AGENCE
DU NUMÉRIQUE
EN SANTÉ

PGSSI-S

Référentiel d'identification électronique

Usagers

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
[ART_L1111-8-1]	Article L. 1111-8-1 du code de la santé publique : Utilisation de l'identifiant national de santé pour l'identification des personnes prises en charge à des fins sanitaires et médico-sociales https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042661590
[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
[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/

[IE-ASPM]	Référentiel d'identification électronique - Acteurs des secteurs sanitaire, médico-social et social [personnes morales] https://esante.gouv.fr
[IE-ASPP]	Référentiel d'identification électronique - Acteurs des secteurs sanitaire, médico-social et social [personnes physiques] 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
[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
[RINS]	Référentiel Identifiant National de Santé https://esante.gouv.fr/securite/identifiant-national-de-sante
[RNIV]	Référentiel National d'Identitovigilance https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance

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

L'objet du présent volet est de définir les règles applicables à l'identification électronique des usagers des services numériques de santé - patients/citoyens - et de préciser notamment les différents identifiants et dispositifs d'authentification utilisables pour ces personnes, en fonction du cadre d'usage.

Ce volet se limite à l'étape d'identification et d'authentification des usagers accédant à des services numériques de santé. L'étape d'habilitation, ou de contrôle d'accès, dans laquelle des autorisations sont données à l'usager, 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* »), dès lors que le service numérique en santé facilite ou permet toute activité de prévention, de diagnostic, de soin, de prise en charge, de suivi de la personne, à des fins sanitaire, médico-sociale ou sociale.

Au sein de ce périmètre, le présent volet s'applique à l'identification électronique des usagers de ces services numériques.

2 DEFINITIONS ET CONCEPTS GENERAUX

2.1 Personne physique

Dans ce document, le terme **personne physique** désigne un usager du système de santé (patient, citoyen, aidant, etc.).

Il s'agit bien ici des utilisateurs directs des services numériques en objet du présent référentiel. Lorsqu'une personne physique effectue une démarche sur un service numérique pour le compte d'un tiers (en tant que responsable légal, de tuteur ou d'aidant par exemple), cette personne physique est l'usager qui est identifié sur le service. L'identification de la personne pour laquelle elle intervient ou le contrôle de son habilitation à effectuer cette démarche sont en dehors du périmètre de ce référentiel.

2.2 Services numériques

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 portail patients ou de préadmission des établissements de santé ;
- Un site de consultation de résultats d'analyse biologique ou d'imagerie médicale ;
- Un site de prise de rendez-vous médicaux ;
- Une plateforme de téléconsultation.

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'un moyen d'identification électronique sur FranceConnect, 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 détenteur est tenu de respecter un ensemble de mesures de sécurité et de précautions de conservation et d'utilisation de ce dispositif. Ces engagements lui sont rappelés par le fournisseur du moyen d'identification électronique, typiquement dans les conditions générales d'utilisation associées.

Un couple identifiant / mot de passe, une application mobile d'identité 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 :
- L'identifiant attribué à cette personne ;
- L'ensemble des attributs (ou traits) d'identité enregistrés associés à l'identifiant.

Cet ensemble de données, des « données d'identification personnelles […] permettant d'établir l'identité d'une personne » au sens du règlement eIDAS, est désigné communément comme étant une **identité électronique**.

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 ;
- Les prénoms ;
- La date de naissance ;
- Le lieu de naissance ;
- Le genre.

Selon le répertoire d'identité, 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.

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 d'identité nationaux** sont définis comme des répertoires gérant des données d'identité pour des populations nationales clairement définies. Leur existence et leurs règles de fonctionnement sont consacrées dans un texte législatif ou règlementaire.
- Les **répertoires d'identité privés** sont des répertoires d'identité qui ne sont pas des répertoires d'identité nationaux. 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 d'identité nationaux (solution à privilégier) ou des identifiants privés propres.

Dans le cadre de ce référentiel dédié aux usagers des services numériques de santé, le répertoire d'identité national utilisé est le RNIPP (Répertoire national d'identification des personnes physiques), géré par l'INSEE. Il s'agit d'un répertoire national d'identité régalien, c'est-à-dire géré par l'Etat et non limité au secteur de la santé.

Le RNIPP référence des attributs d'identité issus des registres d'état civil, tels que le nom de naissance, les prénoms, le sexe, la date et le lieu de naissance (code officiel géographique), ainsi que le NIR (Numéro d'inscription au répertoire).

Le RNIPP est en réplication synchrone avec le SNGI (Système national de gestion des identifiants), géré par la CNAV, qui attribue le NIR aux personnes nées à l'étranger venant travailler en France.

2.8 Identifiant national de santé

La loi [ART_L1111-8-1] consacre le numéro d'inscription au RNIPP (NIR) comme **identifiant national de santé** (INS) des personnes pour leur prise en charge à des fins sanitaires et médico-sociales.

Deux notions doivent être distinguées :

- Le matricule INS : c'est soit le NIR pour les personnes immatriculées, soit le NIA (numéro identifiant d'attente) pour les personnes en attente d'immatriculation. Pour pouvoir faire la distinction entre ces deux types de numéro, l'organisme qui a affecté l'INS est précisé sous la forme d'un OID.
- L'identité INS : c'est l'association du matricule INS (comme identifiant) aux traits d'identité de la personne identifiée, constituant des « données d'identification personnelle » (i.e. une identité électronique) au sens du règlement eIDAS.

Le référencement des données de santé avec l'identité INS est obligatoire pour les acteurs de santé, ainsi que le respect de mesures d'identitovigilance. Les modalités d'application sont décrites dans le Référentiel Identifiant National de Santé ([RINS]) et le Référentiel National d'Identitovigilance ([RNIV]), pris en application des dispositions des articles R. 1111-8-1 à R. 1111-8-7 du code de la santé publique.

L'identité INS est accessible pour les acteurs de santé via le téléservice INSi[1] opéré par l'Assurance Maladie, ainsi qu'au travers de l'appli carte Vitale (ApCV). Le téléservice INSi permet de :

- Rechercher une identité INS à partir de traits d'identité relatifs à l'usager ou de sa carte Vitale ;
- Vérifier l'exactitude d'une identité INS vis-à-vis des données de référence.

[1] L'accès au téléservice INSi est restreint à un périmètre défini dans le référentiel [RINS]

2.9 Exigences d'identitovigilance

Afin d'établir des règles homogènes concernant le partage des identités des usagers, un référentiel national d'identitovigilance ([RNIV]) a été construit en 2020 pour être rendu opposable en 2021. Il distingue une identité :

- **Validée**, lorsqu'elle a fait l'objet d'une identification électronique de niveau eIDAS substantiel ou d'une vérification d'un titre d'identité officiel (carte nationale d'identité, passeport, titre de séjour…) ;
- **Récupérée**, lorsqu'elle a été récupérée ou vérifiée auprès du répertoire de référence par l'intermédiaire du téléservice INSi, ou d'un dispositif équivalent comme l'ApCV ;
- **Qualifiée**, lorsqu'elle est à la fois validée et récupérée. Ce statut permet, lors de l'échange ou du partage d'une donnée de santé, d'y associer l'identité INS (selon des formats définis dans une annexe du CI-SIS) afin que le destinataire puisse automatiquement associer la donnée de santé au bon patient lors de la réception.

Une identité n'ayant été ni validée, ni récupérée est considérée comme une identité provisoire. Ce statut ne permet pas, lors de l'échange ou du partage d'une donnée de santé, d'y associer l'identité INS.

2.10 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 d'identité pour obtenir des informations complémentaires sur la personne identifiée. Une structure, fournisseur de service en tant que responsable de traitements au sein de son système d'information, est son propre fournisseur d'identité lorsqu'elle délivre des moyens d'identification électronique aux usagers de ses services numériques en santé.

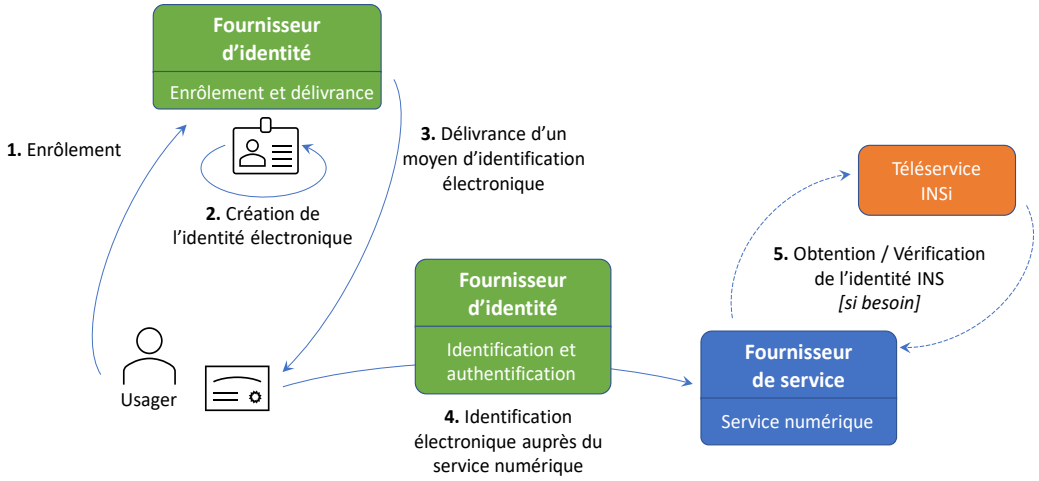
Un **fournisseur d'identité** est une entité qui délivre un moyen d'identification électronique à une personne physique ou morale qui a demandé ce moyen et dont elle a établi une identité électronique fiable.

L'identité électronique est créée suite à un processus d'enrôlement au cours duquel le fournisseur d'identité vérifie l'identité du demandeur et y associe un identifiant unique. 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 personnes physiques ciblées par ce volet du référentiel :
- L'Assurance Maladie est le fournisseur du service DMP (Dossier Médical Partagé) ;
- La Poste est un fournisseur d'identité délivrant un moyen d'identification électronique de niveau substantiel ;
- L'ApCV a vocation à devenir un moyen d'identification électronique de niveau substantiel de référence dans le secteur de la santé.

2.11 Processus d'identification électronique

Lorsque le service recourt à un moyen d'identification électronique certifié de niveau eIDAS substantiel, le processus d'identification électronique d'un usager peut être schématisé ainsi :



L'usager doit obtenir au préalable un moyen d'identification électronique de niveau eIDAS substantiel auprès d'un fournisseur d'identité. Pour les services numériques en santé, ce moyen sera à terme soit l'ApCV, soit un MIE référencé sur FranceConnect au niveau substantiel (par exemple l'Identité Numérique de La Poste).

L'usager initie une connexion vers le service numérique d'un fournisseur de service, qui lui demande de s'authentifier en utilisant un MIE de niveau substantiel. Cette authentification se fait à travers une interface du fournisseur d'identité qui exploite et vérifie le moyen d'identification électronique présenté par l'usager.

En application du référentiel RNIV (cf. §2.9), le service numérique en santé peut interroger le téléservice INSi[2] pour rechercher ou vérifier l'identité INS de l'usager lorsque l'identité obtenue n'est pas qualifiée au sens du RNIV (cf. §2.9). Le service numérique peut conserver ces informations afin de ne pas avoir à répéter cet appel à chaque identification électronique, mais doit les réactualiser conformément aux règles du référentiel INS [RINS].

Une fois l'identification électronique finalisée, le fournisseur de service octroie à l'usager 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]).

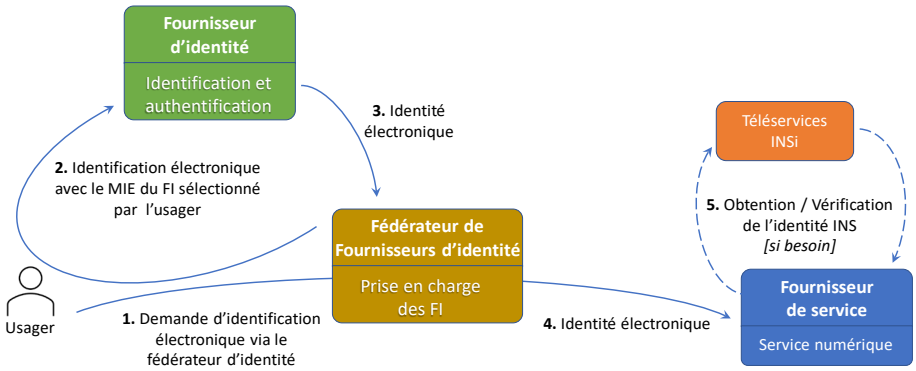
2.12 Fédérateur de fournisseurs d'identité

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.

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.

[2] L'accès au téléservice INSi est restreint à un périmètre défini dans le référentiel [RINS]

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.

Dans le cadre de l'identification électronique des usagers, le principal fédérateur de fournisseurs d'identité est FranceConnect, à destination des citoyens. Ce fédérateur regroupe plusieurs fournisseurs d'identité publics et privés qui, chacun, propose son moyen d'identification électronique, dont certains sont ou seront de niveau substantiel ou élevé.

3 MOYENS D'IDENTIFICATION ELECTRONIQUE

3.1 Sélection des moyens d'identification électronique

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 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 cette analyse de risque selon une méthodologie formalisée et éprouvée, telle que la méthode EBIOS RM (voir [EBIOS RM]) proposée par l'ANSSI.

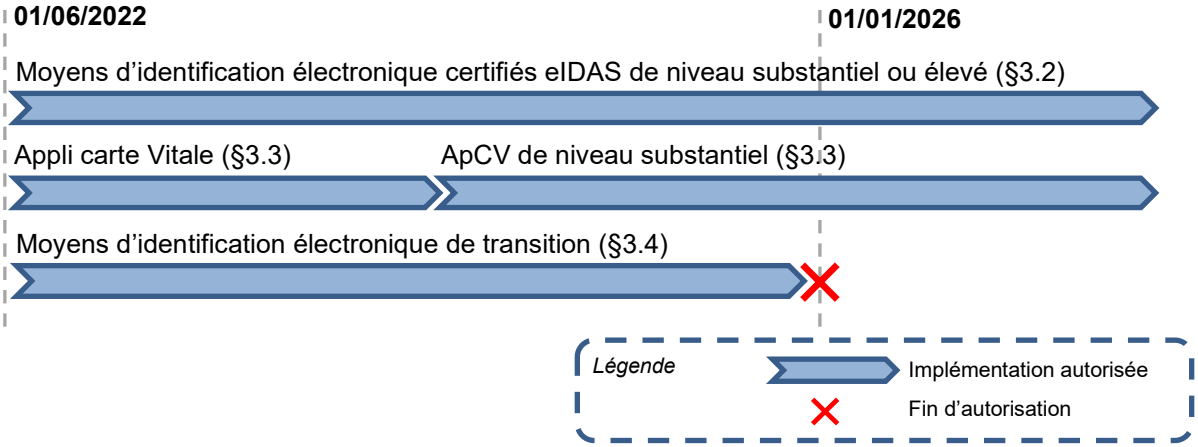
Pour rappel, les autorités administratives doivent appliquer le Référentiel Général de Sécurité ([RGS]) pour la sécurisation de leurs échanges avec d'autres autorités administratives ou avec des usagers. L'analyse de risque et le choix des moyens d'identification électronique pour ces échanges font partie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

Ce référentiel fixe pour objectif d'identifier électroniquement les usagers des services numériques en santé par un moyen d'identification électronique de niveau de garantie substantiel ou élevé au sens du règlement eIDAS. 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.

Du fait de la faiblesse de l'offre actuelle de moyens d'identification électronique de niveau substantiel, et afin de donner le temps nécessaire aux fournisseurs de services numériques de se mettre en conformité, un calendrier progressif est fixé.

Exigence n°1
[EXI 01] Les moyens d'identification électronique autorisés pour l'identification électronique des usagers sur les services numériques en santé doivent être limités : - À des moyens d'identification électronique certifiés eIDAS de niveau de garantie substantiel ou élevé ; - À l'application mobile carte Vitale (ApCV). 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.

Le calendrier d'implémentation de ces moyens d'identification électronique est schématisé ci-dessous :



La carte Vitale dématérialisée (appli carte Vitale) sera proposée à tous les citoyens sous la forme d'une application « ApCV » pour appareil mobile. L'ApCV devrait à terme obtenir le niveau eIDAS substantiel et devenir un moyen d'identification électronique de référence dans le secteur de la santé.

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

3.2.1 Généralités

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

L'identification électronique sur un service numérique de santé traitant des données de santé à caractère personnel est autorisée avec un moyen d'identification électronique certifié conforme au niveau de garantie substantiel ou élevé.

Exigence n°2
[EXI 02] L'identification électronique des usagers est autorisée avec les moyens d'identification électronique certifiés eIDAS suivants : - Les moyens notifiés par tout Etat Membre de l'UE (au titre de l'identité électronique de citoyens) au niveau de garantie substantiel ou élevé ; - En France, les moyens d'identification électronique ayant obtenu une attestation de conformité au niveau de garantie substantiel ou élevé délivrée par l'ANSSI au titre du règlement eIDAS ou de l'article L102 du Code des postes et des communications électroniques.

Les identités électroniques obtenues par ces moyens d'identification électronique ne comprennent pas le matricule INS.

Exigence n°3
[EXI 03] Un service numérique en santé, qui recourt à un moyen d'identification électronique certifié eIDAS et qui est soumis à l'obligation de référencement des données de santé avec l'INS selon le périmètre défini à l'article R1111-8-3 du Code de la santé publique, doit établir l'identité INS de l'usager et peut conserver l'association établie entre cette identité et celle donnée par le moyen d'identification électronique. Ce lien doit être vérifié régulièrement selon les règles du référentiel de l'INS [RINS].

Le service numérique peut faire appel au téléservice INSi pour obtenir le matricule INS et qualifier ainsi l'identité de l'usager (cf. §2.8 et §2.9).

3.2.2 Identité électronique

L'identité électronique communiquée au service par le fournisseur d'identité comprend au minimum les données suivantes :

- Un identifiant attribué par le fournisseur d'identité ou le fédérateur d'identité ;
- Nom de naissance ;
- Prénom (s) ;
- Date de naissance.

Dans le contexte français, cette identité est complétée par le genre et le lieu de naissance (code géographique INSEE de la ville ou du pays de naissance). L'ensemble constitue l'identité pivot du fédérateur FranceConnect.

3.2.3 Moyens d'identification électronique

La liste des moyens d'identification électronique notifiés de niveau substantiel ou élevé est publiée par la Commission Européenne[3].

La liste des moyens d'identification électronique certifiés par l'ANSSI est disponible sur son site institutionnel[4]. Au mois d'octobre 2021, la liste ne comprend qu'un seul MIE :

- Identité Numérique La Poste : ce MIE de niveau de garantie substantiel est fourni par La Poste.

La liste présentée par l'ANSSI fait aussi apparaître le portail FranceConnect, qui fédère les moyens d'identification électronique de niveau substantiel ou élevé dans un service particulier, dénommé FranceConnect Plus. Les fournisseurs de service qui utilisent FranceConnect et indiquent que leurs utilisateurs ne doivent pouvoir s'identifier qu'avec des moyens d'identification électronique de niveau substantiel au minimum seront basculés sur FranceConnect Plus.

3.3 Appli carte Vitale (ApCV)

3.3.1 Généralités

L'ApCV est une application pour appareil mobile qui offre des services équivalents à la carte Vitale ainsi que de nouveaux usages. Elle est proposée par le GIE SESAM-Vitale. Chaque citoyen disposant d'une carte Vitale pourra à terme créer son identité électronique dans l'application ApCV.

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

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

Les identités électroniques fournies par l'ApCV pour un usager d'un service numérique de santé intègrent l'identité INS, permettant de considérer l'identité comme 'récupérée' au sens du référentiel national d'identitovigilance (RNIV). Ce moyen d'identification électronique sera fourni dans un premier temps avec le niveau faible puis à terme devrait être certifié de niveau de garantie substantiel. A cette échéance, l'identité INS pour le porteur de l'ApCV sera considérée comme 'validée' au sens du RNIV et le responsable du référencement n'aura plus à valider l'identité (cf. §2.9) par une autre méthode (identification électronique de niveau substantiel eIDAS ou vérification d'un titre d'identité officiel).

L'ApCV sera aussi disponible comme fournisseur d'identité au sein du fédérateur FranceConnect. Dans ce cas, l'identité électronique fournie est une identité « civile » et ne comprend pas le matricule INS. Les données d'identité reçues par le service effectuant l'identification électronique sont alors identiques à celles délivrées par tout autre MIE de niveau substantiel présenté au §3.2. Des réflexions sont en cours pour permettre la fourniture de l'identité INS directement par FranceConnect, pour les fournisseurs de service habilités à la référencer.

3.3.2 Identité d'électronique

L'identité INS fournie par l'ApCV est composée des données suivantes :

- Matricule INS (et OID de l'entité source pour distinguer le NIR du NIA) ;
- Nom de naissance ;
- Prénoms ;
- Genre ;
- Date de naissance ;
- Lieu de naissance (code officiel géographique).

3.3.3 Moyens d'identification électronique

L'ApCV est une application pour appareil mobile (téléphone, tablette).

L'application permet de choisir un code PIN personnel pour s'authentifier sur un service de santé.

3.4 Moyens d'identification électronique de transition

3.4.1 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 dont un dispositif d'authentification à deux facteurs. 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 et le type et la volumétrie des données traitées.

3.4.2 Identité électronique

3.4.2.1 Identifiant

Exigence n°4
[EXI 04] L'identifiant de l'usager fourni par un moyen d'identification électronique de transition doit être : - De préférence le matricule INS ; - A défaut un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

Le matricule INS constitue l'identifiant à privilégier, en particulier lorsque le service numérique doit référencer l'INS.

Un identifiant privé est établi sous la responsabilité directe du fournisseur de service ou sous celle d'une personne morale attribuant cet identifiant pour un ensemble d'applications. Dans ce cas, toutes les applications qui, au sein d'une organisation de santé, utilisent le même identifiant pour désigner un patient forment un « Domaine d'identification » au sens du référentiel [RNIV]. Le recours à un identifiant privé reste nécessaire pour traiter les cas où l'usager ne dispose pas d'un matricule INS (un touriste étranger par exemple).

Exigence n°5
[EXI 05] Pour se conformer à l'obligation de référencer les données de santé des usagers avec le matricule INS, les services numériques en santé utilisant un identifiant privé doivent l'associer au plus tôt au matricule INS en recourant au téléservice INSi.

3.4.2.2 Attributs d'identité

L'identité électronique attribuée à l'usager doit comprendre un ensemble de données suffisantes pour caractériser la personne identifiée et pouvoir traiter efficacement ses données.

Exigence n°6
[EXI 06] Les attributs d'identité fournis par un moyen d'identification électronique de transition doivent au minimum comprendre : - Nom de naissance ; - Premier prénom ; - Genre ; - Date de naissance ; - Lieu de naissance.

Il est recommandé de formater ces attributs selon les règles du référentiel [MOS-NOS]. D'autres attributs peuvent être ajoutés selon les besoins et le contexte des services utilisant cette identité électronique.

L'association de l'identifiant de l'usager à une identité INS permet de répondre à cet objectif.

3.4.3 Moyens d'identification électronique

3.4.3.1 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.

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.

3.4.3.2 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°7
[EXI 07] Le processus d'enrôlement pour l'obtention d'un moyen d'identification électronique de transition doit répondre aux exigences suivantes : - L'enrôlement de l'usager doit se baser sur une vérification d'identité systématique ; - Lorsqu'une adresse électronique et/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 à l'enrôlement.

La vérification d'identité de l'usager peut être effectuée par exemple par l'une des méthodes suivantes :

- En se basant sur l'identification électronique de la personne via 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 dans « Mon espace santé » associée à l'usager.

La vérification des coordonnées de l'utilisateur peut se faire par l'envoi d'un code ou d'un lien d'activation.

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

Exigence n°8
[EXI 08] 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).

3.4.3.3 Mécanisme d'authentification

Le mécanisme d'authentification doit garantir un niveau de sécurité adapté au contexte.

Exigence n°9
[EXI 09] L'authentification d'un usager par un moyen d'identification électronique de transition doit reposer sur deux facteurs de types différents parmi les trois : - 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 de l'usager.

Cette exigence peut prendre la forme d'un facteur d'authentification dynamique ajouté à la demande de mot de passe, comme par exemple :

- de préférence un code TOTP (défini par la [RFC 6238]) généré sur un terminal enregistré et en possession de l'usager, par exemple un téléphone ou un ordinateur pour lesquels il existe des applications compatibles et disponibles en libre accès ;
- un code à usage unique (OTP) envoyés par SMS (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).

L'authentification peut aussi être réalisée par la saisie d'un mot de passe depuis un terminal enregistré et en possession de l'usager.

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.

Cette liste d'exemples 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. En particulier, lorsque l'un des facteurs d'authentification repose sur la possession d'un matériel, il faut demander à l'usager de s'assurer qu'il lui soit bien personnel et non partagé avec d'autres personnes (membres de son foyer par exemple).

Du fait de l'absence de garantie sur la sécurité des terminaux des utilisateurs, des mesures doivent être mises en place afin d'éviter le vol ou la réutilisation frauduleuse des secrets de l'authentification. Des informations et avertissements circonstanciés sont à fournir aux usagers sur la protection de leur moyen d'authentification. De plus :

Exigence n°10
[EXI 10] L'authentification d'un usager avec un moyen d'identification électronique de transition doit être renforcée par : - Des mesures de restriction de l'accès au compte, par au moins l'une des méthodes suivantes : o 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 ; o Un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : « captcha ») ; o Un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10, assorti d'un mécanisme de déblocage proportionnel aux risques d'usurpation d'identité ; - Des critères de construction du mot de passe, lorsque ce type de facteur est utilisé : o La complexité du mot de passe doit permettre d'assurer, au minimum, une entropie de 27 bits (cf. [ENTROPIE]), par exemple : o Le mot de passe comporte au minimum 8 chiffres décimaux ; o Le mot de passe comporte au minimum 6 caractères alphanumériques ; o Le respect de ces contraintes est vérifié automatiquement à la définition et à chaque renouvellement du mot de passe ; - L'application de mesures de sécurité adaptées au contexte et relatives aux modalités de gestion des facteurs d'authentification 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.

De façon générale, il est fortement recommandé :
- 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 (comme cela est fait par exemple par FranceConnect).

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.

3.4.3.4 Gestion des sessions

Les sessions ouvertes après authentification doivent être fermées au plus tôt afin d'éviter la réutilisation par un tiers.

Exigence n°11
[EXI 11] Après une authentification de l'usager avec un moyen d'identification électronique de transition, une déconnexion automatique doit être mise en place pour forcer une nouvelle identification électronique après un délai d'inactivité à définir par le responsable du service numérique en santé selon les risques et les contraintes propres au service.

4 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°12
[EXI 12] Les fournisseurs de services numériques en santé doivent produire un engagement de sécurisation de l'identification électronique des usagers à leurs services numériques, 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 présent 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 usagers 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°13
[EXI 13] 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 numériques en santé 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 demandent une mise à jour annuelle.

Exigence n°14
[EXI 14] 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, et a minima annuellement.

5 SYNTHESE DES EXIGENCES

5.1 Sélection des moyens d'identifications électronique

[EXI 01] Les moyens d'identification électronique autorisés pour l'identification électronique des usagers sur les services numériques en santé doivent être limités :

- À des moyens d'identification électronique certifiés eIDAS de niveau de garantie substantiel ou élevé ;
- À l'application mobile carte Vitale (ApCV).

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.

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

[EXI 02] L'identification électronique des usagers est autorisée avec les moyens d'identification électronique certifiés eIDAS suivants :

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

[EXI 03] Un service numérique en santé, qui recourt à un moyen d'identification électronique certifié eIDAS et qui est soumis à l'obligation de référencement des données de santé avec l'INS selon le périmètre défini à l'article R1111-8-3 du Code de la santé publique, doit établir l'identité INS de l'usager et peut conserver l'association établie entre cette identité et celle donnée par le moyen d'identification électronique. Ce lien doit être vérifié régulièrement selon les règles du référentiel de l'INS [RINS].

5.3 Moyens d'identification électronique de transition

[EXI 04] L'identifiant de l'usager fourni par un moyen d'identification électronique de transition doit être :

- De préférence le matricule INS ;
- A défaut un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.).

[EXI 05] Pour se conformer à l'obligation de référencer les données de santé des usagers avec le matricule INS, les services numériques en santé utilisant un identifiant privé doivent l'associer au plus tôt au matricule INS en recourant au téléservice INSi.

[EXI 06] Les attributs d'identité fournis par un moyen d'identification électronique de transition doivent au minimum comprendre :

- Nom de naissance ;
- Premier prénom ;
- Genre ;
- Date de naissance ;
- Lieu de naissance.

[EXI 07] Le processus d'enrôlement pour l'obtention d'un moyen d'identification électronique de transition doit répondre aux exigences suivantes :

- L'enrôlement de l'usager doit se baser sur une vérification d'identité systématique ;
- Lorsqu'une adresse électronique et/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 à l'enrôlement.

[EXI 08] 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 09] L'authentification d'un usager par un moyen d'identification électronique de transition doit reposer sur deux facteurs de types différents parmi les trois :

- 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 de l'usager.

[EXI 10] L'authentification d'un usager avec un moyen d'identification électronique de transition doit être renforcée par :

- Des mesures de restriction de l'accès au compte, 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, assorti d'un mécanisme de déblocage proportionnel aux risques d'usurpation d'identité ;
- Des critères de construction du mot de passe, lorsque ce type de facteur est utilisé :
  - La complexité du mot de passe doit permettre d'assurer, au minimum, une entropie de 27 bits (cf. [ENTROPIE]), par exemple :
    - Le mot de passe comporte au minimum 8 chiffres décimaux ;
    - Le mot de passe comporte au minimum 6 caractères alphanumériques ;
  - Le respect de ces contraintes est vérifié automatiquement à la définition et à chaque renouvellement du mot de passe ;
- L'application de mesures de sécurité adaptées au contexte et relatives aux modalités de gestion des facteurs d'authentification et au mécanisme d'authentification.

[EXI 11] Après une authentification de l'usager avec un moyen d'identification électronique de transition, une déconnexion automatique doit être mise en place pour forcer une nouvelle identification électronique après un délai d'inactivité à définir par le responsable du service numérique en santé selon les risques et les contraintes propres au service.

5.4 Engagement de sécurisation de l'identification électronique

Exigence n°12

[EXI 12] Les fournisseurs de services numériques en santé doivent produire un engagement de sécurisation de l'identification électronique des usagers à leurs services numériques, dès la date d'entrée en vigueur du présent référentiel.

[EXI 13] 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 numériques en santé concernés, ou, à défaut, par un délégataire dument habilité.

[EXI 14] 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, et a minima annuellement.

Annexe 1 : Abréviations

Sigle / Acronyme	Signification
ANS	Agence du numérique en santé
ANSSI	Agence nationale de sécurité des systèmes d'information
ApCV	Appli Carte Vitale
CNAV	Caisse nationale d'assurance vieillesse
eIDAS	electronic IDentification Authentication and trust Services
INS	Identité nationale de santé/identifiant national de santé
INSEE	Institut national de la statistique et des études économiques
MOS	Modèle des objets de santé
MSS	Messagerie Sécurisée de Santé
NIA	Numéro d'immatriculation d'attente
NIR	Numéro d'Inscription au RNIPP (« numéro de sécurité sociale »)
MIE	Moyen d'Identification Electronique
OID	Object IDentifier
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
RNIPP	Répertoire national d'identification des personnes physiques
SNGI	Système national de gestion des identifiants
TOTP	Time-based One Time Password ([RFC 6238])
UE	Union Européenne