

Journées Nationales

30 novembre et 1^{er} décembre 2023

**Réussir ensemble le virage numérique
dans le médico-social**



Programme du jeudi 30 novembre :

- 9h00 : Accueil
- 9h45-10h00 : Ouverture des Journées nationales et annonce du programme et du déroulement des 2 journées
- 10h-10h15 : Que retenir de 2023 ? Bilan des actions menées et des résultats obtenus collectivement
- 10h15-10h45 : Les belles histoires : le numérique progresse dans le médico-social.
- 11h15 - 12h30 : ateliers session #1

N°	Public concerné	Thématique	Titre	Description de l'atelier
#1.1	Editeurs	Technique	Quels moyens d'identification et d'authentification électronique privilégier pour le secteur médico-social ?	Un atelier technique d'échange sur les évolutions des moyens d'identification électroniques adaptées aux usages dans le secteur social et médico-social pour ces prochaines années.

1.1 : Moyens d'identification et authentification

Fanny HANNAUX, Florian CATTEAU

Salle 201

SOMMAIRE

- 01** **LES MOYENS D'IDENTIFICATION ET D'AUTHENTIFICATION POUR LE
SECTEUR MÉDICO-SOCIAL ET SOCIAL** 30'
- 02** **L'APPEL A PROJET A VENIR** 10'
- 03** **ATELIER DE REFLEXION** 35'

Contexte réglementaire - le référentiel relatif à l'identification électronique (RIE) des acteurs des secteurs sanitaire, médico-social et social

- Le référentiel relatif à l'identification électronique (RIE) des acteurs des secteurs sanitaire, médico-social et social est un pilier de la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S). Rendu opposable par arrêté ministériel le **28 mars 2022**, il vise à renforcer la sécurité autour de l'identification électronique, c'est-à-dire le processus utilisé par une personne pour s'identifier et s'authentifier.
- Concernant les professionnels, l'identification électronique repose :
 - D'une part sur le **répertoire partagé des professionnels intervenant dans le système de santé (RPPS)**. C'est le répertoire d'identité sectoriel de référence, permettant d'attribuer à chaque professionnel une identité unique au niveau national (demain au niveau européen).
 - D'autre part, chaque professionnel enregistré doit utiliser **un moyen d'identification électronique adapté** pour s'authentifier sur les services numériques en santé (apporter la preuve que la personne identifiée est bien celle qui se connecte).
- **Le RIE détermine la trajectoire de sécurisation progressive de l'identification électronique des professionnels intervenant dans le système de santé.**

Au 1er janvier 2026, les moyens d'identification électronique (MIE) utilisés devront faire intervenir une authentification renforcée (double facteur), par l'intermédiaire des MIE encadrés par la puissance publique (carte CPS, Pro Santé Connect) ou de MIE homologués en référence au niveau de garantie substantiel du règlement européen eIDAS.

Présentation des niveaux de garantie du règlement européen eIDAS

eIDAS est un règlement de l'UE qui instaure un cadre commun en matière d'Identité Numérique et services de Confiance Numérique.

Il introduit notamment 3 niveaux de garantie pour les solutions MIE : **FAIBLE**, **SUBSTANTIEL** et **ÉLEVÉ**.

L'ANS vise atteindre le niveau SUBSTANTIEL pour les MIE mis à disposition des professionnels de santé, d'ici 2027.

Exemples d'exigences de sécurité par niveau



Preuve et vérification d'identité
(enregistrement)



Gestion des Moyens d'identification électronique



Faible

Vérification basique de l'identité du demandeur

→ Ex : enrôlement à distance avec un simple scan d'une pièce d'identité



Substantiel

Vérification de la possession d'un titre authentique et du lien avec son détenteur

→ Ex : enrôlement à distance avec présentation de la pièce et comparaison photo avec selfie « vivant » (PVID niveau substantiel par exemple)



Élevé

Validation évidente de l'identité du demandeur

→ Ex : présentation CNI en face à face
→ Ex : enrôlement à distance avec CNIE (lecture puce crypto)
→ Ex enrôlement via VID niveau élevé

MIE avec un unique facteur, offrant une protection contre un attaquant avec potentiel de base

→ Ex : un mot de passe activé à l'aide d'un OTP reçu sur le mobile ou le mail du demandeur

MIE avec deux facteurs, offrant une protection contre un attaquant avec potentiel modéré

→ Ex : possession d'un smartphone avec une application d'authentification + code PIN (ou biométrie du téléphone)

MIE utilisant un module cryptographique de niveau de sécurité élevé, offrant une protection contre un attaquant avec potentiel élevé

→ Ex : carte à puce qualifiée avec PIN
→ Ex : application sur smartphone utilisant un composant matériel (SE/TEE)

Les exemples donnés ici ne portent que sur une partie des exigences de chaque niveau de garantie.



**LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ**

La faiblesse de l'Identification électronique dans le numérique en santé



- Les professionnels utilisent majoritairement des moyens d'identification électronique (MIE) de niveau faible
 - Ils n'ont pas toujours conscience des risques associés
- Ces MIE ne permettent pas la consultation du DMP (2FA)
 - Et ils ne seront pas conformes à la réglementation (RIE : 01/01/2026)
- L'usage d'un MIE 2FA est perçu comme une « entrave »
 - S'il n'est pas adapté au contexte (mobilité, manipulations...)
 - S'il doit être utilisé pour se réauthentifier de manière récurrente
- Le choix d'un MIE est engageant pour les acteurs
 - Investissements, organisation, conduite de changement
- Une prise de conscience croissante
 - Et une double opportunité de sécuriser et de simplifier l'IE des PS

D'après une étude de Verizon de 2021, 81% des notifications de violations de données mondiales seraient liées à une problématique de mots de passe.



**LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ**



Un défi particulier dans le secteur médico-social

- Un secteur impliquant à la fois de très grosses structures et de nombreuses petites structures
 - Les solutions adaptées pour une petite structure ne le sont pas forcément pour une plus grosse structure
 - Diversification également des domaines d'activité (PA, PH avec du soins et du social en mobilité => pas les mêmes besoins de MIE)
- Une stratégie impulsée par la puissance publique qui investit massivement depuis plusieurs années dans le fédérateur de fournisseurs d'identité Pro Santé Connect, qui permet de proposer des moyens d'identification électroniques simples et sécurisés aux professionnels enregistrés dans le répertoire RPPS.
 - Le portail RPPS+ permet l'enregistrement des professionnels du social et du médico-social (ayant un rôle dans la prise en charge et l'accompagnement des usagers et patients) non-inscrits au RPPS afin de les doter d'une identité numérique (n°RPPS) et d'un Moyen d'Identification Electronique (MIE) associé.

Une stratégie de déploiement de MIE basée exclusivement sur la délivrance de e-CPS pour se connecter aux services numériques en santé via Pro Santé Connect...

e-CPS

- l'enregistrement de l'ensemble des professionnels du social et du médico-social au RPPS permet de les doter d'une identité numérique sectorielle (esanté) et du Moyen d'Identification Electronique (MIE) associé : la e-CPS...
 - ✓ qui leur permet d'accéder, de manière sécurisée, aux services numériques en santé (connexion au DUI, à MSSanté, au DMP...)
 - ✓ et d'être conformes à la cible fixée par le référentiel d'Identification Electronique (RIE)

des freins à l'utilisation exclusive d'un smartphone en tant que moyen d'identification électronique pour les professionnels du secteur

Même si l'utilisation de la e-CPS est relativement simple → démo



Des freins existent quand même pour le secteur MS

- Des contraintes budgétaires pour financer l'équipement en smartphone de tous les professionnels
- Des contraintes pour l'utilisation du smartphone personnel du professionnel

Une démarche d'extension des MIE compatibles Pro Santé Connect

- la carte CPS et sa version dématérialisée (application mobile e-CPS) peuvent être utilisées pour se connecter aux services numériques en santé via Pro Santé Connect
 - Mais tous les professionnels du secteur médico-social ne sont pas éligibles à la délivrance d'une carte CPS
 - et les freins identifiés réinterrogent la stratégie basée exclusivement sur la e-CPS.
- L'ajout d'un autre dispositif sécurisé compatible Pro Santé Connect : la clé de sécurité FIDO2 (modèles certifiés par l'ANSSI).



Temps de questions/réponses



Focus sur les solutions FIDO2 (Fast IDentity Online)

FIDO Alliance est un consortium qui vise à harmoniser la gestion de l'authentification forte sur Internet.

FIDO2 est le standard le plus récent parmi d'autres publiés (UAF, U2F) par la FIDO Alliance.

FIDO2 permet aux utilisateurs de s'authentifier facilement aux services en ligne dans les environnements mobiles et de bureau. Le principe de cette technologie est de protéger de façon matérielle un secret qui sera utilisé pour s'authentifier à différents services. Cette protection peut prendre deux formes : un module intégré à l'appareil utilisé, ou un composant externe.

Identificateurs intégrés

Appui grandissant

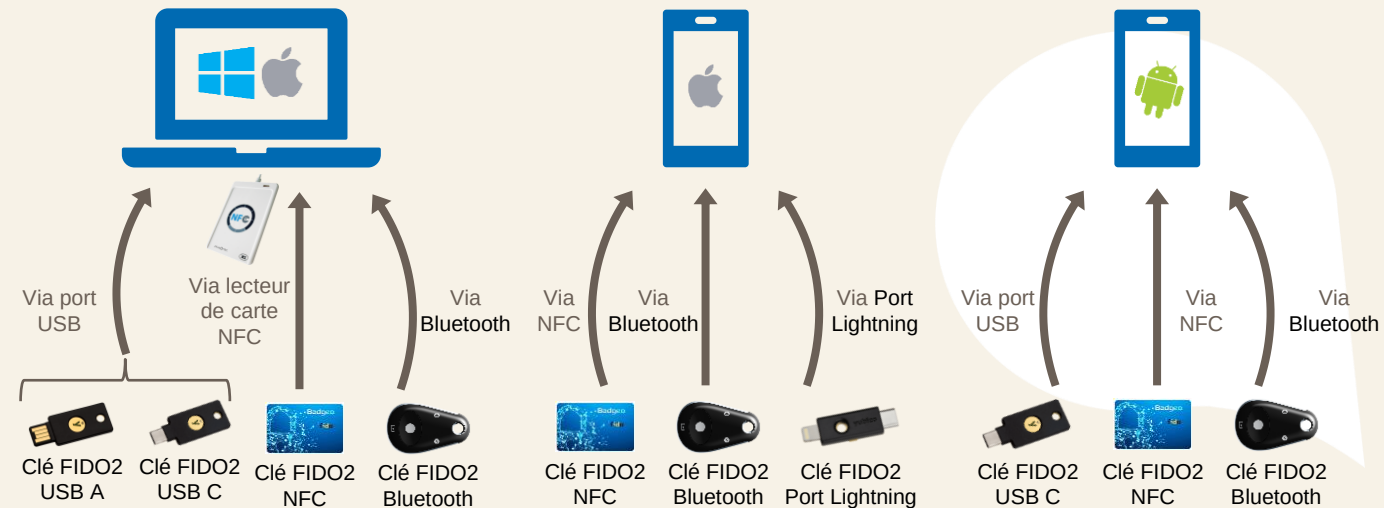
- Windows 10/11 (Windows Hello)
- Android (7.0 ou supérieur)
- IOS/macOS (14 ou supérieur)



Identificateurs externes

Généralement 2 à 3 interfaces (filaire/sans fil)

- USB (A ou C)
- NFC
- Bluetooth
- Port Lightning



LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ

Utilisation d'une clé FIDO2 pour s'authentifier sur Pro Santé Connect



Connectez-vous

Utilisez un de vos moyens d'authentification PSC ou un moyen déjà enrôlé

e-CPS CPS

Clé de sécurité



Nouveau moyen d'authentification

Sélectionnez le moyen d'authentification que vous souhaitez enrôler

Clé de sécurité

Carte sans contact

Certificat électronique

Etc.

Utilisation d'une clé FIDO2 pour s'authentifier sur Pro Santé Connect

**PRO SANTÉ CONNECT**
Un service du ministère chargé de la Santé

Nouveau moyen d'authentification

Pour lier votre clé de sécurité à votre compte Pro Santé Connect, veuillez l'introduire dans votre ordinateur et « appuyer sur suivant »

Suivant

[En savoir plus sur la gestion de vos données et vos droits](#)

**PRO SANTÉ CONNECT**
Un service du ministère chargé de la Santé

Nouveau moyen d'authentification

Cinématique propre au MIE choisi

Suivant

[En savoir plus sur la gestion de vos données et vos droits](#)

Utilisation d'une clé FIDO2 pour s'authentifier sur Pro Santé Connect

 **PRO SANTÉ CONNECT**
Un service du ministère chargé de la Santé

Nouveau moyen d'authentification

Pour finaliser l'enrôlement de votre clé de sécurité, veuillez lire et accepter les CGU, et appuyer sur « Valider »

[Conditions générales d'utilisation](#)

☐ J'accepte les CGU

Valider

[En savoir plus sur la gestion de vos données et vos droits](#)

 **PRO SANTÉ CONNECT**
Un service du ministère chargé de la Santé

Validation



Renseignez votre numéro RPPS puis validez la demande d'enrôlement sur votre application e-CPS

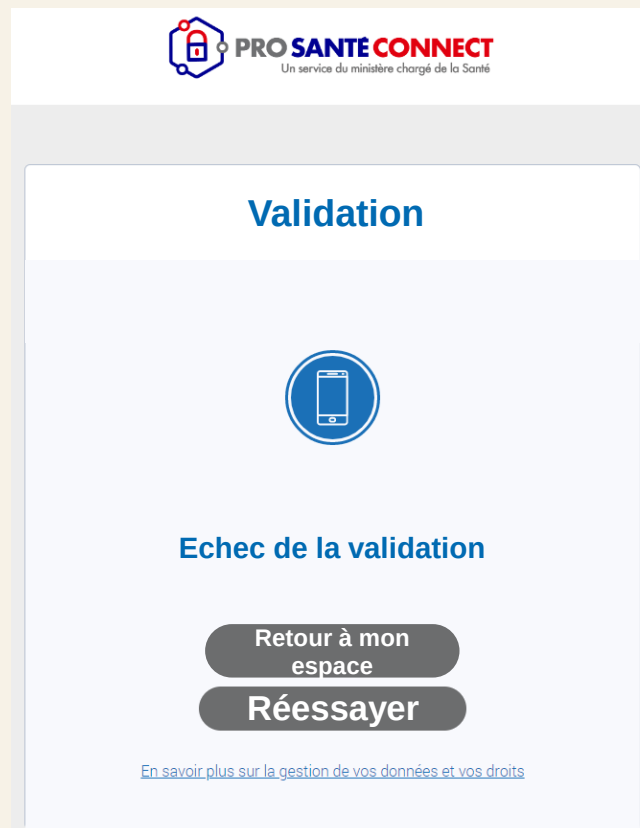
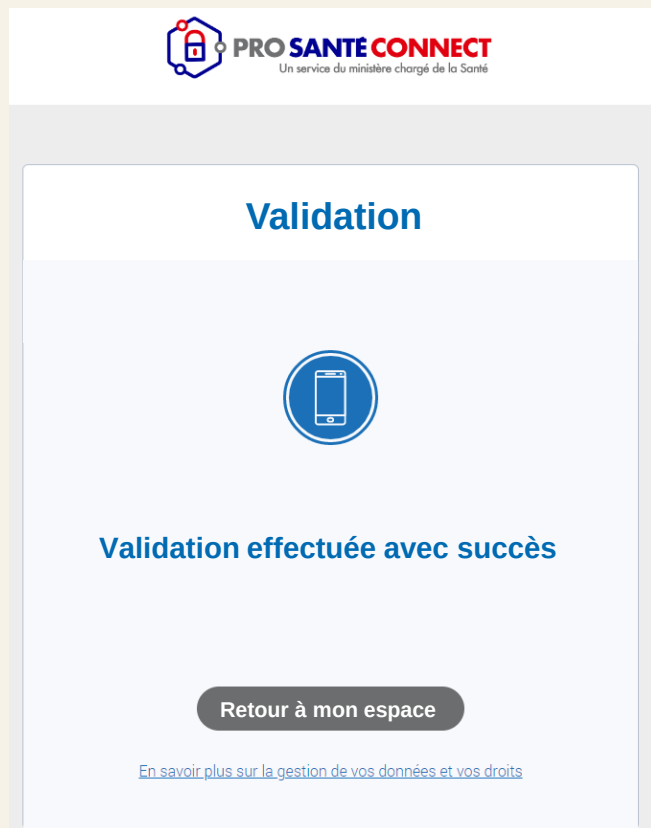
Votre identifiant RPPS 

☐ Mémoriser mon identifiant sur ce poste

Suivant

[En savoir plus sur la gestion de vos données et vos droits](#)

Utilisation d'une clé FIDO2 pour s'authentifier sur Pro Santé Connect



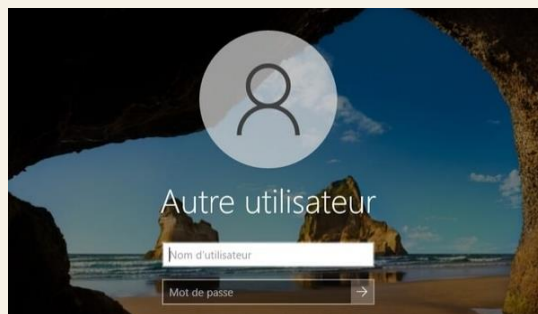
Mais également la possibilité de mettre en place une fédération d'identité entre un fournisseur d'identité local et Pro Santé Connect

- Pro Santé Connect va offrir la possibilité pour une structure de devenir un **fournisseur d'identité tiers** de la fédération Pro Santé Connect
- Et ainsi permettre aux structures de déléguer l'authentification de leurs utilisateurs à un fournisseur de service compatible avec PSC .
- Ceci permettant la navigation entre les services du système d'information local de la structure et l'ensemble des services numériques en santé déléguant l'authentification à Pro Santé Connect sans nécessiter une action de réauthentification par l'utilisateur et si possible avec une authentification unique de chaque professionnel dès l'ouverture de son poste de travail.

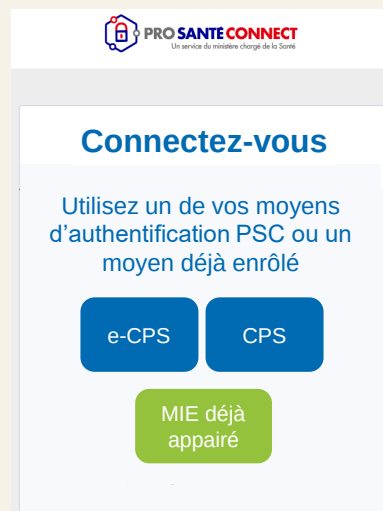
Cas d'usage authentification PSC

Un PS accède à son ordinateur et ouvre un service numérique. En l'absence d'un fournisseur d'identités (FI) fédérant ses identités avec PSC, il est redirigé vers PSC pour s'authentifier avec un MIE natif ou avec un MIE additionnel qu'il aura pu enrôlé par le passé. Il accède ensuite à son service numérique.

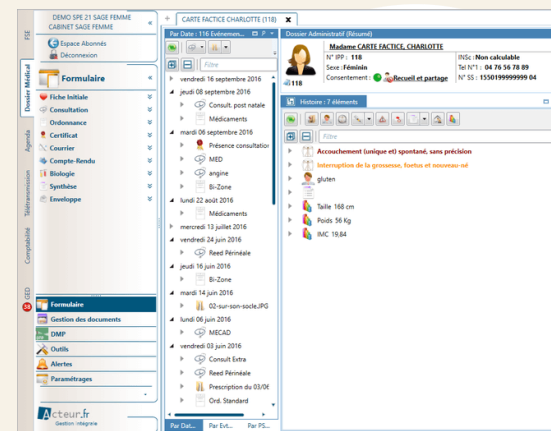
1. Ouverture de session



2. Ouverture du service numérique et authentification à PSC



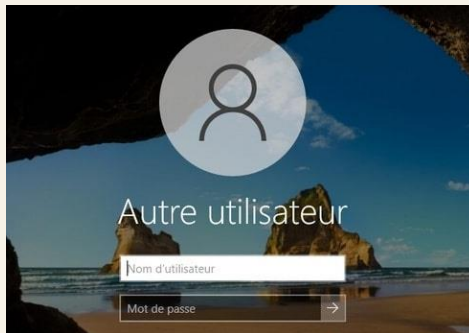
3. Accès au service numérique



Cas d'usage FI local dès l'ouverture de session avec fédération d'identité PSC

Si le PS travaille dans un établissement de santé utilisant un FI fédérant ses identités avec PSC et permettant aussi l'ouverture de session alors il bénéficiera d'une expérience sans couture dès l'ouverture de session **pour tous ses services numériques**, qu'ils soient internes à l'établissement ou raccordés à PSC. En cas d'accès à un service connecté à PSC, il pourra gérer sa session en cours grâce à une mire PSC (écran 2 ci-dessous).

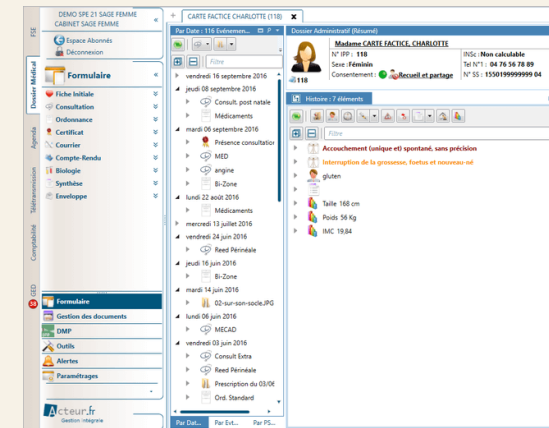
1. Ouverture de session Windows via Azure AD



2. Validation de la session par le PS (uniquement en cas de connexion à un service connecté à PSC*)



3. Accès transparent à tous les services numériques internes ou raccordés à PSC durant 4 heures

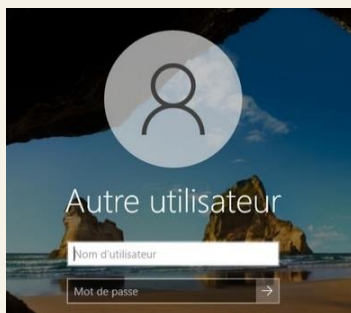


*Si après l'ouverture de session, le PS accède à un service numérique local à l'établissement (non raccordé à PSC), alors le processus est le même, avec l'écran de validation en moins (écran 2). L'accès à l'application est totalement transparent.

Cas d'usage FI local avec fédération d'identité PSC sans pris en charge de l'ouverture de session

Un professionnel de santé (PS) ouvre sa session poste de travail. Lors du premier accès à un service numérique interne à l'établissement ou raccordé à PSC, il sera redirigé vers son FI pour s'authentifier. Si le compte est déjà appairé, alors le PS a directement accès à son service numérique, **et à tous les services suivants de façon transparente durant 4 heures**. En cas d'accès à un service connecté à PSC, il pourra gérer sa session en cours grâce à une mire PSC (écran 3 ci-dessous).

1. Ouverture de session



2. Accès à un service numérique et redirection vers le FI local pour authentification

Fournisseur d'identités local

Choisir un mode de connexion

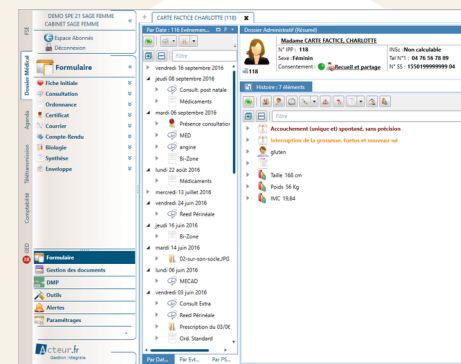
-  Utiliser Windows Hello ou une clé de sécurité
-  Utiliser mon mot de passe
-  Utiliser un certificat ou une carte à puce

Retour

3. Validation de la session par le PS (uniquement en cas de connexion à un service connecté à PSC)



4. Accès transparent à tous les services numériques internes ou raccordés à PSC durant 4 heures



Zoom sur l'appairage de compte

En cas de première utilisation d'un compte externe (ou de fin de validité de l'appairage précédent), le PS devra effectuer un appairage de ce compte avec son compte PSC. Cette étape nécessite une validation de l'identité du PS par e-CPS.

1. Vérification PSC

PRO SANTE CONNECT
Un service du ministère chargé de la Santé

Nouveau compte externe

Bonjour « médecin@chu.com », pour accéder à PSC avec votre compte @chu, merci de vérifier votre identité PSC

Appairer mon compte chu.com à mon compte PSC

Annuler et utiliser mon compte PSC

[En savoir plus sur la gestion de vos données et vos droits](#)

2. Numéro RPPS

PRO SANTE CONNECT
Un service du ministère chargé de la Santé

Validation

Renseignez votre numéro RPPS puis validez la demande d'enrôlement sur votre application e-CPS

Votre identifiant RPPS

☐ Mémoriser mon identifiant sur ce poste

Suivant

[En savoir plus sur la gestion de vos données et vos droits](#)

3. Validation

PRO SANTE CONNECT
Un service du ministère chargé de la Santé

Validation

Merci de confirmer l'appairage de votre compte@chu à votre compte ProSantéConnect et d'accepter les CGU

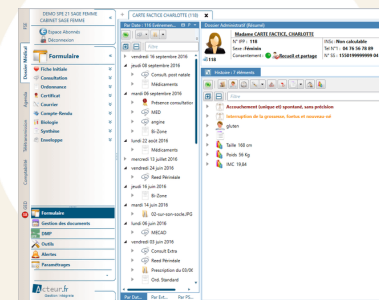
[Conditions générales d'utilisation](#)

☐ J'accepte les CGU

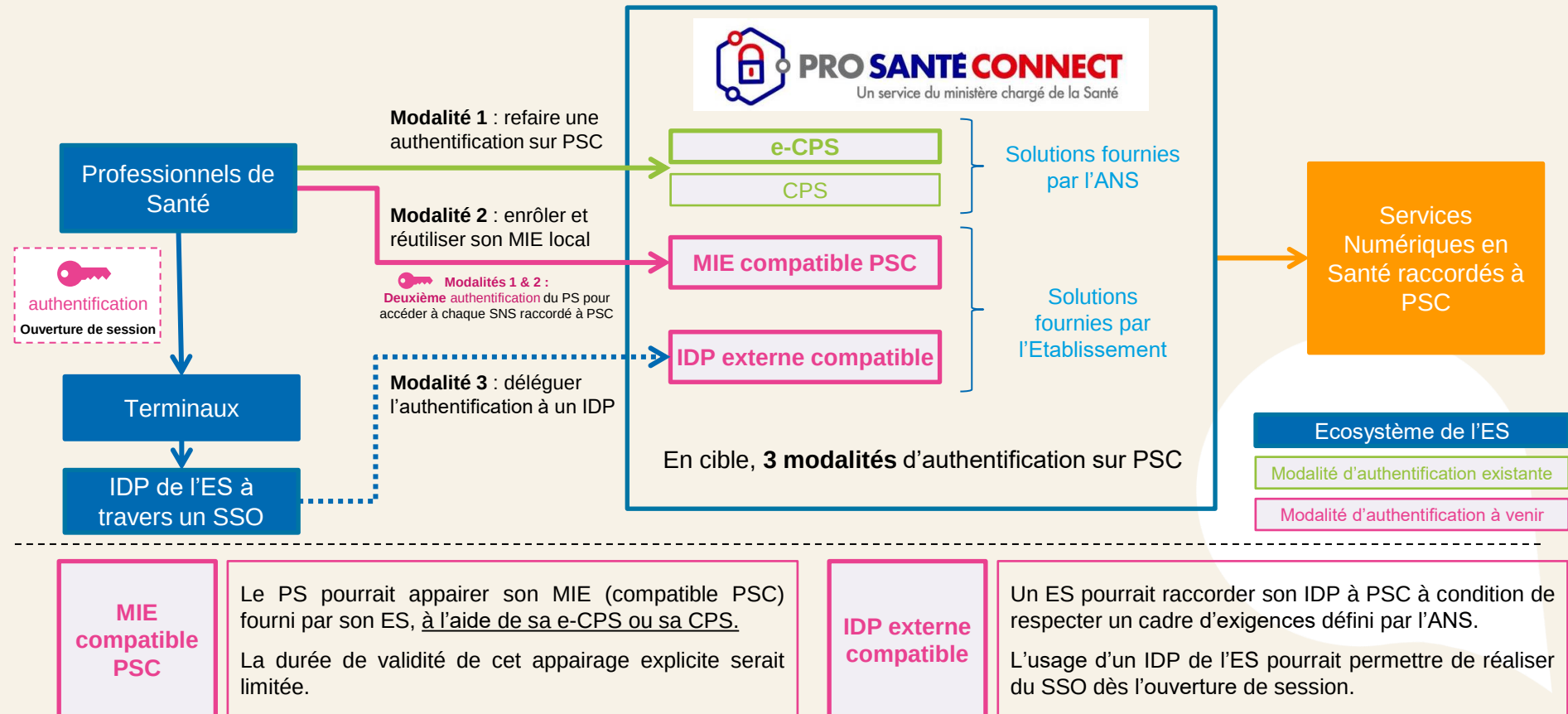
Valider l'appairage et accéder au service

Ne pas associer et accéder au service

4. Accès au service numérique



Synthèse des évolutions de PSC pour une ergonomie adaptée aux usages





Temps de questions/réponses



Le programme « HospiConnect » pour accélérer et accompagner l'écosystème dans les travaux de sécurisation et de simplification de l'identification électronique des professionnels.

- le programme « HospiConnect » est en cours de lancement, par l'intermédiaire d'appels à projets (AAP) à destination des établissements de santé et de certains établissements médico-sociaux.
- Ce programme porte sur **l'accompagnement technique et financier** des établissements pour déployer auprès des professionnels qui y exercent les MIE les mieux adaptés.
- Plusieurs Appel à Projets sont prévus dès 2024, avec des financements dédiés à destination des structures candidates :
 - Pour un nombre restreint d'établissements, afin de réaliser des pilotes en 2024 sur différents types de solutions avec leurs partenaires technologiques et de partager un retour d'expérience au sein de l'écosystème.
 - Pour une généralisation des meilleures solutions identifiées au cours des pilotes au sein de l'ensemble des établissements (2025).

Le programme « HospiConnect » pour accélérer et accompagner l'écosystème dans les travaux de sécurisation et de simplification de l'identification électronique des professionnels.

Il vise à accompagner les établissements dans le choix et le déploiement de solutions permettant :

- ✓ L'utilisation par les professionnels de MIE conformes au référentiel d'identification électronique : MIE proposés par Pro Santé Connect (carte CPS, e-CPS, autres MIE en cours d'homologation comme des clés de sécurité FIDO), autres MIE éventuellement homologués par la structure conformément au niveau de garantie substantiel eIDAS.
- ✓ L'enregistrement au RPPS des professionnels exerçant dans l'établissement, y compris les professionnels non obligatoirement enregistrés par les Ordres, qui doivent donc être enregistrés par leur employeur. Une procédure d'enregistrement conforme au niveau de garantie eIDAS substantiel est privilégiée, par exemple avec l'utilisation de France Connect + par les professionnels lors de leur inscription ;
- ✓ L'accès simplifié des professionnels aux applications du système d'information à l'aide de solutions d'Identity & Access Management (IAM) ou de Single Sign On (SSO), évitant les multiples réauthentifications ;
- ✓ La possibilité pour un établissement de devenir un fournisseur d'identité tiers de la fédération Pro Santé Connect.

Le programme « HospiConnect » pour accélérer et accompagner l'écosystème dans les travaux de sécurisation et de simplification de l'identification électronique des professionnels.



Le projet proposé devrait répondre *a minima* aux **objectifs** suivants :

- **Authentification 2FA** pour l'accès au DPI/DUI et en consultation au DMP sur un sous-ensemble de services/unités de soins
- **Enregistrement** de l'ensemble des professionnels **dans un répertoire d'identité local** avec :
 - une vérification d'identité conforme au niveau substantiel eIDAS (contrôle en face à face d'une pièce d'identité ou utilisation d'un MIE conforme lors d'une procédure à distance (ex: France Connect +)
 - une procédure en vigueur de contrôle et de mise à jour des habilitations (profession, catégorie professionnelle, diplôme ...) et de gestion des début/fin d'activités au sein de l'établissement.
- **Enregistrement au RPPS** de tous les professionnels
 - Susceptibles d'accéder à des services numériques sensibles externes au SI de l'établissement, dont le DMP
 - Se connectant au DPI/DUI de l'établissement
 - Susceptibles d'utiliser des MIE compatibles avec Pro Santé Connect
 - Cartes CPS, e-CPS, autres MIE de type clé FIDO autorisés en authentification directe par Pro Santé Connect,
 - MIE de niveau substantiel eIDAS ou prévus pour faire l'objet d'une procédure d'auto-homologation par l'établissement, en vue de leur utilisation au sein d'une structure visant à devenir un fournisseur d'identité tiers dans l'espace de confiance de Pro Santé Connect).
- L'authentification 2FA doit être réalisée au moyen d'un ou plusieurs moyens d'identification électronique 2FA, **conformes au référentiel d'identification électronique de la PGSSI-S** (MIE conforme à la cible, ou MIE de transition valable jusqu'au 01/01/2026). Il n'y a pas d'obligation cependant à l'utilisation du même type de MIE par l'ensemble des professionnels d'une même structure.
- L'authentification 2FA au DMP peut être réalisée via ProSantéConnect ou AIR Simplifié.

Le programme « HospiConnect » pour accélérer et accompagner l'écosystème dans les travaux de sécurisation et de simplification de l'identification électronique des professionnels.



En complément, le projet proposé pourrait également couvrir les objectifs suivants :

- Authentification 2FA sur un composant IAM/webSSO d'authentification interne à la structure et délégation de l'authentification *a minima* du DPI/DUI à ce composant interne d'authentification via un connecteur OIDC.
- mettre en place et déployer la fédération d'identités entre le composant d'authentification interne à la structure et ProSantéConnect .



LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ

Atelier – Pistes de réflexion

- **Situations spécifiques rencontrées chez vos clients ESMS ?**
 - Certains ont-ils déjà d'autres types de MIE ?
- **Difficultés rencontrées ?**
- **Pour l'AAP MIE : quels prérequis et critères retenir pour les ESMS ?**