux moyens d'identification électronique de transition du référentiel d'identification électronique (usager) : double facteur d'authentification, renouvellement régulier, règles de construction des mots de passe, etc. De même, ces exigences spécifient que **l'authentification à ces services doit respecter dès que possible, et au plus tard le 1er janvier 2026, un niveau de garantie au moins « substantiel » du règlement européen eiDAS (cela est notamment le cas de FranceConnect+) ou reposer sur l'utilisation de l'appli carte Vitale (qui atteindra prochainement ce niveau de garantie).**

Ref.	En tant que …	… je souhaite …	… et pour cela …
1	Usager	Accéder aux services numériques mis à ma disposition.	Dès que possible, et au plus tard le 1er janvier 2026, je me connecte avec France Connect+ ou tout autre moyen d'identification électronique certifié eIDAS (*), de niveau substantiel ou élevé, à l'ensemble des services numériques en santé proposant ces moyens d'identification électronique. Je peux également me connecter avec l'Appli carte Vitale à l'ensemble des services numériques en santé proposant ce moyen d'identification électronique. En tant qu'usager, si je suis détenteur de l'Appli carte Vitale, et que je me connecte à un service numérique avec celle-ci, je peux véhiculer mon INS sans que les professionnels n'aient besoin

[7] Référentiel d'Identification Electronique, partie usagers

			de me demander un justificatif d'identité à haut niveau de confiance.

Les fournisseurs de services ont la possibilité de mettre à disposition de leurs usagers des moyens d'identification électronique de transition pour une connexion à leurs services. Ces moyens d'identification électronique de transition, utilisables au plus tard jusqu'au 31/12/2025, ***doivent a minima proposer une authentification à deux facteurs****. Les exigences liées aux moyens d'identification électronique de transition sont décrites dans le référentiel d'identification électronique des usagers[8].*

Exemples de moyens d'identification électronique de transition :

Les usagers peuvent se connecter aux services numériques en santé (ex. portail usager du DUI, Mon Espace Santé, ViaTrajectoire, etc.) via les moyens d'identification électronique de transition suivants :

- *Un mot de passe associé à un OTP SMS (mot de passe à usage unique) ou à un code TOTP (mot de passe à usage unique basé sur le temps)*
- *Une application mobile enrôlée sur le téléphone de l'utilisateur associée à un code PIN*
- *Un mot de passe associé à une empreinte digitale vérifiée par le téléphone de l'utilisateur*

1.2.4. Recommandations d'urbanisation

Recommandation 7.1.1 : Tout échange de données relatif à un usager, qu'il soit réalisé dans le cadre de son orientation ou de son accompagnement, repose sur l'utilisation de l'INS de l'usager. A ce titre, l'INS[9] doit être utilisée par l'ensemble des professionnels ou structures concourant à l'orientation et l'accompagnement de l'usager.

Les acteurs du secteur médico-social – ESMS MDPH[10] ou services de PMI[10] doivent utiliser l'INS dès lors qu'ils référencent, échangent et/ou partagent des données de santé relatives à un usager[9]. Les acteurs publics tiers tels que les services de la protection sociale ne manipulent pas de données de santé à caractère personnel. Le référencement des données via l'INS n'est donc pas obligatoire. Les informations afférentes au dossier social de l'usager sont généralement associées au NIR[10] de ce dernier.

Dans ces conditions, la mise en œuvre d'un identifiant unique de l'usager – pour l'ensemble des actions d'accompagnement et dans le cadre d'un « parcours sans couture »[11] - demeure un défi.

L'INS d'un usager pourra permettre en cible de reconsolider l'ensemble des données associées à son accompagnement, selon des modalités qui devront être définies par une étude juridique dont les conclusions seront soumises à la validation de la CNIL.

Recommandation 7.1.2 : Toute structure ou professionnel du secteur sanitaire, médico-social ou social doit identifier un usager et référencer ses données de santé, grâce à son Identité Nationale de Santé (INS).

[8] Référentiel d'Identification Electronique, partie usagers

[9] Plusieurs textes réglementaires régissent l'utilisation de l'INS : L'article L.1111-8-1 du Code de la Santé Publique précisé par les articles R 1111-8-1 à 7 prévoient que le NIR constitue l'identifiant national dans les champs de la santé et du médico-social / Le décret d'application n 2019-1036 du 8 octobre 2019 rend obligatoire l'utilisation de l'INS pour référencer les données de santé depuis le 01/01/2021 / L'arrêté du 27/05/2021 rend opposable le référentiel INS v2 et ses annexes, le référentiel national d'identitovigilance et le guide d'implémentation

[10] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire

[11] Le parcours sans couture est un parcours intégrant deux notions : la non-nécessité de se reconnecter lors du passage d'un service à un autre et une ergonomie aussi proche que possible. L'intérêt du parcours sans couture est d'offrir une expérience utilisateur fluide, transparente et sans interruption.

Pour pouvoir référencer les données de santé et les échanger et partager, l'INS doit être **qualifiée.** Pour ce faire, deux conditions doivent être respectées :

- L'identité de l'usager doit être vérifiée sur la base d'un **dispositif à haut niveau de confiance** (carte nationale d'identité, passeport)
- L'INS doit être récupérée ou vérifiée par le biais du **téléservice INSi**[12], garantissant ainsi sa conformité avec les bases nationales de référence.

L'appli carte Vitale véhiculera l'INS qualifiée de l'usager qui l'aura activée, ainsi les 2 conditions ci-dessus ne seront pas nécessaires dans ce cas précis.

Recommandation 7.1.3 : Au plus tard le 1er janvier 2026, les usagers devront utiliser des moyens d'identification électronique de niveau eIDAS substantiel (appli carte Vitale, France connect +) pour se connecter aux services numériques de santé.

Recommandation 7.1.4 : De manière transitoire et jusqu'au 1er janvier 2026, les usagers peuvent accéder aux services numériques en utilisant une solution d'authentification répondant aux exigences associées aux moyens d'identification électronique de transition du référentiel d'identification électronique (usager) : double facteur d'authentification, renouvellement régulier, règles de construction des mots de passe, etc.

De manière transitoire, et jusqu'au 1er janvier 2026, l'usager peut s'authentifier à un portail de service au travers d'une authentification à double facteurs (2FA). Par exemple, l'authentification à Mon espace santé avec France Connect « simple » est renforcée avec un 2nd facteur (i.e. OTP SMS ou mail).

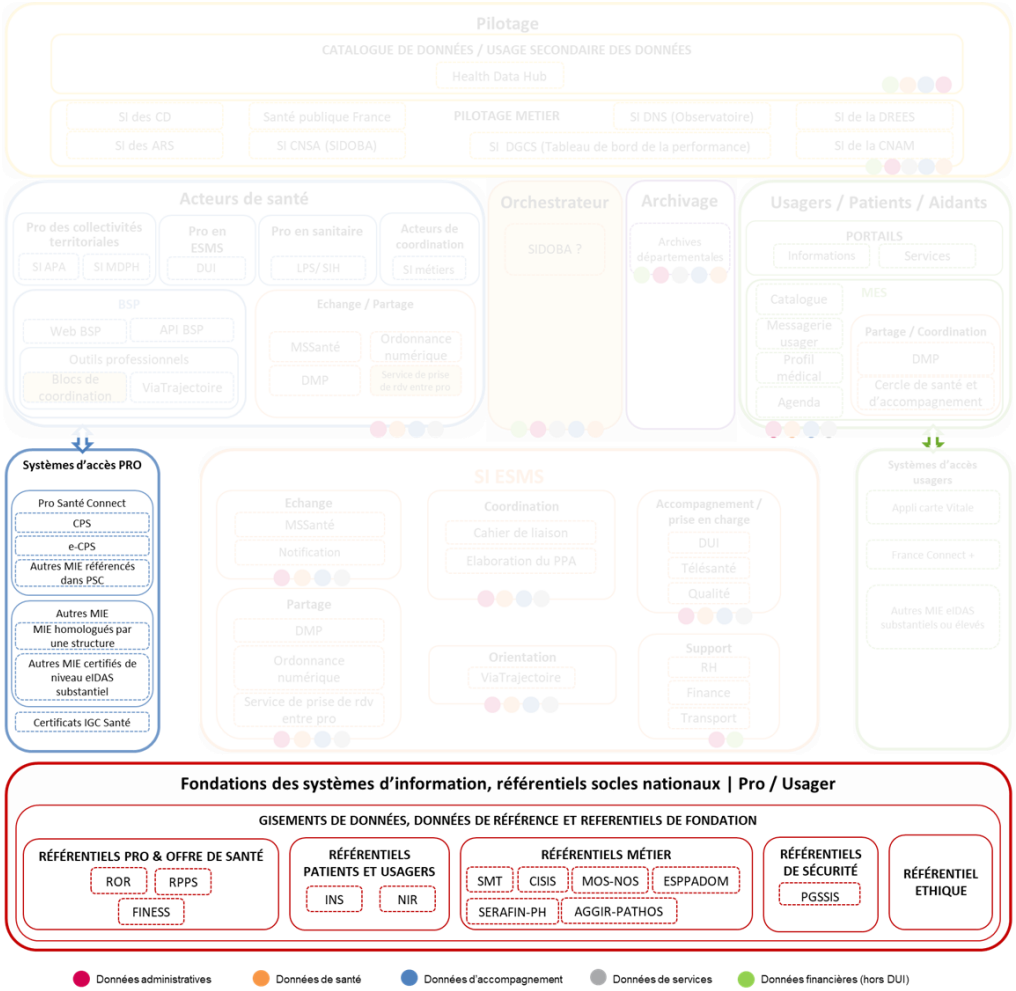
[12] Référentiel National d'Identitovigilance (RNIV)

1.3. Axe 7.2 – IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS DE SERVICE : PERSONNES MORALES

1.3.1. Services concernés en cible

L'axe de travail 7.2 concerne plus spécifiquement les sections fonctionnelles[13] suivantes, introduites dans la schématisation de l'architecture fonctionnelle :

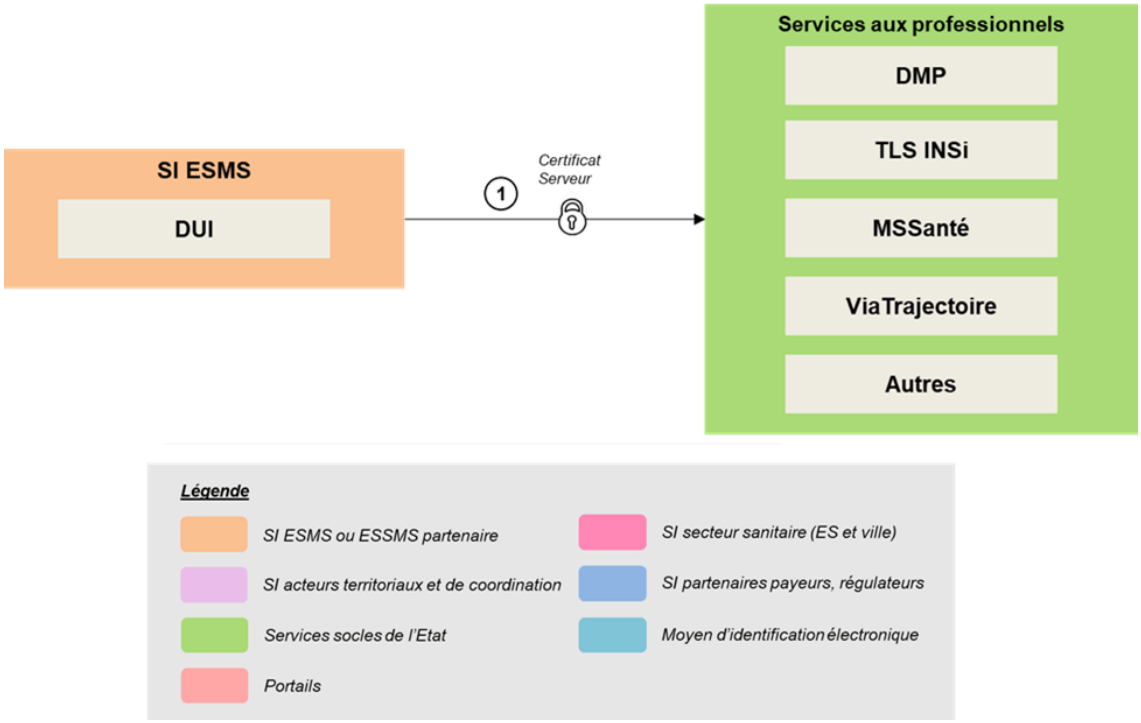
- Systèmes d'accès professionnel, notamment les certificats IGC Santé
- Fondations des systèmes d'information, référentiels socles nationaux | Pro / Usager et notamment les référentiels PGSSI-S



1.3.2. Orchestration des services

Le schéma ci-dessous présente l'orchestration des services d'identification et d'authentification des utilisateurs de services (personnes morales).

[13] Voir chapitre Présentation des concepts et services du " document cœur : démarche, principes, schémas et glossaire »



1.3.3. Déclinaison des cas d'usage

Les niveaux de sécurité concernant l'authentification d'une personne morale (c'est-à-dire un ESMS) dépendent des finalités et des données collectées par les services numériques concernés. Les exigences associées à chaque niveau de sécurité sont rappelées dans la Politique Générale de Sécurité des Systèmes d'Information (PGSSI-S)[14] :

- Dans le cas où le service héberge des données de santé, la personne morale utilise un certificat de personne morale (ex : IGC Santé[15]), idéalement échangé selon un TLS mutuel[16] (i.e. l'ESMS et le service auquel il accède s'authentifient réciproquement pour garantir la sécurité de l'échange).
- Dans le cas où le service n'héberge pas de données de santé, la personne morale utilise un certificat serveur pour se connecter au service.

Ref.	En tant que …	… je souhaite …	… et pour cela …
1	ESMS	Accéder à un service externe partagé hébergeant des données de santé avec des données ou informations dans le cadre de l'accompagnement de l'usager.	En tant que personne morale, afin d'accéder à un service partagé, j'utilise le certificat logiciel adéquat parmi les trois types de certificats qui existent (ORG, SERV et SIGN) délivrés par l'IGC Santé (un service de l'ANS).

[14] RIE des acteurs des secteurs sanitaire, médico-social et social [personnes morales]
[15] Présentation de IGC Santé Certificats *(site esante.gouv.fr)*
[16] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire

			Pour le secteur médico-social, il est préconisé d'utiliser des certificats délivrés à la maille de l'entité juridique. Les droits d'accès au service par certificat dépendent du fournisseur de services (exemple : le DMP ne permet que l'alimentation par certificat, la consultation du DMP ne peut pas se faire avec un certificat).

En cible, l'identification électronique privilégiée sera celle des personnes physiques (les professionnels officiant dans les structures). L'identification électronique en tant que personne morale sera restreinte à des flux comme l'automatisation d'échanges de documents entres différents services.

Selon le service concerné (DMP, TLS INSi, MSSanté, ViaTrajectoire, etc.), le responsable de traitement a la charge de définir les règles de traçabilité de la personne physique qui se connecte au service numérique (notamment dans le cadre de l'identification indirecte).

Dans le cadre du DMP, le référentiel de sécurité et d'interopérabilité définissant les modalités d'accès au DMP pour les professionnels a été publié en concertation publique.

1.3.4. Recommandations d'urbanisation

Recommandation 7.2.1 : Le numéro FINESS[17] est l'identifiant unique d'une personne morale agissant dans le secteur sanitaire, médico-social ou social. Toute structure sanitaire, médico-sociale ou sociale doit être inscrite dans le Fichier National des Etablissements Sanitaires et Sociaux et être identifiée par son numéro FINESS lorsqu'elle accède à un service numérique de santé.

Les actions réalisées à l'initiative de la structure (i.e. échange de données, ajout ou modification de données de santé, etc.) doivent être a minima associées au numéro FINESS de ladite structure, et en cible à la personne physique réalisant ces actions.

Les structures intervenant dans le cadre de l'accompagnement d'un usager – et ne disposant pas aujourd'hui d'un numéro FINESS – peuvent en faire la demande auprès de leur ARS ou de leur Conseil Départemental[18].

Recommandation 7.2.2 : L'Annuaire Santé rassemble les répertoires sectoriels de référence des personnes physiques et personnes morales : le répertoire partagé des professionnels intervenant dans le système de santé (RPPS), et le répertoire FINESS. Il est destiné aux professionnels et structures des secteurs sanitaire, social et médico-social. L'Annuaire Santé peut être interrogé « en temps réel » via une API par les services numériques de santé afin d'obtenir une donnée fiable et actualisée. Néanmoins, ce fonctionnement repose sur une connectivité minimum de la solution utilisée par le professionnel.

Ainsi, pour les professionnels disposant d'une connectivité limitée – du fait de leur situation géographique ou de conditions de travail en mobilité – il est recommandé que le service télécharge une copie de l'Annuaire Santé à un rythme régulier (journalier ou hebdomadaire par exemple, ce rythme devant être confirmé en lien avec l'ANS et l'éditeur de la solution métier). Ce téléchargement peut être réalisé de manière asynchrone (i.e. le soir et/ou le week-end) afin de ne pas impacter la performance du service utilisé par le professionnel.

[17] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire
[18] Répertoire FINESS

Recommandation 7.2.3 : L'authentification d'une personne morale, c'est-à-dire l'authentification d'un système d'information associée à une structure morale auprès d'un 2nd système d'information – doit reposer sur l'utilisation d'un certificat IGC Santé[19].

Dans le cadre d'une telle authentification, seule la structure est identifiée dans le cadre d'un échange de données (par exemple, l'alimentation du Dossier Médical Partagé est réalisée au nom de l'ESMS et non pas d'un professionnel). Une authentification indirecte (i.e. authentifier une personne physique sous la responsabilité d'une personne morale) ne permet usuellement pas de consulter et/ou de modifier un document de santé.

La doctrine du numérique en santé définit que ces ***certificats ne peuvent être délivrés qu'à des personnes morales identifiées comme des structures de soins ou d'accompagnement*** *et ayant la capacité de respecter les exigences de sécurité associées.*

Recommandation 7.2.4 : En cible, l'authentification des professionnels au sein des structures sera privilégiée. L'authentification en tant que personne morale sera restreinte à la seule automatisation des échanges de documents entres différents services.

Le certificat de personne morale ne porte aucune information sur la personne physique (identifiée par le numéro RPPS[19]) étant à l'origine de la consultation et/ou du dépôt d'un document. La généralisation de Pro Santé Connect (qui permettra un parcours sans couture sans besoin de réauthentification entre les services) facilitera l'identification de la personne physique dans l'ensemble des actions qu'elle réalise [voir axe 7.3].

1.4. Axe 7.3 – IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS DE SERVICE : PERSONNES PHYSIQUES

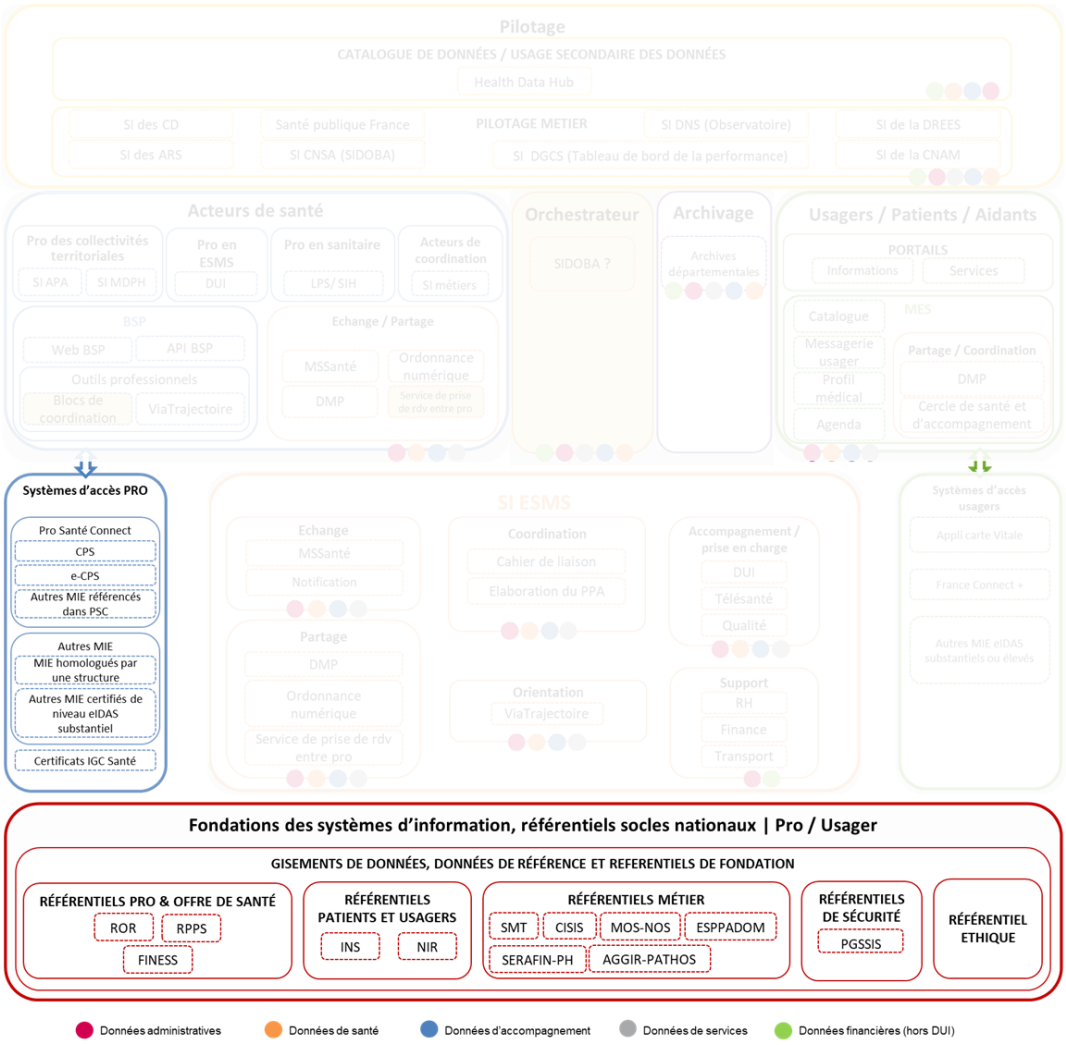
1.4.1. Services concernés en cible

L'axe de travail 7.3 concerne plus spécifiquement les sections fonctionnelles[20] suivantes, introduites dans la schématisation de l'architecture fonctionnelle :

- Systèmes d'accès professionnel, notamment la CPx et Pro Santé Connect (via e-CPS)
- Fondations des systèmes d'information, référentiels socles nationaux | Pro / Usager et notamment les référentiels professionnels – notamment le RPPS

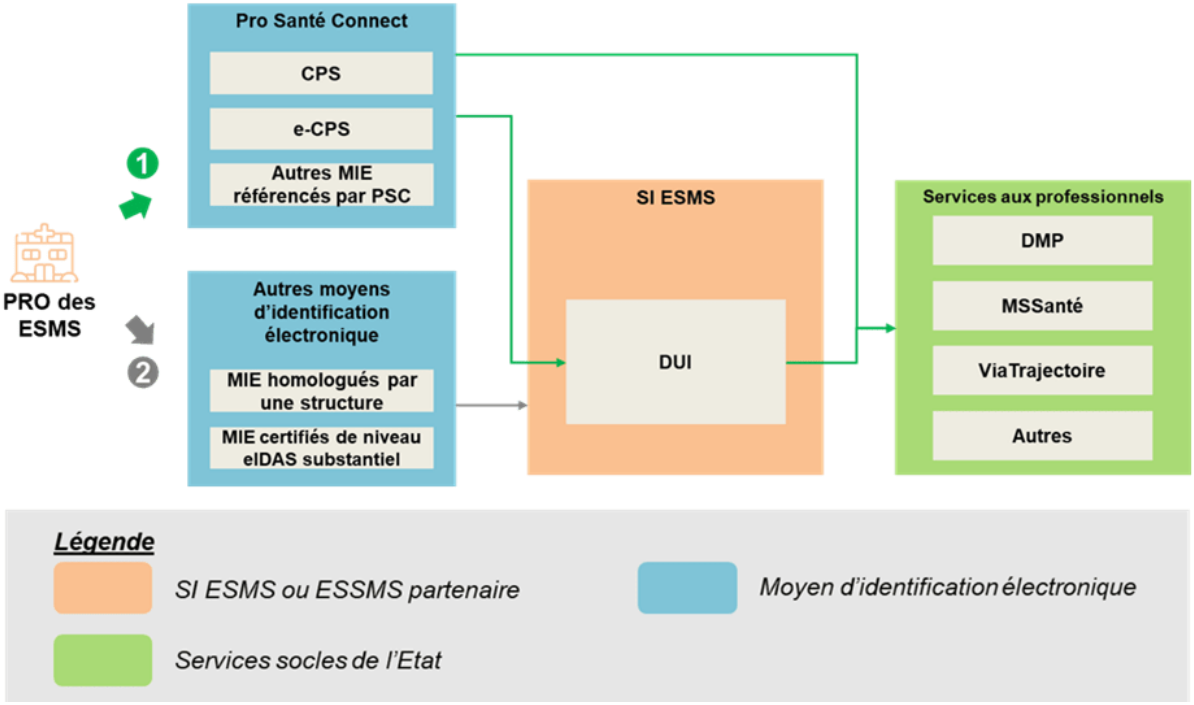
[19] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire

[20] Voir chapitre Présentation des concepts et services du " document cœur : démarche, principes, schémas et glossaire »


Pilotage
CATALOGUE DE DONNÉES / USAGE SECONDAIRE DES DONNÉES
Health Data Hub
SI des CD
Santé publique France
PILOTAGE METIER
SI DNS (Observatoire)
SI de la DREES
SI des ARS
SI CNSA (SIDOBA)
SI DGCS (Tableau de bord de la performance)
SI de la CNAM
Acteurs de santé
Pro des collectivités territoriales
SI APA
SI MDPH
Pro en ESMS
DUI
Pro en sanitaire
LPS/ SIH
Acteurs de coordination
SI métiers
BSP
Web BSP
API BSP
Outils professionnels
Blocs de coordination
ViaTrajectoire
Echange / Partage
MSSanté
Ordonnance numérique
DMP
Service de prise de rdv entre pro
Orchestrateur
SIDOBA ?
Archivage
Archives départementales
Usagers / Patients / Aidants
PORTAILS
Informations
Services
MES
Catalogue
Messagerie usager
Profil médical
Agenda
Partage / Coordination
DMP
Cercle de santé et d'accompagnement
Systèmes d'accès PRO
Pro Santé Connect
CPS
e-CPS
Autres MIE référencés dans PSC
Autres MIE
MIE homologués par une structure
Autres MIE certifiés de niveau eIDAS substantiel
Certificats IGC Santé
SI ESMS
Echange
MSSanté
Notification
Partage
DMP
Ordonnance numérique
Service de prise de rdv entre pro
Coordination
Cahier de liaison
Elaboration du PPA
Orientation
ViaTrajectoire
Accompagnement / prise en charge
DUI
Télésanté
Qualité
Support
RH
Finance
Transport
Systèmes d'accès usagers
Appli carte Vitale
France Connect +
Autres MIE eIDAS substantiels ou élevés
Fondations des systèmes d'information, référentiels socles nationaux | Pro / Usager
GISEMENTS DE DONNÉES, DONNÉES DE RÉFÉRENCE ET REFERENTIELS DE FONDATION
RÉFÉRENTIELS PRO & OFFRE DE SANTÉ
ROR
RPPS
FINESS
RÉFÉRENTIELS PATIENTS ET USAGERS
INS
NIR
RÉFÉRENTIELS MÉTIER
SMT
CISIS
MOS-NOS
ESPPADOM
SERAFIN-PH
AGGIR-PATHOS
RÉFÉRENTIELS DE SÉCURITÉ
PGSSIS
RÉFÉRENTIEL ETHIQUE
Données administratives
Données de santé
Données d'accompagnement
Données de services
Données financières (hors DUI)

1.4.3. Orchestration des services

Le schéma ci-dessous présente l'orchestration des services d'identification et d'authentification des utilisateurs de services (personnes physiques).



1.4.4. Déclinaison des cas d'usage

Les niveaux de sécurité concernant l'authentification d'une personne physique (c'est-à-dire un acteur de santé) dépendent des finalités du service et des données collectées et/ou hébergées. Les exigences associées à chaque niveau de sécurité sont rappelées dans la Politique Générale de Sécurité des Systèmes d'Information (PGSSI-S)[21]. Celle-ci rappelle que les services ayant pour finalité le diagnostic, la prise en charge, l'accompagnement, le soin ou la prévention, les identifiants nationaux à utiliser pour l'identification des acteurs personnes physiques intervenant en santé sont :

- Soit l'identifiant RPPS, à utiliser en priorité s'il existe pour la personne à identifier ;
- Soit l'identifiant ADELI, toléré de façon transitoire jusqu'à son remplacement définitif par l'identifiant RPPS pour les professions encore enregistrées dans ADELI.

A ce titre, le professionnel est invité à utiliser la carte CPx[22], la eCPx, Pro Santé Connect, un couple identifiant / mot de passe / code OTP reçu par email ou SMS ou encore une carte physique associée à un code PIN pour se connecter à un service collectant, traitant ou hébergeant des données de santé.

Ref.	En tant que …	… je souhaite …	… et pour cela …
1	Professionnel sanitaire,	Accéder à un service collectant, traitant ou hébergeant des données de santé, pour	Je peux m'identifier via :

[21] RIE des acteurs des secteurs sanitaire, médico-social et social [personnes physiques]
[22] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire

	médico-social ou social	consulter ou partager des données dans le cadre de l'accompagnement de l'usager.	▸ Pro Santé Connect ▸ Des moyens d'identification électronique homologués par l'ESMS pour cet usage (ex. clé FIDO2 à 2 facteurs, etc.) ▸ Des moyens d'identification électronique certifiés eIDAS de niveau substantiel ou élevé *NB : Des exigences en matière de traçabilité du professionnel sont déjà exprimées dans les référentiels d'exigences SEGUR. En cible, la connexion d'un professionnel via un moyen d'identification électronique devra permettre de faciliter cette traçabilité.*

Pro Santé Connect, en tant que fédérateur de fournisseurs d'identité :

- Permet au DUI de lui déléguer l'identification et l'authentification ;
- Permet au professionnel de se connecter par l'ensemble des moyens d'identification électronique fédérés par celui-ci.

NB. Les modalités d'authentification à PSC vont être élargies aux dispositifs de type clé FIDO2 (la clé FIDO2 permet notamment d'être utilisée à titre personnel, en parallèle du numérique en santé, pour stocker ses mots de passe). Il s'agira dans un premier temps des dispositifs certifiés par l'ANSSI.

Le déploiement de Pro Santé Connect avec une e-CPS auprès des professionnels est dès à présent possible, notamment pour accéder au DUI. Pro Santé Connect étant obligatoirement implémenté dans les DUI référencés Ségur, cela permet aux ESMS d'être conformes à la cible fixée par le RIE, sans nécessité d'homologuer un autre MIE : c'est donc la solution la plus simple, celle que les ESMS doivent privilégier.

D'autres moyens d'identification électronique de transition sont toutefois possibles jusqu'au 31/12/2025, par exemple :

- Un mot de passe associé à un OTP SMS (mot de passe à usage unique) ou à un code TOTP (mot de passe à usage unique basé sur le temps)
- Un badge contenant une puce avec contact associée à un code PIN ou un badge contenant une puce sans contact associé à un mot de passe
- Une clé de sécurité USB associée à un code PIN ou une empreinte digitale enregistrée sur la clé

En matière de connexion à un DUI, les fournisseurs de services doivent répondre à deux cas de figure :

1. La connexion à un DUI avec un accès externe (ex. les DUI en mode SaaS) doit être réalisée via une authentification à deux facteurs. Pro Santé Connect étant la solution la plus simple, il s'agit de celle qu'il faut privilégier ;
2. La connexion à un DUI sans accès externe (ex. application hébergée on Premise) est possible avec un identifiant et un mot de passe jusqu'au 31/12/2025 sous réserve que le fournisseur de services respecte les exigences du RIE *(complexité du mot de passe, renouvellement du mot de passe, etc.).*

Concernant l'accès au web PS DMP, des travaux sont actuellement en cours pour permettre aux logiciels métiers (tels que le DUI) via API Pro Santé Connect. Dans ce cadre, le référentiel Pro Santé Connect sera mis à jour d'ici fin 2023. Celui-ci reste cependant disponible pour les professionnels depuis décembre 2022 et il est donc déjà possible d'accéder aux documents qu'il contient sous réserve d'avoir été inscrit dans la matrice d'habilitation.

Enfin, le référentiel DMP a fait l'objet d'une demande de conseil auprès de la CNIL puis d'une consultation de la commission européenne. Le référentiel est désormais consultable dans le cadre d'une concertation publique sur le site de l'ANS. La version officielle devrait être publiée prochainement.

NB. Des travaux sont en cours sur la future génération de carte CPS, la CPS v4 qui devrait arriver en 2024 en établissements. Cette carte pourra être mise à jour à distance lors d'un changement d'activité contrairement au fonctionnement actuel où il est encore nécessaire de réimprimer une carte lors d'un changement d'activité.

En parallèle, une procédure a été mise en place pour permettre au gestionnaire ADELI EPARS de stocker un mail et un numéro de téléphone qui peuvent ensuite être transmis jusqu'à Pro Santé Connect de façon à permettre une activation de la e-CPS sans carte physique.

1.4.5. Recommandations d'urbanisation

L'ensemble des recommandations décrites ci-dessous explicite et précise les orientations définies dans la doctrine du numérique en santé :

Recommandation 7.3.1 : Le numéro RPPS[23] constitue l'identifiant unique d'un professionnel de santé, médico-social et social. Tout professionnel du secteur doit être inscrit dans le RPPS afin de disposer d'un MIE lui permettant d'accéder aux services hébergeant ou traitant des données de santé, qu'ils soient nationaux ou locaux. Il est alors identifié par ces services grâce à son numéro RPPS.

Le professionnel est alors identifié par le service grâce à son numéro RPPS[24] et les actions qu'ils réalisent au sein du service numérique (échange de données, modification d'une donnée, consultation des données, etc.) sont tracées et associée au numéro RPPS du professionnel.

L'ensemble des professionnels intervenant dans le champ de la santé, du médico-social et du social ainsi que les autres professionnels souhaitant disposer d'un MIE permettant d'accéder à un service numérique de santé doivent être enregistrés au sein du RPPS qui regroupera alors :

- *Les professions à ordre (médecin, masseur-kinésithérapeute, pharmacien, chirurgien-dentiste, sage-femme, pédicure-podologue). Ces différentes catégories de professionnels, y compris les internes et étudiants, sont inscrites au RPPS à l'issue de leur enregistrement auprès de leur ordre professionnel.*
- *Les ARS enregistrent les professions réglementées par le Code de la Santé Publique ou du Code de l'Action Sociale et des Familles (psychologue, assistant de service social, opticien-lunetier, orthophoniste, psychomotricien, ergothérapeute, orthoptiste, audioprothésiste, etc.). Le CSP et le CASF décrivent les exigences d'exercice pour ces professionnels (notamment au regard des diplômes devant être obtenus). Il est à noter que certaines professions sont basculées depuis le référentiel ADELI vers le RPPS durant l'année 2023 et que l'ensemble du référentiel ADELI aura été basculé dans le RPPS courant 2024.*
- *Les professions à « titre » (chiropracteur, psychothérapeute, psychologue et ostéopathe) sont également enregistrées au RPPS par leur Agence Régionale de Santé.*
- *Les professions à rôle, quel que soit leur employeur, qui accèdent à des données de santé (accompagnant éducatif et social, aide médico-psychologique, éducateur spécialisé, assistant médical, professionnels exerçant en conseil départemental, en MDPH, en CARSAT ou en PMI, etc.) qui ne sont pas inscrits par leur ordre ou par l'ARS dans les annuaires nationaux. Ces professionnels doivent être inscrits par leurs employeurs au sein du RPPS au travers du portail RPPS+.*

[23] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire
[24] Doctrine du numérique en santé – Version 2022

- *Le nouvel arrêté RPPS[25] précise qu'un moyen d'identification électronique doit être fourni à tout acteur ayant besoin d'accéder à des données de santé. Ainsi,* ***toute personne ayant besoin d'accéder à un service numérique en santé*** *(incluant les sphères de la justice, de l'éducation…) doit pouvoir, en cible, être enregistrée au RPPS. L'autorité d'enregistrement et les conditions d'enregistrement des professionnels qui ne relèvent pas des processus d'enregistrement au RPPS déjà encadrés juridiquement (par ex professionnels de la sphère justice ou de l'éducation) restent à déterminer.*

- *L'ensemble des professionnels listés ci-dessus sont nommés* ***« acteurs habilités à accéder à des services numériques de santé ».***

Il est nécessaire d'utiliser les informations personnelles (état civil – nom, prénoms, civilité, date et lieu de naissance, données de contact – adresse email, numéro de téléphone mobile, situation professionnelle – nom et prénom d'usage/d'exercice, FINESS géographique du lieu d'exercice, profession et rôle du professionnel, date de prise de fonction) pour enregistrer les acteurs habilités à accéder à des services numériques de santé au RPPS étant donné qu'il s'agit d'un moyen d'identification personnel.

Concernant l'accès aux différents services pour des professionnels ne possédant pas de téléphone portable, une étude est en cours. La cible privilégiée est la dématérialisation des cartes. Néanmoins, la dématérialisation des cartes pouvant être incompatible avec certains usages, la commande d'une carte CPS doit rester possible. Par ailleurs, d'autres moyens d'identification électronique telles que les clés FIDO2 citées ci-dessus seront prochainement utilisables avec Pro Santé Connect.

Des API sont en cours d'étude pour pouvoir réaliser ces enregistrements au RPPS plus facilement (i.e. en évitant l'enregistrement individuel des situations d'exercice). Une fonctionnalité de "chargement en masse" sera par exemple mise en service prochainement, permettant d'enregistrer tous les salariés (via un fichier csv préparé par l'ESMS) sans remplir des formulaires individuels pour chacun d'entre eux.

Recommandation 7.3.2 : L'Annuaire Santé[26] est l'unique service devant être interrogé pour obtenir le numéro RPPS qui identifie un professionnel de santé, médico-social ou social.

L'Annuaire Santé peut être interrogé « en temps réel » via une API par les services numériques de santé afin d'obtenir une donnée fiable et actualisée. Néanmoins, ce fonctionnement repose sur une connectivité minimum de la solution utilisée par le professionnel.

Ainsi, pour les professionnels disposant d'une connectivité limitée – du fait de leur situation géographique ou de conditions de travail en mobilité – il est recommandé que le service télécharge une copie de l'Annuaire Santé à un rythme régulier (journalier ou hebdomadaire par exemple, ce rythme devant être confirmé par l'ANS en lien avec la structure). Ce téléchargement peut être réalisé de manière asynchrone (i.e. le soir et/ou le week-end) afin de ne pas impacter la performance du service utilisé par le professionnel.

Recommandation 7.3.3 : Pro Santé Connect[27] est le fédérateur d'identité défini pour le secteur de la santé, du médico-social et social. A ce titre, il s'agit de la solution de connexion à privilégier.

Pro Santé Connect est le fédérateur d'identité en santé mis en œuvre par les pouvoirs publics, qui repose sur l'utilisation d'une CPx (carte de professionnel de santé, de personnel d'établissement ou de personnel autorisé) ou de sa version dématérialisée qui est priorisée pour le secteur médico-social : la e-CPx. La mise à disposition d'une carte – physique ou dématérialisée – repose sur l'inscription du professionnel au RPPS.

[25] Arrêté du 23 septembre 2022 relatif à la mise en œuvre du « Répertoire partagé des professionnels intervenant dans le système de santé » (RPPS) | esante.gouv.fr
[26] Présentation de l'Annuaire Santé et des données exposées | esante.gouv.fr
[27] Présentation de Pro Santé Connect | esante.gouv.fr

En complément, Pro Santé Connect prévoit l'homologation future d'autres moyens d'identification électronique matériels que la CPS (ex: clé ou carte à puce FIDO2). Par ailleurs, une structure peut homologuer son propre MIE deux facteurs (cf. RIE et guide d'auto-homologation MIE de la PGSSI-S).

Recommandation 7.3.4 : De manière transitoire et jusqu'au 1er janvier 2026, les professionnels peuvent accéder aux services numériques en utilisant une solution d'authentification répondant aux exigences associées aux moyens d'identification électronique de transition du référentiel d'identification électronique (personnes physiques).

Recommandation 7.3.5 : L'authentification d'un professionnel à Pro Santé Connect lui permettra d'accéder à l'ensemble des solutions utilisant Pro Santé Connect sans besoin de s'authentifier à nouveau et sans rupture de parcours.

Un volet du CI-SIS définira les modalités permettant de conserver un même contexte patient lors de l'utilisation de plusieurs solutions numériques de santé.

L'authentification d'un professionnel au sein de son logiciel métier lui permet d'accéder à l'ensemble des services ou référentiels socles du numérique en santé, ainsi qu'aux autres services nationaux sans devoir s'authentifier à nouveau et sans rupture de parcours.

A titre d'exemple, un professionnel s'authentifiant avec Pro Santé Connect à son logiciel métier peut alors accéder à l'ensemble des services socles du numérique en santé (DMP[28], MSSanté, TLS INSi[28], ViaTrajectoire, Bouquet de Services aux Professionnels, etc.) ou à des solutions tierces (applications professionnelles, outils de coordination, solution de télésanté, etc.) sans rupture de parcours.

Son accès aux services et les actions qu'il peut réaliser sont déterminés par les matrices des droits propres à chacun des services nationaux.

[28] Voir glossaire annexe 1 du document cœur : démarche, principes, schémas et glossaire

1.5. Prochaines étapes

Les actions restantes à mener, au regard des différents axes de travail de ce domaine d'étude sont les suivantes :

Ref.	Axe de travail	Statut	Actions à mener
Axe 7.1	Identification électronique des utilisateurs de service : Usagers	Axe instruit dans la version actuelle du cadre	▸ [ANS/DNS/CNSA] Concertation du cadre d'urbanisation auprès de l'écosystème ▸ [ANS/DNS] Accompagnement des professionnels, structures, opérateurs de service dans la bonne appropriation de ces principes du RIE ▸ [ANS/DNS] Mise en œuvre de pilotes dans le cadre de la Task force MIE
Axe 7.2	Identification électronique des utilisateurs de service : Personnes morales	Axe instruit dans la version actuelle du cadre	▸ [ANS/DNS/CNSA] Concertation du cadre d'urbanisation auprès de l'écosystème ▸ [ANS/DNS] Accompagnement des professionnels, structures, opérateurs de service dans la bonne appropriation de ces principes du RIE ▸ [ANS/DNS] Mise en œuvre de pilotes dans le cadre de la Task force MIE
Axe 7.3	Identification électronique des utilisateurs de service : Personnes physiques	Axe instruit dans la version actuelle du cadre	▸ [ANS/DNS/CNSA] Concertation du cadre d'urbanisation auprès de l'écosystème ▸ [ANS/DNS] Accompagnement des professionnels, structures, opérateurs de service dans la bonne appropriation de ces principes du RIE ▸ [ANS/DNS] Définition des modalités de mise en œuvre d'une API d'alimentation du RPPS par les ESMS au titre de leur rôle d'autorité d'enregistrement ▸ [ANS/DNS] Mise en œuvre de pilotes dans le cadre de la Task force MIE