AGENCE
DU NUMÉRIQUE
EN SANTÉ

PGSSI-S

Référentiel d'identification électronique

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

Statut : Validé | *Classification : Public* | *Version : v1.0*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Documents de référence

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
[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
[RGS]	Référentiel Général de Sécurité - Version 2.0 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

Autres documents

Renvoi	Document
[AUTHENTIFICATION]	Recommandations relatives à l'authentification multifacteur et aux mots de passe (ANSSI) https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf
[CNIL-MDP]	Authentification par mot de passe : les mesures de sécurité élémentaires (CNIL) https://www.cnil.fr/fr/mot-de-passe
[CSPN]	Certification de Sécurité de Premier Niveau https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/presentation/
[EBIOS RM]	EBIOS Risk Manager https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
[ENGAGEMENT]	Engagement sur la sécurisation des modalités d'identification électronique des utilisateurs des services numériques en santé https://esante.gouv.fr
[ENTROPIE]	Calculer la « force » d'un mot de passe (ANSSI) https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

[HOMOLOGATION]	Démarche d'homologation de sécurité https://www.ssi.gouv.fr/entreprise/management-du-risque/homologation-de-securite/
[IE-ASPM]	Référentiel d'identification électronique - Acteurs des secteurs sanitaire, médico-social et social [personnes morales] https://esante.gouv.fr
[IE-CA]	Référentiel de contrôle d'accès – *à paraître* *Consulter aussi le* Guide gestion des habilitations d'accès au SI https://esante.gouv.fr
[IE-Usagers]	Référentiel d'identification électronique - Usagers https://esante.gouv.fr
[MOS-NOS]	Modèle et nomenclatures des objets de santé https://esante.gouv.fr/interoperabilite/mos-nos
[RFC 6238]	TOTP: Time-Based One-Time Password Algorithm https://tools.ietf.org/html/rfc6238.html

SOMMAIRE

1 PREAMBULE

Note : les documents cités en référence sous la forme [REF] sont détaillés au début du présent référentiel.

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 minimum de garantie attendu s'agissant des modalités d'identification électronique des utilisateurs des services numériques en santé. Le référentiel est décomposé 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]).

L'objet du présent volet est de définir les modalités d'identification électronique des personnes physiques intervenant dans les secteurs sanitaire, médico-social et social ainsi que les différents identifiants et dispositifs d'authentification utilisables pour ces personnes physiques en fonction du cadre d'usage.

Ce volet se limite à l'étape d'identification et d'authentification des professionnels personnes physiques accédant à des services numériques de santé.

L'étape d'habilitation, ou de contrôle d'accès, dans laquelle des autorisations sont données au professionnel de santé, est traitée dans un référentiel distinct (voir [IE-CA]).

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 du 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* »).

Au sein de ce périmètre, le présent volet du référentiel s'applique à l'identification électronique des acteurs, personnes physiques, en charge d'activités relevant des secteurs sanitaire, médico-social et social ainsi que des personnes exerçant sous leur autorité. L'obtention d'un moyen d'identification électronique est subordonnée à l'enregistrement préalable de ces professionnels dans le répertoire sectoriel de référence des personnes physiques mentionné à l'article L. 1470-4 du code de la santé publique.

2 DEFINITIONS ET CONCEPTS GENERAUX

2.1 Personne physique

Dans le cadre de ce document, le terme **personne physique** est utilisé pour désigner toute personne physique entrant dans le champ de ce volet du référentiel. Il s'agit donc des professionnels, personnes physiques, en charge d'activités relevant des secteurs sanitaire, médico-social et social ainsi que de l'ensemble des personnes exerçant sous leur autorité (tels que, par exemple, les préparateurs en pharmacie, les personnels du secrétariat, des prestataires, etc.).

Le terme personne physique exclut donc, dans ce document, les usagers des services numériques de santé, dont l'identification électronique est traitée au sein d'un volet du référentiel d'identification électronique dédié aux usagers (voir [IE-Usagers]).

2.2 Services numériques et services numériques partagés

Dans la suite du document, le terme **service numérique** désigne tout traitement de données de santé entrant dans le périmètre d'application défini au §1.2, par exemple :

- Un service de consultation de résultats d'examens de biologie médicale ;
- Un Dossier Patient Informatisé ;
- Une application, même interne à une structure, traitant des données de santé à caractère personnel ;
- Une plateforme de télésanté ;
- Un logiciel de gestion de cabinet.

Un service numérique de santé est considéré comme un **service partagé** s'il dépasse le cadre d'une seule personne morale, ou bien s'il est mis en œuvre à l'échelle d'un territoire ou au niveau national. Le dossier médical partagé, le dossier pharmaceutique, une solution de e-parcours, sont des exemples de services partagés.

2.3 Identification électronique

Dans ce référentiel, la locution **identification électronique**, reprise du vocabulaire du règlement [eIDAS], désigne le processus utilisé par une personne physique ou morale pour s'identifier et s'authentifier auprès d'un système d'information.

Par exemple, la saisie d'un identifiant puis d'un mot de passe, ou l'utilisation d'une carte CPx avec saisie de son code PIN, constituent une identification électronique auprès du système cible.

Lorsqu'il est spécifiquement question de l'étape d'identification (communiquer une identité) ou d'authentification (prouver cette identité), ces termes sont utilisés sans le qualificatif « électronique ».

2.4 Moyens d'identification électronique

Un **moyen d'identification électronique** (MIE) est un dispositif matériel et/ou immatériel contenant un identifiant personnel et utilisé pour s'authentifier sur un service numérique, en santé dans le présent document. 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.

Afin de préserver le niveau de sécurité déclaré d'un moyen d'identification électronique, son fournisseur et son détenteur sont tenus de respecter un ensemble de mesures de sécurité sur tout son cycle de vie. En particulier, des engagements concernant la conservation et l'utilisation du dispositif d'authentification sont rappelés au détenteur par

le fournisseur du moyen d'identification électronique, par exemple grâce à des conditions générales d'utilisation associées.

Un couple identifiant / mot de passe, une carte CPx, une application mobile d'identification électronique sont des exemples de moyens d'identification électronique.

2.5 Données d'identité

Dans le cadre de la PGSSI-S, les **données d'identité** d'une personne physique ou morale sont définies comme :
- Le ou les identifiants attribués à cette personne ;
- L'ensemble des attributs (ou traits) d'identité enregistrés associés à l'identifiant.

Les données d'identité sont collectées, validées et actualisées par des autorités d'enregistrement chargées d'établir les répertoires d'identité (cf. §2.7).

Un attribut d'identité est un élément caractérisant une personne physique ou morale mais qui n'est en règle générale pas suffisant à lui seul pour définir l'identité de cette personne. Les attributs d'identité sont considérés au sens large et correspondent à l'ensemble de données collectées lors de l'enregistrement d'une personne physique ou morale. À titre d'exemple non limitatif, on peut citer :

- Pour les personnes physiques :
  - Le nom de naissance ;
  - Le prénom ;
  - La date de naissance;
  - L'adresse ;
  - La profession.
- Pour les personnes morales :
  - La dénomination ;
  - Le type de structure ;
  - La date de création ;
  - L'adresse.

Selon le répertoire d'identité d'où elles sont issues (voir au §2.7), les données d'identité collectées peuvent être plus ou moins nombreuses et de nature diverse. Cependant, elles doivent être suffisantes pour caractériser l'identité d'une personne, permettre de la différencier des autres personnes notamment celles qui partagent une partie de ces attributs d'identité (ex. : homonymes) et ainsi faire un lien univoque entre un identifiant et l'identité de la personne à laquelle il a été attribué.

2.6 Identifiant

Un **identifiant** est un attribut donné dans le cadre d'un répertoire d'identité (voir au §2.7) à une personne physique ou morale, en lien avec son identité, permettant de différencier deux personnes même dans le cas où leurs traits d'identité sont similaires ou très proches.

Un identifiant est constitué selon des règles propres au répertoire d'identité dont il est issu. Il peut être constitué d'une suite de caractères plus ou moins signifiants (numéro aléatoire, numéro déduit à partir de traits d'identité, concaténation de traits d'identité...).

L'enregistrement des personnes physiques ou morales dans un répertoire d'identité doit attribuer un identifiant propre à chaque personne, sans qu'il n'y ait ni doublon ni collision :

- Il y a collision d'identifiants lorsqu'un même identifiant a été attribué à deux personnes distinctes dans le répertoire ;

- Il y a doublon d'identifiants lorsque plusieurs identifiants différents sont attribués à une même personne physique ou morale dans le répertoire d'identité. Cette notion de « même personne » doit être considérée au regard des traits d'identité définis comme différenciants pour le répertoire. Par exemple, dans un répertoire sectoriel de référence dans lequel les conditions d'exercice constituent des traits d'identité différentiant, une même personne physique est susceptible d'avoir autant d'identifiants différents qu'elle a de conditions d'exercice différentes.

Il existe des identifiants nationaux, fournis par les répertoires d'identité nationaux, et les identifiants privés fournis par les répertoires d'identité privés (voir au §2.7).

2.7 Répertoires d'identité

Un répertoire d'identité est un annuaire de personnes physiques ou morales, intégrant les données d'identité de chaque personne enregistrée dans celui-ci.

Dans le cadre de la PGSSI-S, deux types de répertoires sont identifiés :

- Les **répertoires sectoriels de référence** mentionnés à l'article L. 1470-4 du code de la santé publique, qui portent sur l'identification des professionnels personnes physiques (répertoire RPPS et en transitoire ADELI) ou personnes morales (répertoire FINESS) intervenant dans les secteurs d'activité de la santé, du social et médico-social. Ils s'appuient sur les traits d'identité régaliens complétés par des traits d'identité sectoriels (ex : profession, situation d'exercice, …) ;
- Les **répertoires d'identité privés** sont des répertoires d'identité qui ne sont pas des répertoires sectoriels de référence. Leurs règles de fonctionnement sont décidées librement par le responsable de ce répertoire. Les identifiants utilisés par ce type de répertoire peuvent être des identifiants issus des répertoires sectoriels de référence (solution à privilégier) ou des identifiants privés propres.

Le répertoire partagé des professionnels intervenant dans le système de santé (RPPS) est le répertoire de référence des professionnels de santé, commun aux structures et services du secteur sanitaire médico-social français. Historiquement, il recensait uniquement les praticiens relevant de six professions à ordre (médecin, chirurgien-dentiste, sage-femme, pharmacien, masseur-kinésithérapeute et pédicure-podologue). Etendu à d'autres catégories de professionnels en 2017, l'ordonnance du 12 mai 2021 relative à l'identification électronique prévoit son extension à l'ensemble des professionnels intervenant dans les secteurs sanitaire, médico-social et social.

L'inscription d'un professionnel dans le RPPS est réalisée par des autorités d'enregistrement habilitées chargées de collecter et de vérifier les données avant de les inscrire au répertoire. Différentes autorités d'enregistrement distinctes sont définies, en fonction de la profession exercée, et proposent des modalités d'enregistrement adaptées. Les données inscrites au RPPS par les autorités d'enregistrement intègrent l'ensemble des données d'identification, de qualification (diplômes), d'activité, de mode et de structure d'exercice de chaque professionnel.

2.8 Fournisseurs de service et fournisseurs d'identité

Le **fournisseur de service** est l'entité responsable du service numérique de santé entrant dans le périmètre d'application du présent référentiel. Il identifie et authentifie les utilisateurs de son service en s'appuyant sur le fournisseur d'identité, et peut ensuite interroger un répertoire sectoriel de référence pour obtenir des informations complémentaires sur la personne identifiée. Une structure, fournisseur de service en tant que responsable de traitement au sein de son système d'information, est son propre fournisseur d'identité lorsque cette structure délivre des moyens d'identification électronique à son personnel.

Un **fournisseur d'identité** est une entité qui délivre un moyen d'identification électronique à une personne physique ou morale qui a demandé ce moyen et dont elle a établi une identité électronique fiable.

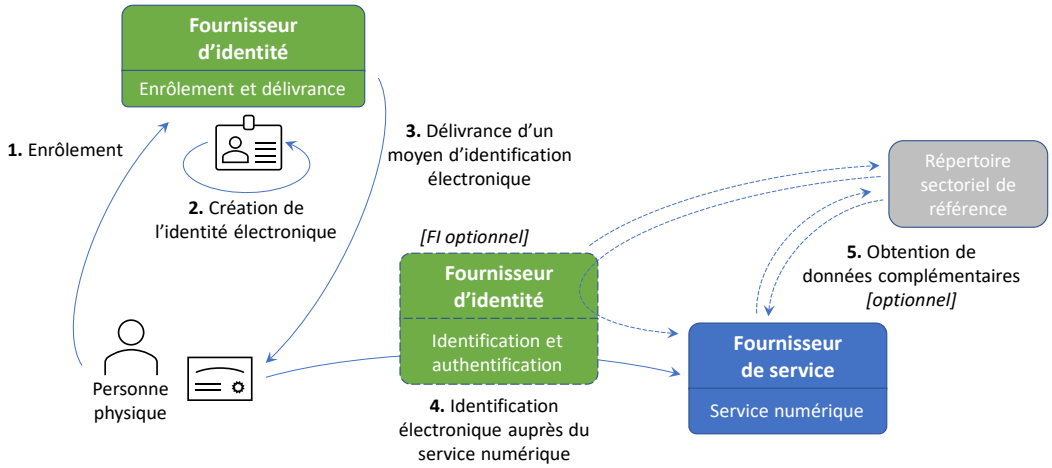
L'identité électronique est créée suite à un processus d'enrôlement au cours duquel le fournisseur d'identité vérifie l'identité du demandeur en s'appuyant sur un répertoire d'identité. Le moyen d'identification électronique est initialisé,

délivré puis géré dans le temps par le fournisseur d'identité afin de garantir le niveau de sécurité de l'identification électronique.

A titre d'exemple pour les professionnels personnes physiques :
- L'Assurance Maladie est le fournisseur du service DMP ;
- L'ANS est un fournisseur d'identité, délivrant les cartes CPx ou e-CPS comme moyen d'identification électronique ;
- Une structure mettant en place un annuaire centralisé de ses collaborateurs et y associant un moyen d'identification électronique (un mot de passe, un moyen homologué) est son propre fournisseur d'identité.

2.9 Processus d'identification électronique

Les processus liés à l'identification électronique d'une personne physique peuvent être schématisés ainsi :



Une personne physique obtient un moyen d'identification électronique auprès d'un fournisseur d'identité. Pour le cas d'une carte CPx, cette demande peut être automatique après une inscription au RPPS.

Lorsque cette personne physique initie une connexion vers le service numérique d'un fournisseur de service, elle peut utiliser son moyen d'identification électronique pour s'identifier et s'authentifier. Cette authentification est le plus souvent réalisée à travers une interface du fournisseur d'identité qui exploite et vérifie le moyen d'identification électronique présenté.

Le service peut obtenir, si nécessaire, des attributs supplémentaires d'identité de la personne physique connectée (spécialités, lieux d'exercice, …) en interrogeant un répertoire sectoriel de référence sur la base de l'identifiant obtenu pour cette personne. Certains fournisseurs d'identité ou fédérateurs de fournisseurs d'identité peuvent transmettre eux-mêmes ces données au service numérique en santé après consultation du répertoire sectoriel de référence.

Une fois l'identification électronique vérifiée, le fournisseur de service octroie à la personne physique les accès correspondant à ses habilitations (se reporter au référentiel de contrôle d'accès [IE-CA]).

Lorsque le service numérique auquel s'est connecté la personne physique accède lui-même à un second service numérique, ce dernier peut demander l'identification voire l'authentification de cette même personne physique. Dans ce cas, 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]).

2.10 Fédérateur de fournisseurs d'identité

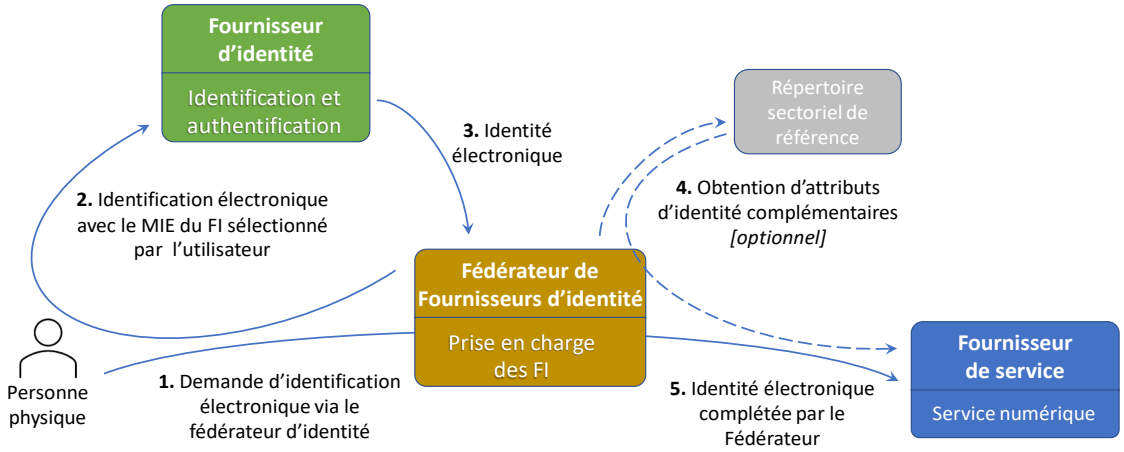
Un **fédérateur de fournisseurs d'identité** est un service d'intermédiation entre des fournisseurs d'identité et des fournisseurs de service. Il permet à un fournisseur de service de disposer d'une solution unique d'identification

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). Le fédérateur de fournisseurs d'identité peut supporter un ou plusieurs fournisseurs d'identité.

Le fédérateur de fournisseurs d'identité transmet au fournisseur de service l'identité numérique de l'utilisateur, après éventuellement l'avoir complétée avec des attributs d'identité obtenus auprès d'un répertoire sectoriel de référence.

Les nouveaux moyens d'identification électronique qui sont pris en charge par un fédérateur de fournisseurs d'identité deviennent ainsi immédiatement utilisables, et de façon transparente, pour l'identification électronique sur tous les services connectés à ce fédérateur.

Le recours à un fédérateur de fournisseurs d'identité peut, selon une vue logique, être schématisé ainsi :



Techniquement, les échanges entre la personne physique, le fédérateur et le fournisseur de service sont plus nombreux, mais ne sont pas représentés pour maintenir une bonne lisibilité du mécanisme.

Les principaux fédérateurs de fournisseurs d'identité sont :

- FranceConnect, à destination des citoyens. Ce fédérateur proposé par la direction interministérielle du numérique (DINUM) regroupe plusieurs fournisseurs d'identité publics et privés qui, chacun, propose son moyen d'identification électronique ;
- Pro Santé Connect, à destination des professionnels de santé. A ce jour, ce fédérateur ne propose que des moyens d'identification électroniques émis par un unique fournisseur d'identité : l'ANS.

3 IDENTITE ELECTRONIQUE DES PERSONNES PHYSIQUES

3.1 Identifiants

3.1.1 Identifiants nationaux du secteur de la santé

Lors d'une demande d'identification électronique d'un acteur personne physique intervenant en santé, l'usage de l'identifiant national du secteur de la santé est à privilégier lorsqu'il existe. Cet identifiant permet d'obtenir des données supplémentaires concernant la personne identifiée depuis le répertoire sectoriel de référence ayant attribué cet identifiant.

Exigence n°1
[EXI 01] Les identifiants nationaux à utiliser pour l'identification des acteurs personnes physiques intervenant en santé sont : - Soit l'identifiant RPPS, à utiliser en priorité s'il existe pour la personne à identifier ; - Soit l'identifiant ADELI, toléré de façon transitoire jusqu'à son remplacement définitif par l'identifiant RPPS pour les professions encore enregistrées dans ADELI.

Les identifiants RPPS et ADELI doivent être formatés conformément au modèle [MOS-NOS].

Après la bascule de l'enregistrement des infirmiers au RPPS en octobre 2021, les dernières professions enregistrées dans ADELI devraient également y basculer en 2022 ou en 2023 selon les cas.

Un moyen d'identification électronique peut transmettre plusieurs identifiants pour un même acteur, par exemple un identifiant national, un identifiant issu d'un référentiel local des ressources humaines ou un identifiant technique.

3.1.2 Autres identifiants

L'usage d'un identifiant issu d'un répertoire sectoriel de référence est fortement recommandé et à privilégier dans tous les cas d'usage d'identification électronique. Une identification électronique reposant uniquement sur un identifiant privé est toutefois admissible pour le cas de services numériques non sensibles ou lorsque la personne physique n'est pas éligible à l'enregistrement dans un répertoire sectoriel de référence.

Cet identifiant privé est établi par le fournisseur du moyen d'identification électronique (par exemple un matricule attribué par un SI RH, un identifiant LDAP / Active Directory, …).

Exigence n°2
[EXI 02] Un service numérique sensible obtenant uniquement un identifiant privé après une identification électronique doit : - Rechercher l'identifiant national du professionnel dès lors que celui-ci est potentiellement éligible à l'enregistrement dans un répertoire sectoriel de référence ; - Vérifier l'exactitude de cet identifiant national au minimum tous les 2 ans s'il conserve et réutilise par la suite son association avec l'identifiant privé. Cette vérification peut être réalisée par une recherche directe dans le répertoire sectoriel de référence ou par l'intermédiaire d'un autre répertoire lui-même synchronisé avec le répertoire de référence à la fréquence requise.

Les services sensibles sont définis au §4.1.2. Pour qu'un tel service puisse associer l'identifiant national du professionnel à son identifiant privé, le fournisseur de l'identité doit veiller à fournir suffisamment d'informations fiables, voire à proposer une méthode de récupération ponctuelle de cette association.

3.2 Attributs d'identité

Les attributs d'identité d'un acteur personne physique intervenant en santé sont, entre autres :

- Nom d'exercice ;
- Prénom(s) ;
- Date de naissance ;
- Pays de naissance ;
- Ville de naissance ;
- Genre ;
- Profession ;
- Rôle ;
- Situation d'exercice :
  - Mode d'exercice ;
  - Structure d'emploi :
    - Dénomination ;
    - Identifiant ;
    - Coordonnées ;
    - Catégorie juridique.

D'autres attributs des acteurs intervenant en santé sont présents dans les répertoires d'identité. Ils sont décrits dans le Modèle des objets de santé, le MOS (voir [MOS-NOS]).

Certains de ces attributs peuvent être intégrés à l'identité électronique communiquée au fournisseur de service, qui peut en obtenir d'autres dans le répertoire sectoriel de référence (ou à défaut dans un répertoire privé) associé à l'identifiant du professionnel.

Le nom d'exercice est le nom sous lequel les personnes physiques sont enregistrées dans les répertoires sectoriels. Ce nom peut être différent du nom de naissance ou du nom d'usage sous lequel est enregistrée une personne physique dans un répertoire national régalien, basé par exemple sur l'état civil (voir au §2.7).

4 MOYENS D'IDENTIFICATION ELECTRONIQUE

4.1 Sélection des moyens d'identification électronique

4.1.1 Analyse de risque et sensibilité des services numériques

Le fournisseur d'un service numérique de santé est responsable du choix des moyens d'identification électronique, parmi ceux listés par le présent référentiel, qu'il autorise sur son service et des mesures de sécurité encadrant le processus d'identification et d'authentification.

Ces choix doivent être pris en regard d'une analyse de risque concernant le service proposé, et prenant explicitement en compte la protection des données de santé à caractère personnel qui y sont traitées. Ceci comprend en particulier la garantie de confidentialité des données (que ce soit un vol massif de données par un attaquant externe, ou la consultation plus ou moins étendue de données par un professionnel, un usager ou un autre type d'intervenant) ainsi que d'intégrité de ces données (modification non autorisée ou accidentelle des données). L'analyse de risque doit couvrir l'ensemble des accès potentiels aux données, qu'ils soient fonctionnels (utilisateurs du service) ou techniques (personnels en charge de la construction et de la maintenance du système d'information et applications de maintenance). Il est fortement recommandé de mener l'analyse de risque selon une méthodologie formalisée et éprouvée, telle que la méthode EBIOS RM (voir [EBIOS RM]) proposée par l'ANSSI.

Pour rappel, les autorités administratives doivent appliquer le Référentiel Général de Sécurité ([RGS]) pour la sécurisation de leurs échanges avec d'autres autorités administratives ou avec des usagers. L'analyse de risque et le choix des moyens d'identification électronique pour ces échanges font partie de la démarche imposée par le référentiel RGS. Une autorité administrative, qui serait de plus une personne morale acteur des secteurs sanitaire, médico-social et social assujettie au présent référentiel, est donc tenue de respecter les deux référentiels.

Le présent référentiel fixe des contraintes applicables en premier lieu pour les services considérés comme les plus sensibles. Ces exigences, dans le cadre de la PGSSI-S, garantissent un niveau de sécurité homogène et considéré comme minimal pour répondre aux exigences règlementaires en vigueur. Le fournisseur du service numérique de santé est libre d'implémenter des mesures de sécurité additionnelles qu'il jugerait nécessaires au regard de son analyse de risque.

Ce volet du référentiel s'applique à l'identification électronique de l'ensemble des acteurs personnes physiques intervenant en santé qui utilisent ces services (y compris les préparateurs en pharmacie, secrétariats médicaux, sous-traitants, prestataires, etc.). L'identification électronique des administrateurs techniques du système d'information devraient respecter des contraintes cohérentes (en particulier une authentification à double facteur) en cohérence avec les résultats de l'analyse de risque. L'identification électronique sur des automates ou appareils médicaux connectés (analyses, imagerie…) est considérée hors périmètre du fait des contraintes spécifiques de ces matériels.

4.1.2 Services numériques dits « sensibles »

L'objectif ciblé à terme et décliné par ce référentiel est d'atteindre, pour l'identification électronique des acteurs personnes physiques intervenant en santé, un niveau de sécurité équivalent au niveau de garantie substantiel des identités électroniques eIDAS. Dans cette optique, des critères de sélection des services considérés sensibles et un calendrier de déploiement sont définis ci-dessous.

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 qui appartiennent au moins à l'une des catégories suivantes :

- Les services partagés, définis comme dépassant le cadre d'une personne morale et/ou mis en œuvre à l'échelle d'un territoire ou au niveau national (ex : dossier médical partagé, plateforme de e-parcours, dossier pharmaceutique, etc.) ;
- Par transitivité, les services numériques qui intègrent des services partagés (ex : dossier patient informatisé, système de gestion de laboratoire, système d'information de radiologie, boites de messageries sécurisées de santé, etc.) ;
- Les services proposant un accès web externe aux SI, pour les professionnels d'un établissement (ex : services accessibles en mobilité ou télétravail) ou leurs correspondants de ville ;
- Les services non partagés mais qui intègrent des traitements de données ou des accès de grande échelle, définis comme les situations où :
  - Soit le nombre de patients dont les données sont nouvellement référencées dépasse 10 000 par an ;
  - Soit le nombre de professionnels distincts s'identifiant électroniquement dépasse 1 000 par an.

Exigence n°3

[EXI 03] Les moyens d'identification électronique autorisés pour accéder aux services sensibles doivent être limités :
- Aux moyens d'identification électronique disponibles sous Pro Santé Connect ;
- À la carte CPx ;
- À des moyens d'identification électronique homologués pour cet usage ;
- À des moyens d'identification électronique certifiés de niveau de garantie eIDAS substantiel ou élevé, et associés à un identifiant conforme aux exigences du référentiel.

Les moyens d'identification électronique de transition, tels que définis dans le présent référentiel, sont néanmoins autorisés jusqu'au 31 décembre 2025 au plus tard, sous réserve que les risques résiduels associés à leur utilisation soient considérés comme acceptables par le responsable du service numérique.

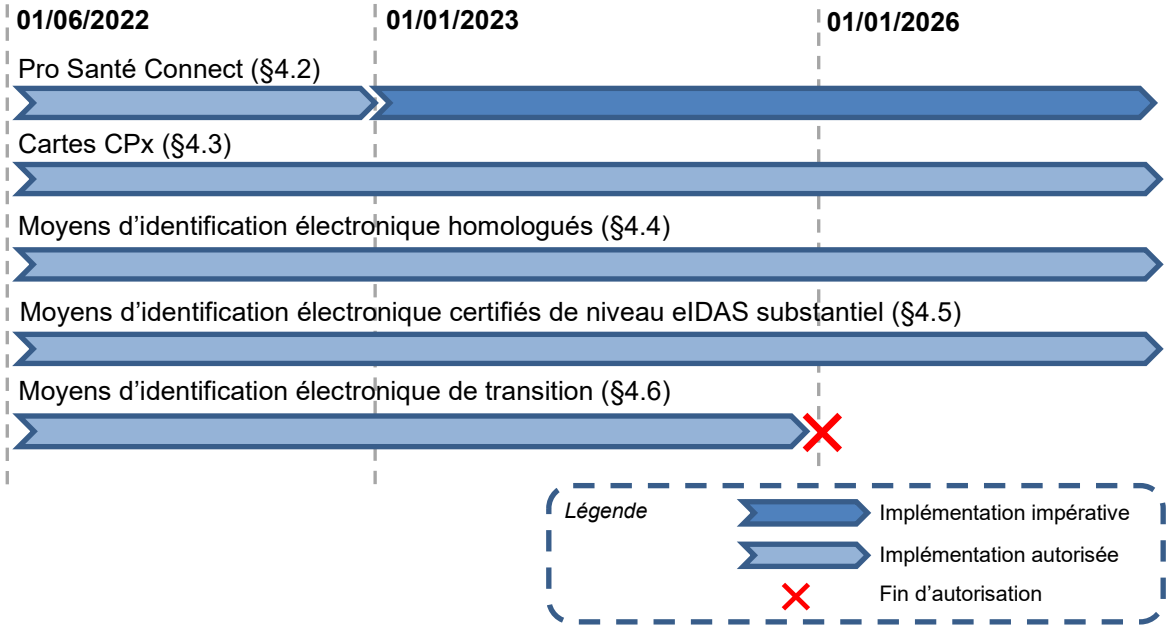
Les différents moyens autorisés sont les suivants :

- Le fédérateur d'identité Pro Santé Connect est la solution à privilégier en règle générale du fait de son interopérabilité. Son implémentation étant rendue obligatoire à brève échéance pour certains services numériques en santé, il sera largement disponible et permettra aux fournisseurs de services numériques en santé de s'abstraire des mécanismes techniques propres au dispositif d'authentification utilisé par la personne physique. Le niveau de sécurité de Pro Santé Connect est directement supervisé par l'ANS, qui vise à terme une certification eIDAS de niveau substantiel par l'ANSSI ;
- Les cartes e-CPS répondent bien aux besoins en mobilité alors que les cartes CPx sont adaptées à un poste de travail. Comme Pro Santé Connect, ces deux moyens ne sont pas certifiés par l'ANSSI mais l'ANS vise à terme une conformité de niveau substantiel eIDAS ;
- Les moyens d'identification électronique homologués par un fournisseur de service numérique en santé ont vocation à répondre à des problématiques locales d'une entité, par exemple d'ergonomie ou d'urbanisation du SI, dans un contexte spécifique et maîtrisé. Ces moyens sont utilisés en complément des moyens mis à disposition par l'ANS. Le fournisseur de service qui les homologue est chargé de juger de l'adéquation entre le niveau de sécurité effectivement offert et les risques identifiés sur son service. Un audit de conformité au niveau substantiel eIDAS est demandé ;
- Les moyens d'identification électronique certifiés de niveau de garantie eIDAS substantiel ou élevé, et associés à un identifiant sectoriel peuvent répondre à des besoins non couverts par les moyens mis à disposition par l'ANS, et peuvent être utilisés de façon plus large que les moyens homologués puisqu'ils peuvent avoir une portée nationale. La certification du moyen d'identification électronique apporte des garanties sur l'enrôlement initial et sur le dispositif d'authentification. La garantie d'exactitude et de pérennité du lien avec une identité sectorielle est à apprécier au cas par cas.

Il est recommandé aux fournisseurs de services de rendre les services numériques en santé compatibles avec plusieurs moyens d'identification électronique. Les structures responsables de plusieurs services numériques sont invitées à délivrer leur propre moyen d'identification électronique homologué. Ceci permettra d'améliorer l'ergonomie de l'identification électronique en autorisant le choix du moyen le plus adapté au contexte d'utilisation, et aussi de favoriser la disponibilité en disposant de moyens alternatifs en cas d'indisponibilité de l'un d'entre eux.

Exigence n°4
[EXI 04] Les services sensibles devront a minima avoir implémenté l'identification électronique par Pro Santé Connect au 1er janvier 2023 au plus tard.

Le calendrier d'implémentation des moyens d'identification électronique pour les services sensibles est schématisé ci-dessous :



4.1.3 Services numériques non sensibles

Pour les services qui ne sont pas considérés comme faisant partie des services « sensibles », les exigences de ce volet du référentiel d'identification électronique deviennent des recommandations qu'il est souhaitable d'appliquer, en particulier pour préparer un probable renforcement du niveau de sécurité attendu.

4.2 Pro Santé Connect et e-CPS

4.2.1 Généralités

Pro Santé Connect est le fédérateur de fournisseurs d'identité mis à disposition par l'ANS pour l'identification électronique des acteurs personnes physiques intervenant en santé. Il offre le choix de plusieurs moyens d'identification électroniques pour la personne physique, et transmet au service de santé cible une identité électronique complétée par les données des répertoires sectoriels de référence.

A ce jour, tous les moyens d'identification électronique disponibles dans Pro Santé Connect satisfont aux exigences de sécurité demandées par ce référentiel, y compris pour les services « sensibles » (tels qu'identifiés au §4.1.2).

A terme, Pro Santé Connect indiquera les niveaux de garantie de l'enrôlement et du mécanisme d'authentification du moyen d'identification électronique utilisé par l'acteur intervenant en santé.

Exigence n°5
[EXI 05] Les services sensibles ne doivent accepter, parmi les moyens d'identification électronique fournis par Pro Santé Connect, que ceux de niveau substantiel ou supérieur dès lors que ce niveau est précisé.

Pro Santé Connect implémente le standard OpenID Connect (tout comme FranceConnect). Des détails d'implémentation sont fournis en ligne par l'ANS[1].

4.2.2 Identité électronique

Pro Santé Connect fournit au service de santé cible une identité électronique composée des données suivantes :

- Identifiant national du professionnel de santé ;
- Nom d'exercice ;
- Prénom ;
- Ensemble des données du répertoire sectoriel de référence pour le PS identifié (professions, activités, structures d'exercice…).

4.2.3 Moyens d'identification électronique

Pro Santé Connect supporte à ce jour :

- Un seul Fournisseur d'Identité : l'ANS ;
- Deux moyens d'identification électronique :
  - Les carte CPx (CPS RPPS, CPS ADELI, CPF, CPE libérale, CPE structure, ...) ;
  - L'application mobile e-CPS.

D'autres moyens d'identification électroniques pourront compléter cette offre à l'avenir. En particulier, des moyens d'identification électronique de niveau de garantie eIDAS substantiel ou élevé (tels que ceux présents sous FranceConnect) sont susceptibles d'être ajoutés à Pro Santé Connect si un lien fiable est réalisé avec l'identité issue d'un répertoire sectoriel de référence.

L'utilisation de la carte CPS pour s'authentifier au travers de Pro Santé Connect se fait de façon classique par saisie du code PIN associé à la carte insérée dans un lecteur. Le bénéfice de Pro Santé Connect est toutefois ici de proposer une interface unique au service numérique pour l'authentification de ses utilisateurs, sans avoir à implémenter les spécificités de chaque moyen.

Pro Santé Connect est le seul portail permettant d'utiliser l'application e-CPS qui dématérialise la carte CPS en la transposant sur téléphone mobile. Le professionnel doit avoir au préalable initialisé son e-CPS en suivant les consignes d'enregistrement données par ailleurs par l'ANS.

Les deux moyens d'identification électroniques, carte CPS et e-CPS, produisent une identification électronique totalement équivalente du point de vue du service de santé sur lequel la connexion est réalisée. Le professionnel est libre d'utiliser le moyen qui lui convient le mieux si les circonstances lui autorisent le choix.

[1] https://integrateurs-cps.asipsante.fr/pages/prosanteconnect/presentation-generale

4.3 Dispositifs de la famille CPx

4.3.1 Généralités

La carte CPS ou Carte de Professionnel de Santé est une carte d'identité professionnelle électronique dédiée aux secteurs de la santé et du médico-social. Elle permet à son titulaire d'attester de son identité et de ses qualifications professionnelles, et de façon générale, de sécuriser les échanges des données de santé à caractère personnel.

Les professionnels de santé peuvent obtenir une carte CPS. D'autres professionnels peuvent obtenir des cartes adaptées à leur situation :

- Carte de Personnel d'Etablissement (CPE) ;
- Carte de Directeur d'Établissement (CDE) ;
- Carte de Personnel Autorisé (CPA ou CDA) ;
- Carte de Personnel en Formation (CPF).

L'ensemble de ces cartes sont désignées sous l'appellation générique de carte CPx.

4.3.2 Identité électronique

Les certificats présents sur la carte portent les données d'identité suivantes du professionnel personne physique :

- L'identifiant national sectoriel de la personne lorsque la personne est éligible à l'enregistrement dans ce type de répertoire, ou un identifiant privé à défaut ;
- Le prénom et le nom d'exercice de la personne ;
- La profession ou une mention appropriée à la situation de la personne (personnel santé ou social, personnel autorisé…) ;
- Optionnellement :
  - L'identifiant et le nom de la structure à laquelle est rattaché la personne ;
  - La spécialité ;
  - Les tableaux sur lesquels un pharmacien est inscrit.

L'identifiant national sectoriel permet de retrouver les données d'identité de la personne dans le répertoire d'identité dont est issu l'identifiant. Cette recherche est à la charge du service numérique cible de l'identification électronique lorsque celui-ci utilise directement la carte CPx, et sinon elle peut être réalisé par le fournisseur d'identité ou le fédérateur de fournisseurs d'identité auquel a été déléguée cette identification électronique.

4.3.3 Cartes CPx autorisées

Exigence n°6
[EXI 06] L'ensemble des cartes de la famille CPx (CPS, CPF, CPE/CDE et CPA/CDA) peuvent être utilisées pour l'identification électronique de leur porteur lors de l'accès à un service numérique en santé. Pour le cas d'une carte non nominative, il revient au fournisseur de service de définir s'il accepte ou non ce type d'identification.

Selon le protocole d'authentification proposé par le service, c'est le certificat d'authentification ou de signature de la carte qui est exploité, après saisie du code PIN.

Les cartes CPx disposent de plus d'une puce sans contact, qui peut être utilisée pour le contrôle d'accès physique ou logique, sans saisie du code PIN de la carte. Il s'agit alors d'une authentification à un seul facteur, qui ne satisfait pas les exigences de sécurité exigées pour l'accès aux services numériques en santé.

Exigence n°7
[EXI 07] La puce sans contact d'une carte CPx ne peut être utilisée pour réaliser une identification électronique que dans le cadre d'un moyen d'identification électronique homologué ou de transition.

4.4 Moyens d'identification électronique homologués

4.4.1 Homologation

Dans le cadre de ce référentiel, un fournisseur de service numérique en santé peut homologuer, selon les modalités exposées ci-dessous, tout moyen d'identification électronique qui respecte strictement les exigences décrites dans ce chapitre, en particulier celles définies par règlement d'exécution européen pour le niveau de garantie substantiel.

Exigence n°8
[EXI 08] L'homologation d'un moyen d'identification électronique des personnes physiques accédant à un service numérique sensible est à la charge de l'entité responsable de ce service. Lorsqu'une structure délivre le MIE à ses propres collaborateurs (elle joue alors le rôle de fournisseur d'identité), elle réalise cette homologation une fois pour le compte de l'ensemble des services numériques sensibles dont elle est responsable.

Exigence n°9
[EXI 09] L'homologation d'un moyen d'identification électronique doit garantir que : - Le niveau de sécurité atteint avec l'utilisation de ce moyen est conforme aux objectifs de sécurité issus de l'analyse de risque des services numériques en santé pour lesquels il est utilisé ; - Le MIE est conforme aux exigences portant sur un moyen d'identification électronique de niveau de garantie substantiel ou élevé du règlement eIDAS (cf. [eIDAS-MIE]).

Exigence n°10
[EXI 10] L'homologation du moyen d'identification électronique doit être réalisée par le responsable d'un service numérique sensible une fois tous les 4 ans et au maximum 2 ans après tout changement du référentiel européen d'exigences pour les identités électroniques, en s'appuyant sur la démarche décrite par l'ANSSI (cf. [HOMOLOGATION]). Cette homologation doit s'appuyer sur : - Un audit de conformité au référentiel européen d'exigences pour les identités électroniques de niveau substantiel et au exigences concernant un moyen d'identification électronique homologué dans le présent référentiel ; - Une analyse de risque du système d'information de gestion du moyen d'identification électronique ; - Une évaluation technique de la sécurité du dispositif d'authentification. La décision d'homologation ainsi que les pièces listées ci-dessus sont à communiquer à l'ANS.

Les moyens d'identification électronique ainsi homologués peuvent par exemple être utilisés pour assurer l'authentification au sein d'un établissement de santé. Toutefois, aucun autre fournisseur de service n'est tenu d'accepter ces dispositifs pour l'identification électronique, chacun devant effectuer une nouvelle homologation en prenant en compte son propre contexte et les risques inhérents à son activité s'il souhaite accepter ces dispositifs.

L'ANS publie sur son site internet un guide décrivant les principes à respecter dans le cadre de l'homologation. Les modalités d'envoi des documents d'homologation seront précisées dans l'espace de publication de la PGSSI-S.

4.4.2 Identité électronique

Exigence n°11
[EXI 11] L'identifiant de personne physique fourni par un moyen d'identification électronique homologué doit être : - L'identifiant issu d'un répertoire sectoriel de référence (RPPS pour la quasi-totalité des cas) lorsque la personne est éligible à l'enregistrement dans ce type de répertoire ; - A défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

Les exigences spécifiées au §3.1 concernant les identifiants sont applicables, comme pour rappel la possibilité pour un moyen d'identification électronique de transmettre plusieurs identifiants pour une même personne.

Exigence n°12
[EXI 12] Les attributs d'identité fournis par un moyen d'identification électronique homologué doivent au minimum comprendre : - Le nom d'exercice ; - Le prénom d'exercice.

Il est recommandé que les informations suivantes soient aussi communiquées dans le cas où elles peuvent être garanties par le fournisseur d'identité :

- Rôle (pour cette identification électronique) ;
- Secteur d'activité (pour cette identification électronique) ;
- Nom et identifiant de la structure d'exercice (pour cette identification électronique).

Il est recommandé de formater les attributs selon les règles du référentiel [MOS-NOS]

4.4.3 Moyens d'identification électronique

Exigence n°13
[EXI 13] Le dispositif d'authentification délivré comme moyen d'identification électronique homologué doit posséder, par conception, un niveau de sécurité compatible avec le niveau de confiance global accordé à l'identité électronique transmise. Le référentiel européen d'exigences pour les identités électroniques de niveau de garantie eIDAS substantiel indique en particulier : - 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 ; - La diffusion de données d'identification personnelle est précédée d'une vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique ; - Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il soit hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire au mécanisme d'authentification.

Ces exigences reposent pour une part sur les caractéristiques intrinsèques du dispositif, matériel ou logiciel, d'authentification, et pour une autre part sur le mécanisme d'authentification. Pour cette raison, l'homologation du moyen d'identification électronique doit intégrer une évaluation technique de la sécurité du dispositif et du mécanisme d'authentification. Celle-ci doit s'assurer que l'authentification ne présente pas de vulnérabilité exploitable dans le cadre d'utilisation prévu et pour le niveau de sécurité visé.

Il est recommandé au fournisseur de service de s'appuyer sur des rapports d'évaluation déjà existants, de type visa de sécurité de l'ANSSI (certification [CSPN], qualification). L'évaluation de sécurité peut aussi être menée ou

commanditée par le fournisseur de service s'il n'existe pas de résultats disponibles pour le dispositif visé ou si les conditions d'évaluation ayant produit ces résultats ne correspondent pas à l'environnement d'utilisation prévue du dispositif.

Certains cas d'usage peuvent présenter des contraintes spécifiques (changement fréquent de poste de travail par exemple, services de réanimation, services d'accueil aux urgences, etc.) pour lesquelles l'authentification systématique à deux facteurs n'est pas réalisable en pratique.

Exigence n°14

[EXI 14] Un fournisseur de service peut autoriser une authentification par un seul des deux facteurs du moyen d'identification électronique homologué aux conditions cumulatives suivantes :

- Que les cas d'usages soient formellement identifiés par le fournisseur de service ;
- Qu'une analyse de risque identifie les risques induits par cette autorisation et garantisse que ceux-ci sont acceptables dans le contexte des cas d'usage ;
- Qu'une authentification nominale avec les deux facteurs d'authentification ait été réalisée précédemment dans le délai minimal jugé compatible avec les contraintes du cas d'usage ;
- Que le facteur utilisé soit l'un des deux facteurs du moyen d'identification électronique utilisé précédemment.

La décision d'homologation du moyen d'identification électronique visée au §4.4.1 doit explicitement prendre en compte les cas d'usage concernés.

4.5 Moyens d'identification électronique certifiés de niveau eIDAS substantiel ou élevé

4.5.1 Généralités

Le Règlement eIDAS [eIDAS] définit pour les moyens d'identification électronique trois niveaux de garantie : faible, substantiel et élevé. Un règlement d'exécution européen n°2015/1502 [eIDAS-MIE] a ensuite précisé les exigences applicables (spécifications techniques et procédures minimales) pour chacun de ces niveaux.

Exigence n°15

[EXI 15] L'identification électronique pour accéder à un service numérique en santé est autorisée avec un moyen d'identification électronique certifié conforme au règlement d'exécution n°2015/1502 pour le niveau de garantie eIDAS substantiel ou élevé.

Il est a priori proscrit d'utiliser pour cet usage des moyens d'identification électronique à destination des citoyens (FranceConnect, ApCV, etc.), afin de conserver une séparation franche entre les sphères professionnelles et personnelles, ainsi que pour permettre d'avoir une gestion de l'identité sectorielle. Le recours ponctuel à un moyen d'identification électronique délivré à titre personnel peut cependant être prévu à l'enrôlement d'une personne physique, ou par exemple pour un renouvellement après une révocation en urgence du moyen d'identification électronique à usage professionnel.

Sont ainsi autorisés des moyens d'identification électronique à usage professionnel parmi les catégories suivantes :

- Les moyens notifiés par tout Etat Membre de l'UE (au titre de l'identité électronique de citoyens) au niveau substantiel ou élevé ;
- En France, les moyens d'identification électronique ayant obtenu une attestation de conformité délivrée par l'ANSSI au titre du règlement eIDAS ou de l'article L102 du Code des postes et des communications électroniques.

4.5.2 Identité électronique

Exigence n°16
[EXI 16] Lors de l'enrôlement sur un service numérique en santé d'une personne physique voulant utiliser un moyen d'identification électronique certifié de niveau eIDAS substantiel ou élevé, le fournisseur de service doit associer la personne enrôlée à : - L'identifiant issu d'un répertoire sectoriel de référence (RPPS pour la quasi-totalité des cas) lorsque la personne est éligible à l'enregistrement dans ce type de répertoire ; - A défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

Cela peut se faire par confrontation des traits d'identité de la personne avec ceux disponibles au répertoire sectoriel de référence ou par présentation de la carte CPS ou e-CPS par le professionnel de santé. Le fournisseur de service est responsable de la définition des modalités de cet enrôlement et de la création de ce lien.

Les exigences spécifiées au §3.1 concernant les identifiants sont applicables, comme pour rappel la possibilité pour un moyen d'identification électronique de transmettre plusieurs identifiants pour une même personne.

Exigence n°17
[EXI 17] Les attributs d'identité fournis par un moyen d'identification électronique certifié de niveau eIDAS substantiel ou élevé doivent au minimum comprendre : - Nom de famille ; - Prénom (s) ; - Date de naissance.

Il est recommandé que le service recherche aussi dans ce répertoire des attributs supplémentaires et actualisés de l'identité de l'utilisateur, tels que :

- Nom d'exercice :
- Professions, activités, structures d'exercice ;
- Rôle (pour cette identification électronique) ;
- Secteur d'activité (pour cette identification électronique) ;
- Nom et identifiant de la structure d'exercice (pour cette identification électronique).

Il est à noter que les données d'identité fournies par un moyen d'identification électronique notifié au niveau Européen ou certifié par l'ANSSI intègrent potentiellement des données supplémentaires telles que le lieu de naissance, le genre voire dans certains cas l'adresse personnelle actuelle. Il appartient au fournisseur de service de s'assurer que la personne est informée et non opposée à ce transfert d'information (le cas échéant), ainsi que d'informer clairement ces personnes du traitement effectué sur leurs données.

4.5.3 Moyens d'identification électronique

Les moyens d'identification électronique conformes sont les moyens à usage professionnel parmi :

- La liste des moyens d'identification électronique notifiés publiée par la Commission Européenne[2].
- La liste des moyens d'identification électroniques certifiés par l'ANSSI disponible sur son site institutionnel[3].

[2] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[3] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

4.6 Moyens d'identification électronique de transition

4.6.1 Généralités

Avant de parvenir à la généralisation de l'identification électronique par un moyen d'identification électronique de niveau de garantie eIDAS substantiel, la sécurité des accès aux services numériques traitant de données de santé à caractère personnel doit être progressivement renforcée. Dans cet objectif, ce référentiel définit des moyens d'identification électronique dits « de transition » qui apportent un niveau de sécurité considéré comme minimal étant donné la nature des informations à protéger et l'état de l'art en la matière. Les exigences de sécurité associées à ces moyens d'identification électronique sont exposées ci-dessous.

Il n'est pas demandé que ces moyens d'identification électronique aient obtenu une certification ou une attestation de conformité à un quelconque niveau de garantie eIDAS. Le principe est cependant de viser une conformité au niveau de garantie eIDAS faible (exigences définies dans [eIDAS-MIE]), complété par plusieurs exigences complémentaires détaillées ci-après. Le fournisseur de service peut délivrer et gérer lui-même les moyens d'identification électronique de son service ou s'appuyer sur des solutions mutualisées.

Le fournisseur d'un service numérique de santé est responsable des mesures de sécurité mises en œuvre pour la protection des données de santé à caractère personnel. Ainsi, ce référentiel encourage l'adoption d'un moyen d'identification électronique de niveau substantiel à brève échéance. Chaque fournisseur doit prendre en compte dans sa décision, par exemple via une analyse de risque, les spécificités de son service, le type et la volumétrie des données traitées.

4.6.2 Identité électronique

4.6.2.1 Identifiant

Exigence n°18
[EXI 18] L'identifiant de personne physique fourni par un moyen d'identification électronique de transition doit être : - De préférence un identifiant issu d'un répertoire sectoriel de référence (RPPS pour la quasi-totalité des cas) ; - A défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

Les exigences spécifiées au §3.1 concernant ces types d'identifiants sont applicables, comme pour rappel la possibilité pour un moyen d'identification électronique de transmettre plusieurs identifiants pour une même personne.

4.6.2.2 Attributs d'identité

Exigence n°19
[EXI 19] Les attributs d'identité fournis par un moyen d'identification électronique de transition doivent au minimum comprendre : - Nom d'exercice ; - Prénom d'exercice.

Il est recommandé que le service recherche également dans le répertoire sectoriel de référence, à partir de l'identifiant national de l'acteur intervenant en santé, des attributs supplémentaires et actualisés de l'identité de l'utilisateur, tels que :

- Professions, activités, structures d'exercice ;
- Rôle (pour cette identification électronique) ;
- Secteur d'activité (pour cette identification électronique) ;
- Nom et identifiant de la structure d'exercice (pour cette identification électronique).

Il est recommandé de formater les attributs selon les règles du référentiel [MOS-NOS].

4.6.3 Moyens d'identification électronique

4.6.3.1 Introduction

La fiabilité de l'identification électronique repose en particulier sur :

- Le processus d'enrôlement et de vérification d'identité ;
- Les processus de gestion du moyen d'identification électronique délivré (délivrance, renouvellement…) ;
- La sécurité du dispositif et du mécanisme d'authentification.

Le mécanisme d'authentification doit garantir un niveau de sécurité adapté au contexte. Ce référentiel distingue ainsi les accès locaux et les accès à distance.

Un moyen d'identification électronique de transition doit être d'un niveau minimum de garantie eIDAS faible (cf. [eIDAS-MIE]), Les chapitres ci-dessous détaillent ou apportent des compléments d'exigences pour les différents processus et facteurs d'authentification mis en œuvre.

4.6.3.2 Processus d'enrôlement et de gestion du moyen d'identification électronique

Le processus d'enrôlement doit garantir l'exactitude des données de l'identité électronique en mettant en place des vérifications.

Exigence n°20
[EXI 20] Le processus d'enrôlement pour l'obtention d'un moyen d'identification électronique de transition doit répondre aux exigences suivantes : - L'enrôlement de la personne physique doit se baser sur une vérification de l'identité du professionnel concerné, par exemple par l'une des méthodes suivantes : ○ En se basant sur l'identification électronique de la personne via Pro Santé Connect ou FranceConnect ; ○ Par la vérification d'une pièce d'identité, numérisée ou non, éventuellement confrontée (manuellement ou automatiquement) à une photo de l'utilisateur, à une visioconférence ou à un face-à-face physique ; ○ Par l'envoi d'un lien de confirmation sur la boîte de messagerie du professionnel dans l'espace de confiance MSSanté. - 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 (RPPS), lorsque la profession est couverte dans son périmètre.

Les processus de gestion du moyen d'identification électronique doivent couvrir le cycle de vie complet de celui-ci :

Exigence n°21

[EXI 21] Les processus de gestion d'un moyen d'identification électronique de transition doivent respecter les exigences suivantes :

- Les informations obtenues par la vérification d'identité initiale ne peuvent être modifiées qu'après une nouvelle vérification au moins aussi fiable ;
- Un renouvellement régulier du moyen d'identification électronique doit être prévu afin de s'assurer de l'identité du détenteur du moyen et du maintien à l'état de l'art des garanties de sécurité (par exemple concernant la longueur d'un mot de passe ou d'une clé cryptographique) ;
- Le détenteur et le gestionnaire du moyen d'identification électronique doivent pouvoir à tout moment révoquer ce moyen, afin d'empêcher son éventuelle utilisation frauduleuse (par exemple après la compromission de ce moyen).

4.6.3.3 Authentification lors d'un accès à distance

Lorsqu'un professionnel accède à un service numérique depuis un poste connecté à Internet, en télétravail, en mobilité ou même sur le Wifi « invité » de l'établissement, la connexion est considérée comme un accès à distance. Ceci est valable même si le poste est distribué et géré par l'établissement et/ou si un VPN a été mis en place. L'ouverture du VPN par un moyen d'identification électronique à deux facteurs dispense toutefois d'exiger une authentification à deux facteurs pour les services accédés via ce VPN.

Exigence n°22

[EXI 22] L'authentification lors d'un accès à distance avec un moyen d'identification électronique de transition doit impérativement reposer sur deux facteurs de types différents parmi les trois suivants :

- Connaissance : par exemple d'un mot de passe ;
- Possession : par exemple d'un appareil fixe ou mobile sur lequel s'effectue l'enregistrement ;
- Biométrie : par exemple une empreinte digitale stockée et vérifiée sur un matériel en possession du professionnel.

Les mécanismes d'authentification à deux facteurs listés ci-dessous sont des exemples de solutions acceptables :

- Un badge contenant une puce avec contact associée à un code PIN ;
- Un badge contenant une puce sans contact associé à un mot de passe ;
- Une clé de sécurité USB associée à un code PIN ou une empreinte digitale enregistrée sur la clé ;
- Un mot de passe associé à :
  - un code TOTP (défini par la [RFC 6238]) généré sur un matériel en possession de l'utilisateur, par exemple un téléphone ou un ordinateur pour lesquels il existe des applications compatibles et disponibles en libre accès ;
  - un code OTP envoyé par SMS sur un terminal en possession de l'utilisateur (le recours aux SMS est toutefois déconseillé, et donc à éviter s'il est possible de s'en passer, du fait des multiples vulnérabilités connues).

La liste établie ici n'est pas limitative, d'autres moyens d'identification électronique à deux facteurs sont possibles dès lors qu'ils reposent sur deux facteurs de types différents et que le niveau de sécurité apparaisse adapté au contexte. La conception du moyen d'identification électronique doit minimiser le risque de partage de ce moyen avec des tiers.

L'usage d'un mot de passe associé à un code OTP envoyé par mail est une méthode déconseillée par ce référentiel, notamment car elle repose sur deux facteurs du type connaissance (le mot de passe principal et le mot de passe de la messagerie) et qu'il peut exister des scénarios d'attaque plausibles tel que la réinitialisation du mot de passe principal par accès à la messagerie utilisée pour le code OTP. Le mot de passe associé à un code OTP envoyé par mail est toutefois toléré lorsque des mesures de sécurité complémentaires ont été prises et jugées suffisantes, telles que le recours à une boîte de messagerie sécurisée, ou distincte de celle permettant la réinitialisation du mot de passe principal, ou bien encore le recours à un code OTP par SMS si le mot de passe a été réinitialisé récemment.

Concernant les codes TOTP générés par des applications conformes à la norme, le fournisseur de service devrait recommander aux utilisateurs certaines applications identifiées comme fiables, en veillant surtout à déconseiller celles impactées par des vulnérabilités connues.

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), activées par défaut et désactivables par l'utilisateur.

Il est par ailleurs utile de se référer au guide de l'ANSSI concernant l'authentification (cf. [AUTHENTIFICATION]) afin de prendre connaissance des recommandations génériques à l'état de l'art sur le sujet.

4.6.3.4 Authentification lors d'un accès local

Un accès est considéré comme étant local lorsque l'identification électronique est réalisée sur un appareil connecté directement au SI du service cible. Ceci est le cas pour un poste de travail connecté en filaire au réseau de l'établissement hébergeant le service ou connecté en Wifi à une borne du réseau de cet établissement. Dans le cas de deux établissements appartenant au même GHT, un accès depuis l'un des établissements vers un service localisé dans un second établissement peut être considéré comme local si la connexion est établie à travers un canal sécurisé propre aux deux établissements (extension du réseau sur les deux établissements, liaison sécurisée, VPN, …).

Exigence n°23
[EXI 23] Pour un accès local à un service numérique en santé, les moyens d'identification électronique de transition suivants peuvent être utilisés : - Un moyen d'identification électronique à deux facteurs de type différents ; - Un mot de passe associé à des mesures de sécurité complémentaires.

Les exigences et recommandations décrites pour l'accès à distance s'appliquent au moyen d'identification électronique à deux facteurs utilisé en local. Toutefois, dans un contexte d'accès local, certains cas d'usage peuvent nécessiter des identifications électroniques répétées pour lesquelles l'authentification systématique à deux facteurs n'est pas réalisable en pratique.

Exigence n°24
[EXI 24] Après utilisation d'un moyen d'identification électronique de transition à deux facteurs pour un accès local, les identifications électroniques successives peuvent être réalisées avec un seul facteur dans les conditions suivantes : - Qu'une authentification nominale avec les deux facteurs d'authentification ait été réalisée précédemment dans le délai minimal jugé compatible avec les contraintes du cas d'usage ; - Que le facteur utilisé soit l'un des deux facteurs du moyen d'identification électronique utilisé précédemment ; - Que les cas d'usages pour lesquels ceci est autorisés soient formellement identifiés ; - Qu'une analyse de risque identifie les risques induits par cette autorisation et garantisse que ceux-ci sont acceptables dans le contexte des cas d'usage.

Alternativement, l'authentification pour un accès local peut être réalisée avec un mot de passe seul.

Exigence n°25

[EXI 25] Un mot de passe seul peut être utilisé comme moyen d'identification électronique de transition pour un accès local à un service numérique en santé, à condition d'appliquer les exigences suivantes :

- Des mesures de restriction d'accès par au moins l'une des méthodes suivantes :
  - ○ Une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; il est recommandé que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives infructueuses par 24 heures ;
  - ○ Un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : « captcha ») ;
  - ○ Un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10 ;
- Des critères de construction du mot de passe :
  - ○ La complexité du mot de passe doit permettre d'assurer, au minimum, une entropie de 50 bits (cf. [ENTROPIE]), par exemple :
    - ○ le mot de passe comporte 8 caractères, avec 3 des 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux) ;
    - ○ la phrases de passe, fondée sur des mots de la langue française, est composée d'au minimum 5 mots ;
    - ○ le mot de passe est composé d'au minimum 15 chiffres ;
  - ○ Le respect de ces contraintes est vérifié automatiquement à la définition et à chaque renouvellement du mot de passe ;
- Des mesures de sécurité adaptées au contexte et relatives aux modalités de gestion du mot de passe et au mécanisme d'authentification.

Le guide [AUTHENTIFICATION] de l'ANSSI et la recommandation sur les mots de passe [CNIL-MDP] de la CNIL fournissent des recommandations de référence décrivant l'état de l'art concernant la sécurisation de l'authentification et des mots de passe en particulier.

Lorsqu'un mot de passe est utilisé comme unique facteur d'authentification, le recours ponctuel à un second facteur devrait être envisagé dans les cas suivants :

- Lors de la réalisation d'opérations particulièrement sensibles ;
- Lors d'un changement de terminal de connexion ;
- A échéance régulière.

4.6.3.5 Gestion des sessions

Dans une même session authentifiée, l'identification électronique réalisée peut être réutilisée localement sans forcément demander au professionnel de reprendre entièrement le processus d'authentification, par exemple :

- Lorsqu'un professionnel s'authentifie avec un moyen d'identification électronique à deux facteurs sur une brique de SSO, cette dernière se charge de lui donner, de façon transparente et dans la limite de ses habilitations, les accès aux services numériques qui y sont intégrés. Cet accès peut reposer sur un mot de passe, géré par la brique SSO, transmis de façon sécurisé et utilisable exclusivement par cette composante ;
- Après une connexion par VPN avec un moyen d'identification électronique à deux facteurs, un professionnel peut accéder à différents services numériques depuis la session ouverte, sans avoir à rejouer l'authentification à deux facteurs.

Ces facilités doivent être étudiées afin de s'assurer que les risques d'usurpation d'identité ne sont pas significativement augmentés et restent acceptables.

Dans tous les cas, la durée de vie de la session authentifiée ouverte doit être strictement contrôlée.

Exigence n°26
[EXI 26] Après une authentification avec un moyen d'identification électronique de transition, une déconnexion automatique doit être mise en place pour forcer une nouvelle identification électronique après un certain délai d'inactivité. Ce délai est à définir par le responsable du service numérique en santé selon les risques et les contraintes propres au service.

5 FEUILLE DE ROUTE POUR LA GESTION DES IDENTITES ET DES ACCES

5.1 Feuille de route

Avant de parvenir à la généralisation de l'identification électronique par un moyen d'identification électronique de niveau de garantie eIDAS substantiel, la sécurité des accès aux services numériques traitant de données de santé à caractère personnel doit être progressivement renforcée. En sus de l'adoption rapide de moyens d'identification électronique de transition, une feuille de route est définie ci-dessous pour améliorer la fiabilité de l'identification électronique et contribuer à sécuriser le contrôle d'accès.

La démarche concerne l'ensemble des structures entrant dans le champ d'application de ce référentiel. Néanmoins, dans un esprit de proportionnalité des efforts demandés, chacune des exigences de ce chapitre précise la date et le périmètre d'application imposés.

Les étapes successives définies portent sur la mise en œuvre :

- D'un répertoire d'identité local reposant sur des processus formalisés d'alimentation ;
- D'une brique de SSO (Single Sign-On) destinée à centraliser l'identification électronique sur les services sensibles ;
- Optionnellement, d'une brique de gestion de contrôle d'accès (IAM : « Identity Access Management »).

Il convient de traiter ces sujets dans le cadre une démarche globale de gestion des moyens d'identification électronique et de gestion des accès. Les choix de conception (informations traitées, processus de gestion, interfaces techniques…) doivent être réalisés en plaçant chaque brique dans une architecture globale cible. La solution SSO devra en particulier pouvoir gérer, à terme, l'authentification des utilisateurs à l'aide des moyens d'identification électronique préconisés par le présent référentiel.

5.2 Mise en œuvre d'un répertoire d'identité local

Un répertoire d'identité local, communément désigné comme l'annuaire de la structure, constitue une brique essentielle pour la gestion des moyens d'identification électronique puis pour le contrôle d'accès. Dans cette optique, il est attendu que cet annuaire soit :

- Complet : l'ensemble des professionnels de santé doivent être répertoriés dans l'annuaire, et si possible l'ensemble des personnels (y compris administratifs par exemple) pouvant recevoir un moyen d'identification électronique sur un service sensible ;
- A jour : l'annuaire doit être maintenu à jour en continu afin de refléter les entrées et sorties de personnels avec la plus grande réactivité possible ;
- Exact : les attributs d'identité associés aux personnels répertoriés dans l'annuaire 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 l'un des répertoires sectoriels de référence, l'identifiant du répertoire sectoriel doit être associé aux attributs d'identité de ce professionnel.

Les exigences portant sur le répertoire d'identité local sont les suivantes :

Exigence n°27
[EXI 27] Afin de garantir un niveau de fiabilité à l'état de l'art des identités, au 1/01/2024 au plus tard, les structures responsables d'au moins un service sensible, doivent avoir mis en place un répertoire d'identité local dans les conditions suivantes : - Le répertoire d'identité local doit concerner a minima l'ensemble des professionnels de santé de la structure ; - Les processus d'arrivée et de départ de personnel sont formalisés et appliqués dans la gestion des ressources humaines de la structure ; - Le répertoire d'identité local est synchronisé régulièrement avec le référentiel des ressources humaines ; - Lorsqu'une personne est enregistrée dans un répertoire sectoriel de référence, son identifiant national est associé à son identité dans le répertoire local et vérifié au moins tous les 2 ans.

Il est ainsi attendu que chaque structure concernée organise des revues ou contrôles périodiques de cohérence entre les données présentes dans son répertoire d'identité local, par exemple son Active Directory, et la base de données des personnels issue de son SI RH.

5.3 Mise en œuvre d'une brique de SSO

La mise en place d'une solution SSO apporte à la fois de l'ergonomie aux utilisateurs, une plus grande facilité de gestion des problématiques d'authentification et l'opportunité d'augmenter le niveau de sécurité de l'identification électronique.

La solution SSO doit se baser sur le répertoire d'identité local mis en place préalablement ou parallèlement. Il devient alors possible de proposer plusieurs méthodes d'authentification aux utilisateurs, s'appuyant sur les moyens d'identification électroniques nationaux ou délivrés en interne à la structure. L'enrichissement dans le temps de l'offre de moyens d'identification électronique est grandement simplifié.

L'effort initial de raccordement de la solution SSO avec les différents services numériques et applications du système d'information est cependant relativement important. Ce référentiel n'impose donc ce déploiement que pour les structures les plus importantes, tout en le conseillant toujours lorsque cela est possible. Dans tous les cas, chaque structure peut décider d'intégrer ou non un service numérique particulier dans le périmètre d'application du SSO, en fonction du contexte et des difficultés techniques ou fonctionnelles de chaque cas.

Les exigences relatives à la brique de SSO sont les suivantes :

Exigence n°28
[EXI 28] Afin de garantir un niveau de fiabilité à l'état de l'art des identités, au 1/01/2025 au plus tard, la mise en œuvre d'une brique de SSO (Single Signa-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.

Il est conseillé d'assurer au plus tôt la compatibilité de la solution SSO avec les moyens d'identification électroniques imposés par ce référentiel au-delà du 1/1/2026, et tout spécifiquement les moyens d'identification délivrés par la structure et à homologuer avant cette date.

Le protocole OpenID Connect est un protocole de référence, implémenté par les services Pro Santé Connect et FranceConnect, et par de nombreuses solutions du marché. Pour favoriser l'interopérabilité des systèmes mis en œuvre, la compatibilité d'une brique SSO avec ce protocole paraît essentielle.

Exigence n°29
[EXI 29] Pour les cas où ce référentiel exige la mise en œuvre d'une brique de SSO, celle-ci doit être rendue compatible avec le protocole OpenID Connect au plus tard au 1/01/2025.

5.4 Mise en œuvre d'une brique de contrôle d'accès (IAM)

Le déploiement d'une solution de contrôle d'accès (*IAM : Identity Access Management*) peut être envisagé en complément de la brique SSO, ou en tant que système intégrant le SSO. Ce type de solution doit faciliter la définition et le contrôle des autorisations d'accès, grâce à une centralisation de la configuration et de la supervision associée. Il s'agit toutefois d'un projet complexe qui demande des études préalables précises afin d'aboutir dans de bonnes conditions.

La thématique du contrôle d'accès est adressée par un référentiel spécifique ([IE-CA]). Le présent référentiel ne formule donc aucune exigence sur le sujet, mais incite simplement chaque structure à prendre en compte ce type de solutions dans sa démarche générale de sécurisation des identités et des accès.

6 ENGAGEMENT DE SECURISATION DE L'IDENTIFICATION ELECTRONIQUE

Le présent référentiel étant juridiquement opposable, il revient au responsable légal d'un fournisseur de service numérique en santé concerné de s'assurer de sa mise en œuvre et de la pertinence des mesures implémentées. Du fait de la criticité du sujet pour la protection des données de santé, il est demandé de formaliser l'application du référentiel dans un document d'engagement de sécurisation de l'identification électronique des utilisateurs de services numériques en santé.

Cette démarche permet en outre d'informer les tiers, utilisateurs et partenaires du service par exemple, des modalités d'identification électronique mises en place et de leur donner ainsi un élément d'appréciation du niveau de sécurité atteint. Cet engagement pourra notamment être demandé par un autre fournisseur de service numérique en santé avec lequel serait établie une identification électronique indirecte (voir [IE-ASPM]).

Exigence n°30
[EXI 30] Les fournisseurs de services numériques en santé doivent produire un engagement de sécurisation de l'identification électronique des personnes physiques à leurs services numériques sensibles, dès la date d'entrée en vigueur du présent référentiel.

Lorsqu'une entité fournit plusieurs services numériques en santé, un seul document d'engagement est nécessaire pour chaque catégorie d'utilisateurs (professionnels personnes physiques, professionnels personnes morales et usagers). Plusieurs documents peuvent toutefois être établis pour une même catégorie si cela facilite la présentation, par exemple dans le cas où les moyens d'identification électronique autorisés diffèrent selon les services.

L'engagement est décomposé en deux parties :

- Un document principal, communicable sur demande, et comprenant :
  - L'identification de l'entité émettrice ;
  - L'identité du signataire de l'engagement ;
  - La catégorie des utilisateurs concernés par cet engagement ;
  - Le nom du ou des services numériques de santé concernés par cet engagement ;
  - Le niveau de conformité au référentiel constaté sur ces services ;
  - Le type et la description des moyens d'identification électronique autorisés sur ces services ;
- Une annexe confidentielle comprenant :
  - Une liste de risques résiduels relatifs à l'identification électronique des utilisateurs sur les services numériques identifiés ;
  - En cas d'identification de non-conformité(s) au référentiel ou pour atteindre le niveau exigé à l'échéance du 1/01/2026, un plan d'action. Ce plan d'action doit préciser :
    - Les différents chantiers identifiés ;
    - Les actions récentes et futures ;
    - Les responsables de chaque action ;
    - Les échéances fixées ;
    - Les budgets estimés.

Le document principal de l'engagement décrit les moyens d'identification électronique mis en œuvre sur les services numériques en santé dont l'entité est responsable. Il peut être demandé par des entités tierces, par exemple en vue d'autoriser l'identification électronique indirecte d'utilisateurs sur un service numérique en santé externe à l'entité.

L'annexe confidentielle permet au responsable légal d'un fournisseur de service numérique en santé de s'assurer de la pertinence des mesures effectives ou planifiées pour le respect des exigences du référentiel d'identification

électronique. Elle peut être demandée par des autorités règlementaires dont dépend la structure, ou bien dans le cadre d'audits de sécurité des systèmes d'information.

Des modèles de documents sont mis à disposition par l'ANS dans l'espace de publication de la PGSSI-S (voir [ENGAGEMENT]).

Exigence n°31
[EXI 31] L'engagement de sécurisation de l'identification électronique doit suivre les modèles proposés par l'ANS et être signé par un responsable légal du fournisseur des services sensibles concernés, ou, à défaut, par un délégataire dument habilité.

L'engagement pris concerne les mesures déployées à la signature du document. Toute évolution des modalités d'identification électronique doit faire l'objet de la signature d'un nouvel engagement. Par ailleurs, la description du plan d'action et la réévaluation des risques résiduels nécessitent une mise à jour annuelle.

Exigence n°32
[EXI 32] L'engagement de sécurisation de l'identification électronique doit être renouvelé à chaque modification des modalités d'identification électronique d'un service numérique en santé sensible, et a minima annuellement.

7 SYNTHESE DES EXIGENCES

7.1 Identité électronique des personnes physiques

[EXI 01] Les identifiants nationaux à utiliser pour l'identification des acteurs personnes physiques intervenant en santé sont :

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

[EXI 02] Un service numérique sensible obtenant uniquement un identifiant privé après une identification électronique doit :

- Rechercher l'identifiant national du professionnel dès lors que celui-ci est potentiellement éligible à l'enregistrement dans un répertoire sectoriel de référence ;
- Vérifier l'exactitude de cet identifiant national au minimum tous les 2 ans s'il conserve et réutilise par la suite son association avec l'identifiant privé. Cette vérification peut être réalisée par une recherche directe dans le répertoire sectoriel de référence ou par l'intermédiaire d'un autre répertoire lui-même synchronisé avec le répertoire de référence à la fréquence requise.

7.2 Sélection des moyens d'identification électronique

[EXI 03] Les moyens d'identification électronique autorisés pour accéder aux services sensibles doivent être limités :
- Aux moyens d'identification électronique disponibles sous Pro Santé Connect ;
- À la carte CPx ;
- À des moyens d'identification électronique homologués pour cet usage ;
- À des moyens d'identification électronique certifiés de niveau de garantie eIDAS substantiel ou élevé, et associés à un identifiant conforme aux exigences du référentiel.

Les moyens d'identification électronique de transition, tels que définis dans le présent référentiel, sont néanmoins autorisés jusqu'au 31 décembre 2025 au plus tard, sous réserve que les risques résiduels associés à leur utilisation soient considérés comme acceptables par le responsable du service numérique.

[EXI 04] Les services sensibles devront a minima avoir implémenté l'identification électronique par Pro Santé Connect au 1er janvier 2023 au plus tard.

7.3 Pro Santé Connect et e-CPS

[EXI 05] Les services sensibles ne doivent accepter, parmi les moyens d'identification électronique fournis par Pro Santé Connect, que ceux de niveau substantiel ou supérieur dès lors que ce niveau est précisé.

7.4 Dispositifs de la famille CPx

[EXI 06] L'ensemble des cartes de la famille CPx (CPS, CPF, CPE/CDE et CPA/CDA) peuvent être utilisées pour l'identification électronique de leur porteur lors de l'accès à un service numérique en santé. Pour le cas d'une carte non nominative, il revient au fournisseur de service de définir s'il accepte ou non ce type d'identification.

[EXI 07] La puce sans contact d'une carte CPx ne peut être utilisée pour réaliser une identification électronique que dans le cadre d'un moyen d'identification électronique homologué ou de transition.

7.5 Moyens d'identification électronique homologués

[EXI 08] L'homologation d'un moyen d'identification électronique des personnes physiques accédant à un service numérique sensible est à la charge de l'entité responsable de ce service. Lorsqu'une structure délivre le MIE à ses propres collaborateurs (elle joue alors le rôle de fournisseur d'identité), elle réalise cette homologation une fois pour le compte de l'ensemble des services numériques sensibles dont elle est responsable.

[EXI 09] L'homologation d'un moyen d'identification électronique doit garantir que :

- Le niveau de sécurité atteint avec l'utilisation de ce moyen est conforme aux objectifs de sécurité issus de l'analyse de risque des services numériques en santé pour lesquels il est utilisé ;
- Le MIE est conforme aux exigences portant sur un moyen d'identification électronique de niveau de garantie substantiel ou élevé du règlement eIDAS (cf. [eIDAS-MIE]).

[EXI 10] L'homologation du moyen d'identification électronique doit être réalisée par le responsable d'un service numérique sensible une fois tous les 4 ans et au maximum 2 ans après tout changement du référentiel européen d'exigences pour les identités électroniques, en s'appuyant sur la démarche décrite par l'ANSSI (cf. [HOMOLOGATION]). Cette homologation doit s'appuyer sur :

- Un audit de conformité au référentiel européen d'exigences pour les identités électroniques de niveau substantiel et au exigences concernant un moyen d'identification électronique homologué dans le présent référentiel ;
- Une analyse de risque du système d'information de gestion du moyen d'identification électronique ;
- Une évaluation technique de la sécurité du dispositif d'authentification.

La décision d'homologation ainsi que les pièces listées ci-dessus sont à communiquer à l'ANS.

[EXI 11] L'identifiant de personne physique fourni par un moyen d'identification électronique homologué doit être :

- L'identifiant issu d'un répertoire sectoriel de référence (RPPS pour la quasi-totalité des cas) lorsque la personne est éligible à l'enregistrement dans ce type de répertoire ;
- A défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

[EXI 12] Les attributs d'identité fournis par un moyen d'identification électronique homologué doivent au minimum comprendre :

- Le nom d'exercice ;
- Le prénom d'exercice.

[EXI 13] Le dispositif d'authentification délivré comme moyen d'identification électronique homologué doit posséder, par conception, un niveau de sécurité compatible avec le niveau de confiance global accordé à l'identité électronique transmise. Le référentiel européen d'exigences pour les identités électroniques de niveau de garantie eIDAS substantiel indique en particulier :

- 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 ;
- La diffusion de données d'identification personnelle est précédée d'une vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique ;
- Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il soit hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire au mécanisme d'authentification.

[EXI 14] Un fournisseur de service peut autoriser une authentification par un seul des deux facteurs du moyen d'identification électronique homologué aux conditions cumulatives suivantes :

- Que les cas d'usages soient formellement identifiés par le fournisseur de service ;
- Qu'une analyse de risque identifie les risques induits par cette autorisation et garantisse que ceux-ci sont acceptables dans le contexte des cas d'usage ;
- Qu'une authentification nominale avec les deux facteurs d'authentification ait été réalisée précédemment dans le délai minimal jugé compatible avec les contraintes du cas d'usage ;
- Que le facteur utilisé soit l'un des deux facteurs du moyen d'identification électronique utilisé précédemment.

7.6 Moyens d'identification électronique certifiés de niveau eIDAS substantiel ou élevé

[EXI 15] L'identification électronique pour accéder à un service numérique en santé est autorisée avec un moyen d'identification électronique certifié conforme au règlement d'exécution n°2015/1502 pour le niveau de garantie eIDAS substantiel ou élevé.

[EXI 16] Lors de l'enrôlement sur un service numérique en santé d'une personne physique voulant utiliser un moyen d'identification électronique certifié de niveau eIDAS substantiel ou élevé, le fournisseur de service doit associer la personne enrôlée à :

- L'identifiant issu d'un répertoire sectoriel de référence (RPPS pour la quasi-totalité des cas) lorsque la personne est éligible à l'enregistrement dans ce type de répertoire ;
- A défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

[EXI 17] Les attributs d'identité fournis par un moyen d'identification électronique certifié de niveau eIDAS substantiel ou élevé doivent au minimum comprendre :

- Nom de famille ;
- Prénom (s) ;
- Date de naissance.

7.7 Moyens d'identification électronique de transition

[EXI 18] L'identifiant de personne physique fourni par un moyen d'identification électronique de transition doit être :
- De préférence un identifiant issu d'un répertoire sectoriel de référence (RPPS pour la quasi-totalité des cas) ;
- A défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

[EXI 19] Les attributs d'identité fournis par un moyen d'identification électronique de transition doivent au minimum comprendre :

- Nom d'exercice ;
- Prénom d'exercice.

[EXI 20] Le processus d'enrôlement pour l'obtention d'un moyen d'identification électronique de transition doit répondre aux exigences suivantes :

- L'enrôlement de la personne physique doit se baser sur une vérification de l'identité du professionnel concerné, par exemple par l'une des méthodes suivantes :
  - En se basant sur l'identification électronique de la personne via Pro Santé Connect ou FranceConnect ;
  - Par la vérification d'une pièce d'identité, numérisée ou non, éventuellement confrontée (manuellement ou automatiquement) à une photo de l'utilisateur, à une visioconférence ou à un face-à-face physique ;
  - Par l'envoi d'un lien de confirmation sur la boîte de messagerie du professionnel dans l'espace de confiance MSSanté.
- 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 (RPPS), lorsque la profession est couverte dans son périmètre.

[EXI 21] Les processus de gestion d'un moyen d'identification électronique de transition doivent respecter les exigences suivantes :
- Les informations obtenues par la vérification d'identité initiale ne peuvent être modifiées qu'après une nouvelle vérification au moins aussi fiable ;
- Un renouvellement régulier du moyen d'identification électronique doit être prévu afin de s'assurer de l'identité du détenteur du moyen et du maintien à l'état de l'art des garanties de sécurité (par exemple concernant la longueur d'un mot de passe ou d'une clé cryptographique) ;
- Le détenteur et le gestionnaire du moyen d'identification électronique doivent pouvoir à tout moment révoquer ce moyen, afin d'empêcher son éventuelle utilisation frauduleuse (par exemple après la compromission de ce moyen).

[EXI 22] L'authentification lors d'un accès à distance avec un moyen d'identification électronique de transition doit impérativement reposer sur deux facteurs de types différents parmi les trois suivants :
- Connaissance : par exemple d'un mot de passe ;
- Possession : par exemple d'un appareil fixe ou mobile sur lequel s'effectue l'enregistrement ;
- Biométrie : par exemple une empreinte digitale stockée et vérifiée sur un matériel en possession du professionnel.

[EXI 23] Pour un accès local à un service numérique en santé, les moyens d'identification électronique de transition suivants peuvent être utilisés :

- Un moyen d'identification électronique à deux facteurs de type différents ;
- Un mot de passe associé à des mesures de sécurité complémentaires.

[EXI 24] Après utilisation d'un moyen d'identification électronique de transition à deux facteurs pour un accès local, les identifications électroniques successives peuvent être réalisées avec un seul facteur dans les conditions suivantes :
- Qu'une authentification nominale avec les deux facteurs d'authentification ait été réalisée précédemment dans le délai minimal jugé compatible avec les contraintes du cas d'usage ;
- Que le facteur utilisé soit l'un des deux facteurs du moyen d'identification électronique utilisé précédemment ;
- Que les cas d'usages pour lesquels ceci est autorisés soient formellement identifiés ;
- Qu'une analyse de risque identifie les risques induits par cette autorisation et garantisse que ceux-ci sont acceptables dans le contexte des cas d'usage.

[EXI 25] Un mot de passe seul peut être utilisé comme moyen d'identification électronique de transition pour un accès local à un service numérique en santé, à condition d'appliquer les exigences suivantes :
- Des mesures de restriction d'accès par au moins l'une des méthodes suivantes :
  - ○ Une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; il est recommandé que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives infructueuses par 24 heures ;
  - ○ Un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : « captcha ») ;
  - ○ Un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10 ;
- Des critères de construction du mot de passe :
  - ○ La complexité du mot de passe doit permettre d'assurer, au minimum, une entropie de 50 bits (cf. [ENTROPIE]), par exemple :
    - ○ le mot de passe comporte 8 caractères, avec 3 des 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux) ;
    - ○ la phrases de passe, fondée sur des mots de la langue française, est composée d'au minimum 5 mots ;
    - ○ le mot de passe est composé d'au minimum 15 chiffres ;
  - ○ Le respect de ces contraintes est vérifié automatiquement à la définition et à chaque renouvellement du mot de passe ;
- Des mesures de sécurité adaptées au contexte et relatives aux modalités de gestion du mot de passe et au mécanisme d'authentification.

[EXI 26] Après une authentification avec un moyen d'identification électronique de transition, une déconnexion automatique doit être mise en place pour forcer une nouvelle identification électronique après un certain délai d'inactivité.
Ce délai est à définir par le responsable du service numérique en santé selon les risques et les contraintes propres au service.

7.8 Feuille de route pour la gestion des identités et des accès

[EXI 27] Afin de garantir un niveau de fiabilité à l'état de l'art des identités, au 1/01/2024 au plus tard, les structures responsables d'au moins un service sensible, doivent avoir mis en place un répertoire d'identité local dans les conditions suivantes :

- Le répertoire d'identité local doit concerner a minima l'ensemble des professionnels de santé de la structure ;
- Les processus d'arrivée et de départ de personnel sont formalisés et appliqués dans la gestion des ressources humaines de la structure ;
- Le répertoire d'identité local est synchronisé régulièrement avec le référentiel des ressources humaines ;
- Lorsqu'une personne est enregistrée dans un répertoire sectoriel de référence, son identifiant national est associé à son identité dans le répertoire local et vérifié au moins tous les 2 ans.

[EXI 28] Afin de garantir un niveau de fiabilité à l'état de l'art des identités, au 1/01/2025 au plus tard, la mise en œuvre d'une brique de SSO (Single Signa-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.

[EXI 29] Pour les cas où ce référentiel exige la mise en œuvre d'une brique de SSO, celle-ci doit être rendue compatible avec le protocole OpenID Connect au plus tard au 1/01/2025.

7.9 Engagement de sécurisation de l'identification électronique

[EXI 30] Les fournisseurs de services numériques en santé doivent produire un engagement de sécurisation de l'identification électronique des personnes physiques à leurs services numériques sensibles, dès la date d'entrée en vigueur du présent référentiel.

[EXI 31] L'engagement de sécurisation de l'identification électronique doit suivre les modèles proposés par l'ANS et être signé par un responsable légal du fournisseur des services sensibles concernés, ou, à défaut, par un délégataire dument habilité.

[EXI 32] L'engagement de sécurisation de l'identification électronique doit être renouvelé à chaque modification des modalités d'identification électronique d'un service numérique en santé sensible, et a minima annuellement.

Annexe 1 : Abréviations

Sigle / Acronyme	Signification
ADELI	Automatisation Des Listes
ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
CPE	Carte de Personnel d'Etablissement (carte de la famille CPS)
CPS	Carte de Professionnel de Santé
CSPN	Certification de Sécurité de Premier Niveau
DMP	Dossier Médical Partagé
FIDO	Fast Identity Online
FINESS	Fichier National des Etablissements Sanitaires et Sociaux
GHT	Groupement Hospitalier de Territoire
MOS	Modèle des objets de santé
MSS	Messagerie Sécurisée de Santé
OID	« Object Identifier » : identifiant d'objet
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
RH	Ressources Humaines
RPPS	Répertoire Partagé des Professionnels de Santé
SI	Système d'Information
SIRENE	Système Informatique pour le Répertoire des Entreprises et des Etablissements
SIREN	Système d'Identification du Répertoire des Entreprises
SIRET	Système Informatique pour le Répertoire des Entreprises sur le Territoire
SSO	Single Sign-On
TOTP	Time-based One Time Password ([RFC 6238])
UE	Union Européenne