AGENCE
DU NUMÉRIQUE
EN SANTÉ

PGSSI-S

Référentiel d'Identification électronique

Acteurs des secteurs sanitaire, médico-social et social [personnes physiques]

Statut : En cours | *Classification : Interne* | *Version : v2b.0.g*

Historique du document

Version	Date de publication	Motif et nature de la modification
1.0	Avril 2022	Version initiale
2b.0.g	*25/02/2026*	*Version après concertation*

SOMMAIRE

1 INTRODUCTION

1.1 Objet du référentiel

Pris en application des dispositions des articles L. 1470-2 et L. 1470-5 du code de la santé publique (voir [ART_L1470]), le référentiel d'Identification électronique définit le niveau de garantie attendu au regard des spécifications du règlement eIDAS (cf. [eIDAS-MIE]), s'agissant des modalités d'Identification électronique des utilisateurs des Services numériques en santé. Le référentiel est composé en trois volets, dédiés respectivement :

- Aux acteurs des secteurs sanitaire, médico-social et social [personnes physiques] (le présent document) ;
- Aux acteurs des secteurs sanitaire, médico-social et social [personnes morales] (voir [IE-ASPM]) ;
- Aux usagers (voir [IE-Usagers]).

Le présent volet vise à encadrer les Schémas d'Identification électronique applicables aux personnes physiques intervenant dans les secteurs sanitaire, médico-social et social.

Le référentiel concerne les étapes d'Identification (association d'une identité à une personne) et d'authentification (vérification qu'elle est bien celle qu'elle prétend être) des professionnels personnes physiques accédant à des Services numériques de santé.

1.2 Périmètre d'application du référentiel

En application de l'article L. 1470-1 du code de la santé publique (voir [ART_L1470]), le présent référentiel s'applique aux outils, systèmes d'information et Services numériques qui sont mis en œuvre par voie électronique, par des organismes publics ou privés, à distance ou non, dès lors que ces outils concourent à des activités de prévention, de diagnostic, de soin, de prise en charge, de suivi, ou d'interventions nécessaires à la coordination de plusieurs de ces activités et qu'ils traitent des Données de santé à caractère personnel au sens du RGPD (cf. considérant 35 dans [RGPD]).

Cette définition s'entend au sens large et couvre ainsi tous les traitements de données au sens de l'article 4 du RGPD (« *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de Données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* »).

En application de l'article L. 1470-2, ce volet du référentiel s'applique à l'Identification électronique des utilisateurs professionnels (personnes physiques) des Services numériques en santé.

1.3 Définitions et concepts généraux

Données d'identité

Dans le cadre de ce référentiel, les *Données d'identité* d'une personne physique sont définies comme l'ensemble des traits d'identité permettant d'identifier une personne de manière unique : nom de naissance, liste des prénoms, date et lieu de naissance.

Données sectorielles

Dans le cadre de ce référentiel, les *Données sectorielles* d'une personne physique sont définies comme :
- Les attributs sectoriels associés aux Données d'identité, par exemple la profession, le diplôme autorisant l'exercice de la profession, le(s) lieu(x) d'exercice de la profession... ;
- Le ou les identifiants attribués à cette personne dans les Répertoires sectoriels, par exemple dans le RPPS.

Fournisseur de Service (FS)

Un *Fournisseur de Service* est une personne morale qui fournit un Service numérique en santé dans un environnement de production à des Utilisateurs.

Fournisseur d'identité (FI)

Un *Fournisseur d'identité* est une entité qui crée et gère les identités électroniques de personnes physiques à qui elle délivre un Moyen d'Identification électronique associé à leur identité. Un Fournisseur d'identité est ainsi responsable d'un ou de plusieurs Schémas d'Identification électronique.

Fédérateur de Fournisseurs d'identité

Un *Fédérateur de Fournisseurs d'identité* est un Service d'intermédiation entre des Fournisseurs d'identité et des Fournisseurs de Service. Il permet à un *Fournisseur de Service* de disposer d'une solution unique d'Identification électronique de ses utilisateurs, tout en laissant à ceux-ci le choix du Fournisseur d'identité utilisé (dans la limite du respect d'exigences minimales de sécurité).

Identifiant

Un *Identifiant* est un attribut unique d'un *Utilisateur* dans un *Répertoire d'identité*, permettant de différencier deux personnes y compris dans le cas où leurs traits d'identité sont similaires ou très proches.

Identification électronique

Le terme *Identification électronique* désigne le processus utilisé par un *Utilisateur* pour s'identifier (indiquer qui il est) et s'authentifier (vérification qu'il est bien celui qu'il prétend être) auprès d'un *Service*.

Moyens d'Identification électronique

Un *Moyen d'Identification électronique* (MIE) est un dispositif matériel et/ou immatériel contenant un *Identifiant* utilisé pour s'authentifier sur un *Service*. Dans le règlement eIDAS, un Moyen d'Identification électronique est associé à un niveau de garantie faible, substantiel ou élevé selon le niveau de sécurité qu'il offre.

Un MIE doit être conforme au présent référentiel pour l'accès aux Services numériques en santé.

Moyen d'Identification électronique de secours

C'est un Moyen d'Identification électronique prévu pour une utilisation temporaire et transitoire, pendant une durée limitée, sous le contrôle du Fournisseur de Service en cas d'indisponibilité du Moyen d'Identification électronique prévu en mode de fonctionnement nominal

Un Moyen d'Identification électronique de secours peut ne pas être conforme à l'ensemble des exigences du référentiel, d'où la nécessité de limiter son utilisation à certaines circonstances et dans le temps, sous le contrôle du Fournisseur de Service.

Répertoire d'identité

Un *Répertoire d'identité* est une base de données ou un système d'enregistrement qui contient les Données d'identité des personnes physiques reconnues dans le cadre d'un Schéma d'Identification électronique.

Répertoire d'identité sectoriel

Un Répertoire d'identité sectoriel intègre des *Données sectorielles* associées aux *Données d'identité*. On peut distinguer les Répertoires sectoriels de référence mentionnés à l'article L. 1470-4 du code de la santé publique et les Répertoires d'identité sectoriels locaux (par exemple au sein d'un établissement de santé).

Schéma d'Identification électronique

Un *Schéma d'Identification électronique* est un ensemble de règles, processus et technologies utilisé pour émettre des *Moyens d'Identification électronique* permettant de vérifier l'identité d'un *Utilisateur*. Il comprend par exemple les Fournisseurs d'identités, les Moyens d'Identification électronique, les procédures d'enregistrement, d'enrôlement, de révocation, d'authentification et de vérification (par exemple pour des Données sectorielles).

Service numérique en santé

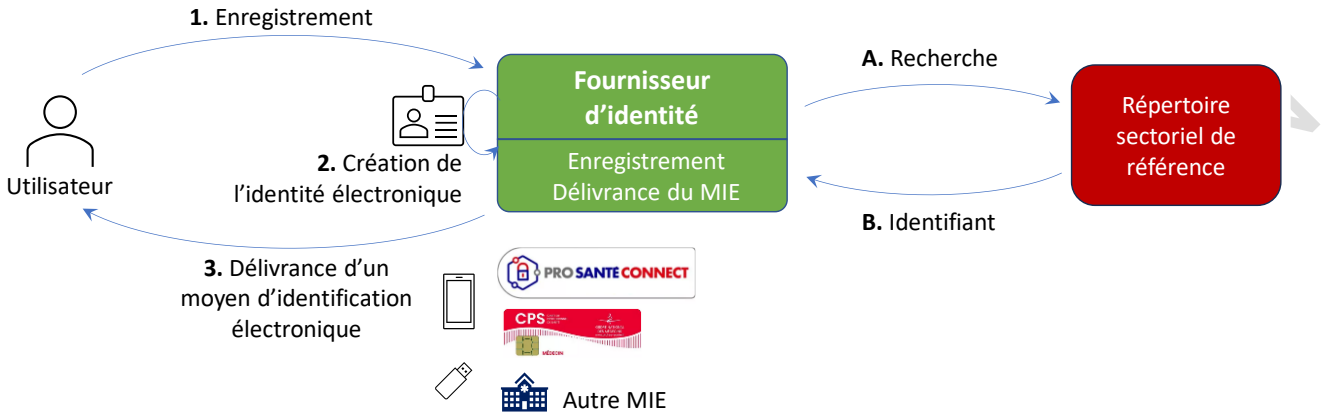
L*es Services numériques en santé sont les systèmes d'information ou les Services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités (article L. 1470-1 du CSP)..*

Utilisateur

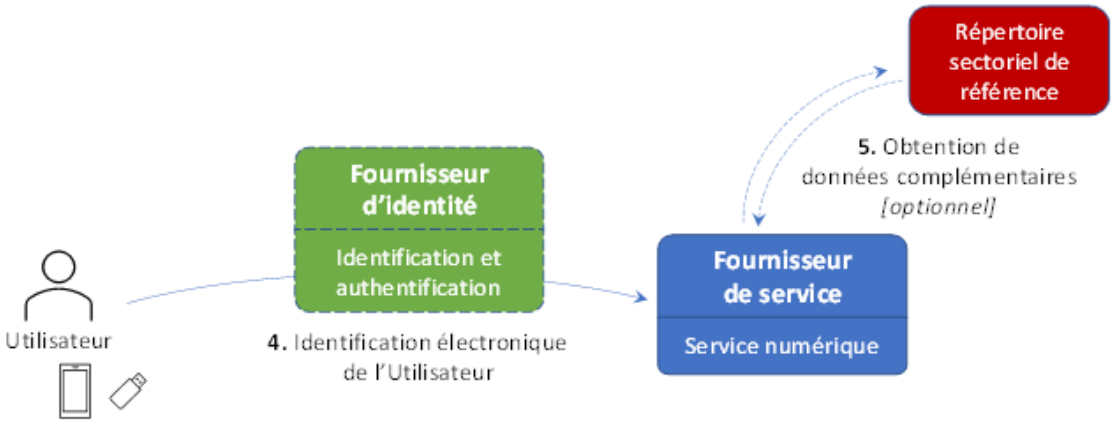
Le terme *Utilisateur* désigne toute personne physique entrant dans le champ de ce volet du référentiel. Il s'agit donc des professionnels, personnes physiques (par opposition aux personnes morales), en charge d'activités relevant des secteurs sanitaire, médico-social et social ainsi que de l'ensemble des personnes exerçant sous leur autorité.

1.4 L'Identification électronique des utilisateurs

Un *Utilisateur* obtient dans un premier temps un *Moyen d'Identification électronique* auprès d'un *Fournisseur d'identité* selon les modalités de son *Schéma d'Identification électronique*.



Le *Fournisseur d'identité* associe l'identité qu'il gère avec l'I*dentifiant* de l'*Utilisateur* dans le *Répertoire sectoriel* de référence : le RPPS (lorsque celui-ci y est inscrit).



Lorsque l'U*tilisateur* se connecte à un *Service numérique*, le *Fournisseur de Service* délègue son *Identification électronique* auprès du *Fournisseur d'identité*. L'authentification se fait avec le Moyen d'I*dentification électronique* délivré par le *Fournisseur d'identité*. Les Données d'identité et les D*onnées sectorielles* de l'Utilisateur sont transmises au *Fournisseur de Service*. Une fois l'I*dentification électronique* vérifiée, le *Fournisseur de Service* octroie à l'*Utilisateur* les accès correspondant à ses habilitations (hors périmètre du présent référentiel).

Lorsque le Service numérique auquel s'est connecté l'utilisateur accède lui-même à un second *Service numérique*, il est possible de mettre en œuvre une Identification électronique indirecte, selon des modalités décrites dans le volet du référentiel d'Identification électronique dédié aux personnes morales (cf. [IE-ASPM]).

1.5 Documentation et liens utiles

1.5.1 Réglementation

Renvoi	Document
[ART_L1470]	Articles L. 1470-1 à 1470-5 du code de la santé publique (issus de l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'Identification électronique des utilisateurs de Services numériques en santé et des bénéficiaires de l'assurance maladie) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464
[Arrêté RPPS]	Arrêté du 23 septembre 2022 relatif à la mise en œuvre du « Répertoire partagé des professionnels intervenant dans le système de santé » https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046349842
[eIDAS]	Règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23/07/2014 (« règlement eIDAS ») https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR
[eIDAS-MIE]	Règlement d'exécution (UE) 2015/1502 de la Commission du 8/09/2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des Moyens d'Identification électronique https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27/04/2016 (« règlement général sur la protection des données ») https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée) https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

1.5.2 Autres documents

Renvoi	Document
[IE-ASPM]	Référentiel d'Identification électronique - Acteurs des secteurs sanitaire, médico-social et social [personnes morales] https://esante.gouv.fr
[IE-Usagers]	Référentiel d'Identification électronique - Usagers https://esante.gouv.fr
[PSC]	Référentiel Pro Santé Connect https://esante.gouv.fr/produits-services/referentiel-pro-sante-connect
[RFC 6238]	TOTP: Time-Based One-Time Password Algorithm https://tools.ietf.org/html/rfc6238.html

2 SCHEMAS D'IDENTIFICATION ELECTRONIQUE

2.1 Sélection des Schémas d'Identification électronique

2.1.1 Inventaire des Services et des Schémas d'Identification électronique

Afin de s'assurer de sa conformité au présent référentiel, chaque *Fournisseur de Service* doit identifier les *Services numériques en santé* dont il est responsable et sélectionner les *Schémas* et *Moyens d'Identification électronique* permettant aux *Utilisateurs* de s'y connecter. Dans certains cas, les MIE utilisables peuvent dépendre du contexte (type d'*Utilisateur*, situation de mobilité…).

EXI RIE-PS 01

Le Fournisseur de Service DOIT inventorier :

- L'ensemble des Services numériques en santé qu'il fournit à des Utilisateurs et dont il est responsable ;
- Pour chaque Service les Schémas d'Identification électronique et les Moyens d'Identification électronique permettant aux Utilisateurs de s'y connecter, le cas échéant en distinguant les contextes d'emploi.

2.1.2 Moyens d'Identification électroniques autorisés

L'objectif est d'atteindre, pour l'Identification électronique des *Utilisateurs*, un niveau de sécurité équivalent au niveau de garantie substantiel des identités électroniques au sens du règlement eIDAS (cf. [eIDAS] et [eIDAS-MIE]). Un *Fournisseur de Service* peut s'appuyer sur les Moyens d'Identification électronique proposés par l'ANS et mettre en place ses propres MIE dans le cadre d'un *Schéma d'Identification électronique* dédié.

EXI RIE-PS 02

Le *Fournisseur de Service* DOIT proposer des *Moyens d'Identification électronique* des *Utilisateurs* parmi :

1- Pro Santé Connect, dans le cadre des *Schémas d'Identification électronique* proposés, avec :
   a. L'application mobile d'Identification sectorielle de Pro Santé Connect ;
   b. Les cartes d'Identification sectorielles fournies par l'ANS compatibles avec Pro Santé Connect ;
   c. Les autres *Moyens d'Identification électronique* compatibles de Pro Santé Connect ;

2- Les *Moyens d'Identification électroniques* proposés par les *Fournisseurs d'identité* de Pro Santé Connect, préalablement habilités par l'ANS ;

3- Les *Moyens d'Identification électronique* reposant sur un *Schéma d'Identification électronique* ayant fait l'objet d'une attestation de conformité aux exigences du présent référentiel par le *Fournisseur d'identité*, au plus tard le 31/12/2026 pour les services en production à cette date;

4- Les cartes de la famille CPx délivrées par l'ANS pour l'authentification directe du porteur (hors Pro Santé Connect), pour les *Fournisseurs de Services* historiques spécifiquement autorisés par l'ANS pour cet usage.

Remarques :

1- L'application mobile d'Identification sectorielle de Pro Santé Connect est l'application « e-CPS » (le nom de l'application pourra évoluer).
Les cartes d'Identification sectorielles fournies par l'ANS compatibles avec Pro Santé Connect pour l'accès aux *Services numériques en santé* sont les cartes, reposant sur l'enregistrement dans le RPPS du porteur de la carte.
La liste des autres MIE compatibles avec Pro Santé Connect, est mise à jour régulièrement sur le site de l'ANS. Il est à noter que l'usage local, hors Pro Santé Connect, de ces mêmes MIE nécessite une attestation de conformité, telle que prévue au point 3-.

2- Les *Fournisseurs d'identités* de Pro Santé Connect doivent être habilités par l'ANS. Il peut s'agir par exemple :
- De *Fournisseurs d'identité* conformes au niveau de garantie substantiel ou élevé du règlement eIDAS (par exemple les portefeuilles d'identité numérique Européens : EUDI Wallet) ;
- De certains établissements habilités par l'ANS comme Fournisseurs d'identité de Pro Santé Connect, sur la base d'une vérification de conformité aux exigences dédiées du référentiel Pro Santé Connect. Ces établissements doivent s'appuyer sur une solution logicielle de gestion des identités et des accès (IAM) ayant elle-même fait l'objet d'une habilitation technique en regard du même référentiel.

3- Les modalités d'attestation de conformité sont décrites dans la suite de ce document. Un guide est proposé par l'ANS pour accompagner les structures concernées dans leur démarche.
Il peut s'agir par exemple des MIE compatibles ou non avec PSC mis à disposition des PS au sein d'un ES pour accéder au SI local de l'ES hors PSC.
Au plus tard le 31/12/2026 : une attestation de conformité aux exigences du présent référentiel doit être établie par le Fournisseur d'identité délivrant les MIE, avec des réserves éventuelles sur certaines exigences, qui devront être levées au plus tard le 31/12/2028.

4- L'authentification directe par carte CPS ou par carte de la famille CPx, hors Pro Santé Connect, concerne essentiellement les téléservices nationaux de l'Assurance maladie et quelques Services publics nationaux historiques. Ces Services ont vocation à basculer progressivement sur Pro Santé Connect.
L'utilisation de la carte CPS ou d'une carte CPx hors Pro Santé Connect pour l'accès à d'autre *Services numériques* doit faire l'objet d'une attestation de conformité du *Schéma d'Identification électronique* utilisé au présent référentiel (par exemple en cas d'enrôlement sur un Répertoire d'identité local d'une structure de santé). Les cartes CPx (autres que CPS) ne reposant pas sur un enregistrement dans le Répertoire sectoriel de référence (RPPS) ne devraient pas être utilisées pour l'accès à des *Services numériques en santé.*

2.2 Pro Santé Connect

Pro Santé Connect est le *Fédérateur de Fournisseurs d'identité* mis à disposition par l'ANS permettant l'Identification électronique des acteurs personnes physiques intervenant dans le système sanitaire, social et médico-social.

EXI RIE-PS 03
Le *Fournisseur de Service* DOIT permettre l'utilisation de Pro Santé Connect.

Un *Service numérique* doit toujours permettre l'utilisation de Pro Santé Connect (par exemple les logiciels métier des professionnels), même si d'autres *Moyens d'Identification électronique* peuvent être utilisés, sous réserve de conformité aux autres exigences du présent référentiel (par exemple au sein du système d'information d'un établissement disposant d'une solution locale de gestion des identités et des accès offrant une fonctionnalité de « single sign on » avec ses propres *Moyen d'Identification électronique*).

Lorsque le Service numérique utilise Pro Santé Connect comme solution nominale d'Identification électronique, , selon la criticité et les engagements de disponibilité du Service, le *Fournisseur de Service* doit prévoir une alternative en cas d'indisponibilité d'indisponibilité de Pro Santé Connect (exemple : coupure internet).

2.3 *Moyens d'Identification électronique* autres que ProSantéConnect

2.3.1 Généralités

En complément de Pro Santé Connect, ou en alternative locale (par exemple au sein d'une structure de santé qui voudrait disposer d'une solution autonome), un *Fournisseur de Service* peut s'appuyer sur d'autres *Fournisseurs d'identité*, ou se constituer lui-même *Fournisseur d'identité,* afin de s'adosser à un *Répertoire d'identité* local, ou de permettre l'utilisation d'autres *Moyens d'Identification électronique.*

Le ou les *Schémas d'Identification électronique* mis en œuvre doivent alors être conformes aux exigences du présent référentiel et faire l'objet d'une attestation de conformité.

Le *Fournisseur d'identité* peut éventuellement être habilité comme *Fournisseur d'identité* de Pro Santé Connect, sous réserve de satisfaire à des exigences spécifiques, vérifiées lors de l'habilitation par l'ANS en regard du Référentiel Pro Santé Connect (cf. [PSC]).

2.3.2 Données d'identité

EXI RIE-PS 04
Le Fournisseur d'identité DOIT utiliser et être en mesure de fournir par l'intermédiaire des Moyens d'Identification électronique proposés : - L'Identifiant issu du Répertoire sectoriel de référence (RPPS) dès qu'il existe ; - A défaut, un Identifiant local conforme à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

Un *Identifiant* local est établi par le FI, par exemple en utilisant un matricule attribué par un SIRH, ou un identifiant LDAP / Active Directory. Un *Moyen d'Identification électronique* peut transmettre plusieurs identifiants pour un même acteur, par exemple à la fois un identifiant RPPS et un identifiant local.

Lorsqu'un Répertoire d'identité local est utilisé, l'identifiant local et l'identifiant RPPS coexistent et un lien doit être établi entre les deux.

EXI RIE-PS 05
Le Fournisseur d'identité DOIT enregistrer au moins les attributs d'identité des Utilisateurs suivants : - Nom de naissance ; - Prénoms de naissance; - Sexe ; - Date de naissance ; - Ville de naissance (code géographique INSEE) ; - Pays de naissance (code géographique INSEE).

Ces données pourront être utilisées pour un rapprochement avec les Répertoires sectoriels nationaux comme le RPPS. D'autres Données d'identité, comme par exemple le nom d'usage, ou le nom d'exercice, peuvent également être enregistrées.

2.3.3 Répertoire d'identité local

Un *Répertoire d'identité* local constitue une brique essentielle pour la gestion des *Moyens d'Identification électronique* puis pour le contrôle d'accès à des Services numériques en santé, notamment au sein d'un établissement. Dans cette optique, il est attendu que ce Répertoire soit :

- Complet : l'ensemble des professionnels auxquels un *Moyen d'Identification électronique* peut être remis pour l'accès aux Services concernés ;
- A jour : le Répertoire d'identité local doit être maintenu à jour en continu afin de refléter les mouvements (entrées, sorties, changements d'affectation) des professionnels avec la plus grande réactivité possible, et de mettre à jour en conséquence les habilitations d'accès aux Services concernés ;
- Exact : les attributs d'identité associés aux professionnels répertoriés dans le Répertoire d'identité local doivent être exacts, donc avoir été vérifiés en amont, afin que les *Moyens d'Identification électronique* diffusent des informations fiables ;

- Relié au Répertoire sectoriel de référence : lorsque qu'un professionnel du secteur de la santé est enregistré dans le Répertoire sectoriel de référence (RPPS), l'identifiant du Répertoire sectoriel doit être utilisé ou associé à l'identifiant utilisé localement.

EXI RIE-PS 06

Le Fournisseur d'identité DOIT mettre en place un Répertoire d'identité dans les conditions suivantes :

- Le Répertoire d'identité doit concerner l'ensemble des professionnels auxquels un Moyen d'Identification électronique peut être fourni par le Fournisseur d'identité ;
- L'identité d'un professionnel doit être associée à son identifiant dans le Répertoire sectoriel de référence (RPPS) dès que le professionnel y est enregistré. Les Données d'identité doivent être synchronisées avec le Répertoire sectoriel régulièrement, au moins tous les 3 ans ;
- Si le Répertoire d'identité est mis en œuvre au sein d'une organisation disposant d'un Service numérique de gestion des ressources humaines, les mouvements de personnels doivent être synchronisés avec ce Service.

Il est ainsi attendu que chaque Fournisseur d'identité organise des revues ou contrôles périodiques de cohérence entre les données présentes dans son Répertoire d'identité, par exemple son Active Directory, la base de données des personnels issue de son SIRH et le Répertoire sectoriel de référence.

Le déploiement d'une solution d'IAM (*Identity Access Management*) peut être envisagé, par exemple au sein d'un établissement, afin d'automatiser la gestion des identités et des accès des professionnels au sein du système d'information.

2.3.4 Schéma d'Identification électronique

2.3.4.1 Processus d'enrôlement et de vérification d'identité

Le processus d'enrôlement doit garantir l'exactitude des *Données d'identité* par une vérification d'identité fiable, via un face-à-face ou un autre Moyen d'Identification électronique de confiance.

EXI RIE-PS 07

Le Fournisseur d'identité DOIT implémenter un processus d'enrôlement des Utilisateurs répondant aux exigences suivantes :

- L'enrôlement de l'utilisateur doit se baser sur une vérification de l'identité du professionnel concerné, par l'une des méthodes suivantes :
  - ○ Par une Identification électronique via Pro Santé Connect ou un Moyen d'Identification électronique certifié au niveau de garantie substantiel ou élevé du règlement eIDAS ;
  - ○ Par une vérification d'identité en face-à-face physique (ou à distance par un Service en ligne certifié équivalent au face-à-face physique) avec présentation d'un document d'identité à haut niveau de confiance (ex : passeport ou carte d'identité) ;
- Lorsqu'une adresse électronique ou un numéro de téléphone mobile sont enregistrés, pour le mécanisme d'authentification ou pour la récupération des Moyens d'Identification électronique, une vérification de ces coordonnées doit être réalisée par l'envoi d'un code ou d'un lien d'activation ;
- L'enrôlement doit intégrer la vérification de l'existence de la personne dans le Répertoire sectoriel de référence.

2.3.4.2 Processus de gestion du Moyen d'Identification électronique

Les processus de gestion du *Moyen d'Identification électronique* doivent couvrir le cycle de vie complet de celui-ci et garantir que l'identité électronique établie à l'enrôlement est protégée dans le temps :

EXI RIE-PS 08

Le Fournisseur d'identité DOIT implémenter des processus de gestion des Moyens d'Identification électronique respectant les exigences suivantes :

- La délivrance d'un Moyen d'Identification électronique doit permettre de garantir qu'il est exclusivement remis en la possession de l'Utilisateur attendu ;
- Un renouvellement régulier de l'enrôlement d'un Moyen d'Identification électronique doit être prévu, a minima tous les 3 ans, et maintenir à l'état de l'art la vérification de l'identité et la robustesse de l'authentification ;
- L'Utilisateur et le Fournisseur d'identité doivent pouvoir à tout moment révoquer ce Moyen, afin d'empêcher son éventuelle utilisation frauduleuse (par exemple après la compromission de ce Moyen) ;
- Les informations obtenues par la vérification d'identité initiale ne peuvent être modifiées qu'après une nouvelle vérification au moins aussi fiable ;
- Des notifications explicites sont envoyées à l'Utilisateur au moment de la délivrance, du renouvellement et de toute modification du Moyen d'Identification électronique.

La délivrance du Moyen d'Identification électronique peut par exemple être réalisée par l'une des méthodes ci-dessous :

- En main propre, avec une vérification d'une pièce d'identité en face à face ;
- En ligne, avec un mécanisme garantissant que seul le professionnel enregistré peut activer le MIE (par exemple avec l'application mobile de Pro Santé Connect, un autre Moyen d'Identification électronique de niveau eIDAS substantiel ou élevé).

L'identité du demandeur d'une révocation doit être vérifiée afin d'éviter des demandes abusives, pour tenter un renouvellement frauduleux ou pour nuire à un professionnel. Elle peut par exemple devoir être réalisée auprès d'un opérateur d'enregistrement, d'un opérateur de sécurité physique ou bien en ligne après vérification d'informations confidentielles du porteur.

2.3.5 Moyens d'Identification électronique

La sécurité du dispositif et du mécanisme d'authentification garantit qu'une Identification électronique effectuée sur un Service numérique est bien réalisée par l'*Utilisateur* légitime de ce Moyen d'Identification électronique.

EXI RIE-PS 09

Le Fournisseur d'identité DOIT respecter les exigences suivantes :

- Le Moyen d'Identification électronique utilise au moins deux facteurs d'authentification de différentes catégories ;
- Le Moyen d'Identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession ;
- Le mécanisme d'authentification met en œuvre des mesures de sécurité protégeant l'authenticité et la confidentialité des données échangées.

Les deux facteurs d'authentification doivent appartenir à l'une des catégories suivantes :

- Connaissance : par exemple d'un mot de passe ou un code PIN ;
- Possession : par exemple d'un badge, d'une carte, d'une clé USB ou d'un terminal fixe ou mobile ;
- Biométrie : par exemple une empreinte digitale stockée et vérifiée sur un matériel en possession du professionnel.

La sécurité du mécanisme d'authentification doit empêcher un fraudeur opportuniste ou non outillé, ou bien une attaque classique par phishing par exemple, de parvenir à usurper une identité. Ainsi, de façon générale, il est fortement recommandé :

- Que l'authentification repose sur un Moyen d'Identification électronique matériel (carte à puce, clé FIDO, application TOTP sur téléphone, etc.) ou sur des éléments biométriques ;
- Que l'authentification soit dynamique, c'est-à-dire qu'elle implique des échanges de données différentes à chaque authentification (empêchant le rejeu), par exemple reposant sur des mécanismes cryptographiques, des OTP (One Time Password ou code à usage unique), etc. ;
- Que des notifications de connexion soient communiquées à l'utilisateur (envoyées par email ou rendues disponibles sur son compte par exemple).

Certains cas d'usage peuvent présenter des contraintes spécifiques (session nomade : changement fréquent de poste de travail) pour lesquelles l'authentification systématique à deux facteurs est difficilement réalisable ou acceptable en pratique.

EXI RIE-PS 10

Le Fournisseur de Service qui autorise une authentification par un seul des deux facteurs DOIT :

- Identifier formellement les cas d'usages concernés ;
- Identifier les risques induits par cette autorisation et garantir que ces risques sont acceptables dans le contexte des cas d'usage ;
- Exiger qu'une authentification nominale avec les deux facteurs d'authentification ait été réalisée précédemment et dans un délai maximal jugé compatible avec les contraintes du cas d'usage ;
- Imposer que le facteur d'authentification employé soit l'un des deux facteurs du Moyen d'Identification électronique utilisé précédemment.

Par exemple, un utilisateur ouvre initialement une session utilisant un badge sans contact et en saisissant un mot de passe. Tant que la session est ouverte et qu'une durée maximale d'authentification par un seul facteur n'a pas été dépassée, il peut s'authentifier sur différents Services en utilisant seulement son badge sans contact. A l'expiration de la durée autorisée, il doit de nouveau saisir le mot de passe.

D'une manière générale, la durée maximale d'authentification par un seul facteur ne devrait pas dépasser 4 heures.

2.4 Exigences transverses

2.4.1 Gestion des accès et des habilitations

La mise en place d'une fonctionnalité de Single Sign On (SSO) permet d'améliorer l'expérience utilisateur et d'augmenter le niveau de sécurité de l'Identification électronique. Son déploiement est imposé seulement aux organisations de taille importante.

EXI RIE-PS 11
Un *Fournisseur d'identité* DOIT mettre en œuvre une fonctionnalité de SSO (Single Sign-On) lorsqu'il fournit des Moyens d'Identification électronique sur plus d'un Service numérique en santé à plus 5.000 professionnels.

Pour favoriser l'interopérabilité des systèmes mis en œuvre, la compatibilité d'une fonctionnalité SSO avec le protocole OpenID Connect est indispensable.

EXI RIE-PS 12
Un *Fournisseur d'identité* DOIT rendre compatible la fonctionnalité de SSO avec le protocole OpenID Connect lorsqu'elle est mise en œuvre.

Le déploiement d'une solution d'IAM (*Identity Access Management*) peut être envisagé afin d'automatiser la gestion des identités et des accès des professionnels, en particulier au sein du système d'information d'une organisation de taille importante. Ces solutions intègrent généralement des fonctionnalités de SSO.

2.4.2 Gestion des sessions

La gestion de la durée de vie des sessions est un point clé de la sécurité et de l'expérience utilisateur des Services numériques en santé. Il faut distinguer le Fournisseur d'identité et le Fournisseur de Service, car chacun gère sa propre session avec ses propres règles.

Dans tous les cas, la durée de vie d'une session, pour laquelle l'*Utilisateur* s'est authentifié, doit être strictement contrôlée. A défaut, le risque d'usurpation de la session par un tiers devient plus important.

Le Fournisseur d'identité est responsable de l'authentification primaire de l'utilisateur. Il doit assurer un bon équilibre entre sécurité et expérience utilisateur, donc maîtriser les risques liés à la persistance de la session, avec éventuellement plusieurs Services utilisateurs.

EXI RIE-PS 13
Le *Fournisseur d'identité* DOIT définir, en prenant en compte le contexte de ses *Utilisateurs* et des Services raccordés, les mécanismes et la périodicité des demandes de réauthentification des Utilisateurs.

D'une manière générale, la durée de session d'un Fournisseur d'identité ne devrait pas excéder 4 heures et la durée maximale d'inactivité avant déconnexion ne devrait pas excéder 30 minutes. Selon le contexte des Utilisateurs et des Services raccordés, Le Fournisseur d'identité doit également définir une politique de gestion des sessions en cas de changement de Moyen d'Identification électronique, d'adresse IP ou de navigateur.

Le Fournisseur de Service gère la session applicative de l'utilisateur sur son Service, indépendante de celle du Fournisseur d'identité. Il doit protéger les ressources applicatives, tout en synchronisant, tant que possible, la durée de vie de sa session applicative avec celle du Fournisseur d'identité.

Afin d'éviter qu'une session applicative reste ouverte alors que l'utilisateur est déconnecté du Fournisseur d'identité, la durée de vie d'une session applicative ne doit pas dépasser celle de la session du Fournisseur d'identité. Lorsque le Fournisseur de Service estime que la durée de vie de la session du Fournisseur d'identité induit un risque important sur son Service, il peut prévoir une durée de vie et une demande de réauthentification de l'utilisateur dans un délai plus restrictif.

EXI RIE-PS 14
Le *Fournisseur de Service* DOIT définir, selon les risques et les contraintes propres au Service, le délai d'inactivité entrainant la fermeture de la session applicative de l'*Utilisateur* sur le Service, en s'assurant que la durée de vie d'une session applicative n'excède pas celle de la session du Fournisseur d'identité utilisé.

Un Utilisateur est souvent amené à s'authentifier sur plusieurs Services numériques, que ce soit successivement, en parallèle ou par des appels entre Services numériques. La mise en place de solution d'authentification unique (SSO) ou de propagation de sessions authentifiées évite à l'*Utilisateur* de réaliser de multiples Identifications électroniques en vue de l'interopérabilité entre les Services. Ces mécanismes doivent toutefois être évalués et contrôlés afin d'éviter l'apparition de failles de sécurité.

EXI RIE-PS 15
Le *Fournisseur de Service* DOIT s'assurer que la propagation d'une identité numérique d'un Utilisateur, entre ses Services ou avec des Services d'un autre Fournisseur de Service, s'effectue au sein d'un même *Schéma d'Identification électronique*.

Ce mécanisme de propagation d'identité au sein d'un même Schéma d'Identification électronique est par exemple le cas de l'espace de confiance pour la mise en œuvre des API Pro Santé Connectées.

2.4.3 Continuité d'activité

Des incidents mineurs, comme la perte ou l'oubli d'un Moyen d'Identification électronique ou de l'un des facteurs d'authentification, peuvent rendre impossible l'utilisation d'un Service par un utilisateur.

Des incidents majeurs, comme une coupure réseau persistante ou une défaillance matérielle ou logicielle, peuvent rendre indisponibles l'ensemble des Moyens d'Identification électronique nominaux d'un Service.

Selon la criticité et les engagements de disponibilité du Service, le Fournisseur de Service doit prévoir des Moyens d'Identification électronique de secours afin d'assurer que les utilisateurs dont les fonctions le nécessitent peuvent continuer à accéder au Service.

Dans la mesure du possible, un même dispositif d'authentification pourrait être utilisé dans différentes conditions. Par exemple, un badge ou une clé de sécurité compatible, prévu pour être utilisé avec Pro Santé Connect, peut alternativement être utilisé pour une authentification sur un Service local avec ses 2 facteurs d'authentification, même en cas d'indisponibilité de Pro Santé Connect. L'Identification sur certains Services distants sera impossible mais l'Identification locale restera ainsi conforme au référentiel.

En cas d'incident majeur rendant impossible l'utilisation des Moyens d'Identification électronique nominaux sur un Service, il peut être nécessaire d'utiliser des Moyens d'Identification électronique de secours, non conformes à l'ensemble des exigences du présent référentiel. Leur utilisation ne peut être envisagée que pour une durée transitoire, sous le contrôle du Fournisseur de Service.

EXI RIE-PS 16
Lorsque le Fournisseur de Service prévoit un Moyen d'identification électronique de secours pour garantir ses engagements de disponibilité du service, il DOIT limiter et contrôler strictement son activation et son utilisation.

Le Fournisseur de Service peut, par exemple :

- Préconiser l'activation des MIE de secours par un administrateur du Service et/ou une bascule automatique vers le MIE nominal dès qu'il est disponible ;
- Préconiser une durée maximale d'autorisation des MIE de secours inférieure ou égale à 24h ;
- Limiter les accès concernés au strict nécessaire ;
- Imposer une Identification électronique avec au moins un facteur d'authentification ;
- Conserver des traces de l'activation des MIE de secours et de l'ensemble des accès effectués avec ce mode.

L'accès à un Service par un MIE de secours peut induire des risques importants du fait de la diminution du niveau de sécurité, notamment si l'ensemble des exigences du référentiel ne sont pas respectées.

La responsabilité du Fournisseur de Service pourrait être engagée en cas d'atteinte à la sécurité des Services ou des données du fait de l'utilisation d'un MIE de secours trop peu sécurisé ou dont l'utilisation n'aurait pas été assez encadrée ou limitée dans le temps, en lien avec la cause d'indisponibilité du MIE prévu en mode de fonctionnement nominal conforme au référentiel.

3 ATTESTATION DE CONFORMITE DES SCHEMAS D'IDENTIFICATION ELECTRONIQUE

3.1 L'attestation de conformité

L'établissement et la signature de l'attestation de conformité est une démarche visant à évaluer formellement le niveau de conformité des Schémas d'Identification électronique mis en œuvre par un Fournisseur d'identité, par rapport aux exigences du présent référentiel. En cas de non-conformité, des réserves sont acceptables temporairement mais doivent être documentées et faire l'objet d'un plan d'action.

Les risques induits par ces éventuelles réserves vis-à-vis des exigences de ce référentiel sont acceptés par le Fournisseur d'identité qui en assume la responsabilité. Celui-ci pourra notamment mettre en œuvre toutes les mesures qu'il juge nécessaires afin de mitiger ces risques le temps de mettre en œuvre le plan d'action visant à lever l'ensemble des réserves qu'il aura identifiées.

La démarche de préparation de l'attestation de conformité consiste notamment à :

- Préparer un support documentaire, à minima sous format d'une présentation synthétique et intelligible des Schémas d'Identification électronique mis en œuvre et des Services et utilisateurs concernés ;
- Tenir une commission de conformité au référentiel, avec le responsable légal de la personne morale constituant le Fournisseur d'identité (par exemple le directeur de l'établissement) ou son représentant, avec les acteurs pertinents : responsable de la sécurité des systèmes d'information (RSSI), délégué à la protection de données (DPO), direction des Services numériques ou des systèmes d'information, direction des ressources humaines, direction médicale, éditeur des Services numériques, représentants des patients, etc ;
- Faire signer par le responsable légal ou son représentant l'attestation de conformité, avec la mention "la conformité au référentiel d'Identification électronique est attestée pour [nombre] mois, [avec les (éventuelles) réserves suivantes : [réserves]]".

La durée sera à l'appréciation du responsable qui pourra utilement prononcer une conformité pour une période courte si certaines réserves nécessitent de refaire un point à brève échéance. Un rappel calendaire sera utilement programmé peu avant l'expiration pour organiser une nouvelle commission. Dans tous les cas, la durée de l'attestation de conformité ne peut excéder 3 ans, délai au bout duquel la procédure devra être obligatoirement être renouvelée ;

- Ce document est conservé et tenu à disposition des Fournisseurs de Services raccordés, ainsi que de tout organisme auditeur (CNIL, ANSSI, ANS etc.).

3.2 Nécessité de production de l'attestation de conformité

Le référentiel d'Identification électronique impose la réalisation de l'attestation de conformité pour les *Schémas d'Identification électronique* mis en œuvre pour les Fournisseurs d'identité, autre que ceux habilités comme Fournisseurs d'identité de Pro Santé Connect par l'ANS.

En effet, la procédure d'habilitation d'un Fournisseur d'identité de Pro Santé Connect repose sur la vérification par l'ANS des preuves de conformité du Fournisseur d'identité et de la solution d'IAM utilisée au référentiel d'exigences dédiées du référentiel Pro Santé Connect, qui intègrent, voire dépassent les exigences de sécurité du présent référentiel.

Un délai est fixé pour la réalisation de la première attestation de conformité afin de lancer si nécessaire un plan de mise en conformité de l'Identification électronique sur les Services numériques.

EXI RIE-PS 17

Le *Fournisseur d'identité* DOIT produire une attestation de conformité des *Schémas d'Identification électronique* sur lesquels reposent les Moyens d'Identification électronique qu'il fournit, au plus tard le 31/12/2026, excepté dans les cas suivants :

- Le Schéma d'Identification électronique est basé sur Pro Santé Connect ;
- Le Schéma d'Identification électronique est opéré par un Fournisseur d'identité de Pro Santé Connect habilité par l'ANS.

En cas de réserve sur le respect d'une ou plusieurs exigences du référentiel, l'attestation de conformité doit lister, à minima, pour chaque Schéma d'Identification électronique concerné : le numéro de l'exigence, la description des réserves ainsi que le plan d'action et le délai prévu pour les lever.

Les réserves ne peuvent induire des faiblesses avec un impact significatif sur la sécurité du Schéma d'Identification électronique. Par exemple, les réserves pouvant entrainer un impact significatif sont :

- La mise en œuvre comme unique facteur d'authentification d'un mot de passe faible, c'est-à-dire avec un niveau d'entropie inférieur à 50 bits (exemple : lorsqu'un mot de passe de 6 caractères est accepté) ;
- La mise en œuvre comme unique facteur d'authentification d'un mot de passe sans mise en œuvre de mesures de restriction d'accès après plusieurs échecs d'authentification (exemple : temporisation d'accès, mécanismes de type captcha, blocage du compte, etc.) ;
- La mise en œuvre d'un mot de passe comme facteur unique d'authentification sur un Service exposé sur internet ;
- L'absence de déconnexion automatique de l'utilisateur au bout d'un délai d'inactivité sur le *Service* ;
- L'impossibilité de révoquer et/ou renouveler un Moyen d'Identification électronique ;
- La possibilité pour l'utilisateur d'activer un Moyen d'Identification électronique de secours de sa propre initiative et sans la validation d'un administrateur ;

3.3 Levée des réserves

Afin de laisser le temps nécessaire aux Fournisseurs de Service ou Fournisseur d'identité pour satisfaire l'ensemble des exigences de cette nouvelle version du référentiel, des réserves seront tolérées jusqu'au 31 décembre 2028.

EXI RIE-PS 18

Le *Fournisseur d'identité* DOIT lever, au plus tard au 31/12/2028, l'ensemble des réserves de l'attestation de conformité des *Schémas d'Identification électronique* mis en œuvre en regard des exigences du présent référentiel.

3.4 Renouvellement de l'attestation

L'attestation de conformité doit être revue périodiquement afin de s'assurer qu'elle est toujours à jour et que les évolutions du Service, de son contexte ou de la menace cyber, ne remettent pas en cause la sécurité du ou des Schémas d'Identification électronique.

EXI RIE-PS 19

Le *Fournisseur d'identité* DOIT renouveler l'attestation de conformité du *Schéma d'Identification électronique* :
- Au moins une fois tous les 3 ans ;
- Au moins tous les ans en cas de présence de réserves dans la dernière attestation réalisée.

4 GLOSSAIRE

ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
CPS	Carte de Professionnel de Santé
FI	Fournisseur d'identité
FS	Fournisseur de Service
FIDO	Fast Identity Online
IAM	Identity Access Management
MIE	Moyen d'Identification électronique
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PSC	Pro Santé Connect
SIRH	Système d'Information des Ressources Humaines
RPPS	Répertoire Partagé des Professionnels intervenant dans le système de Santé
SI	Système d'Information
SSO	Single Sign-On
TOTP	Time-based One Time Password ([RFC 6238])
UE	Union Européenne