PHARMAGEEK | IAtrogénique × IAtus

IDENTITÉ NUMÉRIQUE EN SANTÉ

De la carte à l’infrastructure de confiance

Identifier. Connecter. Simplifier.

Lionel Reichardt • Livre blanc • 8 octobre 2026



Pourquoi ce livre blanc

Une identité reconnue doit ouvrir la bonne porte. Dans la santé numérique, elle peut aussi ouvrir la mauvaise si le dossier, les droits ou le contexte sont mal interprétés. Le changement de support de la carte Vitale invite à examiner cette chaîne de confiance dans son ensemble.

Ce livre blanc développe la note « De l'objet à l'infrastructure » fournie par Lionel Reichardt. Il conserve les axes Identifier, Connecter, Simplifier et les élargit aux portefeuilles d'identité, à la résilience, à l'inclusion et à la gouvernance.

Il s'adresse aux directions d'établissements, industriels, éditeurs, responsables de parcours, équipes de sécurité, DPO, professionnels et représentants des usagers. Sa promesse : fournir un vocabulaire commun et des décisions concrètes pour passer de la fonctionnalité à l'usage.

La publication est datée du 8 octobre 2026, avant les Vitale DAYS des 13 et 14 octobre. Elle ne constitue pas une restitution de cet événement ni une publication officielle du GIE SESAM-Vitale. L'annonce publique fournit le contexte de la conférence ; les analyses et recommandations relèvent de l'auteur. [28]

À LIRE EN COMPLÉMENT

Édition spéciale VITALE DAYS 2026
Identifier. Connecter. Simplifier.

La newsletter IAtrogénique × IAtus de Lionel Reichardt, publiée le 7 octobre 2026. [34]
Lire la newsletter sur LinkedIn →

La confiance se construit dans les parcours. Elle se vérifie aussi dans leurs exceptions.

Méthode, corpus et niveau de confiance

Le travail repose sur la note Pages et le cadre stratégique complémentaire fournis par l’auteur, puis une recherche ciblée dans des sources primaires : Assurance Maladie, ANS, GIE SESAM-Vitale, DINUM, France Identité, ANSSI, CNIL, Insee, Commission européenne et textes de référence. Les spécifications OpenID et FIDO éclairent les mécanismes techniques ; Apple et Google décrivent leurs propres offres.

Les références numérotées renvoient à une bibliographie cliquable. Les sources décrivent selon les cas une règle, une fonctionnalité, un objectif ou un constat. Les données d’activation ne sont pas transformées en taux d’usage ; les objectifs ne sont pas présentés comme des résultats.

Les scénarios de terrain sont illustratifs et les outils de déploiement sont proposés par l’auteur. Ils ne constituent ni une étude clinique, ni une certification, ni un avis juridique individualisé. Les périmètres de raccordement et versions doivent être revalidés avant mise en œuvre.

Le texte écarte les formulations absolues et les chiffres dont le périmètre n’a pas été confirmé. Les perspectives européennes et agentiques sont distinguées des usages documentés. Les recommandations sur l’organisation sont conçues pour être adaptées et testées localement.

Édition du 8 octobre 2026, révision enrichie. Rédaction, recherche documentaire et mise en page assistées par IA. La vérification des sources et la responsabilité de diffusion demeurent humaines. Illustration de couverture générée par IA ; infographies construites à partir des informations citées.

Documenter le présent. Nommer les hypothèses. Mesurer la valeur.

Votre parcours de lecture

OUVERTURE — p. 6

La thèse, le corpus, les décisions prioritaires

IDENTIFIER — p. 8

INS, identité professionnelle, enrôlement et niveaux de garantie

CONNECTER — p. 15

FranceConnect, FI appli carte Vitale, OIDC et rapprochement

SIMPLIFIER — p. 21

Cabinet, préadmission, parcours contrasté et droits d’assurance

WALLETS — p. 27

EUDI, Apple/Google et passkeys

EUROPE — p. 31

EHDS et convergence des programmes nationaux et européens

PROTÉGER — p. 34

Signature, données, consentement, IA et résilience

INCLURE — p. 40

Compétences numériques, accompagnement et représentation

MESURER — p. 43

Activations, valeur et pilote

GOUVERNER / DÉCIDER — p. 46

Responsabilités, souveraineté et agents IA

OUTILS ET SOURCES — p. 51

Fiches, outils, glossaire et bibliographie

Lecture express : résumé exécutif (p. 5), fiches et outils.
Trois ajouts : parcours patient (p. 24), convergence (p. 32), inclusion (p. 41).

Résumé exécutif : cinq décisions prioritaires

1. Choisir le parcours avant la technologie. Cabinet, préadmission, télésanté et recherche ne mobilisent pas les mêmes données ni les mêmes permissions. Le projet doit partir d’une action et d’une population définies.

2. Distinguer les preuves. Enrôlement, identification, authentification, autorisation, traçabilité et signature répondent à des questions différentes. L’INS référence les données ; la connexion ne remplace pas la politique d’accès.

3. Traiter les exceptions comme des usages. Homonymies, ayants droit, représentation, perte de téléphone et panne doivent être testés avant la généralisation. La possibilité de corriger participe à la confiance.

4. Préparer la convergence sans annoncer ce qui n’est pas établi. Le fournisseur d’identité appli carte Vitale, FranceConnect+, Pro Santé Connect et les wallets européens sont des objets distincts. L’interopérabilité exige aussi des règles d’association et de gouvernance.

5. Piloter par la valeur et l’accès effectif. Mesurer le parcours complet, l’aide nécessaire, les erreurs et la charge des équipes. Les activations apportent un repère de diffusion, pas une preuve de simplification.

Identifier juste. Autoriser avec mesure. Simplifier pour tous.

La bonne personne. Le bon accès. Le bon soin.

Un patient se connecte à une téléconsultation. Une secrétaire prépare une admission. Une pharmacienne facture une délivrance. Un chercheur accède à un environnement de données. Ces gestes ont un point commun : ils supposent de savoir qui agit, pour qui, dans quel contexte et avec quels droits. Un écran de connexion peut sembler secondaire. Son échec peut pourtant interrompre tout le parcours.

L'identité numérique en santé mérite donc une autre place dans le débat. Elle relie une personne réelle à un compte, un dossier, un statut professionnel ou une action. Elle devient utile quand ce lien est fiable, compréhensible et exploitable par les équipes. Son succès se juge au point de rencontre entre le patient, le professionnel et l'organisation.

Le smartphone ne résume pas cette transformation. Un dossier bien identifié, une habilitation révoquée au départ d'un salarié, une alternative accessible lors d'une panne ou une procédure de correction des homonymies produisent aussi de la confiance. Le livre blanc propose de regarder l'ensemble de cette chaîne.

Notre thèse : la valeur d'une identité numérique se mesure à ce qu'elle permet d'accomplir sans erreur évitable, sans exposition excessive des données et sans obstacle disproportionné à l'accès aux soins. Cette grille déplace l'attention de l'application vers les usages et les responsabilités.

Références : [6] G_NIUS / ANS, [10] CNIL

Ce que l'appli carte Vitale change vraiment

Le 18 novembre 2025 marque la généralisation nationale de l'appli carte Vitale, après un déploiement progressif. Elle constitue une alternative à la carte physique pour les assurés remplissant les conditions d'activation et disposant d'un smartphone compatible. Disponibilité nationale ne signifie cependant ni activation par tous les assurés ni acceptation par tous les professionnels.

Le changement concerne plusieurs maillons. L'application renouvelle le support présenté au professionnel ; elle peut véhiculer des informations d'identité et s'articuler avec la consultation des droits. Un référentiel distinct organise son utilisation comme fournisseur d'identité pour des services à distance. Il faut traiter séparément ces fonctions, leur équipement nécessaire et leurs conditions de raccordement.

Pour un décideur, la question pertinente devient : quel problème concret cette brique résout-elle dans notre parcours ? Une activation réussie ne renseigne pas, à elle seule, sur l'accès à une plateforme ou sur la qualité d'un rapprochement de dossiers. La démonstration d'une fonctionnalité ne décrit pas non plus son usage quotidien à grande échelle.

Le passage de la carte à l'infrastructure est ainsi une lecture stratégique : une même base de confiance peut contribuer à différents parcours. Chaque service doit encore construire l'autorisation, l'expérience utilisateur et le traitement des exceptions adaptés à sa mission.

Références : [1] Assurance Maladie, [2] Assurance Maladie, [3] ANS / GIE SESAM-Vitale

Six verbes pour éviter les confusions

Enrôler consiste à établir le lien initial entre une personne et son moyen d'identification. Identifier revient à distinguer cette personne des autres. Authentifier vérifie qu'un utilisateur contrôle le moyen associé à son compte. Autoriser détermine ensuite l'action qu'il peut réaliser. Tracer conserve les éléments utiles à l'explication d'une opération. Signer engage un processus de preuve portant sur un document ou une action définie.

Ces fonctions sont complémentaires. Une authentification techniquement réussie peut ouvrir une session rattachée au mauvais dossier si le rapprochement est mal conçu. Un professionnel reconnu peut recevoir une habilitation trop large. Une trace peut être inexploitable si elle ne permet pas d'identifier le contexte de l'action.

Les achats et projets devraient donc décrire chacune de ces fonctions. Qui vérifie l'identité lors de l'enrôlement ? Quel attribut associe le compte au patient ? Quel composant prend la décision d'accès ? Qui examine les anomalies ? Quelle preuve doit être conservée ? La réponse « notre solution est sécurisée » ne remplace aucune de ces informations.

Une architecture mature rend ces responsabilités explicites tout en proposant un parcours lisible. Le patient n'a pas besoin de connaître le vocabulaire des protocoles. L'organisation, elle, doit savoir distinguer ce que chaque composant prouve et ce qu'il laisse à sa charge.

Références : [4] RNIV, [8] DINUM, [10] CNIL

Six contrôles, une chaîne de confiance

Fonction	Question	Preuve à demander
Enrôlement	Qui est cette personne ?	Origine et vérification de l’identité
Identification	À quel dossier la relier ?	Identifiant, traits, statut et rapprochement
Authentification	Contrôle-t-elle le moyen ?	Événement et niveau de garantie
Autorisation	Que peut-elle faire ici ?	Rôle, finalité, contexte et périmètre
Traçabilité	Qui a fait quoi ?	Acteur, action, date et résultat
Signature	Quel engagement est prouvé ?	Contenu validé et processus de preuve

Une connexion réussie ne prouve pas à elle seule le droit d’accès ni la signature d’un acte.

Références : [3] ANS / GIE SESAM-Vitale, [4] RNIV, [10] CNIL, [14] OpenID Foundation, [21] ANSSI

L'INS : relier les données à la bonne personne

L'Identité nationale de santé sert au référencement des données de santé. Elle associe un matricule et des traits d'identité de référence. L'enjeu clinique est simple : permettre aux informations produites dans différents lieux de rester rattachées à la personne concernée. La qualité de ce rattachement compte autant que la circulation des documents.

La qualification d'une INS relève d'un cadre d'identitovigilance. Le RNIV décrit notamment le cas du titulaire d'une appli carte Vitale et celui des ayants droit présents dans son application. Ces situations ne sont pas interchangeables : l'enrôlement du titulaire ne vaut pas vérification équivalente de chaque ayant droit.

Sur le terrain, une identité discordante peut apparaître à l'admission, lors d'une transmission ou au rapprochement avec un dossier ancien. L'équipe doit disposer d'une procédure de traitement et d'un responsable identifiable. Une fusion erronée peut être plus dommageable qu'un compte temporairement séparé.

Nous recommandons de documenter le cycle de vie de l'identité : origine des traits, statut, méthode de qualification, corrections et décisions de rapprochement. L'évaluation doit inclure les homonymes, les variations d'état civil et les dossiers déjà existants. L'INS apporte un socle commun ; son intégration réussie dépend aussi des pratiques locales et de la qualité du logiciel.



INS : le matricule ne suffit pas

L’INS associe un matricule (NIR ou NIA) et cinq traits de référence : nom de naissance, liste des prénoms de naissance, date de naissance, sexe et lieu de naissance. Le matricule est complété par son OID. La qualification suit le cadre INS / RNIV ; elle réduit le risque de mauvais rattachement, sans supprimer les contrôles locaux.
À retenir : qualifier, rapprocher et corriger sont des opérations à organiser.

Références : [4] RNIV, [5] ANS

Le professionnel : un statut, un contexte, des droits

Pro Santé Connect permet aux professionnels des secteurs sanitaire, médico-social et social enregistrés au RPPS de s'authentifier auprès des services raccordés, notamment avec la e-CPS ou une carte CPS. Il fournit une brique de confiance sur l'identité professionnelle. L'application métier doit ensuite décider des accès pertinents.

Un même professionnel peut exercer dans plusieurs structures. Il peut changer de fonction, remplacer un collègue ou intervenir exceptionnellement. Un statut valable dans un répertoire ne suffit donc pas à représenter toutes les permissions locales. Le besoin d'en connaître reste lié à l'activité effectivement exercée et au contexte de prise en charge.

La gouvernance des habilitations devrait couvrir l'arrivée, la mobilité et le départ, avec un contrôle spécifique des droits temporaires. Le projet doit éviter de transformer un raccordement national en prétexte pour conserver des comptes locaux trop permissifs. Les rôles, les exceptions et les accès d'urgence doivent être expliqués aux équipes.

La CPS4 introduit une clé FIDO2 et une télé-mise à jour en cours de déploiement. La compatibilité se prépare : Cryptolib 5.2 au minimum et lecteur MIFARE DESFire pour le sans-contact, selon l'ANS. Un changement de carte engage donc aussi les postes, lecteurs et procédures de support. [29]

Une bonne question de comité de pilotage : si un professionnel quitte aujourd'hui la structure, quel événement retire demain ses accès ? La réponse doit nommer un flux, un responsable et une vérification. L'identité nationale et l'autorisation locale forment deux étages complémentaires du même dispositif.

Références : [7] ANS, [10] CNIL, [29] ANS

Patient et professionnel : une confiance à deux faces

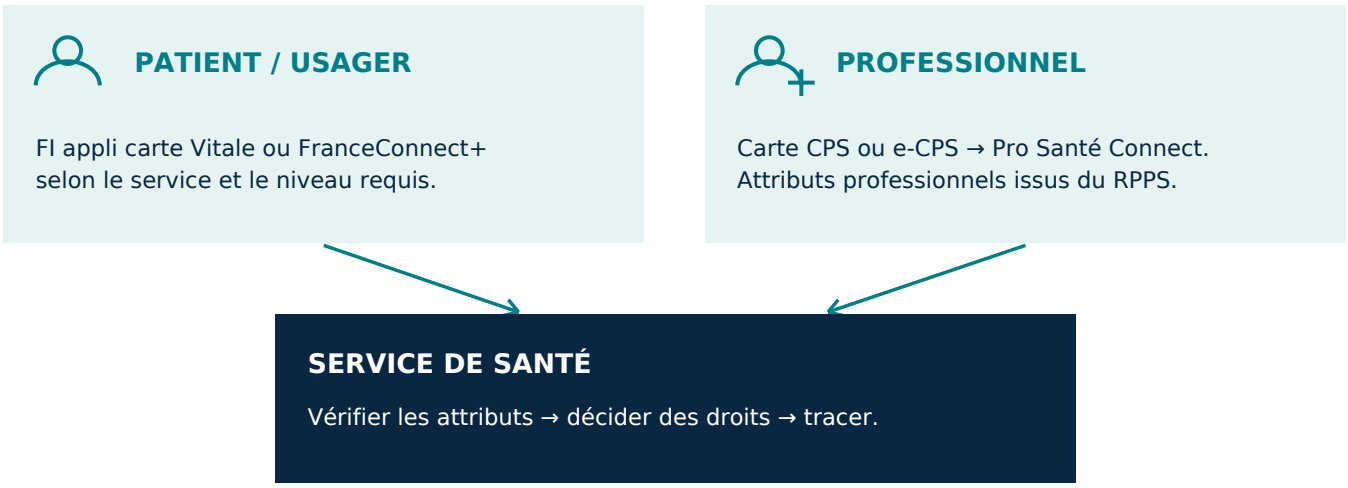
Les parcours numériques mettent souvent en relation deux personnes à identifier : l'usager et le professionnel. Leur confiance repose sur des moyens, répertoires et procédures distincts. Cette séparation évite d'attribuer au patient un rôle professionnel ou de traiter la connaissance d'une identité comme une permission générale d'accès.

Dans une téléconsultation, l'identification de l'usager peut contribuer au rattachement du compte à son dossier. Celle du professionnel contribue à vérifier qui intervient. Le service doit encore déterminer les conditions de consultation, d'accès aux documents et de conservation des traces. Le fait que les deux côtés utilisent des standards compatibles facilite l'intégration ; il ne règle pas toutes les obligations du parcours.

Cette architecture invite à traiter également les représentants, aidants et personnels administratifs. Qui agit pour qui ? Comment l'étendue d'un mandat est-elle vérifiée ? Comment sa fin est-elle prise en compte ? Le compte d'un tiers ne devrait pas être confondu avec l'identité de la personne soignée.

Le bénéfice attendu est une attribution plus claire des actions. Pour l'obtenir, les tests doivent suivre une transaction entière : ouverture du service, identification, rapprochement, décision d'accès, action métier, déconnexion et correction d'une erreur éventuelle. Deux authentifications réussies ne constituent pas automatiquement un acte juridiquement signé.

DEUX AUTHENTIFICATIONS, UNE DÉCISION D’ACCÈS



INS : rattachement des données au patient, distinct de l’authentification.
Schéma de principe ; moyens disponibles selon le raccordement du service.

Références : [3] ANS / GIE SESAM-Vitale, [7] ANS

L'enrôlement : le premier moment de vérité

Une identité numérique commence avant la première connexion. Il faut établir que la personne qui active le moyen d'identification correspond bien à l'identité annoncée. Le parcours doit résister aux tentatives de fraude tout en restant praticable pour les usagers légitimes.

Pour l'appli carte Vitale, les parcours officiels incluent notamment l'utilisation de France Identité et la vérification à distance. La généralisation de novembre 2025 a élargi l'accès national. Les pièces admises et conditions d'éligibilité doivent cependant être vérifiées dans la documentation en vigueur au moment de l'accompagnement.

L'ANSSI traite la robustesse de la vérification à distance à travers le cadre PVID. Le sujet dépasse la prise d'un selfie : il concerne l'examen des preuves, le lien avec la personne et les garanties du processus. La résistance de l'enrôlement ne doit pas être déduite du seul nom d'un algorithme ou d'une promesse commerciale.

Notre proposition de déploiement : observer les étapes où l'usager échoue, distingue mal les applications ou attend une réponse. Prévoir une explication simple, un support humain et une voie de résolution pour les discordances. Sans ce service, la sécurité peut devenir une expérience de blocage dont personne ne porte clairement la responsabilité.

Références : [1] Assurance Maladie, [11] ANSSI, [12] France Identité

Les niveaux de garantie ne sont pas des slogans

Les niveaux faible, substantiel et élevé du cadre eIDAS caractérisent des garanties attachées à l'identification électronique. Ils ne doivent pas devenir des adjectifs généraux appliqués à tout un parcours. Le niveau d'un moyen d'identification ne décrit pas la qualité d'un dossier, l'habilitation d'un utilisateur ou la fiabilité du service clinique.

La documentation FranceConnect distingue FranceConnect, qui prend en charge le niveau faible, de FranceConnect+, qui prend en charge les niveaux substantiel et élevé. Cette distinction influe sur le choix du service et du fournisseur d'identité, ainsi que sur les exigences d'intégration.

Le décideur doit demander des éléments précis : périmètre couvert, version, organisme d'évaluation, modalités d'enrôlement, mécanismes d'authentification et conditions de maintien des garanties. Une ambition de certification et une certification obtenue sont deux informations différentes. De même, une qualification d'un prestataire ne se transfère pas automatiquement à tous ses clients.

La proportionnalité est une question d'architecture. On définit le risque de l'action, puis le niveau de confiance nécessaire et les contrôles complémentaires. La bonne décision évite à la fois la protection insuffisante d'une action sensible et la surenchère de contraintes sur un usage qui ne les justifie pas.

Références : [8] DINUM, [13] Commission européenne

FranceConnect : fédérer sans tout confondre

FranceConnect et FranceConnect+ organisent une relation entre des services en ligne et des fournisseurs d'identité. Ils permettent à l'usager de réutiliser un moyen d'identification plutôt que de créer un compte indépendant pour chaque démarche. Cette fédération repose sur une intégration technique et un cadre d'habilitation.

France Identité figure parmi les fournisseurs disponibles sur les deux plateformes ; son utilisation sur FranceConnect+ nécessite une identité numérique certifiée. La liste officielle consultée ne présente pas l'appli carte Vitale comme un fournisseur FranceConnect+ déjà disponible. Le livre blanc ne transforme donc pas une convergence envisagée en raccordement effectif.

Il faut également distinguer un fournisseur d'identité d'un fournisseur de données. Le premier contribue à établir qui se connecte ; le second peut transmettre des informations selon un cadre et une finalité propres. L'accès à un service de santé ne justifie pas par défaut la transmission de tous les attributs disponibles.

La conséquence opérationnelle est importante : chaque parcours doit préciser l'identité reçue, son rapprochement avec le compte local et les données réellement nécessaires. « Un bouton unique » décrit l'expérience visible. En arrière-plan, plusieurs contrats de confiance et règles métier restent à organiser.



FranceConnect+ : choisir le niveau requis

FranceConnect et FranceConnect+ ne portent pas le même niveau de garantie : faible pour le premier, substantiel ou élevé pour le second. Le choix dépend du parcours et des exigences applicables. Une garantie renforcée ne donne ni un droit clinique d’accès ni une permission générale de rapprocher des dossiers.
À retenir : documenter le niveau requis, les attributs reçus et les habilitations.

Références : [8] DINUM, [9] DINUM, [12] France Identité

L’identité a plusieurs rôles

Brique	Rôle documenté	À distinguer
Appli carte Vitale	Alternative mobile ; fournisseur d’identité à distance selon raccordement	Compte local et permission métier
INS	Référencement des données de santé	Authentification de session
RPPS	Répertoire professionnel	Droits locaux dans un établissement
Pro Santé Connect	Authentification professionnelle des services raccordés	Décision d’accès aux dossiers
FranceConnect / +	Fédération entre identités et services	Fournisseur de données
France Identité	Identité issue de la CNIe ; parcours certifié pour FC+	Appli carte Vitale

Le patient, l’assuré, l’aidant et le professionnel ne sont pas des rôles interchangeables.

Références : [3] ANS / GIE SESAM-Vitale, [5] ANS, [7] ANS, [8] DINUM, [12] France Identité

Le fournisseur d'identité appli carte Vitale

Le référentiel de l'appli carte Vitale décrit l'authentification à distance de son utilisateur auprès d'un fournisseur de services autorisé. Le fournisseur d'identité délivre des jetons conformes à OpenID Connect. Ce cadre constitue une base documentée pour penser l'application au-delà de la présentation au guichet.

Le raccordement implique des obligations concernant les flux, la protection des informations techniques de connexion, les tests et la gestion de comptes. Le document traite aussi la simplicité d'utilisation, la compréhension et l'assistance. L'expérience de l'usager fait donc partie du problème d'intégration.

Pour un éditeur, ajouter une connexion ne suffit pas. Il faut concevoir l'association à un dossier existant, l'information de l'usager et le comportement en cas d'échec. Le parcours doit empêcher qu'une nouvelle méthode d'accès multiplie les comptes ou fusionne abusivement deux identités.

Notre recommandation est de mener ensemble la conception métier, l'intégration et les tests d'exception. Un dossier de raccordement utile décrit ce qui se produit après le retour du jeton : quelle correspondance est établie, quels droits sont ouverts et comment l'usager peut contester un rattachement. La confiance initiale doit rester explicable tout au long du service.

Appli carte Vitale : distinguer les usages

En présentiel, la lecture QR / NFC permet un usage dans les logiciels compatibles. À distance, le rôle de fournisseur d’identité relève d’un raccordement, d’un profil et de fonctionnalités effectivement disponibles. Une activation sur smartphone ne prouve pas qu’un portail patient est raccordé.
À retenir : vérifier séparément le support, le flux d’authentification et les droits ouverts.

Références : [3] ANS / GIE SESAM-Vitale

OIDC : ce que le protocole apporte

OpenID Connect ajoute une couche d'identité au cadre OAuth 2.0. Il permet à un service client de recevoir des informations sur l'authentification réalisée par un fournisseur d'identité. L'ID Token porte des assertions ; le jeton d'accès sert à accéder à une ressource selon le profil retenu. Les confondre crée des erreurs de conception.

Un JWT n'est pas, par nature, un contenu secret. Il peut être signé et, selon le cas, chiffré. La signature sert à contrôler son origine et son intégrité ; le chiffrement répond à la confidentialité. Le transport sécurisé ne dispense pas de vérifier les propriétés du jeton et les règles du protocole.

L'intégration doit s'appuyer sur la documentation du fournisseur : émetteur attendu, destinataire, durée de validité, paramètres du flux, traitement des sessions et rotation des clés. Ces points sont à vérifier par les équipes techniques dans le profil applicable, sans improviser une implémentation à partir d'un schéma de présentation.

L'intérêt stratégique du standard est de rendre les intégrations plus cohérentes et testables. Il ne produit pas automatiquement une conformité réglementaire, un droit clinique d'accès ou une signature de prescription. La confiance se construit aussi dans les configurations, les procédures et l'exploitation.

OIDC : signé ne signifie pas chiffré

OpenID Connect ajoute une couche d’authentification à OAuth 2.0. L’ID Token est un JWT signé selon le profil ; son chiffrement est optionnel. Le destinataire doit contrôler notamment l’émetteur, l’audience, la validité et la signature. Les attributs reçus dépendent de l’enrôlement et du fournisseur.
À retenir : un standard facilite l’intégration ; il ne sécurise pas seul tout le parcours.

Références : [14] OpenID Foundation

Un compte unique exige un rapprochement prudent

La fédération peut simplifier les connexions tout en compliquant la gestion des comptes existants. Un patient possède parfois un dossier créé à l'accueil, un compte de portail et un accès provenant d'un autre service. L'introduction d'une identité externe doit organiser leur rapprochement.

Le référentiel appli carte Vitale prévoit une procédure sécurisée de fusion et la vérification de correspondance des INS lorsque le service les possède. La similitude d'un nom ou d'une adresse électronique ne constitue pas une preuve suffisante dans toutes les situations.

Nous proposons de distinguer trois décisions : associer une méthode d'authentification à un compte, rapprocher deux comptes et fusionner deux dossiers métier. Leurs conséquences diffèrent. Une fusion de dossiers peut modifier les données visibles, l'historique et les actions possibles. Elle doit être contrôlable et réparable.

Un test réaliste inclut deux personnes homonymes, une erreur ancienne d'état civil, une adresse partagée et un représentant. Le service doit pouvoir suspendre une association incertaine sans interrompre inutilement la prise en charge. La qualité d'une architecture se voit aussi dans la manière dont elle renonce à automatiser une décision quand les preuves ne suffisent pas.

Références : [3] ANS / GIE SESAM-Vitale, [4] RNIV

Interopérabilité : partager un sens, pas seulement un flux

Deux services peuvent échanger un jeton ou un document tout en donnant une signification différente aux mêmes informations. L'interopérabilité technique ne suffit donc pas. Il faut préciser ce que représente chaque identité, quel événement l'a validée et à quelle action elle peut être liée.

L'identité de l'assuré, celle du patient et celle du représentant ne se superposent pas toujours. Une information de couverture, un statut professionnel ou un identifiant de dossier ne doivent pas être utilisés comme substituts les uns des autres. Un modèle commun doit expliciter ces relations.

Le projet devrait produire un dictionnaire d'attributs compréhensible par le métier et la technique : origine, finalité, fraîcheur, caractère obligatoire, durée de conservation et procédure de correction. Les relations avec les répertoires doivent être décrites, ainsi que les conditions de mise à jour.

Le DPI est le dossier informatisé de la structure, utilisé dans son travail quotidien. Le DMP est le dossier partagé national intégré à Mon espace santé. Consulter le DMP depuis un DPI implique deux systèmes, avec leurs propres règles d'accès et de traçabilité. [30]

Un exemple documenté : l'authentification indirecte renforcée pour la consultation du DMP à l'hôpital. Le guide prévoit un certificat de structure, le transport du FINESS et du RPPS, et une authentification à deux facteurs du professionnel dans le DPI, le SSO ou la session SIH. L'identité de la structure ne remplace donc pas celle de l'acteur à tracer. [30]

La trajectoire européenne renforce l'intérêt de cette discipline. Un attribut reçu d'un autre contexte national ne peut pas être supposé immédiatement compatible avec un dossier local. L'équipe doit vérifier le sens et les règles d'association avant d'ouvrir des accès. Un échange réussi devient un usage sûr lorsque la donnée conserve son interprétation tout au long du parcours.

Références : [5] ANS, [7] ANS, [15] Commission européenne, [30] ANS / Assurance Maladie

Le cabinet et l'officine : réussir le geste réel

En présentiel, l'appli carte Vitale rencontre une organisation, un logiciel et un équipement de lecture. La documentation destinée aux médecins décrit notamment les modalités QR code ou NFC, les informations accessibles et l'appel systématique au service de droits ADRi pour la part obligatoire. Le parcours dépend de la compatibilité effective de l'ensemble.

La bonne démonstration est celle que l'équipe peut reproduire lors d'une journée normale. Où le patient présente-t-il son téléphone ? Qui réalise la lecture ? Que voit le professionnel ? Que fait-on si la caméra échoue, si le téléphone est déchargé ou si une mise à jour modifie le comportement ?

L'évaluation locale devrait comparer les opérations complètes, pas seulement le temps de lecture. Une seconde gagnée sur une étape peut être annulée par une recherche de compte ou une erreur de routage. Les gains attendus restent des hypothèses tant qu'ils ne sont pas mesurés dans le parcours choisi.

Nous recommandons un pilote associant des professionnels, l'accueil et des patients aux profils variés. Il doit déboucher sur une consigne simple, un matériel compatible, une assistance et une alternative physique. Le geste devient une simplification lorsque chacun sait comment avancer, y compris en cas d'exception.

Références : [2] Assurance Maladie

Trois mécanismes à comparer

Mécanisme	Ce qu’il permet	Ce qu’il ne suffit pas à prouver
OIDC	Recevoir des assertions sur l’authentification selon un profil	Conformité de tout le parcours ou signature juridique
FIDO / passkey	Contrôler l’accès à un compte avec une preuve cryptographique liée au service	Identité civile ou qualité professionnelle
Portefeuille d’identité	Présenter des attributs ou attestations vérifiables selon leur cadre	Disponibilité universelle ou droit clinique d’accès

DES MÉCANISMES COMPLÉMENTAIRES

OIDC

Assertions sur l’authentification

FIDO / PASSKEY

Preuve cryptographique d’accès

PORTEFEUILLE

Attributs et attestations

Logos à titre de référence documentaire ; aucune affiliation ou certification du livre blanc.

Le niveau de confiance dépend de l’enrôlement, de l’émetteur, du profil et de la vérification du destinataire.

Références : [13] Commission européenne, [14] OpenID Foundation, [19] FIDO Alliance

La préadmission hospitalière : éviter le double travail

Scénario illustratif : une personne complète sa préadmission depuis son domicile puis se présente à l'hôpital. L'identification à distance peut contribuer à préparer le dossier. Le bénéfice organisationnel apparaît seulement si les informations sont correctement retrouvées, comprises et utilisées à l'accueil.

Un parcours mal coordonné demande les mêmes pièces plusieurs fois, recrée un dossier et laisse aux agents la charge de résoudre les incohérences. L'ajout d'une identité externe peut alors déplacer la friction au lieu de la réduire. L'équipe doit savoir ce qui a été vérifié en amont et ce qui reste à contrôler sur place.

Nous proposons de cartographier les responsabilités avant le pilote : service en ligne, cellule d'identitovigilance, admissions, unité de soins et support informatique. Chaque étape devrait avoir un résultat attendu et une voie d'escalade. Les éléments déjà établis ne doivent pas être refaits par habitude ; les contrôles utiles ne doivent pas disparaître par automatisme.

Le tableau de bord peut suivre les préadmissions retrouvées, dossiers en doublon, demandes répétées de pièces et corrections après arrivée. Une amélioration crédible combine un parcours plus simple et un niveau de sécurité maintenu. Ce scénario décrit un objectif de conception, pas un déploiement national déjà constaté.

Références : [3] ANS / GIE SESAM-Vitale, [4] RNIV, [10] CNIL

Même patient, deux parcours

Scénario fictif : des organisations différentes, pas une promesse de déploiement universel.

Un parcours avec friction

Monsieur Dupont, 72 ans, arrive à l’hôpital. Son identité est ressaisie à plusieurs étapes. Une discordance entre deux dossiers impose une vérification supplémentaire avant de rattacher un résultat d’examen. Le patient répète ses informations ; les équipes consacrent du temps à résoudre l’écart.

Un parcours mieux intégré

Dans un établissement équipé et organisé, la lecture de son appli carte Vitale facilite la récupération de son identité, selon les modalités applicables. Les logiciels compatibles et les procédures d’identitovigilance permettent de mieux rattacher les documents à son dossier.

Le professionnel s’authentifie auprès d’un service raccordé à Pro Santé Connect, puis accède aux informations selon ses habilitations. La connexion, le rapprochement des dossiers et l’autorisation d’accès restent des opérations distinctes.

Le bénéfice se mesure sur le terrain

L’objectif est de réduire les ressaisies, les erreurs de rapprochement et les demandes répétées. Le résultat dépend de l’intégration des logiciels, de la qualité des données, de la formation et de l’organisation du travail. Il doit être vérifié sur le parcours entier.

La fluidité se construit entre les services.
Elle ne se déduit pas d’une connexion réussie.

Références : [4] RNIV, [5] INS, [6] ApCV, [7] Pro Santé Connect, [10] CNIL

La télésanté : reconnaître sans perdre le contexte

Scénario illustratif : un patient rejoint une téléconsultation depuis un lien reçu. Le service doit relier cette connexion à la personne attendue, au rendez-vous et au professionnel intervenant. L'authentification constitue une étape de ce parcours, mais elle ne remplace ni l'échange clinique ni les autres contrôles nécessaires.

La présence d'un proche, un appareil partagé ou une connexion réalisée pour un enfant soulèvent des questions distinctes. La plateforme devrait permettre d'exprimer qui agit et pour qui, selon les règles du service. L'ouverture d'une session ne doit pas masquer le rôle d'un représentant.

En télésurveillance, l'identité se combine aussi avec celle du dispositif et l'origine d'une mesure. Le compte qui transmet, la personne suivie et le capteur utilisé sont trois objets différents. Leur association doit pouvoir être corrigée lors d'un remplacement de matériel ou d'un changement d'organisation.

Notre recommandation : tester l'arrivée depuis un lien, la reconnexion, le changement d'appareil et l'absence du patient attendu. Définir également le recours à l'assistance et la continuité de l'échange. Une connexion forte ne compense pas une ambiguïté persistante sur la personne effectivement prise en charge.

Références : [3] ANS / GIE SESAM-Vitale, [7] ANS

Tiers payant : relier identité, droits et paiement

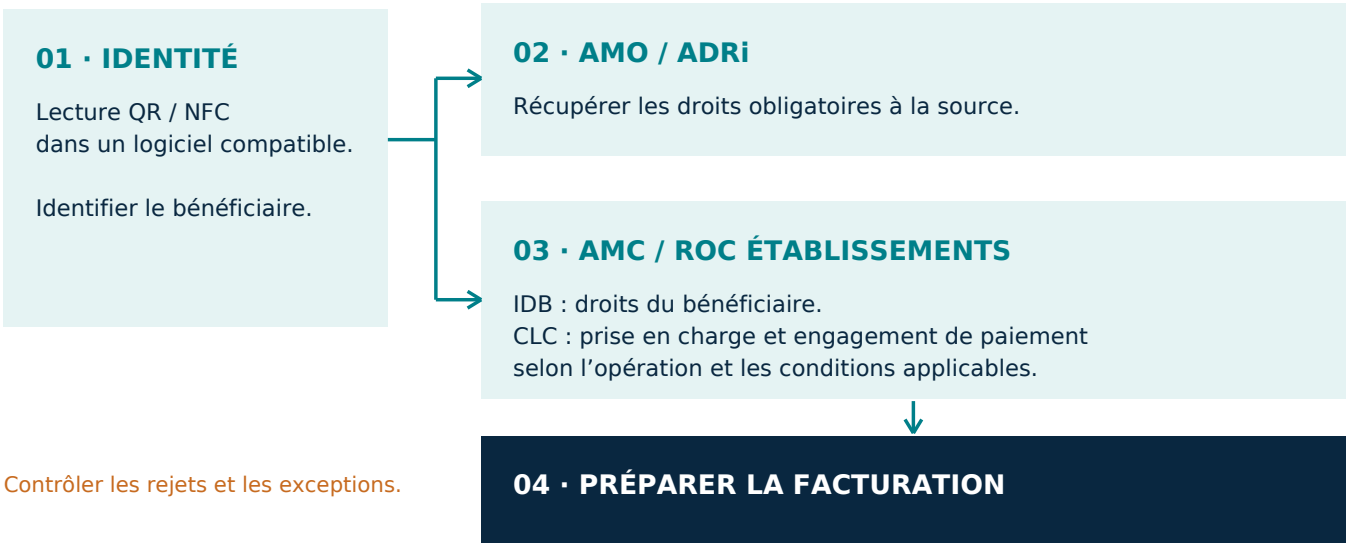
Une identité juste ouvre le parcours ; une information de droits à jour prépare la facturation ; un engagement de paiement sécurise la recette dans son périmètre contractuel. Ces trois fonctions doivent être articulées dans le logiciel, sans être confondues. Le professionnel a besoin de savoir qui est couvert, pour quelle prestation et à quelles conditions.

Des mécanismes existent déjà. Pour l'AMO, ADRi permet de récupérer les droits à la source. Pour l'AMC, ROC Établissements distingue IDB, qui renseigne les droits du bénéficiaire, de CLC, qui retourne le montant pris en charge et un numéro d'engagement valant garantie de paiement. La garantie porte sur une opération et ses conditions, pas sur toutes les factures futures. [2,32]

Notre exigence de conception : proposer un parcours coordonné de vérification AMO/AMC, afficher la date des droits et l'engagement associé, conserver les éléments nécessaires à une contestation, puis orienter chaque exception vers un responsable. La cible est une chaîne lisible depuis l'identification jusqu'au rapprochement du paiement, sans multiplier les ressaisies.

L'intégration de données AMC à l'appli carte Vitale reste une évolution annoncée à terme ; elle n'atteste pas une garantie universelle synchronisée en 2027. La priorité opérationnelle est de raccorder les services effectivement disponibles et d'évaluer les rejets, le délai de paiement et le temps de traitement. Réduire cette charge administrative constitue un levier d'adoption à mesurer sur le terrain.

IDENTITÉ, DROITS ET ENGAGEMENT : TROIS FONCTIONS



Objectif : fiabiliser le circuit. Aucun raccordement ne garantit l’absence de rejet ou d’avance de frais.

Références : [2] Assurance Maladie, [6] G_NIUS / ANS, [32] Inter AMC

Un portefeuille n'est pas une simple collection d'images

Un portefeuille d'identité numérique permet de présenter des attributs ou attestations vérifiables. La valeur de la preuve dépend de son émetteur, de son format, des mécanismes de présentation et des vérifications du destinataire. Une photographie de document dans un téléphone ne constitue pas l'équivalent de cette chaîne.

Le cadre européen organise les portefeuilles EUDI et leurs garanties. Des offres privées proposent également des fonctions d'identité dans les systèmes mobiles. Ces approches doivent être comparées selon les mêmes questions : qui émet, qui conserve, qui vérifie et qui peut révoquer ?

Pour la santé, le portefeuille pourrait contribuer à présenter une identité ou un attribut adapté à un usage. Il ne devient pas pour autant un dossier médical ni une source universelle de droits. Le design doit éviter d'accumuler des informations sensibles sans finalité explicite.

Notre analyse : le potentiel principal réside dans une preuve mieux adaptée à la demande, avec moins de données exposées. Cette promesse doit être vérifiée par l'implémentation. Les modèles de gouvernance, la récupération après perte et les possibilités d'usage sans équipement compatible comptent autant que la commodité de présentation.

Références : [13] Commission européenne, [16] Apple, [17] Google

EUDI : l'ambition européenne et ses conditions

La Commission européenne présente la mise à disposition des portefeuilles d'identité numérique européens par les États membres comme une échéance de fin 2026. Leur usage est volontaire. Le cadre poursuit une interopérabilité européenne et une maîtrise accrue des données présentées par les utilisateurs.

Ce calendrier n'autorise pas à supposer que tous les usages de santé seront opérationnels immédiatement. Les portefeuilles, émetteurs d'attestations et services destinataires doivent fonctionner dans des conditions compatibles. L'acceptation juridique, la certification et l'intégration sectorielle restent des objets à vérifier.

Pour un acteur de santé, la décision pertinente consiste à préparer l'architecture à plusieurs modes de preuve sans annoncer une migration générale prématurée. Il faut identifier les attributs réellement nécessaires et suivre les spécifications applicables au cas d'usage. Le passage à un portefeuille ne devrait pas rendre les parcours plus dépendants d'un seul équipement.

Nous recommandons de distinguer trois niveaux dans la feuille de route : cadre adopté, mécanismes effectivement disponibles et usages locaux validés. L'organisation peut ainsi investir progressivement tout en conservant une information honnête pour les usagers. L'interopérabilité européenne est un objectif structurant, avec un travail d'exécution à accomplir.

Références : [13] Commission européenne, [18] Commission européenne

Apple et Google : comparer les chaînes de confiance

Apple décrit plusieurs modalités d'ajout d'une identité à Wallet, avec des rôles différents pour Apple et l'autorité émettrice selon le parcours. Google documente le provisionnement d'identifiants et la vérification en ligne de preuves numériques, notamment à travers les mécanismes Digital Credentials. Ces documents donnent des informations d'architecture, pas une garantie de disponibilité identique dans tous les pays.

Pour comparer ces offres aux portefeuilles publics, le critère pertinent est la chaîne de confiance : qui approuve l'identité, qui voit les données et quelle preuve reçoit le service ? La présence d'une application dans le système d'exploitation ne constitue pas, à elle seule, une reconnaissance eIDAS.

L'avantage potentiel est une interface familière, proche des usages quotidiens. Le risque stratégique concerne la dépendance à des appareils, comptes, politiques de distribution et mécanismes de récupération maîtrisés par d'autres acteurs. Cette dépendance doit être documentée, pas supposée inacceptable par principe.

Notre grille d'achat demande la disponibilité géographique, les appareils couverts, le contrôle des attributs, les modalités de révocation et la portabilité. Elle demande aussi ce qui se passe lorsqu'un téléphone est remplacé ou qu'un fournisseur modifie ses conditions. La facilité d'usage et la maîtrise à long terme doivent être évaluées ensemble.

Références : [16] Apple, [17] Google

FIDO et passkeys : retirer le secret réutilisable

Avec FIDO, l'utilisateur prouve le contrôle d'une clé par une réponse cryptographique liée au service attendu. Un faux site ne peut pas simplement récupérer un mot de passe puis le rejouer sur le vrai service. C'est un changement concret face au phishing et à la réutilisation des mots de passe. OIDC organise l'échange d'assertions ; il n'apporte pas, à lui seul, cette résistance au phishing. [19,31]

Deux modèles doivent être distingués. Une passkey liée à un appareil reste sur cet authentificateur, par exemple une clé physique ; une passkey synchronisée peut être disponible sur plusieurs appareils via son fournisseur. Toutes les passkeys ne sont donc pas attachées exclusivement à un seul matériel. Elles prouvent le contrôle d'un moyen, et non, à elles seules, une identité civile ou professionnelle. [31]

Pour la santé, notre recommandation est de remplacer les secrets réutilisables par des moyens individuels adaptés au risque, avec enrôlement vérifié et révocation. Cela réduit une voie importante d'usurpation, sans démontrer la disparition de la fraude à l'Assurance Maladie. Le prêt volontaire d'un authentificateur, le partage d'une session et la compromission d'un poste restent à traiter.

Le cahier des charges doit préciser le modèle de passkey, les appareils autorisés, le contrôle local et la récupération. Tester perte, vol, départ et accès d'urgence. La protection du parcours normal doit rester cohérente avec celle du secours : un mécanisme résistant au phishing ne sécurise pas une récupération contournable.

Passkeys : résister au phishing, prévoir le secours

Les passkeys utilisent une paire de clés cryptographiques et sont liées au service. Elles peuvent être synchronisées ou liées à un appareil ; la vérification locale peut utiliser un code ou la biométrie. Leur résistance au phishing ne protège pas automatiquement la récupération du compte ou une session compromise.
À retenir : choisir le modèle et tester perte, révocation et récupération.

Références : [19] FIDO Alliance, [31] FIDO Alliance

EHDS : quatre horizons à distinguer

Le règlement sur l'Espace européen des données de santé a été publié le 5 mars 2025 et est entré en vigueur le 26 mars. Son application est progressive. La Commission situe plusieurs actes d'exécution clés en 2027, puis des étapes importantes en 2029 et 2031.

Pour l'usage primaire, 2029 concerne notamment les résumés de patients, prescriptions électroniques et délivrances électroniques. Les images médicales, résultats de laboratoire et comptes rendus de sortie relèvent de l'étape 2031. Pour l'usage secondaire, le calendrier distingue également différentes catégories de données.

Cette progression modifie la lecture stratégique. Il faut préparer les systèmes et la gouvernance tout en évitant de présenter mars 2029 comme une date unique applicable à tous les logiciels et toutes les fonctions. Les obligations doivent être examinées par catégorie et périmètre de produit.

L'identité participe à cette préparation, avec le rapprochement des données, l'attribution des actions et les droits d'accès. Elle ne remplace pas les exigences d'interopérabilité des dossiers. Notre recommandation est une cartographie de conformité associant chaque usage à ses textes, composants et jalons, puis une révision à la publication des actes d'exécution pertinents.

Références : [15] Commission européenne, [20] Union européenne

Une convergence à organiser

Ségur, feuille de route nationale et EEDS : des transformations complémentaires, avec des périmètres et des calendriers distincts.

01 · Ségur du numérique en santé

Le programme soutient l'évolution des logiciels et le partage sécurisé des données. À l'hôpital, les exigences couvrent notamment des documents intégrant l'INS qualifiée et leur transmission au DMP de Mon espace santé.

02 · Feuille de route 2023-2027

Elle poursuit la transformation engagée avec les services socles et Mon espace santé. Elle inscrit les usages, l'accès aux services et l'accompagnement dans une stratégie nationale ; elle ne signifie pas que tous les parcours locaux sont déjà intégrés.

03 · Espace européen des données de santé

L'application est progressive. Pour l'usage primaire, 2029 concerne notamment les résumés de patients et les prescriptions et délivrances électroniques. Les images médicales, résultats de laboratoire et comptes rendus de sortie relèvent de 2031.

La décision à prendre maintenant

Relier la trajectoire nationale aux besoins du terrain : fiabiliser les identités, vérifier les habilitations, assurer l'interopérabilité, tracer les accès et organiser la continuité. L'identité numérique est une fondation de cette architecture ; elle ne remplace ni la sécurité des systèmes ni la gouvernance des usages.

Sources complémentaires · ANS : Ségur à l'hôpital ; feuille de route 2023-2027.
Calendrier européen : [15] Commission européenne, [20] règlement EEDS.

Usage primaire et secondaire : deux décisions d'accès

L'usage primaire concerne la prise en charge et l'accès de la personne à ses informations. L'usage secondaire concerne notamment la recherche, l'innovation et des missions d'intérêt public dans un cadre organisé. Le fait qu'une identité soit connue ne permet pas de passer librement de l'un à l'autre.

Pour un chercheur, l'identification contribue à attribuer l'accès et les actions. L'accès aux données relève cependant d'un processus spécifique : finalité, autorisation, environnement et protections appropriées. Le système ne devrait pas utiliser un compte authentifié comme raccourci vers un ensemble de données sensibles.

La distinction protège aussi l'usager. Accepter une étape de connexion ou un partage d'attributs d'identité n'est pas l'équivalent d'accepter toute réutilisation des informations de santé. Les interfaces doivent expliquer la décision réellement demandée et le cadre de l'accès.

Nous proposons une séparation lisible des registres : identité du demandeur, mandat, périmètre autorisé, finalité et traces d'activité. Pour la recherche, les besoins de pseudonymisation et d'environnement sécurisé doivent être instruits dans leur cadre propre. Une identité forte facilite la responsabilité ; elle ne constitue pas une justification suffisante de la réutilisation.

Références : [15] Commission européenne, [20] Union européenne

Authentification et signature : deux preuves différentes

Une connexion prouve un événement d'authentification selon un mécanisme donné. Une signature porte sur un engagement ou un document défini, dans un processus de preuve adapté. Le rattachement des deux opérations doit être explicite. Leur coexistence ne suffit pas à produire automatiquement une signature qualifiée.

Une prescription, un consentement ou une décision administrative soulèvent des questions différentes : qui a validé, quel contenu exact, à quel instant et avec quelle intention ? Les réponses doivent résister à la contestation et à l'évolution des systèmes. Un journal de connexion ne décrit pas nécessairement ce qui a été accepté.

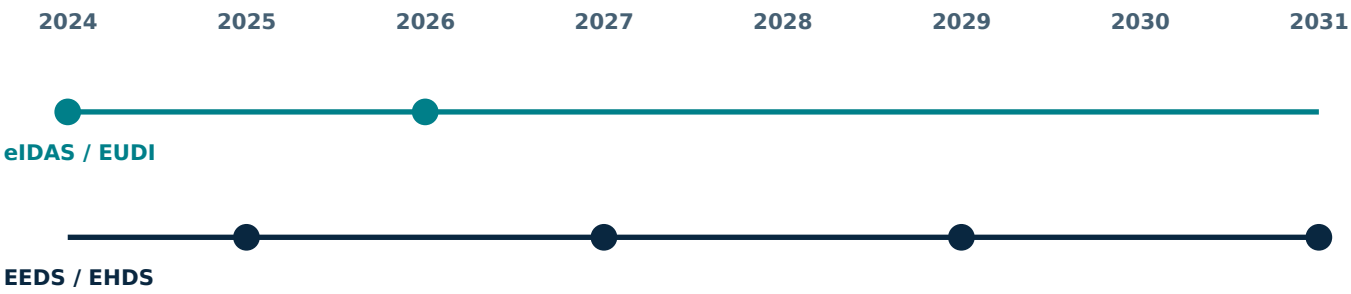
Pour les équipes, le risque est de surinterpréter les mots « signé », « certifié » et « sécurisé ». Le cahier des charges doit demander la nature de la preuve et son périmètre. Une signature cryptographique de jeton ne doit pas être présentée comme l'engagement juridique du patient sur un acte clinique.

Notre recommandation est une revue commune du métier, du juridique et de la sécurité pour les actions engageantes. Elle précise le contenu présenté, le mécanisme de validation, les données conservées et la procédure de vérification. Le bon niveau de preuve se construit pour l'action considérée, pas à partir du seul protocole d'accès.

Références : [14] OpenID Foundation, [21] ANSSI

Le calendrier européen sans raccourci

DEUX TRAJECTOIRES, DES ÉCHÉANCES À DISTINGUER



2024 · eIDAS

Cadre européen d’identité numérique renouvelé.
Règlement (UE) 2024/1183.

26 MARS 2025 · EEDS

Entrée en vigueur du règlement.
Début de la transition.

FIN 2026 · EUDI

Mise à disposition prévue des wallets.
Calendrier de la Commission ; usage volontaire.

MARS 2027 · EEDS

Plusieurs actes d’exécution clés.
Précisions pour l’application.

MARS 2029 · EEDS

Résumés patients, e-prescriptions / délivrances ; une partie de l’usage secondaire.

MARS 2031 · EEDS

Images, laboratoires, sorties hospitalières ; autres catégories de l’usage secondaire.

Entrée en vigueur, disponibilité technique et application d’une obligation sont trois événements distincts.

Références : [13] Commission européenne, [15] Commission européenne, [20] Union européenne, [27] Union européenne

Minimiser : transmettre la preuve utile

La CNIL rappelle que les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour la finalité. Cette exigence s'applique à l'identité autant qu'au contenu médical. Un service ne devrait pas recevoir un ensemble complet d'attributs simplement parce qu'ils sont disponibles.

Le projet doit commencer par une question métier : quelle décision exige cette information ? Vérifier une condition d'accès, rapprocher un dossier ou facturer un acte ne mobilise pas forcément les mêmes données. La minimisation consiste à documenter ces besoins et à limiter les transmissions et conservations.

Les traces elles-mêmes nécessitent une gouvernance. Elles peuvent révéler des relations avec des services de santé. Leur utilité pour la sécurité ne justifie pas une exploitation indéfinie ni leur diffusion dans tous les outils de support. Les données envoyées aux prestataires doivent être cartographiées.

Nous proposons une revue par attribut : finalité, origine, destinataire, durée et possibilité de suppression ou correction. Les environnements de test et captures d'écran méritent la même attention. Le succès d'une connexion doit se mesurer aussi à la quantité de données que le service a pu éviter de collecter.

Références : [22] CNIL, [23] CNIL

Le consentement : nommer la décision réelle

Le mot consentement peut recouvrir plusieurs gestes : accepter une transmission d'attributs, autoriser un accès dans un service ou consentir à une intervention. Ces décisions ne sont pas interchangeables. Une interface lisible doit expliquer ce que l'utilisateur accepte à cet instant.

Les traitements de données de santé ne reposent pas tous sur la même base juridique. Le projet doit identifier le cadre applicable avec son délégué à la protection des données et ses responsables métier. Une case à cocher ne remplace pas cette analyse ; elle ne légitime pas un ensemble indéfini d'opérations.

L'accompagnement doit également tenir compte des représentants et des personnes qui ne peuvent pas réaliser seules le parcours. Faire cliquer un proche à la place du patient sans clarifier son rôle peut produire une trace trompeuse. La délégation doit être pensée comme un objet de gouvernance.

Notre proposition : rédiger une phrase spécifique pour chaque décision demandée, puis la tester auprès d'usagers. « Je partage ces attributs pour accéder à ce service » doit être distingué d'une autorisation clinique. L'organisation conserve la responsabilité d'expliquer les conséquences, les alternatives et les voies d'exercice des droits.

Références : [22] CNIL, [23] CNIL

L'IA déplace le risque vers l'enrôlement et le support

Les outils génératifs rendent plausibles de nouveaux scénarios de falsification ou de manipulation : document altéré, voix imitée, image synthétique ou message d'assistance convaincant. Nous les traitons ici comme scénarios de menace à examiner, sans avancer de taux de fraude spécifique à l'appli carte Vitale.

Une architecture doit éviter de concentrer toute la protection sur la connexion habituelle. L'enrôlement, le changement d'appareil et la récupération deviennent des étapes critiques. Un fraudeur peut chercher à convaincre le support plutôt qu'à contourner le protocole cryptographique.

L'IA peut aussi aider l'organisation à détecter des anomalies, mais son résultat ne doit pas devenir une preuve irréfutable. Les faux positifs et voies de recours comptent : un assuré légitime bloqué par une alerte automatisée doit pouvoir obtenir une résolution. L'efficacité se mesure avec une population et un protocole précis.

Nous recommandons un exercice de menace associant sécurité, accueil et support. Chaque scénario indique le contrôle, le signal attendu, la décision humaine éventuelle et la procédure de reprise. La résistance à la fraude et la protection des personnes injustement bloquées doivent être évaluées dans le même programme.

Références : [11] ANSSI, [19] FIDO Alliance

Résilience : que devient le soin quand la connexion échoue ?

Une panne peut toucher le téléphone, le lecteur, le logiciel local, le réseau ou un service distant. La réponse dépend de l'étape concernée. L'organisation doit distinguer l'impossibilité d'authentifier, l'indisponibilité d'un dossier et l'interruption d'une opération administrative.

Une procédure de continuité utile décrit ce qui reste possible, qui décide et comment les actions seront régularisées. Elle n'est pas un mot de passe partagé ni la suppression durable des contrôles. Un accès d'urgence, lorsqu'il existe, doit répondre à des règles et laisser des traces exploitables.

Le maintien d'un support physique apporte une alternative dans certains usages, sans rendre toutes les opérations numériques indépendantes du réseau. Le projet doit tester les dépendances réelles au lieu de supposer qu'un objet de secours garantit toute la continuité.

Le SSO peut réduire la répétition des connexions. La durée des sessions, leur verrouillage et les réauthentifications doivent toutefois suivre le risque et le service. Une connexion centrale ne garantit ni une journée entière sans nouveau contrôle ni un accès de secours universel à tous les services.

Notre recommandation est un exercice avant généralisation : simuler une panne, réaliser un parcours autorisé et vérifier la remise en cohérence après rétablissement. Observer le temps, les informations manquantes, les décisions et les erreurs de saisie. La résilience devient une capacité démontrée lorsque les équipes peuvent appliquer la procédure sans improvisation.

Références : [3] ANS / GIE SESAM-Vitale, [10] CNIL

Le smartphone ne représente pas toute la population

L'Insee rapporte qu'en 2025, 34 % des 16–74 ans n'ont pas toutes les compétences numériques de base : 7 % sont en situation d'illectronisme et 27 % ont des compétences faibles. Le champ est la France hors Mayotte, en logement ordinaire. Ces proportions décrivent des compétences générales, pas l'usage de l'appli carte Vitale.

La même publication indique que 82 % des personnes de 75 ans ou plus manquent de compétences numériques, avec un champ d'âge distinct. Il faut conserver cette distinction : un pourcentage global de population ne se déduit pas en additionnant ces groupes.

L'implication de conception est claire. Un parcours accessible ne se réduit pas à une interface épurée. Il doit aussi tenir compte de la compréhension, des capacités physiques, de la langue, du matériel et du recours à l'aide. Ces difficultés peuvent apparaître chez des personnes qui utilisent déjà Internet.

Nous recommandons de recruter pour les tests des usagers variés et de documenter les besoins d'assistance. La mesure du succès doit distinguer réalisation autonome, réalisation accompagnée et recours à une alternative. Le but est l'accès effectif au service, avec une charge d'accompagnement assumée par l'organisation.

Références : [24] Insee, Valentin Guilloton

Éviter la double peine

Pour une personne malade, âgée ou en difficulté avec les outils numériques, une démarche complexe peut devenir un obstacle supplémentaire. La simplification doit se mesurer à la capacité de chacun à accéder au service.

Préserver le choix du canal

La carte physique et l’accueil humain doivent rester des voies d’accès à part entière. L’Assurance Maladie précise que l’appli carte Vitale complète la carte physique sans la remplacer. Nous recommandons de vérifier qu’une absence de smartphone ne pénalise pas le parcours.

Organiser l’accompagnement

L’activation, la récupération d’accès et la résolution des difficultés demandent des équipes formées, des procédures accessibles et du temps de médiation. L’aide doit tenir compte de la langue, du handicap, du matériel et de la compréhension.

Prévoir la représentation

Lorsque le besoin existe, les services devraient proposer des délégations explicites, limitées et révocables, adaptées au cadre applicable. Aider un proche ne devrait pas obliger à utiliser ses identifiants personnels. Cette exigence de conception ne présume pas que toutes les fonctionnalités de délégation sont déjà disponibles.

**L’inclusion doit figurer dans les budgets,
les procédures et les critères d’évaluation.**

Références : [1] Assurance Maladie, [6] ApCV, [24] Insee.
Recommandations organisationnelles proposées par l’auteur.

Aider sans prendre l'identité de l'autre

Les aidants rendent de nombreux parcours possibles. Leur place doit être reconnue sans confondre leur identité avec celle du patient. Un compte partagé ou une session ouverte au nom d'un tiers peut masquer qui a réellement effectué une opération.

Les situations de représentation varient : parent, proche, représentant légal ou professionnel d'accompagnement. Le service doit préciser les justificatifs, la portée et la durée de la délégation selon le cadre applicable. Il doit aussi permettre d'enregistrer les changements et la fin du rôle.

Notre proposition de conception consiste à séparer trois éléments : la personne qui s'authentifie, la personne concernée par le dossier et le mandat autorisant l'action. Les écrans doivent rendre cette relation visible avant une opération engageante. Les traces doivent conserver l'acteur réel.

L'assistance peut se faire sans demander au patient de révéler durablement ses secrets de connexion. Les équipes doivent disposer de méthodes sûres et d'une consigne claire sur ce qu'elles peuvent manipuler. Aider à comprendre le parcours, saisir avec autorisation ou agir en représentation sont des gestes différents qui méritent des procédures distinctes.

Références : [4] RNIV, [22] CNIL

Des activations à l'usage : changer le tableau de bord

Une communication de l'Assurance Maladie de septembre 2026 mentionne plus de 3,5 millions d'activations au niveau national. C'est un repère de diffusion. Ce nombre ne renseigne pas à lui seul sur la fréquence d'utilisation, les professionnels équipés ou le succès des parcours à distance.

La feuille de route nationale mentionne un objectif de 20 millions d'utilisateurs en 2027. Un objectif et un résultat observé doivent apparaître sous des libellés différents. Leur rapprochement exige aussi de vérifier que les définitions d'utilisateur et d'activation sont comparables.

Nous proposons un tableau de bord à cinq étages : éligibilité, activation, disponibilité du service, usage réalisé et valeur produite. Chaque indicateur doit préciser sa population, sa période et sa source. Les abandons et appels au support doivent être suivis au même titre que les succès.

Pour la valeur, mesurer des effets locaux : ressaisies évitées, erreurs corrigées, délais et charge des équipes. Une hausse d'utilisation ne démontre pas un gain clinique ou financier. Le pilotage mature relie les résultats au parcours observé et conserve la possibilité d'identifier une simplification qui ne fonctionne que pour une partie de la population.

Références : [25] Assurance Maladie, [26] ANS

Le pilote : observer une opération entière

Nous proposons un pilote centré sur un cas d'usage précis plutôt qu'une généralisation simultanée à tous les parcours. Il définit les usagers visés, la situation de départ, le service, le matériel et les responsabilités. Les critères de succès et d'arrêt sont discutés avant les premiers tests.

L'observation suit l'opération complète, avec les reprises et exceptions. Il faut éviter de sélectionner uniquement les personnes déjà à l'aise ou de laisser l'équipe projet résoudre silencieusement tous les problèmes. Le support réel fait partie de l'expérience à évaluer.

Une comparaison avant/après doit tenir compte des changements d'activité, d'effectifs et de population. Les résultats sont décrits par site et période. Si le protocole ne permet pas une attribution causale, on présente une évolution observée plutôt qu'un gain démontré imputable à la seule identité numérique.

La décision de passer à l'échelle repose sur un ensemble : faisabilité, qualité d'identification, charge de travail, accessibilité et continuité. Une démonstration réussie est une étape utile. Le pilote ajoute les conditions et limites nécessaires à une décision de déploiement responsable.

Références : [2] Assurance Maladie, [3] ANS / GIE SESAM-Vitale

Trois chiffres, trois dénominateurs

Repère	Nature	Lecture correcte
Plus de 3,5 millions	Activations nationales mentionnées en septembre 2026	Diffusion ; pas un nombre d’usages réussis
20 millions en 2027	Objectif national d’utilisateurs	Cible ; pas un résultat atteint
34 % des 16–74 ans	Compétences insuffisantes, enquête Insee 2025	7 % illectronisme + 27 % niveau faible ; pas un taux d’échec de l’appli

Avant toute comparaison : préciser la population, la période, la définition et la source.

Références : [24] Insee, Valentin Guilloton, [25] Assurance Maladie, [26] ANS

Qui porte la chaîne de confiance ?

La confiance traverse plusieurs organisations : émetteur d'identité, opérateur de fédération, éditeur, établissement, professionnel et usager. Chacun contrôle une partie du parcours. Sans répartition claire, l'utilisateur peut être renvoyé d'un support à l'autre lorsqu'une opération échoue.

Nous proposons de nommer un responsable métier du parcours, avec un binôme technique et un lien explicite vers l'identitovigilance, la sécurité et la protection des données. Le dossier doit préciser qui corrige une identité, qui décide d'une fusion, qui retire un accès et qui informe l'usager après incident.

La gouvernance doit couvrir les fournisseurs et leurs évolutions. Un changement de version, de règle d'accès ou de sous-traitant peut avoir un effet sur le parcours local. Les contrats et procédures doivent prévoir l'information, les tests et la continuité.

La responsabilité ne se résume pas à désigner l'auteur d'un incident après coup. Elle consiste à donner à chaque acteur les moyens d'agir avant qu'il survienne. Le comité de pilotage devrait examiner les échecs récurrents et décisions de correction, pas seulement le nombre de comptes créés.

Références : [3] ANS / GIE SESAM-Vitale, [10] CNIL, [22] CNIL

Souveraineté : les dépendances à rendre visibles

La souveraineté d'une identité numérique se comprend à travers les décisions que l'organisation peut réellement prendre. Elle doit savoir qui contrôle l'émission des preuves, leur stockage, leur vérification et leur récupération. Elle doit également examiner les dépendances au matériel, au réseau et aux conditions d'un fournisseur.

Un acteur public peut dépendre d'un système mobile privé pour l'usage quotidien. Un portefeuille privé peut présenter une attestation émise par une autorité publique. Cette combinaison exige une cartographie plutôt qu'un classement binaire entre souverain et non souverain.

Notre proposition est un registre de dépendances : composant, opérateur, fonction critique, alternative et conséquence d'une interruption. Le registre distingue la capacité de changer de prestataire de la capacité de reprendre un service en urgence. La portabilité doit être testée, pas seulement annoncée.

Pour la santé, la décision cherche un équilibre : profiter d'interfaces efficaces tout en conservant des voies d'accès et une maîtrise suffisante de la preuve. La question du comité de direction devient : si cette dépendance évolue demain, comment maintenons-nous les soins, les droits des personnes et la traçabilité ?

Références : [13] Commission européenne, [16] Apple, [17] Google

Agents IA : identifier l'exécutant et tracer le mandat

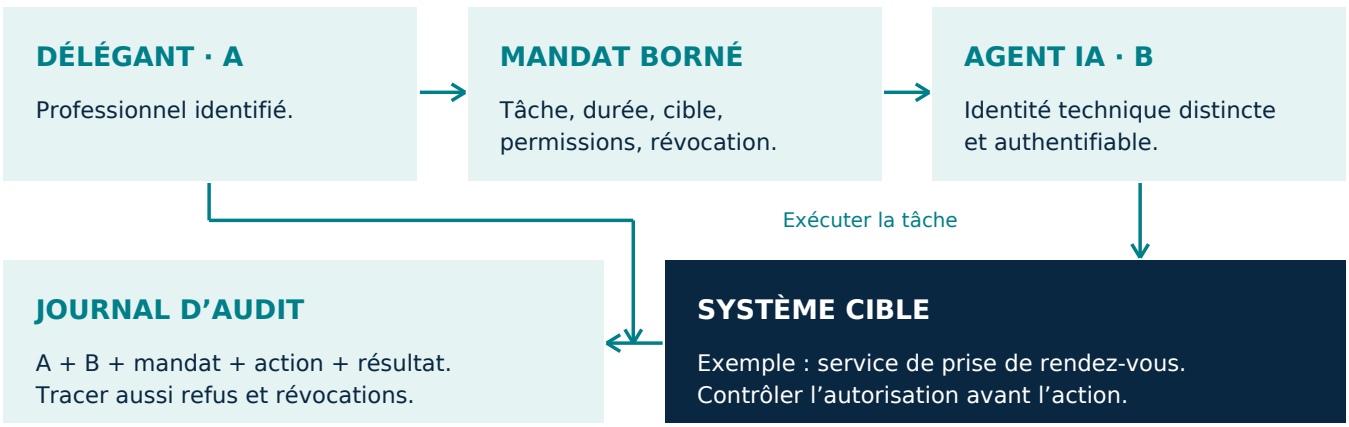
Un agent peut préparer un dossier ou exécuter une opération sur délégation. Si toutes ses actions sont enregistrées sous la session du médecin, les journaux ne permettent plus de distinguer ce que celui-ci a demandé, validé ou réellement réalisé. Cette ambiguïté complique l'enquête et l'attribution des responsabilités ; elle ne rend pas toute détermination juridique impossible.

Notre recommandation : attribuer à l'agent une identité technique distincte, authentifiable et révocable, associée à son service et à son opérateur. Relier chaque opération à l'identité du délégant et au mandat accordé. Selon l'architecture, cela peut mobiliser une identité de service et des justificatifs de délégation ; aucun identifiant national unique d'agent en santé n'est présupposé. Les travaux de l'OpenID Foundation éclairent ces besoins d'identité et de délégation. [33]

La « traçabilité de l'intention » signifie ici conserver une instruction ou une autorisation explicite, pas reconstruire une intention psychologique. Le journal doit relier : délégant, agent, tâche autorisée, cible, périmètre, durée, approbation éventuelle, action exécutée et résultat. Conserver aussi les refus et révocations, avec minimisation des données.

Exemple hypothétique : l'annulation d'un rendez-vous doit être attribuable à l'agent exécutant et à une délégation précise. Une modification de posologie engage un contrôle clinique d'un autre niveau : elle exige une autorisation spécifique et une validation adaptée, distinctes d'un mandat administratif. Des permissions bornées, une interruption possible et une vérification avant exécution évitent qu'un « tout valider » masque une séquence d'actions.

DÉLÉGUER SANS CONFONDRE LES IDENTITÉS



Architecture proposée ; validation adaptée au risque et collecte limitée aux traces nécessaires.

Références : [7] ANS, [10] CNIL, [33] OpenID Foundation

De la vision au terrain : une feuille de route réaliste

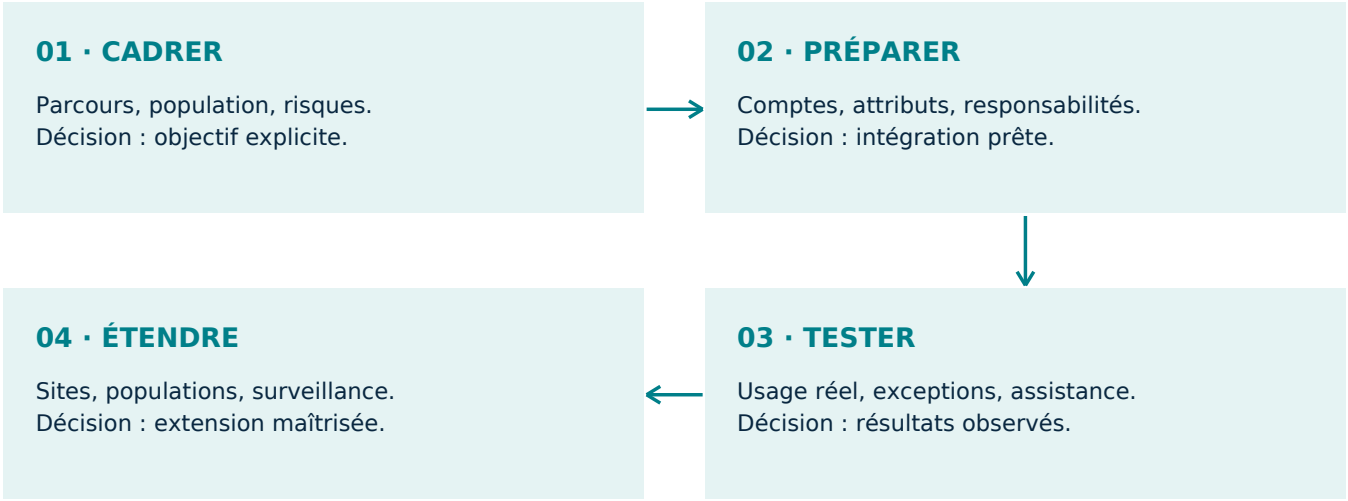
Nous proposons quatre séquences de travail. D'abord cadrer un parcours et ses risques, puis préparer les comptes, attributs et responsabilités. Ensuite tester l'usage réel avec les exceptions. Enfin étendre progressivement les sites et populations en conservant un suivi des effets et de l'assistance.

Chaque séquence doit produire une décision vérifiable. Le cadrage donne un besoin et une population. La préparation donne un dossier d'intégration et une procédure de traitement des identités. Le pilote donne des résultats observés. L'extension donne un mécanisme de surveillance et de réévaluation.

La feuille de route doit aussi réserver une capacité de correction. Un déploiement qui consacre toutes ses ressources aux raccordements peut laisser les problèmes de qualité et d'inclusion sans solution. Le support, la formation et le traitement des anomalies sont des fonctions durables.

Le principe directeur est de faire disparaître les obstacles évitables tout en gardant les contrôles nécessaires. Une infrastructure de confiance réussie est reconnue par les équipes comme une aide dans leur travail, par les usagers comme une porte accessible et par l'organisation comme un ensemble de responsabilités maîtrisées.

QUATRE ÉTAPES, UNE CAPACITÉ DE CORRECTION CONTINUE



À chaque étape : corriger, former, documenter et réévaluer avant de poursuivre.

Références : [3] ANS / GIE SESAM-Vitale, [15] Commission européenne

Les six préalables d’un déploiement utile

Préalable	Élément vérifiable	Responsable à nommer
1. Usage ciblé	Parcours, population et résultat attendu	Métier
2. Identité juste	Rapprochement, qualification, exceptions	Identitovigilance
3. Accès proportionné	Rôles, délégations, identité des agents, révocation	Métier + sécurité
4. Données nécessaires	Attributs, finalités, durées	DPO + produit
5. Continuité et inclusion	Secours, assistance, tests usagers	Exploitation + accueil
6. Valeur mesurée	Indicateurs, pilote, réévaluation	Direction de projet



1. Usage ciblé



2. Identité juste



3. Accès proportionné



4. Données nécessaires



5. Continuité et inclusion



6. Valeur mesurée

Grille de travail proposée par l’auteur. À adapter au contexte ; elle ne constitue pas une certification.

Matrice de responsabilités

Sujet	Pilote proposé	Contributeurs	Livrable
Rapprochement des dossiers	Identitovigilance	Admissions, éditeur	Règles et décisions tracées
Raccordement	Équipe technique	Opérateur, sécurité	Dossier de tests
Habilitations	Responsable métier	RH, sécurité, DSI	Rôles et révocation
Protection des données	Responsable de traitement	DPO, fournisseurs	Finalités et conservation
Accessibilité	Responsable du parcours	Usagers, accueil	Tests et alternatives
Incident	Exploitation	Sécurité, métier, support	Continuité et correction

Cette répartition est une proposition. Dans chaque organisation, désigner une personne ou une fonction disposant réellement des moyens et du pouvoir de décision. Une responsabilité non attribuée doit bloquer la généralisation du parcours concerné.

Fiche de cadrage du pilote

Champ	À renseigner
Contexte et site	_____
Population concernée	_____
Problème observé avant projet	_____
Action à simplifier	_____
Identités et acteurs impliqués	_____
Périmètre technique / versions	_____
Critères de succès et d’arrêt	_____
Tests d’exception et support	_____
Responsable et réévaluation	_____

Inclure les abandons, le besoin d’aide et les situations non résolues. La durée d’un pilote dépend du parcours et du volume disponible : ce document ne fixe pas un nombre arbitraire de semaines ou de participants.

Tableau de bord : compter les bons événements

Indicateur	Numérateur / dénominateur	Interprétation
Activation	Activations / demandes éligibles observées	Séparer les refus et abandons
Connexion	Connexions réussies / tentatives	Préciser ce qui compte comme tentative
Rapprochement	Comptes correctement associés / associations auditées	Audit avec critères explicites
Autonomie	Parcours sans aide / parcours observés	Ne pas exclure les usagers accompagnés
Charge d’accueil	Temps complet par parcours	Inclure reprises et exceptions
Qualité	Corrections ou erreurs / opérations contrôlées	Distinguer anomalie et incident
Continuité	Scénarios de panne exécutables / scénarios testés	Compte rendu d’exercice

Conserver la période, le site, la population et les versions. Décrire les données manquantes. Toute comparaison avant/après doit examiner les différences d’activité et de population.

Continuité : préparer le jour où cela échoue

Situation	Décision à préparer	Contrôle de reprise
Téléphone perdu / déchargé	Alternative et support au patient	Compte et appareil à sécuriser
Lecture impossible	Support compatible ou parcours alternatif	Pas de rattachement improvisé
Réseau indisponible	Opérations autorisées en mode dégradé	Réconciliation après rétablissement
Identité discordante	Escalade vers le responsable	Décision justifiée, dossier corrigé
Professionnel sans accès	Support, rôle, règles d’urgence	Pas de compte partagé
Incident de sécurité	Isolement, information, continuité	Révocation et vérification

Tester la procédure avec les équipes qui l’appliqueront. Pour chaque ligne, ajouter : responsable, canal d’appel, document de référence et date du dernier exercice. Le secours ne doit pas devenir un contournement permanent.

Les affirmations à maîtriser avant publication

Formulation risquée	Formulation retenue
« L’appli est déjà dans FranceConnect+ »	Non confirmé par la liste officielle consultée ; distinguer le FI santé
« OIDC scelle juridiquement l’acte »	Authentification et signature ont des fonctions distinctes
« Toutes les INS des ayants droit sont qualifiées »	Suivre les cas et règles décrits par le RNIV
« L’AMC est disponible partout en 2027 »	Évolution à terme ; calendrier universel non établi
« Tous les logiciels sont conformes EHDS en 2029 »	Calendrier progressif par catégorie et périmètre
« Vérification d’identité tous les cinq ans »	Périodicité universelle non établie dans le corpus
« SSO : aucune réauthentification toute la journée »	Durée et reprise de session à définir selon le risque
« Toutes les CPS durent six ans »	Vérifier carte et certificats ; divergence documentaire à lever

Les volumes industriels et le taux de 75–80 % de pharmacies équipées proposés dans les notes ne sont pas repris sans date ni périmètre vérifiés. Pour la CPS4, le guide de septembre 2025 annonce six ans, tandis que la page générale consultée indique trois ans : faire confirmer le cycle applicable avant de planifier les renouvellements. [29,30]

Un vocabulaire commun

Terme	Définition de travail
INS	Identité nationale de santé utilisée pour référencer les données
INSi	Téléservice de récupération ou vérification de l’INS
RPPS	Répertoire partagé des professionnels intervenant dans le système de santé
PSC / e-CPS	Pro Santé Connect / moyen mobile d’authentification professionnelle
FI / FS	Fournisseur d’identité / fournisseur de services
OIDC / OAuth 2.0	Couche d’identité / cadre d’accès délégué
DPI	Dossier patient informatisé géré par une structure de soins
EUDI Wallet	Portefeuille européen d’identité numérique
DMP / Mon espace santé	Dossier médical partagé national / espace numérique personnel qui l’intègre ; distinct du DPI local
AMO / AMC / ADRi	Assurance obligatoire / complémentaire / service de droits AMO
EHDS / EEDS	Espace européen des données de santé
Passkey	Moyen cryptographique FIDO, synchronisé ou lié à un appareil

Les acronymes décrivent des objets différents. Leur proximité dans un parcours ne les rend pas interchangeables.

Sources et références

[1] Assurance Maladie
Généralisation de l’appli carte Vitale
18 novembre 2025 • Ouvrir la source officielle

[2] Assurance Maladie
L’appli carte Vitale sur le smartphone des patients
Documentation professionnels • Ouvrir la source officielle

[3] ANS / GIE SESAM-Vitale
Référentiel appli carte Vitale : authentification à distance
Version du 7 avril 2025 • Ouvrir la source officielle

[4] RNIV
Principes communs
Version 2.0, février 2024, sections 4.3.4.1–4.3.4.2 • Ouvrir la source officielle

[5] ANS
Référentiel Identité nationale de santé
Référentiel officiel • Ouvrir la source officielle

[6] G_NIUS / ANS
Appli carte Vitale (ApCV)
Fiche réglementaire • Ouvrir la source officielle

[7] ANS
Pro Santé Connect : documentation technique
Documentation officielle • Ouvrir la source officielle

[8] DINUM
Différences entre FranceConnect et FranceConnect+
Documentation partenaires • Ouvrir la source officielle

[9] DINUM
FranceConnect : documentation partenaires
Architecture de fédération • Ouvrir la source officielle

Sources consultées le 8 octobre 2026. Les documents dynamiques et versions doivent être vérifiés avant intégration. Les liens sont actifs dans le PDF.

Sources et références

[10] CNIL
Sécurité et confidentialité de l’accès au dossier patient informatisé
Rappel aux établissements • Ouvrir la source officielle

[11] ANSSI
Identité et confiance numérique
Cadre PVID et confiance • Ouvrir la source officielle

[12] France Identité
S’authentifier avec FranceConnect
FranceConnect+ et identité certifiée • Ouvrir la source officielle

[13] Commission européenne
European Digital Identity Regulation
Cadre EUDI et échéance des wallets • Ouvrir la source officielle

[14] OpenID Foundation
OpenID Connect Core 1.0, errata set 2
Spécification, notamment ID Token et validation • Ouvrir la source officielle

[15] Commission européenne
European Health Data Space Regulation
Calendrier 2025 / 2027 / 2029 / 2031 • Ouvrir la source officielle

[16] Apple
IDs in Apple Wallet: privacy and security overview
Documentation de l’opérateur • Ouvrir la source officielle

[17] Google
Verify with Google Wallet : overview
Documentation de l’opérateur • Ouvrir la source officielle

[18] Commission européenne
Technical standards for cross-border EUDI Wallets
Standards communs des portefeuilles • Ouvrir la source officielle

Sources consultées le 8 octobre 2026. Les documents dynamiques et versions doivent être vérifiés avant intégration. Les liens sont actifs dans le PDF.

Sources et références

[19] FIDO Alliance
Passkeys and Verifiable Digital Credentials
Livre blanc technique • Ouvrir la source officielle

[20] Union européenne
Règlement (UE) 2025/327
Espace européen des données de santé • Ouvrir la source officielle

[21] ANSSI
Référentiel général de sécurité
Identification, signature, horodatage • Ouvrir la source officielle

[22] CNIL
Minimiser les données collectées
Principe de minimisation • Ouvrir la source officielle

[23] CNIL
L’identité numérique
Dossier thématique • Ouvrir la source officielle

[24] Insee, Valentin Guilloton
Une personne sur trois manque de compétences numériques
Insee Focus 376, 19 février 2026 ; enquête 2025 • Ouvrir la source officielle

[25] Assurance Maladie
Qu’est-ce qui est vert, vital pour la santé et existe aussi en appli ?
22 septembre 2026 ; repère national dans un communiqué territorial • Ouvrir la source officielle

[26] ANS
Bilan de l’axe 3 : accès à la santé
Objectif 20 millions d’utilisateurs en 2027 • Ouvrir la source officielle

[27] Union européenne
Règlement (UE) 2024/1183
Modification du règlement eIDAS • Ouvrir la source officielle

Sources consultées le 8 octobre 2026. Les documents dynamiques et versions doivent être vérifiés avant intégration. Les liens sont actifs dans le PDF.

Sources et références

[28] GIE SESAM-Vitale
Vitale DAYS 2026 : conférence stratégique sur l’identité numérique
Annonce du 30 septembre 2026 • Ouvrir la source officielle

[29] ANS
Cartes de professionnels de santé : CPS4 et compatibilité
Documentation officielle consultée le 8 octobre 2026 • Ouvrir la source officielle

[30] ANS / Assurance Maladie
Guide de la consultation Mon espace santé / DMP
17 septembre 2025 ; authentification indirecte renforcée, p. 19 • Ouvrir la source officielle

[31] FIDO Alliance
Passkeys : modèles synchronisés et liés à un appareil
Documentation officielle consultée le 8 octobre 2026 • Ouvrir la source officielle

[32] Inter AMC
ROC Établissements : services IDB, SIM, CLC et DEL
Documentation de l’opérateur consultée le 8 octobre 2026 • Ouvrir la source officielle

[33] OpenID Foundation
Identity Management for Agentic AI
Livre blanc, octobre 2025 • Ouvrir la source officielle

[34] Lionel Reichardt · IAtrogénique × IAtus

Édition spéciale VITALE DAYS 2026 :
Identifier. Connecter. Simplifier.

7 octobre 2026 · Lire la newsletter LinkedIn

Sources consultées le 8 octobre 2026. Les documents dynamiques et versions doivent être vérifiés avant intégration. Les liens sont actifs dans le PDF.

Pharmageek
IAtrogénique × IAtus
Lionel Reichardt

LIONEL REICHARDT / PHARMAGEEK

Préparer. Animer. Prolonger.



Un partenaire pour faire de votre événement une conversation utile et un contenu qui dure.

Je prépare les échanges avec vos intervenants, construis le fil rouge et anime les conférences, tables rondes et débats. Mon travail consiste à rendre les sujets de santé numérique, d'innovation et d'IA accessibles tout en conservant leur exigence, et à relier les expertises aux questions de votre public.

Avant

Clarifier les objectifs ; travailler avec les intervenants ; construire les questions et transitions.

Pendant

Faire dialoguer les expertises ; solliciter la salle ; faire émerger les convergences et désaccords.

Après

Prolonger les échanges par des articles, newsletters, vidéos et synthèses adaptés au projet.

Un écosystème de veille et de diffusion

Canal	Repères d'audience et de contenu
Scoop.it	60 000 partages · plus de 2,4 millions de vues
LinkedIn	Plus de 29 000 contacts
IAtrogénique × IAtus	Plus de 5 100 abonnés
Morning Routine	Plus de 3 200 abonnés
YouTube	Plus de 220 vidéos · plus de 740 abonnés

Chiffres communiqués par Lionel Reichardt pour cette édition, octobre 2026.
Les audiences sont propres à chaque canal et peuvent se recouper.

Pharmageek
IAtrogénique × IAtus
Lionel Reichardt

CONFÉRENCES / ANIMATION / RELAIS DE COMMUNICATION

Plus de 100 clients

Quelques références parmi les plus de 100 clients que j'ai accompagnés.

Institutions, industriels, sociétés savantes et médias : des interventions et des collaborations adaptées aux objectifs, au public et au format de chaque événement.

Agence du Numérique en Santé	GIE SESAM-Vitale	SofIA-Santé
Mylan	Cegedim Santé	Groupe Profession Santé
Société Française de Cardiologie	Sanofi	Johnson & Johnson

Références communiquées par Lionel Reichardt. Sélection non exhaustive. Logos : marques de leurs titulaires respectifs ; crédit Johnson & Johnson.

Construisons votre prochain événement.

Vous souhaitez m'avoir comme conférencier, animateur ou partenaire pour votre congrès, votre journée professionnelle ou vos tables rondes ? Échangeons sur vos objectifs, la préparation des interventions et les relais de communication qui prolongeront l'événement.

Me contacter sur LinkedIn
lionel@reichardtonline.com

La bonne identité ne suffit pas. Il faut le bon accès.

La carte Vitale sur smartphone ouvre une réflexion plus large : comment construire une confiance utilisable dans les parcours de santé ? Ce livre blanc relie les moyens d’identification aux dossiers, aux habilitations, aux wallets européens et aux réalités du terrain.

60 pages • 33 références • 6 fiches de synthèse
5 outils opérationnels • Glossaire

Pour les décideurs, industriels, établissements et professionnels qui veulent transformer une promesse technique en service utile.

Travaillons ensemble
Conseil, formation, animation et création de contenus
lionel@reichardtonline.com

Pharmageek • IAtrogénique × IAtus • Octobre 2026