AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Appel à projets national

Sécurisation et simplification de l'identification électronique des professionnels dans les établissements sanitaires et médico-sociaux



Cahier des charges

Réponse possible jusqu'au 05/04/2024 (14h00 - heure de Paris).

Statut : Validé | Classification : Publique | Version v1.0

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Table des matières

1. Enjeux et contexte 3
2. Conditions d'éligibilité de l'appel à projets 6
   - 2.1. Thématique et objectifs du projet 6
   - 2.2. Profil et engagement du candidat 11
   - 2.3. Début et durée du projet 11
   - 2.4. Respect des modalités de candidature 12
3. Critères de sélection des projets 13
   - 3.1. Caractéristiques des projets selon la cible 13
   - 3.2. Précisions sur les MIE utilisés 14
   - 3.3. Précisions sur le SSO visé 17
4. Organisation de la procédure de l'appel à projets 19
   - 4.1. Dossier de candidature 19
   - 4.2. Instruction des candidatures 19
   - 4.3. Conventionnement 20
   - 4.4. Suivi et livrables des lauréats 20
5. Règles de financement 22
   - 5.1. Cadre juridique applicable 22
   - 5.2. Montant du financement 22
   - 5.3. Modalités de versement du financement 23
6. Confidentialité et communication 24
7. Glossaire 25
8. Annexes 28
   - 8.1. Annexe 1 : Dérivation des identités 28

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

1. Enjeux et contexte

Lors de leurs accès à des services numériques en santé, les professionnels doivent s'authentifier afin de prouver leur identité. Cette action nécessite l'utilisation de moyens d'identification électronique (MIE) tels que les couples identifiant / mot de passe ou les cartes à puce par exemple.
Le référentiel d'identification électronique de la PGSSI-S, rendu opposable par arrêté du 28 mars 2022, présente notamment les exigences applicables aux MIE, en cible à partir du 01/01/2026, ou pendant la période de transition jusqu'à cette date[1].
La diversité des contextes d'exercice des professionnels, notamment dans les structures des secteurs sanitaire et médico-social, ainsi que la multiplicité des services numériques utilisés, génèrent des procédures d'authentification perçues comme contraignantes, répétitives et peu ergonomiques par les professionnels. Ils sont en effet amenés à s'authentifier à de nombreuses reprises au cours de leurs vacations, qui plus est de façon peu sécurisée, pour accéder à des applications différentes, voire pour accéder de manière récurrente à la même application.

Le programme CaRE « Cybersécurité accélération et Résilience des Établissements » décline un plan d'action concret et ambitieux pour la période de 2023 à 2027. Le programme, doté de plus de 230M€ sur 2023-2024, se décline en 4 axes et 20 objectifs :

1. Gouvernance et résilience
2. Ressources et mutualisation
3. Sensibilisation
4. Sécurité opérationnelle

Publique

Au sein de l'axe 4 « Sécurité opérationnelle », l'objectif de limiter les risques d'usurpation de l'identité numérique des professionnels pour l'accès aux services sensibles[2] se traduit par la mise en place d'HospiConnect pour accélérer l'adoption par les établissements de solutions conformes au référentiel d'identification électronique de la PGSSI-S, par l'intermédiaire d'appels à projets, dotés de financements dédiés à l'atteinte des cibles mentionnées : utilisation de MIE sécurisés (2FA, Pro Santé Connect ou eIDAS substantiel), de solutions d'Identity & Access management (IAM) et de Single Sign On (SSO).

Cette démarche s'inscrit dans la feuille de route du numérique en santé 2023-2027 :

[1] Plus d'explications au chapitre 3.2
[2] Les services « sensibles » sont les services numériques en santé au sens du L. 1470-1 du code de la santé publique, qui traitent des données de santé à caractère personnel au sens du RGPD, et répondant à certains critères. Plus de précisions au chapitre 4.1.2 du Référentiel d'identification électronique (PGSSI-S) personnes physiques : https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Axe 2 – Action 8-5 → En 2027, les professionnels des établissements sanitaires et médico-sociaux disposent de moyens d'authentification à deux facteurs pour se connecter à leurs applications sensibles.

Afin d'améliorer la prise en charge des patients, la feuille de route prévoit également l'accès effectif des professionnels au dossier médical de leurs patients dans Mon espace santé (DMP), qui nécessite de sécuriser leur identification électronique :
Axe 2 – Action 6-1 : → Plus de 50 % des médecins en activité consultent au moins une fois le contenu du profil Mon espace santé de leurs patients dans l'année d'ici fin 2026

L'accès à la consultation des documents du DMP est par ailleurs une des priorités de la vague 2 du programme Ségur numérique.

Dans le cadre d'HospiConnect, il s'agit plus précisément de simplifier et sécuriser l'accès des professionnels aux services numériques sensibles du SI des établissements et aux services socles nationaux du numérique en santé (par exemple le DMP), sur la base :

- D'un identifiant sectoriel unique après enregistrement au RPPS (concerne tous les professionnels intervenant dans le système de santé depuis l'Arrêté du 23 septembre 2022),
- De l'utilisation de moyens d'identification électronique (MIE) à double-facteur d'authentification (2FA), en particulier les dispositifs proposés par la fédération Pro Santé Connect (cible niveau eIDAS substantiel),
- De la mise en œuvre de solutions d'Identity & Access management (IAM) pour améliorer la gestion des habilitations et de briques de Single Sign On (SSO) pour simplifier l'authentification des professionnels.

Publique

Compte tenu du caractère innovant des organisations et des solutions à mettre en œuvre dans les structures pour l'atteinte de cet objectif, une démarche itérative est proposée pour les expérimenter progressivement sur le terrain :

- Phase 1 - ALPHA : AAP d'expérimentation destiné à un nombre limité de structures (15) [3];
- Phase 2 - BETA : AAP destiné à un nombre étendu de structures ;
- Phase 3 - GÉNÉRALISATION : dispositif destiné à toutes les structures.

Ce premier appel à projets « alpha » d'HospiConnect vise ainsi à soutenir l'expérimentation de solutions permettant de fluidifier l'expérience utilisateur et d'élever le niveau de sécurité des accès aux données de santé au sein des structures. Il s'agit également pour l'ANS de tester,

[3] Les coûts financés dans ce premier appel à projets ne pourront pas être financés dans le cadre des dispositifs suivants.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

avec les candidats proposant un projet s'appuyant sur les MIE délivrés par l'ANS, les organisations et processus cibles nécessaires à l'atteinte du niveau de garantie eIDAS substantiel de Pro Santé Connect.

Cet appel à projets repose notamment sur l'arrêté du 11 mai 2020 *modifiant l'arrêté du 9 décembre 2009 fixant les modalités d'attribution par l'ASIP Santé de financements visant à favoriser le développement des systèmes d'information partagés de santé*, pris sur le fondement et pour l'application du troisième alinéa de l'article L. 1111-24 du code de la santé publique.

Les conditions et les modalités de sa mise en œuvre, approuvées par délibération du conseil d'administration de l'ANS du 7 mars 2024, sont définies dans le présent cahier des charges.

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

2. Conditions d'éligibilité de l'appel à projets

Est éligible à l'appel à projets, tout projet qui respecte les conditions cumulatives suivantes.

2.1. Thématique et objectifs du projet

Thématique du projet

Le projet doit porter sur l'expérimentation de solutions permettant de fluidifier l'expérience utilisateur et d'élever le niveau de sécurité des accès aux données de santé au sein des structures.
Le projet est ouvert aux établissements de santé publics, privés d'intérêt collectif et privés mentionnés à l'article L6111-1 du code de la santé publique et aux établissements ou services médico-sociaux (ESMS) cités au L.312-1 du CASF quelle que soit leur taille, leur statut juridique et leur type d'activité, sous réserve qu'ils disposent d'une organisation (DSI, DSN …) à même de piloter la mise en œuvre du projet au sein de l'établissement.

Objectifs du projet

Le projet doit avoir pour objectifs :

- **De co-construire et/ou adapter les organisations existantes**, relatives à la création et à la mise à jour des identités électroniques des professionnels concernés par le périmètre du projet ainsi qu'à la délivrance des moyens d'identification électroniques afférents,
- **De co-construire et/ou d'adapter les solutions expérimentées**, en impliquant les futurs utilisateurs et en tenant compte de leurs remontées terrains,
- **De tester en conditions réelles** les solutions,
- **D'évaluer les solutions**, en particulier leurs capacités à répondre au besoin et/ou à la problématique ciblé, les freins et leviers à leur déploiement et à leur généralisation dans d'autres structures,
- **De partager en toute transparence** les travaux réalisés, les résultats obtenus et les difficultés rencontrées.

Publique

Les objectifs à atteindre dans le cadre de cet appel à projets sont présentés selon trois niveaux de cibles. Le projet proposé par le candidat doit répondre *a minima* aux objectifs de la cible 1, qui sécurise l'accès des professionnels aux services numériques en santé. La cible 2 vise à apporter un complément de sécurisation et de simplification des usages par l'utilisation de briques de gestion des identités et des accès (IAM) permettant une authentification unique à plusieurs services (SSO) au sein de la structure. La cible 3 vise à améliorer encore l'expérience utilisateur, par la recherche de systèmes d'authentification unique sur différents postes de travail et pour l'accès à des services numériques externes à la structure.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Cible 1 : **L'objectif du projet est de mettre en place et déployer une authentification 2FA pour l'accès au DPI/DUI et en consultation au DMP** (en mode Web contextuel ou via API LPS, via Pro Santé Connect ou en AIR Simplifié[4]) **sur un sous-ensemble de services/unités de soins d'une structure.** Le projet porte donc sur un sous-ensemble de la population de professionnels de l'établissement, représentatif des utilisateurs de services numériques sensibles (n'impliquant pas exclusivement des professions réglementées relevant d'un enregistrement au RPPS par les Ordres nationaux, mais également des professionnels dont l'autorité d'enregistrement au RPPS est constituée par l'établissement employeur, qui devra contracter à cet effet avec l'ANS) : *a minima* 100 utilisateurs.

L'atteinte de cette cible nécessite :

- L'utilisation de moyens d'identification électronique 2FA, conformes au référentiel d'identification électronique de la PGSSI-S[5] (MIE conforme à la cible, ou MIE de transition valable jusqu'au 01/01/2026). Il n'y pas d'obligation cependant à l'utilisation du même type de MIE par l'ensemble des professionnels concernés par le périmètre du projet.
- L'enregistrement de l'ensemble des professionnels concernés par le périmètre du projet dans un répertoire d'identités local selon un principe de dérivation de l'identité nationale (cf. 8.1) 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.
- L'enregistrement au RPPS de tous les professionnels concernés par le périmètre du projet dont l'autorité d'enregistrement au RPPS est constituée par l'établissement employeur :
    - Susceptibles d'accéder au DMP et plus généralement à terme à des services numériques sensibles externes au SI de l'établissement,
    - Susceptibles d'utiliser des MIE compatibles avec Pro Santé Connect,

[4] L'utilisation du mode Air Simplifié depuis le DPI permet aux PS d'atteindre le DMP sans réauthentification et sans avoir nécessairement besoin d'utiliser un MIE supporté par PSC (sous réserve d'homologation de l'établissement de santé hôte du secteur sanitaire). Cette méthode permet d'ailleurs aussi une connexion en mode asynchrone d'un professionnel pour effectuer des pré-chargements automatiques temporaires de documents du DMP dans son logiciel. Ce mode d'authentification est un bon moyen de transition en attendant que les établissements aient la possibilité de devenir fournisseurs d'identités tiers de PSC et que les services numériques implémentent les API PSC connectées en s'inscrivant dans l'espace de confiance PSC.

[5] Cf.3.2

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Publique

- Cartes CPS, e-CPS, autres MIE de type clé de sécurité 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.

- La définition des processus d'enrôlement et de remise du MIE (pour les MIE reçus par l'établissement et les MIE directement reçus par les utilisateurs).

La mise en œuvre de ce projet permet aux professionnels de s'authentifier aux services numériques en santé en respectant le référentiel d'identification électronique (RIE) de la PGSSI-S. Un MIE conforme à ce référentiel est requis, et une attention particulière sera portée à ses conditions d'utilisation sur le terrain[6] (l'utilisation d'un seul des deux facteurs mis à disposition par le MIE est par exemple proscrit).

Option auto-enregistrement : Afin de favoriser l'atteinte par Pro Sante Connect d'une cible de qualification au niveau eIDAS substantiel dans les prochaines années, il est fortement souhaité que l'enregistrement de nouveaux professionnels dans le RPPS (hors professions de santé relevant d'un enregistrement par un Ordre) fasse l'objet d'un pré-enregistrement individuel sur le portail eRPPS fourni par l'ANS. Un financement additionnel est prévu dans le cadre de l'appel à projets pour les établissements qui mettront en place un processus d'auto-enregistrement des nouveaux professionnels à inscrire au RPPS, par France Connect (déjà disponible) ou France Connect+ (lorsque celui-ci sera disponible au sein du portail), si 75% des nouveaux professionnels concernés par le périmètre du projet sont enregistrés selon cette modalité.

publique

Cible 2 : **Un projet correspondant à cette cible inclut les objectifs d'un projet « cible 1 » auxquels s'ajoutent des objectifs de sécurisation supplémentaires et de simplification de l'expérience utilisateur vis-à-vis du SI interne de la structure. L'objectif du projet est de mettre en place et déployer l'authentification 2FA sur un composant IAM/SSO d'authentification propre à la structure et de mettre en place et déployer une délégation de l'authentification *a minima* du DPI/DUI à ce composant interne d'authentification selon le flux Authorization Code Flow, via un connecteur OpenID Connect (OIDC).**

Remarques :

- L'exigence SC.SSI/IAM.80 du SONS vague 2 rendra obligatoire la présence d'un tel connecteur OIDC dans les logiciels référencés dans le couloir hôpital (notamment les DPI). Il sera néanmoins nécessaire de s'assurer que ce connecteur sera bien disponible auprès du

[6] Se référer à la partie 3.2

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

fournisseur de DPI, dès la phase d'évaluation de cet AAP (sans attendre le cas échéant le déploiement complet des solutions référencées dans le cadre de la vague 2 du Ségur numérique).

- La mise en œuvre d'une brique de SSO est rendue obligatoire par le RIE pour certaines structures :
    - [EXI 28] Afin de garantir un niveau de fiabilité à l'état de l'art des identités, au 01/01/2025 au plus tard, la mise en œuvre d'une brique de SSO (Single Sign-On) est requise pour les structures qui :
        - Soit sont responsables de plus de 5 services sensibles ;
        - Soit comptent plus de 5.000 professionnels ayant accès à au moins un service sensible.

Cette cible permet aux professionnels de santé de se connecter au minimum à leur DPI/DUI en utilisant leur identité provenant du référentiel d'identités local de l'établissement. Toute application interne à l'établissement compatible OIDC pourra aussi intégrer ce mécanisme de web SSO afin de permettre aux professionnels de l'établissement d'utiliser ces applications sans devoir se réauthentifier (pendant une durée maximale définie par l'établissement en regard des standards de sécurité en vigueur).
On peut noter que l'utilisation d'une brique de SSO locale, intégrée au SIH permet à l'établissement de rester autonome au sein du SIH, en cas d'indisponibilité ponctuelle du service Pro Santé Connect ou d'une coupure Internet (par exemple en cas de cyberattaque). La cible 3 ci-après permettra quant à elle de créer un pont entre les identités locales de l'établissement et l'espace de confiance de Pro Santé Connect.
L'utilisation d'un web SSO OIDC a été choisie pour sa compatibilité avec Pro Santé Connect (PSC), son efficacité pour le SSO et sa cohérence avec l'exigence SC.SSI/IAM.80 du Ségur vague 2. Le flux utilisé pour ce web SSO est l'Authorization Code Flow, dans lequel les clients lourds et les clients légers redirigeront l'utilisateur vers PSC par le biais d'un navigateur.

Publique

Des composants gérant l'authentification Windows® (en complément du credential provider Microsoft®) peuvent être utilisés s'ils permettent de propager cette authentification primaire vers l'outil de web SSO de l'établissement.

Cible 3 : **Un projet correspondant à cette cible inclut les objectifs des projets « cible 1 » et « cible 2 » auxquels s'ajoutent des objectifs d'ergonomie et de simplification de l'expérience utilisateur pour l'accès à des services numériques en santé externes à la structure. L'objectif du projet est**

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

de mettre en place et déployer la fédération d'identités entre le composant d'authentification interne à la structure et Pro Santé Connect[7].

Cette cible présente plusieurs avantages pour un établissement. Elle réunit l'écosystème de l'établissement et l'écosystème Pro Santé Connect au sein de la même brique de web SSO et permet d'éviter une authentification propre à PSC lors d'un accès à un service numérique PSC connecté. Il sera aussi possible de se connecter à PSC en utilisant des MIE propres à l'établissement sans passer nécessairement par des MIE PSC (comme les cartes CPx ou la e-CPS).

A terme, cette fédération impliquera pour un établissement que sa brique d'authentification interne respecte le référentiel Pro Santé Connect – niveau « Espace de confiance » et soit référencée auprès de l'ANS à cet effet. Ce référentiel, en cours de rédaction, définira l'ensemble des exigences applicables pour qu'une solution d'IAM puisse être reconnue dans l'espace de confiance de Pro Santé Connect. La solution utilisée devra donc être approuvée par l'ANS[8], puis, chaque établissement souhaitant l'utiliser pour fédérer ses identités locales avec PSC devra passer par une étape de contractualisation avec l'ANS. Cependant, dans le cadre des projets décrits au sein du présent appel à projets, les étapes de validation des solutions et de contractualisation des établissements seront simplifiées à titre d'expérimentation. Pour continuer à utiliser ce service une fois le présent appel à projets arrivé à son terme, la structure devra se mettre en conformité avec le dispositif de contractualisation en vigueur.
Si la solution de SSO choisie par l'établissement le permet, il est même possible de propager l'authentification primaire à la session du poste de travail à l'ensemble des applications qui seront ensuite utilisées par les professionnels de santé (à condition de respecter les exigences du RIE lors de cette première authentification).

publique

Chaque candidat peut proposer un projet en lien avec la cible de son choix étant entendu que chaque cible possède ses propres caractéristiques décrites dans la suite de ce document. Ces cibles étant cumulatives, un établissement souhaitant réaliser la cible 3, devra par exemple dans le même temps réaliser les cibles 1 et 2 au cours du projet.

[7] PSC offre la possibilité aux structures de faire référencer (sous certaines conditions) le composant local d'authentification (appelé communément IDP tiers ou IDP de la structure) afin que l'authentification réalisée par l'utilisateur sur le composant local vaille authentification sur PSC (après un processus initial d'appairage des deux identités).

[8] Le fournisseur de la solution d'IDP de la structure candidate doit faire une demande sur https://api.gouv.fr/les-api/api-pro-sante-connect

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

2.2. Profil et engagement du candidat

Profil du candidat

Le projet devra être porté par une structure appartenant aux établissements de santé publics, privés d'intérêt collectif et privés mentionnés à l'article L6111-1 du code de la santé publique ou aux établissements et services sociaux et médico-sociaux énumérés au I. de l'article L. 312-1 du code de l'action sociale et des familles.

La structure candidate s'appuiera sur sa propre organisation (DSI, DSN, …) pour la mise en œuvre du projet, sur un ou plusieurs fournisseurs de service numérique impliqués dans les cas d'usages envisagés (DPI, DUI, application IAM/SSO, …) ainsi qu'éventuellement sur des prestataires de services publics ou privés (expertise technique, pilotage de projet, conduite de changement, support).

Engagements du candidat

En candidatant à l'appel à projets, la structure s'engage :

- à mobiliser les équipes nécessaires au bon déroulement du projet. Elle s'engage notamment à mobiliser un chef de projet (mise en œuvre du projet, évaluation, puis partage d'expérience). Un responsable au sein de la direction en charge des systèmes d'information devra également être identifié comme partie prenante du projet (notamment si le chef de projet est externe à la structure) ainsi qu'un responsable au sein de la direction des ressources humaines. Elle s'engage également à mobiliser les professionnels utilisateurs de la solution ;
- à participer activement à l'évaluation (évaluation des impacts de la solution et des freins / leviers à son déploiement) en mettant tous les moyens en œuvre pour sa bonne réalisation ;
- à accepter sans réserve la publication large et transparente des résultats du projet au sein de l'écosystème du numérique en santé, par exemple sur le site de l'ANS (en particulier le rapport d'évaluation précisant les bénéfices de la solution et les freins/leviers à son déploiement).

Publique

2.3. Début et durée du projet

La durée du projet est de 7 mois (sauf exception argumentée) à compter de la signature de la convention prévue à l'article 4.3 du présent cahier des charges.

L'ANS se réserve le droit de proposer une prolongation du projet à un établissement par l'intermédiaire d'un avenant si besoin. De même, un établissement candidat est libre de postuler en demandant un délai supérieur aux délais ci-dessus, à condition de motiver cette demande. Le commencement effectif du projet sera déterminé par la date de signature de la convention par l'ensemble des parties prenantes.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

2.4. Respect des modalités de candidature

Le dossier de candidature doit être soumis conformément aux modalités décrites à l'article 4.1 du présent cahier des charges.

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

3. Critères de sélection des projets

3.1. Caractéristiques des projets selon la cible

Le nombre de places disponibles toutes cibles confondues pour les **candidats** décrits dans le présent appel à projets est limité à 15. L'ANS sélectionne, parmi le ou les projets éligibles, un ou plusieurs projets au regard des critères ci-dessous.

L'ANS sera sensible, durant sa sélection, à :

- Assurer une certaine représentativité et diversité des établissements choisis (secteur public / privé, secteur sanitaire / secteur médico-social, …),
- Favoriser les candidatures portant sur les cibles les plus élevées,
- Viser la plus grande diversité possible de MIE et de solutions testées.

Quelle que soit la cible visée, la réalisation de « l'option auto-enregistrement » n'est pas obligatoire mais sera un avantage pour une structure candidate.

Les caractéristiques du projet proposé par une structure candidate dépendent de la cible visée. Les caractéristiques ci-dessous sont cumulatives (une structure candidate qui propose un projet visant à atteindre les objectifs de la cible 2 devra satisfaire les caractéristiques de la cible 1 et de la cible 2).

Publique

Cible 1 :

- Conformité du/des MIE utilisé(s) vis-à-vis du RIE[9];
- Utilisation du MIE en 2FA pour se connecter au DUI/DPI et en consultation au DMP (via Pro Santé Connect ou AIR Simplifié);
- Utilisation d'un référentiel d'identités local (annuaire LDAP, AD/Entra ID par exemple) ;
- Utilisation d'une version du DPI/DUI référencée dans le cadre des programmes Ségur numérique ;
- Production (projet à minima) de « l'engagement sur la sécurisation des modalités d'identification électroniques » prévu par le RIE (le document final devra être produit à l'issue de l'AAP) ;
- La bonne gestion de l'enregistrement au RPPS de tous les professionnels concernés par la description de la cible 1 ci-dessus, ainsi que leur inscription au référentiel local d'identités de l'établissement ;

[9]Se référer à la partie 3.2

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- La représentativité des professionnels concernés par le projet ;
- Robustesse et maturité de la démarche :
  - Mobilisation des ressources humaines pertinentes (profils/expertises) et suffisantes (temps consacré au projet) ;
  - Capacité à assurer le pilotage du projet dans la durée et à produire les livrables attendus ;
  - Mobilisation des ressources techniques nécessaires (infrastructures SI, matériel, etc.) ;
  - Méthodologie projet adéquate.

Cible 2 :

- Utilisation d'une brique web SSO utilisant les identités du répertoire local pour se connecter au DUI/DPI selon le standard OpenID Connect. Autrement dit, le DUI/DPI doit pouvoir déléguer l'authentification du professionnel à la brique de web SSO de l'établissement grâce à un connecteur OIDC.

Cible 3 :

- La brique de SSO utilisée par l'établissement de santé est compatible avec une fédération d'identité avec PSC selon le standard OIDC (fournir le numéro datapass soumis à PSC pour attester de l'initialisation de la démarche de contractualisation).

Publique

3.2. Précisions sur les MIE utilisés

L'authentification 2FA mise en place dans le cadre du projet doit être réalisée au moyen d'un ou plusieurs MIE conforme(s) au référentiel d'identification électronique des personnes physiques ; à savoir :

- Les MIE proposés par Pro Santé Connect (PSC) : cartes de la famille CPx, e-CPS et prochainement des clés de sécurité FIDO dont la liste sera prochainement communiquée sur le site de l'ANS (la clé de sécurité FIDO compatible devra être activée par l'utilisateur avec sa e-CPS) ;
- MIE certifié de niveau eIDAS Substantiel ;
- MIE destiné à une auto-homologation par la structure (au sens du RIE, même si le MIE peut être utilisé à titre de MIE de transition en amont de la procédure d'homologation jusqu'au 01/01/2026).
  - A noter : la structure pourrait ultérieurement intégrer l'espace de confiance PSC en tant que fournisseur d'identités tiers avec ce type de MIE, sous réserve de mener à terme la procédure d'homologation avec ce type de MIE.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Utiliser un MIE offrant deux facteurs d'authentification ne garantit pas que l'authentification résultante soit du même niveau. Par exemple, un établissement de santé distribuant des cartes à puce avec code PIN à ses PS distribue effectivement des MIE 2FA. Cependant, si les PS s'authentifient aux services numériques en n'utilisant qu'un seul des facteurs de la carte, alors l'authentification résultante n'est pas conforme au RIE.

Afin d'être éligible, quelle que soit la cible visée, la structure doit proposer une utilisation du/des MIE choisi(s) conforme au RIE. Il convient donc de préciser les modalités d'usage envisagées des MIE choisis dans le cadre de cet appel à projets. La liste ci-dessous n'a pas vocation à être exhaustive. Elle vise à préciser les attendus de l'ANS en matière d'authentification.

A noter que, conformément au référentiel d'identification électronique de la PGSSI-S Personnes Physiques, un fournisseur de service peut autoriser une authentification par un seul des deux facteurs du moyen d'identification électronique homologué, à condition qu'une authentification à deux facteurs ait déjà eu lieu avec le MIE en question sur une période définie par l'établissement, acceptable en regard des standards de sécurité (par exemple pendant 4 heures). Pour plus de précisions, se référer au référentiel d'identification électronique de la PGSSI-S Personnes Physiques, exigence n°14.

Utilisation d'une carte à puce

Publique

Il existe différentes façons d'utiliser une carte à puce (incluant l'utilisation des cartes CPx).
Dans le cas d'une utilisation standard avec insertion de la carte dans un lecteur (avec lecture du certificat) et utilisation du code PIN, l'authentification est bien une authentification forte à deux facteurs (possession + connaissance).

En cas d'utilisation de la partie sans contact de la carte (passage de la carte sur un lecteur sans insertion), celle-ci peut selon les cas représenter un facteur d'authentification ou une simple identification n'ayant pas de valeur de sécurité. Pour que l'utilisation de la partie sans contact de la carte soit comptabilisée comme un facteur d'authentification, un échange cryptographique entre le lecteur et la carte doit avoir lieu. La simple lecture d'un identifiant ou du numéro de série de la carte ne sert pas de facteur d'authentification (car trop simple à reproduire).

Exemples de cas d'usage :

Cas d'usage carte à puce	Validité vis-à-vis du RIE
Insertion de la carte dans un lecteur avec lecture du certificat + code PIN	Valide

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Lecture sans contact de la carte avec échange cryptographique + code PIN	Valide
Lecture sans contact de la carte avec échange cryptographique + mot de passe de session utilisateur	Valide
Lecture sans contact de la carte avec lecture d'un numéro d'identification + mot de passe/code PIN	Invalide

Utilisation de cartes sans contact en DESFIRE

L'utilisation de la technologie DESFIRE est une possibilité pour utiliser une carte à puce en mode sans contact à condition d'activer les mécanismes cryptographiques associés. Ces échanges cryptographiques comptent comme un facteur d'authentification, et doivent être couplés avec un autre facteur (code PIN, biométrie, etc.).

Il est ~~recommandé d'éviter~~interdit ~~l~~d'utilis~~ation~~ er ~~d'~~une clé de chiffrement symétrique unique commune à tous~~entre~~ les badges et les terminaux (car trop peu sécurisée). Il est donc obligatoire ~~et d~~e ~~privilégier l'~~utilis~~eration d'~~une clé unique au sein de chaque badge, qui peut être diversifiée ~~elle-même dérivée~~ d'une clé maitresse commune et sécurisée[10]. De plus, il est imposé d'utiliser une solution de type Key Management System (KMS) propre à l'établissement qui contient l'ensemble des clés symétriques et/ou la clé maîtresse à partir de laquelle le KMS diversifie une clé fille propre à chaque carte et qui est encodée dans la puce DESFIRE de la carte lors de son enrôlement dans le système. Il s'agit ici d'une application DESFire locale et propre à l'établissement non fournie par l'ANS.

Publique

En plus de la gestion des clés cryptographiques et des cartes physiques, il convient de définir des processus d'encodage/enrôlement des cartes. Ces trois dimensions peuvent être définies et contractualisées entre l'établissement utilisateur et l'éditeur/intégrateur offrant le service.

Remarque : *a priori* cette solution ne s'adresse qu'à des configurations s'appuyant sur des solutions d'IAM/SSO.

a mis en forme : Soulignement

Utilisation d'une clé de sécurité FIDO2

L'utilisation d'une clé de sécurité FIDO2 est conforme au RIE si certaines conditions sont respectées. La clé de sécurité utilisée doit proposer un facteur supplémentaire au facteur de possession de la clé (et ce facteur ne doit pas être désactivé par l'utilisateur). Par exemple, un code PIN associé à la clé ou l'utilisation de la biométrie sont des facteurs supplémentaires acceptables. Le simple fait de toucher la

[10] Voir guide de l'ANSSI : https://cyber.gouv.fr/sites/default/files/document/anssi-guide-recommandations_securisation_systemes_controle_acces_physique_et_videoprotection-v2.0.pdf

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

clé n'est pas considéré comme un second facteur d'authentification. L'ANS publiera prochainement une liste de modèles de clé de sécurité FIDO acceptés par Pro Santé Connect.

Cas d'usage clé FIDO2	Validité vis-à-vis du RIE
Insertion de la clé + code PIN	Valide
Insertion de la clé + biométrie	Valide
Insertion de la clé	Invalide
Insertion de la clé + contact de la clé pour prouver une présence humaine	Invalide

Attentes particulières vis-à-vis des candidats choisissant le MIE CPS et qui bénéficieront des premières CPS v4 en cours de projet

Les candidats proposant un projet impliquant le MIE CPS pourront bénéficier de cartes CPS v4 à partir de septembre 2024. Le projet devra mettre en exergue les éventuels impacts de la migration vers cette nouvelle version de la carte.

De manière générale, le projet devra couvrir les aspects suivants :

- Usage et fonctionnement avec des lecteurs contacts / sans contacts (puce DESFire) ;
- Authentification forte et identification rapide (utilisation pour une durée limitée de la partie sans contact en tant que MIE 1FA pour du contrôle d'accès logique après enregistrement ou enrôlement 2FA à l'aide de la partie contact) ;
- Usages de moyens tiers d'authentification en cas d'oubli, de perte ou de non-disponibilité de la carte CPS (mise à disposition de clés de sécurité FIDO par exemple) ;
- La définition des process d'enrôlement et de remise du MIE (pour les MIE reçus par l'établissement et les MIE reçus par les utilisateurs).

Publique

Attentes particulières vis-à-vis de la gestion de l'identification électroniques des professionnels en mode dégradé

- Coupure réseau / internet ;
- Oubli/perte du MIE physique.

3.3. Précisions sur le SSO visé

Il existe différents types de SSO utilisables au sein d'une organisation, notamment le eSSO (enterprise SSO) et le web SSO. Ces deux manières de faire sont différentes et ont chacune leurs avantages et leurs inconvénients. Cependant, l'utilisation d'un web SSO suivant un standard comme OpenID Connect

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

est attendu pour les cibles 2 et 3 de cet appel à projets pour plusieurs raisons (adaptabilité, interopérabilité, maturité et sécurité du standard OIDC, etc.). La délégation de l'authentification d'un service numérique vers un fournisseur d'identités (PSC ou fournisseur d'identité interne à la structure) devra donc suivre le standard OpenID Connect et le flux Authorization Code Flow. Le eSSO reste utilisable en cible 1, en suivant quelques conditions. Ci-dessous sont explicités les différents types de SSO ainsi que leurs avantages et inconvénients.

L'enterprise SSO

Le eSSO se traduit par l'installation d'un agent sur le poste de travail utilisé. Cet agent détecte les formulaires de login/mot de passe présentés par les applications au moment de l'authentification des utilisateurs et remplit automatiquement les champs pour l'utilisateur.



1. Ouverture de session « primaire »
2. Agent eSSO chargé
3. Détection formulaire de login et saisie automatique d'un mot de passe « secondaire »

Publique

Le eSSO a l'avantage d'être utilisable sur tout type d'applications présentant une mire d'authentification (en particulier les clients lourds) et est non-intrusif pour les applications (ne demande pas de développements supplémentaires). Cependant le eSSO présente de nombreux désavantages : l'authentification à l'application repose sur l'utilisation d'un login et d'un mot de passe et n'est donc pas une authentification forte (incompatible avec le présent appel à projets), le moteur de eSSO doit être configuré individuellement pour reconnaître la mire de chaque application et est très impacté par une modification de l'interface de ces dernières, la charge de maintenance de ce moteur est élevé pour l'adapter à tout changement au sein des applications, etc.

Dans le cadre de cet appel à projets, l'utilisation d'un moteur de eSSO pour l'authentification aux services numériques concernés ne sera accepté que pour la cible 1, en respectant certaines conditions :

- L'authentification primaire au moteur de eSSO doit se faire à l'aide d'un MIE 2FA respectant le RIE (authentification multifacteur) ;
- La structure candidate doit détailler dans son dossier de candidature le fonctionnement de ce moteur de eSSO et les potentielles mesures de sécurité mises en place (complexité et longueur des mots de passe, potentielle rotation périodique des mots de passe, etc.).

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Le web SSO

Le web SSO utilisant OpenID Connect (OIDC) suit un standard international qui est notamment utilisé par Pro Santé Connect. Il fonctionne aussi bien sur les postes maitrisés que les postes personnels (pas d'agent à installer), il permet l'utilisation de MIE modernes et sécurisés pour réaliser des authentifications fortes aux applications, il suit le protocole OIDC et permet une authentification unique entre toutes les applications compatibles qui n'ont plus à développer leurs propres capacités d'authentification, etc.

Les services numériques concernés par les cibles 2 et 3 (notamment le DUI/DPI) doivent déléguer l'authentification de l'utilisateur à un fournisseur d'identités tiers en suivant le flux Authorization Code Flow du standard OIDC.

4. Organisation de la procédure de l'appel à projets

4.1. Dossier de candidature

Le dossier de candidature est composé :

- De la présentation du projet, d'une dizaine de pages maximum, en utilisant le cadre de réponse téléchargeable sur le site demarches-simplifiees.fr. Le candidat pourra librement ajouter des annexes à ce cadre de réponse. L'ANS sera sensible à la qualité, à la clarté et au caractère synthétique de la candidature.
- Des annexes administratives et financières exigées et dont la liste est précisée dans le cadre de réponse, comprenant notamment un budget prévisionnel sincère du projet détaillant les postes de coûts.

Publique

Le dossier de candidature est déposé sur le site https://www.demarches-simplifiees.fr/commencer/AAPHOSPICONNECTALPHA avant le 5 avril 2024 (14h – heure de Paris), sous peine de rejet de celui-ci.

Il est nécessaire pour chaque porteur de projet de créer un compte. Une fois le compte créé, il est directement dirigé vers le formulaire d'inscription qu'il peut commencer à remplir.

4.2. Instruction des candidatures

Le choix des projets s'effectue au regard des critères d'éligibilité et de sélection décrits au sein des articles 2 et 3 du présent cahier des charges.

L'instruction des candidatures mobilise un comité d'engagement dont la composition a été définie par délibération du Conseil d'administration de l'ANS du 7 mars 2024.

L'instruction des candidatures se déroule en **2 phases** :

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- Analyse des dossiers de candidature par l'équipe CaRE-HospiConnect sur la base d'une grille d'analyse commune reprenant les critères mentionnés dans le cahier des charges ;
- Les dossiers des candidats conformes aux critères et les analyses correspondantes sont remis au comité d'engagement qui propose une liste de lauréats à l'issue d'une séance de délibération organisée par l'ANS.

Sur la base des avis et recommandations du comité d'engagement, le directeur de l'ANS sélectionne les projets lauréats de l'appel à projets « Sécurisation et simplification de l'identification électronique des professionnels dans les établissements sanitaires et médico-sociaux », qui feront l'objet d'un financement. Les avis rendus par le comité d'engagement sont des avis simples qui ne lient par la Direction de l'ANS. Le comité d'engagement en charge de l'instruction des candidatures se réserve le droit de modifier les coûts prévisionnels annoncés dans le budget prévisionnel.
Le choix des projets lauréats procède du pouvoir discrétionnaire de l'ANS. Le rejet d'une candidature ne pourra en aucun cas faire l'objet d'une contestation ou d'un recours.

4.3. Conventionnement

Une convention est signée entre l'ANS et chaque lauréat du présent appel à projets.

Cette convention fixe les objectifs, les moyens, le calendrier et les conditions de réalisation du projet ainsi que les modalités d'évaluation des résultats et de contrôle par l'ANS de la bonne utilisation des crédits, moyens ou services mis à disposition.

Publique

4.4. Suivi et livrables des lauréats

L'ANS assure le suivi de la mise en œuvre des projets sélectionnés. L'ANS organise un **point d'avancement régulier** avec chaque lauréat. Les lauréats remontent chaque mois à l'ANS les éléments d'avancement du projet, incluant les indicateurs qui sont demandés par l'ANS (un support sera fourni pour faire gagner du temps aux lauréats).

A mi-projet (3,5 mois), les lauréats fournissent un bilan d'étape de l'avancement du projet et un rapport financier qui rend compte des dépenses engagées et liquidées, des financements associés et des éventuelles recettes (notamment sous la forme d'autres aides) perçues dans le cadre de la réalisation du projet. Ce bilan d'étape sera à présenter à l'ANS lors d'un des points mensuels ci-dessus (l'ANS fournira un document modèle).
Ce support préétabli demandera à l'établissement de présenter un certain nombre d'éléments, comme (non exhaustif et susceptible d'évoluer) :

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- Des éléments sur l'avancement du déploiement (parcours d'enrôlement et de gestion des cartes, nombre de moyens d'identification électroniques déployés, nombre d'enregistrements RPPS réalisés…) ;
- Des indicateurs sur l'utilisation des solutions accessibles avec ces moyens d'identification électroniques (nombre d'accès au DPI, nombre d'accès au DMP…) ;
- Les freins rencontrés et un plan d'action pour les résoudre ;
- Les besoins d'accompagnement ou de support spécifique que pourraient apporter l'ANS sur les prochaines étapes.

Un certain nombre de ces éléments pourra être déjà présenté ou utilisé lors des points d'avancement mensuel, en fonction du besoin de l'établissement et de l'avancement du projet.

En fin de projet, les lauréats transmettent un bilan du projet et un rapport financier qui rend compte des dépenses engagées et liquidées, des financements associés et des éventuelles recettes (notamment sous forme d'aides) perçues dans le cadre de la réalisation du projet, toujours sur la base d'un modèle commun fourni par l'ANS aux participants et présenté lors du dernier point mensuel. Les lauréats produisent également un engagement sur la sécurisation des modalités d'identification électronique, finalisé conformément au RIE

Dans un objectif de capitalisation et de partage des retours d'expérience, une partie des éléments de documentation produits dans le cadre des projets retenus a vocation à être rendue publique (en particulier les rapports d'évaluation produits à la fin du projet). Ces éléments seront repris pour déterminer les facteurs clés de succès pour le déploiement de ces solutions dans les autres structures. L'ANS se réserve le droit d'organiser, avec l'accord de l'établissement et même a posteriori de la fin de l'appel à projets, des éléments de communication (interview, vidéo, article…) pour promouvoir cette démarche et ses succès.

publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

5. Règles de financement

5.1. Cadre juridique applicable

Les financements relevant du présent appel à projets sont pris en application de la décision de la Commission Européenne n°2012/21/UE du 20 décembre 2011 relative à l'application de l'article 106, paragraphe 2, du traité sur le fonctionnement de l'Union européenne aux aides d'État sous forme de compensations de service public octroyées à certaines entreprises chargées de la gestion de services d'intérêt économique général.

Ces financements visent à compenser les coûts exposés pour l'exercice du SIEG hospitalier, dont le 6° alinéa de l'article L. 6111-1 du Code de la santé publique indique qu'il comprend la participation à l'innovation en santé. Ils sont attribués dans le cadre d'un système de versement sur atteinte d'objectifs.

5.2. Montant du financement

Pour chaque projet retenu et selon l'atteinte de l'objectif, une aide est attribuée sous la forme d'une subvention calculée sur la base des coûts réels[11] mentionnés dans le rapport financier produit par le lauréat, desquels seront déduites les recettes de toute nature (notamment sous forme d'aides) qui pourraient être perçues.

Publique

Le montant de la subvention est plafonné selon la cible choisie :

- Cible 1 : 30 000 €
- Cible 2 : 40 000 € (donc un total de 70 k€ en cumulant les cibles 1 et 2).
- Cible 3 : 20 000 € (donc un total de 90 k€ en cumulant les cibles 1, 2 et 3).

Le plafond de subvention est augmenté de 5000€ si l'option d'auto-enregistrement a été retenue.

Chaque candidat présente, au moyen de l'annexe financière au dossier de candidature, un budget prévisionnel sincère du projet détaillant les postes de coûts ainsi que les éventuelles recettes (notamment sous forme d'aide) qui pourraient être perçues. Le comité d'engagement en charge de l'instruction des candidatures se réserve le droit de modifier les coûts prévisionnels annoncés.

[11] Les coûts associés à la mise en conformité d'une solution de DUI/DPI avec les dossiers de spécifications de référencement (DSR) Ségur ne seront pas financés (puisque déjà financés par le biais du programme SONS).

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

5.3. Modalités de versement du financement

Le financement est versé à la fin du projet, en une fois, après remise du rapport d'évaluation et du rapport financier final. Le financement est calculé sur la base des coûts réels mentionnés dans le rapport financier final.
Le montant des financements qui sera alloué aux lauréats sera calculé à partir de la déclaration des coûts réellement engagés à partir du 1er janvier 2024 jusqu'à la déclaration d'atteinte de l'objectif retenu dans le cadre de la candidature, dans la limite du plafond mentionné au paragraphe précédent.

La convention mentionnée à l'article 4.3 ci-dessus prévoit les conditions dans lesquelles le financement peut être retiré par l'ANS et le remboursement des sommes perçues ordonné, notamment en cas de méconnaissance par les bénéficiaires, des dispositions du cahier des charges ou des stipulations de la convention ou de fraude.

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

6. Confidentialité et communication

L'ANS s'assure que les documents transmis dans le cadre du présent appel à projets sont soumis à la plus stricte confidentialité. L'ensemble des personnes ayant accès aux dossiers de candidatures est tenu à la plus stricte confidentialité.

Une fois le projet sélectionné, les lauréats sont tenus de mentionner le soutien apporté par le Ministère de la Santé et de la Prévention (délégation au numérique en santé) et de l'ANS dans leurs actions de communication et la publication de leurs résultats avec la mention unique « ce projet a été soutenu par la délégation au numérique en santé (DNS) et l'agence du numérique en santé (ANS) ».

Toute opération de communication doit être concertée entre les lauréats et l'ANS, afin de vérifier notamment le caractère diffusable des informations et la conformité des références.

L'Etat et l'ANS pourront communiquer sur les objectifs généraux de l'appel à projets, ses enjeux et ses résultats, ainsi que sur les projets retenus, dans le respect des secrets des affaires. Ils pourront notamment utiliser à cette fin une « fiche communication » qui sera établie par le lauréat, une fois celui-ci sélectionné.

Enfin, les lauréats sont tenus à une obligation de transparence et de reporting vis-à-vis de l'Etat et de l'ANS, nécessaire à l'évaluation ex-post des projets ou de l'appel à projets.

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

7. Glossaire

- **2FA** : 2 facteurs d'authentification

L'authentification à 2 facteurs est une méthode d'authentification qui renforce la sécurité en ajoutant un second facteur d'authentification.

- **CNI** : Carte nationale d'identité

La carte nationale d'identité est émise par les autorités et permet de prouver l'identité d'une personne.

- **DMP** : Dossier médical partagé

Le dossier médical partagé est un dossier numérique qui contient toutes les informations de santé relatives à une personne (examens médicaux, traitements, etc.).

- **DNS** : Délégation interministérielle au numérique en santé

La délégation au numérique en santé (DNS) est rattachée directement aux Ministères chargés de la santé, de l'action sociale et de la sécurité sociale afin d'assurer le pilotage de l'ensemble des chantiers de transformation du numérique en santé.

Publique

- **DPI** : Dossier patient informatisé

Le dossier patient informatisé a vocation à stocker l'ensemble des documents liés au parcours de soins du patient au sein d'un établissement.

- **e-CPS** : Application mobile d'authentification sur ProSanté Connect

La e-CPS est une application mobile permettant d'accéder aux services numériques de santé via un téléphone mobile ou une tablette électronique sans passer par un lecteur de carte à puce.

- **eIDAS** : Electronic identification and trust services

Le règlement eIDAS est un règlement européen en matière d'identification électronique et de services de confiance. Il vise à instaurer un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres sur l'ensemble des services en ligne des autres États membres. Il induit 3 niveaux de sécurité (faible, substantiel et élevé) et des modalités de vérification associées.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- **ES** : Etablissements de santé

Les établissements de santé peuvent être publics (centres hospitaliers régionaux, centres hospitaliers universitaires, centres hospitaliers, établissements de soins de longue durée) ou privés (structures à but lucratif ou non lucratif).

- **ESMS :** Etablissements et services sociaux et médico-sociaux

Un établissement ou service social ou médico-social (ESMS) est une structure dont la vocation est d'accueillir et d'accompagner, dans son enceinte ou de manière ambulatoire, pour une brève durée ou au long cours, des personnes handicapées, dépendantes ou en situation d'exclusion sociale.

- **FINESS** : Fichier national des Etablissements sanitaires et sociaux

Le répertoire Finess est le répertoire national de référence des personnes morales intervenant dans les domaines sanitaire, médico-social et social et de l'enseignement des professions sanitaires et sociales.

- **IAM** : Identity and access management

La gestion des identités et des accès (*Identity and Access Management*) fait référence à la gestion des identités électroniques ou numériques en interne d'une structure.

Publique

- **IDP** : Identity provider

Le fournisseur d'identité (*Identity provider*) est le service qui stocke et vérifie l'identité des utilisateurs d'un établissement.

- **MIE** : Moyen d'identification électronique

Les moyens d'identification électronique permettent aux professionnels de s'identifier afin d'accéder à des services numériques de santé. Il s'agit par exemple de couples identifiant / mot de passe et de cartes à puces.

- **OIDC** : OpenID Connect

OpenID Connect est un standard d'identification qui autorise des clients à vérifier l'identité d'un utilisateur final en se basant sur l'authentification fournie par un serveur d'autorisation.

- **OTP** : One-time password

Un mot de passe unique (*one-time password*) est un mot de passe qui n'est valable que pour une session ou une transaction.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- **PSC** : Pro Santé Connect

Pro Santé Connect est un fédérateur de fournisseurs d'identité au standard OpenID.
Pro Santé Connect permet aux professionnels de s'authentifier soit avec une e-CPS (application mobile) soit avec une carte CPS physique à tous les services numériques de santé raccordés à Pro Santé Connect.

- **PVID** : Prestataire de Vérification d'Identités à Distance

Le référentiel PVID instaure certaines règles sur la vérification d'identité à distance. Les exigences formulées par ce référentiel portent sur le prestataire et la sécurité du système d'information permettant de fournir le service de vérification d'identité à distance.

- **RIE** : Référentiel d'identification électronique

Le RIE définit des exigences sur les connexions à des services numériques traitant des données de santé. Il concerne les usagers, les professionnels et les structures.

- **RPPS** : Répertoire partagé des professionnels intervenant dans le système de santé

Le répertoire partagé des professionnels de santé (RPPS) est le fichier de référence des professionnels de santé. Il répertorie l'ensemble des données d'identification, de diplômes, d'activité, de mode et de structure d'exercice de tout professionnel de santé.

Publique

- **SNS** : Services numériques sensibles

Les services « sensibles » sont les services numériques en santé qui traitent des données de santé à caractère personnel au sens du RGPD. Ce sont des services partagés (ex : Dossier médical partagé), des services qui intègrent des services partagés (ex : Dossier patient informatisé), des services proposant un accès web externe au SI (ex : services accessibles en télétravail) ou des services qui intègrent des traitements de données ou des accès de grande échelle.

- **SSO** : Single sign-on (authentication unique)

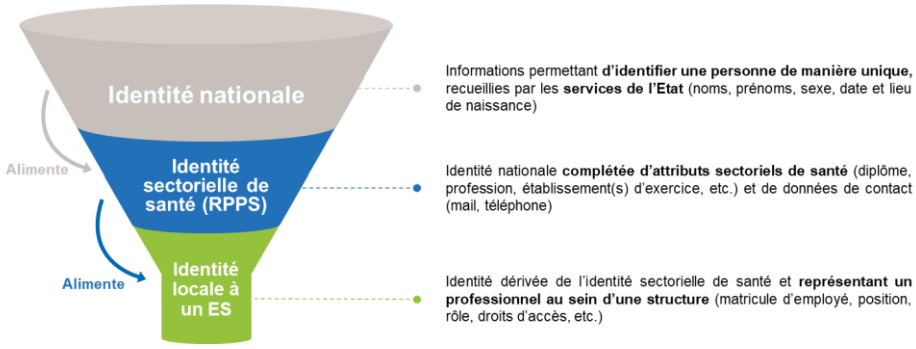
Le Single sign-on (authentification unique) est un service qui permet à un utilisateur d'accéder à plusieurs applications à la suite d'une authentification unique.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

8. Annexes

8.1. Annexe 1 : Dérivation des identités

L'un des objectifs de l'appel à projets (et une des exigences du référentiel d'identification électronique de la PGSSI-S Personnes Physiques) est la mise en place d'un répertoire d'identités local au sein des établissements de santé. Cet objectif ne vise ni à remplacer ni à dupliquer les référentiels d'identités déjà en place au niveau national (comme le RPPS).



Publique

En cible, chaque identité éligible à l'enregistrement au RPPS présente dans un référentiel local d'établissement sera une identité dérivée d'une identité nationale de santé présente au RPPS. L'un des enjeux de l'appel à projets est d'identifier les besoins et d'éprouver sur le terrain les processus à mettre en place pour assurer la création de l'identité locale à partir d'une dérivation de l'identité nationale sectorielle de santé (elle-même déjà dérivée de l'identité nationale du professionnel).

Pour atteindre cette cible, les processus afférents à la création de l'identité sectorielle de santé (RPPS) et à la délivrance des moyens d'identification associés doivent évoluer de telle sorte qu'il soit possible d'obtenir l'immatriculation du professionnel de santé à l'aide d'un numéro RPPS, et de lui mettre à disposition une carte e-CPS immédiatement après sa demande d'enregistrement afin de lui fournir un MIE en quelques minutes. Ce dernier ne sera pleinement utilisable qu'après validation par l'autorité d'enregistrement compétente de la profession et/ou l'activité du professionnel.

Cette évolution devra être mise à disposition :

- Des ordres professionnels, afin d'offrir cette fonctionnalité aux professionnels s'enregistrant par leur guichet ;
- Des professionnels s'enregistrant en ARS sur le portail RPPS mis à disposition par l'ANS ;
- Des professionnels enregistrés par leurs établissements d'exercice (RPPS+).

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Le numéro RPPS pourra être obtenu directement par le professionnel lui-même (auto-enregistrement). Le raccourcissement du temps de délivrance de la e-CPS permettra d'envisager des organisations permettant de gérer les situations où l'immatriculation n'a pas été réalisée en amont de la prise de fonction dans l'établissement. Chaque identité créée au sein du RPPS sera accompagnée d'un indicateur témoignant du niveau de qualité des traits d'identité vis-à-vis du répertoire national d'identification des personnes physiques (RNIPP). Cet indicateur permettra aux établissements de savoir s'ils peuvent directement créer une identité dans leur répertoire local à partir de l'identité sectorielle du PS ou s'ils doivent conduire des vérifications supplémentaires.

Publique

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.