AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Homologation des moyens d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques]

Guide pratique organisationnel PGSSI-S

Publication : décembre 2022 | Classification : Publique | 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
[CNIL]	Délibération no 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038277620
[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
[IE-ASPP]	Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques] Approuvé par arrêté du 28 mars 2022 Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[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/

Documents techniques

Renvoi	Document
[ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information https://www.ssi.gouv.fr/administration/guide/securiser-ladministration-des-systemes-dinformation/
[AUTH_MDP]	Recommandations relatives à l'authentification multifacteur et aux mots de passe https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
[CC]	Certification Critères Communs https://commoncriteriaportal.org/products/
[CC_ANSSI]	Certification Critères Communs par l'ANSSI https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/
[CC_EM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[CERT Santé]	CERT Santé Service d'appui à la gestion des incidents de cybersécurité pour le secteur sanitaire https://esante.gouv.fr/produits-services/cert-sante
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement de mécanismes cryptographique https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques/
[CSPN]	Certification de Sécurité de Premier Niveau https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/presentation/
[EBIOS RM]	La méthode EBIOS Risk Manager https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
[FIDO]	Certification FIDO https://fidoalliance.org/certification/
[FIPS]	Exigences de sécurité FIPS https://csrc.nist.gov/publications/detail/fips/140/2/final
[HOMOLOGATION]	Démarche d'homologation de sécurité https://www.ssi.gouv.fr/entreprise/management-du-risque/homologation-de-securite/
[HYGIENE]	Guide d'hygiène informatique https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
[ISO-27002]	Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information https://www.iso.org
[OIDC]	Recommandations pour la sécurisation de la mise en œuvre du protocole Open ID Connect https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-de-la-mise-en-oeuvre-du-protocole-openid-connect/
[PGSSI-S]	Politique Générale de Sécurité des Systèmes d'Information de Santé https://esante.gouv.fr/securite/politique-generale-de-securite-des-systemes-d-information-de-sante
[PVID]	Référentiel d'exigences applicables aux prestataires de vérification d'identité à distance https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/
[QUALIF]	Qualification de produits ou services de cybersécurité https://www.ssi.gouv.fr/entreprise/qualifications/
[RFC 6238]	TOTP: Time-Based One-Time Password Algorithm https://tools.ietf.org/html/rfc6238.html

SOMMAIRE

1 PREAMBULE

1.1 Objet du guide

Le référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social - personnes physiques, définit le niveau minimum de garantie attendu s'agissant de l'identification électronique des professionnels sur les services numériques en santé.

Le présent guide a pour objectif de préciser les modalités d'homologation de moyens d'identification électronique par un fournisseur de service numérique en santé, solution proposée par le référentiel d'identification électronique en alternative aux moyens sectoriels (carte CPx, e-CPS) ou notifiés au niveau européen au titre du règlement eIDAS.

Ce document s'adresse :

- aux entités ayant déjà déployé ou souhaitant déployer des moyens d'identification électronique locaux, et qui sont tenues de prononcer leur homologation avant le 01/01/2026 ;
- aux éditeurs ou fournisseurs de dispositifs d'authentification qui souhaitent proposer à des entités soumises au référentiel d'identification électronique des produits pouvant entrer dans le cadre d'une homologation de moyens d'identification électronique par ces entités.

1.2 Périmètre d'application du guide

En application de l'article L. 1470-1 du code de la santé publique (voir [ART_L1470]), le référentiel d'identification électronique des professionnels du secteur de la santé 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]).

Le présent guide concerne exclusivement l'homologation de moyens d'identification électronique sur des services numériques en santé « sensibles », telle que proposée par le référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social - personnes physiques ([IE-ASPP]).

2 DEFINITIONS ET CONCEPTS GENERAUX

2.1 Identification électronique

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

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

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

2.2 Moyens d'identification électronique et dispositif d'authentification

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 règlement eIDAS, un moyen d'identification électronique est associé à un niveau de garantie faible, substantiel ou élevé selon le niveau de sécurité qu'il offre.

Un moyen d'identification électronique permet d'établir l'identité d'une personne de façon fiable, basée sur un enregistrement initial et un processus de gestion rigoureux. Dans la suite de ce document, le terme moyen d'identification électronique est souvent utilisé pour désigner à la fois le dispositif matériel et/ou immatériel d'authentification et les autres ressources mises en œuvre (applications de gestion, bases de données…) pour la gestion de son cycle de vie. Le terme **dispositif d'authentification** désigne lui spécifiquement le dispositif remis à un utilisateur pour s'authentifier sur un service (une carte à puce, une clé USB, une application…).

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

Un couple identifiant / mot de passe, une carte CPx, une application mobile d'identification électronique sont des exemples de dispositifs d'authentification, remis dans le cadre d'un service de gestion de moyens d'identification électronique.

2.3 Fournisseurs de service et fournisseurs d'identité

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

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

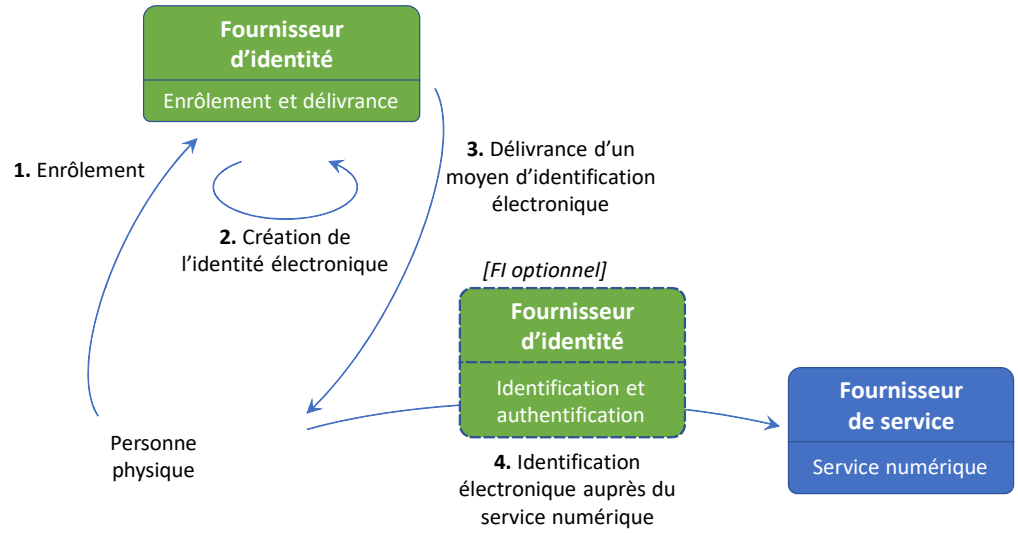
L'identité électronique est créée à la suite d'un processus d'enrôlement au cours duquel le fournisseur d'identité vérifie l'identité du demandeur en s'appuyant sur un répertoire d'identité. Le moyen d'identification électronique est initialisé, délivré puis géré dans le temps par le fournisseur d'identité afin de garantir le niveau de sécurité de l'identification électronique.

A titre d'exemple pour les personnes physiques ciblées par ce référentiel :

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

2.4 Processus d'identification électronique

Les pı



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

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

2.5 Système

Le guide d'homologation de l'ANSSI () présente une démarche applicable à une grande variété de systèmes d'information. La cible (ou périmètre) de l'homologation est désignée de façon générique par le terme « **système** ». Le présent document, par souci d'homogénéité et de cohérence avec le guide ANSSI, emploie aussi parfois ce terme.

Le système recouvre donc les composantes identifiées lors de la première étape de la démarche, décrite au §4.1.2.

3 PROCESSUS D'HOMOLOGATION

3.1 Finalités de l'homologation de MIE

Le référentiel d'identification électronique des acteurs de santé personnes physiques ([IE-ASPP]) liste les moyens d'identification électronique exigés pour l'accès aux services numériques en santé « sensibles ». A terme, seuls les moyens d'identification électronique suivants sont autorisés :

- Les moyens d'identification électronique proposés par Pro Santé Connect (dont la carte e-CPS) ;
- Les cartes CPx ;
- Les moyens d'identification électronique homologués ;
- Les moyens d'identification électronique de niveau eIDAS substantiel certifiés par l'ANSSI.

Cette cible permet d'améliorer l'ergonomie de l'identification électronique en autorisant le choix du moyen le plus adapté au contexte d'utilisation, et aussi de favoriser la disponibilité en disposant de moyens alternatifs en cas d'indisponibilité d'un moyen d'identification électronique.

L'autorisation d'emploi de moyens d'identification électronique homologués par un fournisseur de service numérique en santé poursuit plusieurs objectifs :

- Répondre aux besoins mal couverts par les cartes CPx et l'application e-CPS pour certains cas d'usage ou contextes d'utilisation ;
- Fournir un moyen d'identification électronique local, adapté aux cas d'indisponibilité de solutions nationales nécessitant une connexion réseau, et pouvant être obtenu ou remplacé rapidement en cas d'oubli et de perte ;
- Pouvoir rendre disponible plus rapidement de nouveaux dispositifs d'authentification lorsqu'ils peuvent être déployés localement, avant qu'ils ne soient proposés de façon nationale.

Ces moyens d'identification électronique doivent fournir le même niveau d'assurance que les autres moyens autorisés de façon nationale, afin de ne pas dégrader la sécurité des services numériques en santé pour lesquels ils sont utilisés.

Dans ce but, l'homologation de sécurité demandée par le référentiel impose une démarche formalisée d'analyse de risque et d'évaluation d'un moyen d'identification électronique avant d'autoriser son utilisation. Le niveau minimal de garantie visé est le niveau substantiel défini dans le règlement eIDAS pour les moyens d'identification électronique (voir [MIE]).

3.2 Moyens d'identification électronique pouvant être homologués

Le référentiel d'identification électronique [IE-ASPP] ne fixe pas d'autre exigence sur le moyen d'identification électronique que celle d'être conforme au niveau substantiel défini par le règlement européen, excepté une recommandation concernant l'usage d'un identifiant national du professionnel et la fourniture du nom d'exercice et du prénom de celui-ci.

A titre d'illustration, le dispositif d'authentification du MIE peut être :

- Une application d'authentification sur appareil mobile et ayant obtenu une certification CSPN de l'ANSSI ;
- Une clé USB FIDO2 activée par un code PIN ;
- Une authentification biométrique certifiée et associée à un badge sans contact.

Le cycle de vie du MIE peut reposer sur les processus suivants :

- Vérification d'identité par l'une des méthodes ci-dessous :
  - En face à face physique avec un opérateur d'enregistrement ;
  - En face à face à distance intégrant un service conforme au référentiel d'exigences applicables aux prestataires de vérification d'identité à distance [PVID] de niveau substantiel ou élevé ;
  - Après authentification par Pro Santé Connect ;
- Délivrance du dispositif d'authentification par l'une des méthodes ci-dessous :
  - En main propre, par exemple par un opérateur d'enregistrement ou par le service sécurité ;
  - En ligne ou par courrier, mais avec un mécanisme garantissant que seul le professionnel enregistré peut activer le MIE (par exemple avec code secret remis à l'enregistrement) ;
- Révocation par l'une des méthodes ci-dessous :
  - Auprès d'un opérateur d'enregistrement ou du service sécurité ;
  - En ligne après authentification par des informations confidentielles du porteur ;
- Renouvellement :
  - Imposé tous les 5 ans avec une nouvelle vérification d'identité à chaque fois.

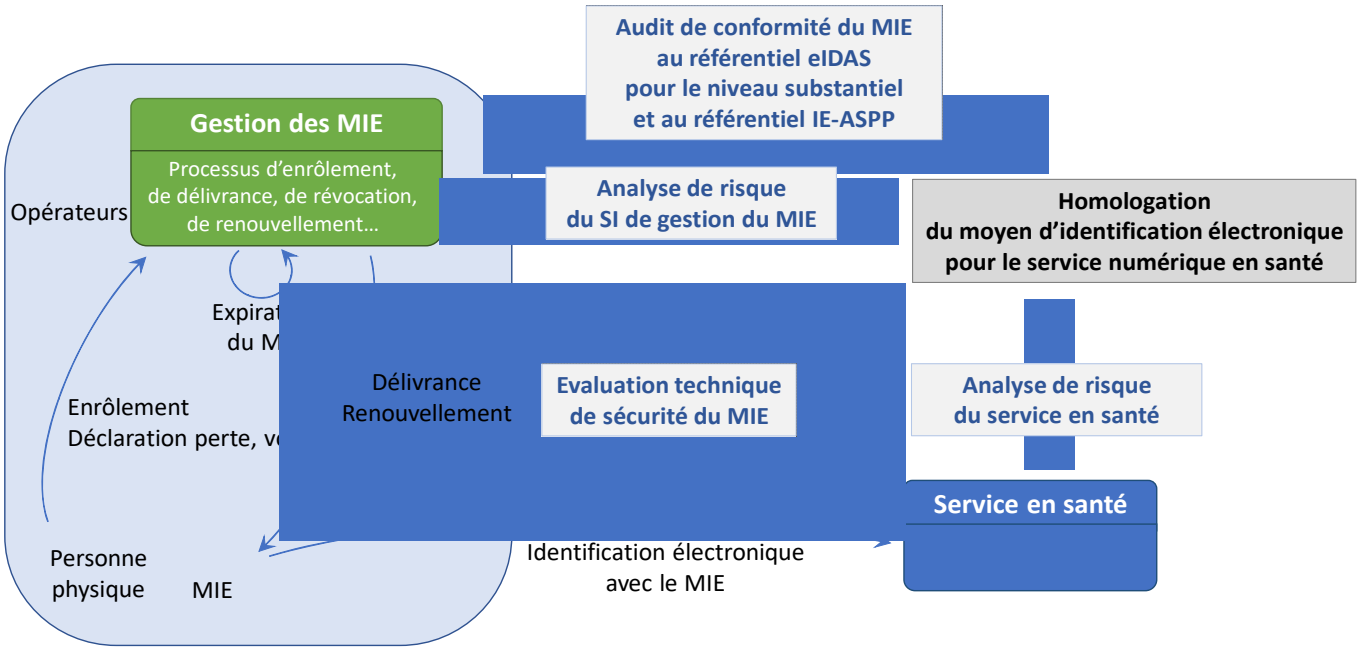
L'homologation intègre un audit de conformité aux spécifications du règlement eIDAS afin de s'assurer que les choix effectués sont sûrs et ne présentent pas de vulnérabilité exploitable dans le contexte d'utilisation fixé.

3.3 Modalités de l'homologation du MIE

Un moyen d'identification électronique est homologué par le responsable du ou des services numériques pour lesquels il est utilisable, afin de s'assurer que ce moyen fournit le niveau de sécurité suffisant au regard du niveau de risque présenté par le ou les services considérés. L'homologation d'un MIE porte ainsi sur :

- Les caractéristiques du dispositif d'authentification ;
- Les processus de gestion du moyen d'identification électronique sur l'ensemble de son cycle de vie :
  - Enrôlement : Demande d'un MIE, enregistrement et vérification d'identité du professionnel ;
  - Délivrance du MIE (i.e. du dispositif d'authentification) et initialisation ou activation le cas échéant ;
  - Utilisation du MIE dans une opération d'identification électronique ;
  - Révocation, expiration du MIE ;
  - Renouvellement du MIE.
- Le ou les systèmes d'information sur lesquels sont basés ces processus (aspects techniques et organisationnels) ;
- L'adéquation du moyen d'identification électronique au niveau de risque des services numériques en santé visés.

Concrètement, l'homologation de sécurité du moyen d'identification électronique doit être menée selon le processus



On peut distinguer :

- Concernant le service numérique en santé :
  - Une analyse de risque permettant de qualifier le risque portant sur le service numérique, et donc d'estimer in fine si le moyen d'identification électronique apporte les garanties suffisantes pour celui-ci ;
- Concernant le moyen d'identification électronique :
  - Une évaluation technique de la sécurité du dispositif d'authentification (matériel et/ou logiciel) ;
  - Une analyse de risque du système d'information utilisé pour la gestion du moyen d'identification électronique ;
  - Un audit de conformité au référentiel européen de spécification des moyens d'identification électronique de niveau substantiel ([MIE]) et au référentiel [IE-ASPP], qui porte sur l'ensemble des processus de gestion et intègre les spécificités du dispositif d'authentification délivré.

Sur la base d'un dossier d'homologation intégrant ces différentes évaluations, l'autorité d'homologation pour le ou les services numériques en santé peut prendre une décision circonstanciée. Il est important de noter que, contrairement aux moyens d'identification électroniques certifiés dans le cadre du règlement eIDAS sur demande de leur fournisseur, il incombe ici aux fournisseurs de services en santé d'homologuer le moyen d'identification électronique. Ceci implique par exemple :

- Lorsqu'une structure délivre le MIE à ses propres professionnels, elle réalise cette homologation en une fois pour le compte de l'ensemble des services numériques sensibles dont elle est responsable ;
- Un moyen d'identification électronique homologué par une entité pour un ou plusieurs de ses services numériques en santé n'est utilisable que sur ces seuls services. L'accès avec ce MIE à d'autres services, fournis par la même entité ou par une autre entité, n'est permis qu'après homologation du MIE pour ces services par leurs responsables respectifs ;
- Lorsque l'entité responsable d'un service numérique n'est pas celle qui délivre le MIE, elle doit effectuer l'homologation avec le concours de l'autorité d'homologation du fournisseur du MIE ou à défaut sur les évaluations de sécurité menées à sa demande ;

- Un fournisseur de dispositif d'authentification (par exemple une carte professionnelle avec et/ou sans contact) peut avoir fait évaluer son produit par l'ANSSI via un visa de sécurité (CSPN, qualification, évaluation CC) mais l'homologation reste toujours à la charge du fournisseur du service numérique en santé ;
- L'accès aux services numériques de santé de dimension nationale, comme par exemple ceux proposés par l'ANS ou la CNAM n'est pas possible avec des moyens d'identification électronique homologués par un autre fournisseur de services numériques en santé.

3.4 Démarche formalisée d'homologation

La démarche d'homologation est présentée en détail par l'ANSSI dans un guide ([HOMOLOGATION]). Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'entité qui la mène. Cette décision constitue un acte formel par lequel ce responsable :

- Atteste de sa connaissance du système d'information déployé, des risques associés et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- Accepte les risques qui subsistent, que l'on appelle les risques résiduels.

L'homologation est imposée en particulier aux autorités administratives, mais elle est aussi applicable à tout autre type d'entité qui propose des services numériques présentant un niveau de risque significatif et/ou soumis à des règlementations spécifiques.

La démarche d'homologation est structurée dans le guide ANSSI en neuf étapes :

- Etapes 1 à 4 : Ces étapes permettent de définir la stratégie d'homologation, c'est-à-dire fixer son périmètre d'étude, le processus à appliquer, les acteurs à impliquer et formaliser l'organisation et les livrables attendus ;
- Etape 5 à 7 : Ces étapes constituent le cœur de la maîtrise des risques, en analysant les risques potentiels, en évaluant la solution déployée et en identifiant les mesures nécessaires à la réduction des risques identifiés ;
- Etape 8 : C'est l'étape de prise de la décision d'homologation, formalisée par le responsable de l'entité ;
- Etape 9 : Cette étape récurrente consiste à maintenir ou améliorer le niveau de sécurité du système d'information dans le temps, en prenant en compte les évolutions du système, de son environnement ainsi que des menaces qui pèsent sur lui.

Le présent guide propose de suivre la démarche proposée par l'ANSSI. Ceci permet aux entités concernées de bénéficier pleinement des précisions, conseils et ressources mises à disposition par l'ANSSI. Les paragraphes suivants fournissent, **en complément du guide**, des consignes adaptées au contexte de l'homologation d'un moyen d'identification électronique utilisable pour des services numériques en santé « sensibles » par des acteurs personnes physiques des secteurs sanitaire, médico-social et social.

4 ETAPES DE L'HOMOLOGATION

4.1 Étape n°1 : Quel système d'information dois-je homologuer et pourquoi ?

4.1.1 Le référentiel règlementaire

L'homologation d'un moyen d'identification électronique est requise par le référentiel d'identification électronique [IE-ASPP] pour son utilisation sur un service numérique sensible en santé à partir du 1/01/2026, sauf si ce moyen est émis par l'ANS (e-CPS, carte CPx) ou s'il est déjà certifié au titre du règlement eIDAS.

Cette homologation se place toutefois dans un contexte règlementaire plus large, comprenant entre autres :

- Le règlement général sur la protection des données ([RGPD]) ;
- La politique générale de sécurité des systèmes d'information de santé ([PGSSI-S]) ;
- Le référentiel général de sécurité ([RGS]).

Il est à noter que le RGPD s'applique sur deux axes :

- La protection des données à caractère personnel des détenteurs de moyens d'identification électronique. La confidentialité des traits d'identité des personnes physiques doit être garantie (protection contre une interception durant les échanges, un vol pendant leur stockage, une consultation non justifiée par le personnel en charge du système d'information de gestion des MIE…), de même que leur disponibilité et leur intégrité (protection contre les modifications accidentelles et/ou non autorisées, sauvegarde des informations…) ;
- La protection des données de santé à caractère personnel qui sont traitées par les services numériques pour lesquels le moyen d'identification électronique est homologué. La sécurité apportée par le moyen doit être adaptée aux risques portant sur ce type de données du service numérique en santé.

Dans le cas où le moyen d'identification électronique intègre des facteurs d'authentification biométriques, des exigences spécifiques issues d'une délibération de la CNIL ([CNIL]) sont aussi à prendre en compte.

Pour rappel, les autorités administratives doivent appliquer le RGS pour la sécurisation de leurs échanges avec d'autres autorités administratives ou avec des usagers. Elles doivent réaliser une homologation de sécurité, sur la base d'une analyse de risque, de tout ou partie de leur système d'information. Une autorité administrative qui est aussi une personne morale acteur de santé, assujettie au référentiel d'identification électronique, est donc tenue de respecter les deux référentiels. Ainsi, lorsqu'une telle entité désire homologuer un moyen d'identification électronique, elle peut :

- Réaliser les deux homologations de façon indépendante, et ainsi adapter et présenter l'homologation du moyen d'identification électronique au plus près du besoin et des exigences du référentiel ;
- Réaliser une seule homologation de sécurité, en prenant soin de respecter, pour ce qui concerne le moyen d'identification électronique, les exigences du référentiel et les indications du présent guide. Le double objectif de l'homologation permet d'éviter la redondance d'informations et de tâches, mais ne doit pas diminuer la précision des informations apportées dans le dossier.

4.1.2 Périmètre du système à homologuer

L'homologation porte sur le moyen d'identification électronique sur tout son cycle de vie, y compris sur son adéquation aux risques du ou des services numériques en santé pour lesquels il est utilisé. Ceci comprend :

- Le système d'information de gestion du moyen d'identification électronique ;
- Le dispositif d'authentification du moyen d'identification électronique.

Lorsque la gestion du moyen d'identification électronique s'appuie sur un répertoire (ou annuaire) interne considéré fiable, les processus d'alimentation ou de modification de contenu de ce répertoire doivent être considérés comme faisant partie du système d'information de gestion du moyen d'identification électronique.

Le périmètre du système à homologuer couvre l'ensemble des processus suivants :

- Enrôlement : Enregistrement des attributs d'identité des porteurs, affectation d'identifiants, vérification de l'identité des porteurs ;
- Délivrance du MIE : Initialisation, remise, activation du MIE et choix par le porteur de ses secrets (mot de passe, code PIN…) ;
- Révocation, expiration, renouvellement du MIE : Déclaration de perte ou vol du MIE, départ du porteur, fin de validité du MIE ou fin de vie du matériel ;
- Utilisation du MIE : Authentification du porteur avec le MIE pour un service numérique en santé.

L'homologation doit de plus prendre en compte le service numérique en santé acceptant le moyen d'identification électronique afin de s'assurer que le niveau de sécurité du MIE est cohérent avec les risques identifiés sur ce service, dépendant par exemple de la nature et de la volumétrie des données de santé à caractère personnel traitées.

Le périmètre de l'homologation doit être décrit précisément comme recommandé par le guide de l'ANSSI, avec :

- Des éléments fonctionnels et organisationnels ;
- Des éléments techniques ;
- Le périmètre géographique et physique.

4.2 Étape n°2 : Quel type de démarche dois-je mettre en œuvre ?

4.2.1 Autodiagnostic des besoins de sécurité et du niveau de maturité SSI

Le guide d'homologation de l'ANSSI propose des questionnaires d'autodiagnostic rapide des besoins de sécurité du système cible de l'homologation et du niveau de maturité SSI de l'organisme qui la mène. La réalisation de ces évaluations est possible à titre informatif, cependant le présent guide fixe un certain nombre de règles (réalisation d'une analyse de risques, d'un audit…) qui priment sur les résultats bruts de la méthode proposée par l'ANSSI.

4.2.2 Démarche appropriée

La démarche proposée ici pour l'homologation d'un moyen d'identification électronique se base sur la démarche nommée « Mezzo Forte » du guide [HOMOLOGATION]. Toutefois, par rapport à la définition donnée pour celle-ci, il n'est pas requis de prévoir systématiquement une assistance conseil externe. Chaque entité doit évaluer, selon ses capacités propres et le contexte de cette homologation, si cette assistance externe est nécessaire ou non.

Les attendus exigés aux étapes suivantes de l'homologation sont précisés dans les paragraphes ci-dessous pour chacune des étapes.

4.3 Étape n°3 : Qui contribue à la démarche ?

4.3.1 L'autorité d'homologation

L'Autorité d'Homologation (AH), qui prend la décision d'homologation, doit être choisie au niveau hiérarchique suffisant pour assumer toutes les responsabilités associées.

Au sein d'une autorité administrative, l'AH est désignée par l'AQSSI (Autorité Qualifiée pour la Sécurité du Système d'information), elle-même désignée par arrêté ministériel. Au sein d'une entité de droit privé, l'AH est par exemple son responsable légal.

4.3.2 La commission d'homologation

La commission d'homologation comprend typiquement :

- Le responsable du système de gestion des moyens d'identification électronique ;
- Le responsable du système d'information des ressources humaines ;
- Le délégué à la protection des données (DPO au sens du RGPD) ;
- Le responsable, ou un expert désigné, de la sécurité des systèmes d'information.

Optionnellement, des membres supplémentaires peuvent être ajoutés comme par exemple :
- Un expert métier de l'identification électronique ;
- Un expert technique du moyen d'identification électronique si besoin ;
- Le ou les responsables des services numériques en santé sur lesquels ces MIE seront utilisés ;
- Un expert juridique.

La composition exacte de la commission doit être adaptée au contexte, en s'assurant que les points de vue juridiques, métier, technique et sécurité soient bien représentés.

4.3.3 Les acteurs de l'homologation

Le guide de l'ANSSI propose comme acteurs de l'homologation :

- La maîtrise d'ouvrage ;
- Le RSSI ;
- Le responsable d'exploitation du système ;
- Les prestataires ;
- Les systèmes interconnectés.

Concernant la maîtrise d'ouvrage, le contexte de cette homologation invite à intégrer à la fois :

- Le responsable du service numérique en santé, qui joue un rôle clé dans l'appréciation des risques liés au moyen d'identification électronique à homologuer ;
- Le responsable du système de gestion du moyen d'identification électronique, qui est capable d'évaluer le niveau de conformité du MIE au référentiel européen et d'identifier les risques propres à celui-ci.

L'homologation d'un moyen d'identification électronique peut faire intervenir des systèmes interconnectés par exemple si :

- Une entité fournissant un service numérique en santé accepte l'authentification par des MIE émis par une autre entité ;
- Une entité fournit des MIE à ses propres agents mais aussi à des agents d'une autre entité.

Dans ce cas, une autorité d'homologation de l'entité responsable du système interconnecté et/ou d'autres acteurs (maîtrise d'ouvrage, responsable sécurité, experts…) peuvent être amenés à participer à l'homologation.

4.4 Étape n°4 : Comment s'organise-t-on pour recueillir et présenter les informations ?

4.4.1 Le dossier d'homologation

En lien avec la démarche proposée par ce guide, le dossier d'homologation doit contenir :

- Un document de définition de la stratégie d'homologation ;
- La liste des référentiels de sécurité, où l'on retrouve :
  - Le référentiel d'identification électronique [IE-ASPP] ;
  - Les spécifications eIDAS d'un moyen d'identification électronique de niveau substantiel [MIE] ;
- L'analyse de risque et le plan de traitement des risques identifiés :
  - Du service numérique en santé ;
  - Du système de gestion des moyens d'identification électronique ;
- La politique de sécurité des systèmes d'information applicable ;
- Les procédures d'exploitation sécurisée du système ;
- Le journal de bord de l'homologation ;
- Les certificats de qualification / certifications des produits ou prestataires, par exemple :
  - La qualification ou la certification (CSPN) du dispositif d'authentification ;
  - La certification ISO 27001 ou HDS d'une composante du système d'information, par exemple d'un hébergeur ;
- Les résultats d'audits, en particulier :
  - Les résultats de l'audit de conformité du système de gestion du MIE au référentiel eIDAS [MIE] ;
  - Les résultats de l'audit de conformité des systèmes à la politique de sécurité de l'information (recommandé) ;
- La liste des risques résiduels identifiés ;
- La décision d'homologation.

Pour les systèmes déjà mis en service, par exemple un moyen d'identification électronique en production avant parution du référentiel d'identification électronique :

- Le tableau de bord des incidents et de leur résolution (recommandé) ;
- Les résultats d'audits précédents ;
- Le journal des évolutions du système.

4.4.2 Le planning

La planification des tâches pour aboutir à l'homologation est à effectuer très précautionneusement, en prenant en compte en particulier les analyses de risque et les audits qui ont un rôle prépondérant et n'apparaissent pas toujours pour les projets non soumis à homologation.

L'objectif est que la décision d'homologation soit prononcée si possible avant la mise en œuvre des moyens d'identification électronique, et dans tous les cas avant le 01/01/2026 tel que requis par le référentiel d'identification électronique [IE-ASPP].

4.5 Étape n°5 : Quels sont les risques pesant sur le système ?

4.5.1 L'analyse de risque

L'identification des risques relatifs au moyen d'identification électronique repose sur :

- L'évaluation technique de la sécurité intrinsèque du dispositif d'authentification remis aux personnes physiques, qui peut être matériel (une carte, une clé USB, …) et/ou logiciel (une application mobile par exemple, ou les composants logiciels et le protocole de communication entre le service d'authentification et le composant matériel) ;
- L'analyse de risque du système d'information de gestion du moyen d'identification électronique.

Par ailleurs, l'analyse de risque du service numérique en santé permet de fixer les objectifs de sécurité à atteindre a minima par le moyen d'identification électronique et son système de gestion. La décision d'homologation repose in fine sur l'assurance de l'adéquation du MIE au service numérique en santé.

4.5.1.1 Evaluation technique de sécurité du dispositif d'authentification

Objectifs de sécurité

Le dispositif d'authentification utilisé comme moyen d'identification électronique homologué doit satisfaire les exigences du référentiel européen [MIE] pour les moyens de niveau de garantie substantiel :

- D'une part des exigences de conception du moyen :
  - Le moyen d'identification électronique utilise au moins deux facteurs d'authentification de différentes catégories.
  - Le moyen d'identification électronique est conçu de sorte qu'on puisse présumer qu'il est utilisé uniquement sous le contrôle de la personne à laquelle il appartient ou en sa possession.
- D'autre part des exigences portant sur le mécanisme d'authentification :
  - La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique.
  - Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire aux mécanismes d'authentification.

Risques liés à la conception du moyen d'identification électronique

Les facteurs d'authentification doivent être choisis dans l'une des catégories suivantes :

- Facteurs d'authentification basés sur la possession (ce que l'on possède, par exemple, une carte à puce) ;
- Facteurs d'authentification basés sur la connaissance (ce que l'on sait, par exemple, un mot de passe) ;
- Facteurs d'authentification inhérents (ce que l'on est, par exemple, une empreinte digitale).

Pour chacune de ces catégories, les risques d'utilisation du moyen d'identification électronique par une autre personne que son détenteur légitime diffèrent :

- Facteur basé sur la possession :
  - Le dispositif matériel d'authentification peut être perdu ou volé à son détenteur : ce risque peut varier selon les caractéristiques physiques du dispositif, il faut permettre une déclaration facile et rapide d'une perte de possession pour révoquer le moyen d'identification électronique ;
  - Le dispositif d'authentification ne doit pas pouvoir être facilement reproduit, altéré ou contrefait, et toute tentative de ce type devrait être facilement détectable : par exemple, lorsqu'un secret (comme une clé cryptographique privée ou secrète) est stocké sur le matériel (puce électronique ou téléphone par exemple), des mesures de protection physique et/ou logicielle doivent empêcher son extraction ;
  - Le dispositif matériel peut être prêté par son détenteur, ou emprunté à son insu pendant son absence : la nature du dispositif peut décourager ces pratiques (un badge personnel multi-usages sera moins susceptible d'être prêté qu'une clé USB dédiée au moyen d'identification électronique) ;
- Facteur basé sur la connaissance :
  - Le secret ne doit être véritablement connu que par le détenteur du moyen d'identification électronique : celui-ci doit donc pouvoir le choisir de façon confidentielle en ayant connaissance des consignes de sécurité adaptées au cas d'usage (règles de choix d'un mot de passe, non réutilisation d'un autre secret…) ;
  - Le secret, s'il est stocké sur le serveur qui doit le vérifier, ne doit pas être enregistré tel quel ni sous aucune forme permettant de reconstituer le secret, par exemple en ne conservant qu'une empreinte cryptographique de celui-ci ;
  - Le secret ne doit pas pouvoir être deviné ni obtenu par attaque de force brute ou par dictionnaire : des mécanismes de blocage du moyen d'identification électronique doivent être prévus ;
  - Le détenteur doit être sensibilisé aux risques d'hameçonnage qui dévoilerait son mot de passe ;
- Facteur inhérent :
  - Le ou les facteurs biométriques utilisés doivent présenter une réelle singularité afin de ne pouvoir être présentés que par une seule personne physique uniquement (empreinte digitale par exemple) ;
  - La robustesse de ce type de facteur tient essentiellement à la précision de l'acquisition et de la vérification de similarité avec le schéma enregistré par le détenteur légitime. Les taux de faux positifs et faux négatifs dans le processus de vérification doivent être strictement connus et encadrés ;
  - La possibilité de tromper la vérification par des moyens frauduleux (moulages, photos…) doit être analysée et réévaluée régulièrement du fait des évolutions rapides dans ce domaine.

Risques liés au mécanisme d'authentification

Le mécanisme d'authentification, c'est-à-dire la façon dont le service s'assure que l'utilisateur est bien en possession du moyen d'identification électronique enregistré, présente aussi en lui-même des risques d'usurpation d'identité ou de divulgation de données confidentielles.

Il est exigé que ce mécanisme soit dynamique, principalement pour contrer les attaques par rejeu (interception des échanges puis réutilisation ultérieure). L'aspect dynamique est obtenu par une requête du service exigeant une réponse de la part du détenteur du moyen (ou du moyen d'identification électronique lui-même) différente à chaque authentification, par exemple via :

- La mise en œuvre d'une clé privée stockée sur un dispositif cryptographique matériel sécurisé et sous le contrôle exclusif du porteur dans le cadre d'un protocole défi-réponse ;
- L'emploi de protocoles s'appuyant sur un échange de clés Diffie-Hellman éphémère ;
- L'utilisation de codes d'accès à usage unique générés de façon dynamique (authentifications par OTP / TOTP).

Le mécanisme d'authentification doit de plus protéger la confidentialité et l'intégrité des échanges, avec des mesures telles que :

- Le chiffrement de tous les échanges, contre le décryptage, l'écoute et la manipulation, par exemple avec le protocole TLS ;
- L'emploi de mécanismes et algorithmes cryptographiques conformes à l'état de l'art ;
- L'utilisation de générateurs de nombres pseudo-aléatoires cryptographiquement sûrs pour la génération de clés cryptographiques, de secret et d'OTP ;
- La protection des secrets lors de leur saisie par le détenteur, par exemple en masquant les caractères ou par des claviers virtuels ;
- Le blocage, définitif ou temporaire, du moyen d'identification électronique après un certain nombre d'échecs successifs ;
- La configuration d'une durée de validité maximale (à fixer selon le contexte d'utilisation) pour les OTP.

Le niveau de garantie eIDAS substantiel est atteint lorsqu'il est acquis que les mesures de sécurité portant sur le dispositif d'authentification et sur le mécanisme d'authentification sont suffisantes contre un attaquant de potentiel « modéré ». Ce niveau de menace correspond à un attaquant déterminé et outillé, disposant de capacités supérieures à une personne agissant par opportunité avec des moyens facilement accessibles, sans toutefois disposer de moyens quasi-illimités ou restreints à quelques agences nationales de cybersécurité. Une grille d'évaluation des potentiels d'attaque est proposée à l'annexe B.4 de la méthodologie Critères Communs [CC_EM].

Méthodes d'évaluation de la sécurité du dispositif d'authentification

L'évaluation des risques portant sur chacun des facteurs d'authentification et sur le mécanisme d'authentification doit être formalisée et menée par des experts de la sécurité compétents dans les technologies employées.

Il est ainsi recommandé de sélectionner un dispositif d'authentification ayant déjà subi une évaluation de sécurité, tel que :

- Une qualification au niveau standard ou renforcé délivrée par l'ANSSI (voir [QUALIF]) ;
- Une certification de sécurité de premier niveau (CSPN), délivrée par l'ANSSI (voir [CSPN]) ;
- Une certification Critères Communs au niveau EAL3 minimum, délivrée par l'ANSSI (voir [CC_ANSSI]) ou par un autre organisme (voir [CC]) ;
- Une certification FIPS (voir [FIPS]) ;
- Une certification FIDO, de type U2F de niveau 2 de préférence (voir [FIDO]).

Il convient de vérifier que la cible de sécurité sur laquelle est basée l'évaluation répond bien aux objectifs de sécurité et aux risques listés ci-dessus pour le dispositif d'authentification.

La réalisation d'une évaluation de sécurité d'un dispositif est onéreuse et demande des délais importants, il est donc très largement préférable de recourir à un dispositif déjà évalué.

Les fonctions de sécurité implémentées par le dispositif d'authentification devraient intégrer typiquement :

- La protection des secrets du dispositif (code PIN, données biométriques, clés cryptographiques…), que ce soit à l'initialisation de ces secrets, sur la durée de leur stockage ou pendant la phase d'authentification ;
- La protection des attributs d'identité du détenteur s'ils sont enregistrés dans le dispositif ;
- La sécurisation des échanges lors de l'authentification ;
- Des mécanismes de blocage en cas d'utilisation frauduleuse ;
- Des mécanismes cryptographiques (type et taille des clés, algorithme cryptographique) à l'état de l'art.

Authentification avec un seul facteur

Le référentiel d'identification électronique prévoit la possibilité de n'exploiter qu'un seul des deux facteurs d'authentification du dispositif dans certains cas et après une nécessaire première authentification à double facteur.

Cette pratique remet fondamentalement en cause l'évaluation de la sécurité de l'identification électronique. Une analyse de risque spécifique aux cas d'usage identifiés pour ce type d'authentification devient nécessaire en sus de l'évaluation de sécurité du dispositif en double facteur.

Cette analyse de risque doit être formalisée en utilisant une méthodologie éprouvée, de préférence EBIOS Risk Manager de l'ANSSI [EBIOS RM]. Les risques identifiés ci-dessus doivent être évalués à nouveau en prenant en considération l'absence du second facteur. Par exemple, s'il ne reste que le facteur de possession, le risque d'utilisation par un tiers d'un dispositif d'authentification, laissé à disposition (même de façon très temporaire) en l'absence du détenteur, devient non négligeable. Seule une étude approfondie des conditions et contraintes d'utilisation ainsi que des conséquences potentielles peut permettre l'acceptation des risques résiduels inévitables.

Il est obligatoire de porter à l'attention de l'autorité d'homologation l'évaluation des risques liés à un tel scénario, en l'intégrant clairement dans le dossier d'homologation du moyen d'identification électronique.

4.5.1.2 Analyse de risque du système d'information de gestion du MIE

La fiabilité de l'identification électronique ne repose pas que sur la sécurité du dispositif d'authentification, mais aussi largement sur les processus de gestion du moyen d'identification électronique. C'est ainsi l'ensemble du système d'information de gestion du MIE et les processus associés qui doivent être considérés.

Afin d'aboutir à un résultat objectif et pertinent, il est nécessaire de mettre en œuvre une méthode d'analyse de risque éprouvée. Il est fortement recommandé d'utiliser la méthode EBIOS Risk Manager de l'ANSSI ([EBIOS RM]), qui peut s'adapter aux enjeux de sécurité et au contexte de l'homologation. La méthode EBIOS RM permet de passer en revue à la fois les risques métier liés aux différentes fonctions d'un système de gestion de MIE, et les risques liés aux infrastructures techniques, en ciblant uniquement les scénarios de risques plausibles.

Les principaux risques à évaluer dans cette analyse sont :

- L'usurpation d'identité :
  - Lors de l'enrôlement de la personne physique,
  - A la remise initiale ou en cas de renouvellement du moyen d'identification électronique,
  - Durant l'authentification,
  - A la révocation du moyen d'identification électronique,
  - En cas de déblocage ou de remplacement d'un moyen d'identification électronique ;
- L'altération de l'identité :
  - Enrôlement initial partiellement erroné,
  - Evolution non gérée des attributs d'identité après délivrance du MIE (changement de statut du PS, cessation d'activité…) ;
- La fuite de données à caractère personnel des détenteurs de MIE :
  - Vol massif de données dans le système d'information de gestion,
  - Vol de données sur les MIE,
  - Vol de données dans les échanges d'authentification ;
- L'indisponibilité du système d'information ou de données hébergées :
  - Pour réaliser une identification électronique lorsque ce système d'information y est nécessaire,
  - Pour l'enrôlement ou la délivrance d'un MIE,
  - Pour la révocation ;
- L'indisponibilité ou l'altération des traces des actions réalisées sur ce système.

L'analyse de risque doit considérer ces risques pour les différents processus de gestion des MIE, en particulier :

- Enrôlement d'un porteur : vérification initiale d'identité, enregistrement des attributs d'identité et de l'identifiant du porteur ;
- Remise du moyen d'identification électronique ;
- Identification électronique d'un porteur de moyen d'identification électronique ;
- Révocation d'un moyen d'identification électronique ;
- Déblocage, remplacement ou renouvellement à expiration d'un moyen d'identification électronique.

L'analyse de risques doit prendre en compte les vulnérabilités propres au dispositif d'authentification et au mécanisme d'authentification, dans les différents contextes d'utilisation du moyen d'identification électronique. L'atteinte du niveau de garantie substantiel requiert de considérer les attaquants de potentiel d'attaque modéré (voir les risques liés au mécanisme d'authentification au §4.5.1.1).

4.5.2 Identifier les mesures de sécurité

L'analyse de risques doit aboutir à :

- Une liste de scénarios de menace dans le contexte de déploiement des moyens d'identification électronique ;
- Une liste de mesures de sécurité couvrant ces menaces ;
- Une liste de risques résiduels non totalement couverts par les mesures de sécurité.

Les mesures de sécurité découlent des scénarios de menace identifiés. Des catalogues de mesures de sécurité classiques de la sécurité des systèmes d'information peuvent se trouver dans :

- Le guide d'hygiène de l'ANSSI ([HYGIENE]) ;
- Les recommandations de l'ANSSI pour la sécurisation de la mise en œuvre du protocole Open ID Connect ([OIDC]) ;
- Les recommandations de l'ANSSI relatives à l'authentification multifacteur et aux mots de passe ([AUTH_MDP]) ;
- Les recommandations de l'ANSSI relatives à l'administration sécurisée des systèmes d'information ([ADMIN]) ;
- Les recommandations de l'ANSSI pour le choix et le dimensionnement de mécanismes cryptographiques ([CRYPTO]) ;
- La norme ISO 27002 ([ISO-27002]).

4.6 Étape n°6 : La réalité correspond-elle à l'analyse ?

4.6.1 Réalisation du contrôle

L'homologation d'un moyen d'identification électronique nécessite un audit formalisé du système d'information de gestion du moyen d'identification électronique.

Cet audit de conformité doit se baser sur les exigences formulées dans les documents suivants :

- Le référentiel des spécifications techniques et procédures minimales relatives au niveau de garantie substantiel des moyens d'identification électronique [MIE] ;
- Le référentiel d'identification électronique [IE-ASPP] portant sur les moyens homologués.

Il se décompose en plusieurs tâches d'audit :
- Un audit fonctionnel (authentification par un ou deux facteurs, identifiant et attributs délivrés par le MIE) ;
- Un audit technique de l'infrastructure du système (architecture, configuration des composantes) ;
- Un audit organisationnel des équipes participant à la fourniture des MIE (opérateurs d'enrôlement, responsables sécurité, exploitants de la plateforme) ;
- Éventuellement des tests d'intrusion sur les interfaces externes (voire internes) de l'infrastructure.

L'audit peut être entièrement mené par des équipes internes de la structure fournissant le moyen d'identification électronique, ou être confié totalement ou partiellement à un organisme d'audit tiers, en fonction de la stratégie d'homologation et des compétences disponibles. De précédent résultats d'audit (ISO 27001 par exemple) peuvent être réutilisés s'ils sont encore valides et pertinents.

4.6.2 Définition du périmètre du contrôle

Le périmètre à auditer est le système d'information utilisé pour la gestion des moyens d'identification électronique (voir au §3.3). Il comporte :

- Le SI de gestion du MIE (enregistrement, délivrance, révocation, renouvellement…) ;
- Le répertoire d'identité des détenteurs des MIE, qui est potentiellement inclus dans le SI RH ;
- Les services techniques et infrastructures partagées du système d'information ;
- Les opérateurs (et leurs postes de travail), qu'ils soient affectés aux tâches métier d'enregistrement ou de délivrance du métier, ou aux tâches techniques d'exploitation du SI.

4.6.3 Conséquences de l'audit sur le dossier d'homologation

Les résultats de l'audit de conformité doivent être consignés dans un rapport formalisé, indiquant si une exigence est satisfaite totalement, partiellement ou pas du tout, et précisant les arguments de conformité ou de non-conformité.

Le rapport doit comporter une synthèse des non-conformités identifiées, et le cas échéant préciser :

- L'évolution potentielle des menaces sur le système ;
- La liste des éventuelles nouvelles vulnérabilités identifiées ;
- Des préconisations de mesures correctrices.

Le rapport d'audit est à intégrer au dossier d'homologation, qui doit être complété en tenant compte des nouveaux risques identifiés.

4.7 Étape n°7 : Quelles sont les mesures de sécurité supplémentaires à mettre en œuvre pour couvrir ces risques ?

4.7.1 Le traitement du risque

A ce stade, certains risques peuvent ne pas être complètement couverts par des mesures de sécurité. Ce sont :

- Des risques résiduels identifiés dans l'analyse de risque ;
- Des risques identifiés au cours de l'audit de conformité.

Il revient à l'autorité d'homologation, sur avis de la commission d'homologation, de se prononcer sur le traitement de ces risques, en choisissant pour chacun de :

- L'éviter : modifier le système de gestion du MIE ou faire évoluer le MIE lui-même de telle sorte que le risque soit supprimé ;
- Le réduire : prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance du risque, de façon à ce que le risque puisse alors être assumé ;
- L'assumer : en supporter les conséquences éventuelles sans prendre de mesure de sécurité supplémentaire. Ceci est nécessaire pour certains risques, comme ceux liés à un attaquant de potentiel supérieur au potentiel modéré visé par le niveau substantiel, ou ceux liés à des utilisateurs ne respectant pas les consignes de sécurité. Il n'est par contre pas possible d'assumer des risques qui remettraient en cause le respect du RGPD ou l'atteinte du niveau de garantie substantiel.
- Le transférer : faire assumer la responsabilité à un tiers. Cette option est à évaluer avec une extrême précaution pour le cas de l'homologation d'un moyen d'identification électronique dans le cadre du référentiel [IE-ASPP] étant donné les enjeux.

4.7.2 La mise en œuvre de mesures de sécurité

De nouvelles mesures de sécurité peuvent être décidées pour éviter ou réduire un risque identifié en audit de conformité ou pour traiter un risque résiduel identifié dans l'analyse de risque. Ces mesures peuvent être de nature technique, organisationnelle ou juridique.

4.7.3 Définition du plan d'action

Les risques résiduels acceptables identifiés lors de l'audit et de l'analyse de risques et qui ne peuvent pas être couverts immédiatement par des mesures de sécurité additionnelles sont identifiés dans un plan d'action. Ce dernier indique les vulnérabilités éventuelles, leur degré (critique, majeure, mineure…), les potentielles actions correctrices envisagées, et le cas échéant le pilote désigné ainsi que l'échéance associée.

4.8 Étape n°8 : Comment réaliser la décision d'homologation ?

4.8.1 Le périmètre de l'homologation

Le périmètre de l'homologation est défini à partir des éléments précisés au cours de l'étape 1 (cf. §4.1) et de leurs éventuelles évolutions au cours de l'élaboration du dossier d'homologation. La décision d'homologation doit être prise sur un périmètre définitif clairement présenté en terme :

- De réglementation (y compris le ou les référentiels de la PGSSI-S) prise en compte ;
- D'identification du moyen d'identification électronique homologué (modèle et version du dispositif d'authentification, conditions d'emploi…) ;
- D'identification des services numériques en santé pour lesquels ce moyen d'identification électronique est utilisable ;
- De périmètre technique (architecture technique détaillée du système d'information).

4.8.2 Les conditions accompagnant l'homologation

L'autorité d'homologation ne doit prendre une décision favorable d'homologation que lorsque les résultats de l'analyse de risque et de l'audit de conformité sont positifs, c'est-à-dire qu'ils ne relèvent aucun risque résiduel de nature à compromettre la sécurité ou le niveau de garantie du moyen d'identification électronique. Un refus d'homologation doit être prononcé dans le cas contraire, car la sécurité des données de santé à caractère personnel ne serait pas garantie, impliquant une responsabilité légale importante de la personne morale et de son responsable légal.

Lorsqu'il existe des risques résiduels qui ne sont acceptables que transitoirement, l'homologation peut n'être prononcée que sous la condition de réalisation du plan d'action convenu pour faire face à ces risques. L'homologation est aussi conditionnée au respect des processus audités pour l'exploitation du système.

4.8.3 La durée de l'homologation

L'homologation du moyen d'identification électronique doit être prononcée pour une durée maximale 4 ans.

Lorsque le plan d'action contient des tâches revêtant une importance significative quant à la sécurité du système (en lien par exemple avec une montée en charge de la volumétrie), il peut être décidé de ramener cette durée à 1 ou 2 ans afin de s'assurer d'un nouvel examen formalisé à cette échéance.

4.8.4 Conditions de suspension ou de retrait de l'homologation

Une décision d'homologation est prise sur la base d'un dossier d'homologation établi sur une version bien spécifique du système. Tout changement significatif doit impliquer un réexamen du dossier. Pour le cas de l'homologation du moyen d'identification électronique, les changements suivants sont en particulier à étudier (cf. §4.9.1) :

- Ajout de nouveaux services numériques en santé accessibles avec le MIE ;
- Evolution d'un service numérique en santé impactant le niveau de risque relatif au service (par exemple augmentation de la nature ou de la volumétrie des données de santé à caractère personnel) ;
- Evolution majeure de l'un des processus de gestion du MIE (délivrance, renouvellement…) ;
- Evolution majeure de l'architecture technique du système d'information de gestion du MIE ;
- Evolution ou apparition de vulnérabilités concernant le dispositif d'authentification ;
- Evolution du référentiel règlementaire national ou européen.

Une décision de suspension ou de retrait de l'homologation serait lourde de conséquence pour le fonctionnement nominal des activités métier dépendant du moyen d'identification électronique. Elle ne peut toutefois pas être exclue en cas de violation constatée de la sécurité ou de découverte d'une vulnérabilité critique non maîtrisable. Il convient donc :

- De construire un système robuste et fiable ;
- De mettre en place des processus de veille permettant d'anticiper au maximum les incidents de sécurité ;
- De prévoir des moyens d'identification électroniques alternatifs à ceux homologués parmi ceux autorisés par le référentiel [IE-ASPP], utilisables en cas de suspension de l'homologation.

4.8.5 Formalisation de la décision d'homologation

Un document de formalisation de la décision d'homologation est proposé par l'ANSSI parmi ses documents types.

Le texte de la décision d'homologation peut être rédigé comme suit :

«

Le *FONCTION_DE_L'AUTORITE_D'HOMOLOGATION*, représentant l'autorité d'homologation désignée par *REFERENCE_ET_DATE_DU_DOCUMENT*

DECIDE

que le moyen d'identification électronique *NOM_DU_MOYEN*, reposant sur le système d'information *NOM_DU_SI* situé à *IMPLANTATION GEOGRAPHIQUE,* mis en place pour être utilisé avec les services numériques en santé NOM_DES_SERVICES_NUMERIQUES_EN_SANTE, dans le cadre du référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques] de la PGSSI-S, est homologué dans la configuration présentée dans le dossier d'homologation [rappelée en annexe *XXX*] [et sous réserve de *XXX*].

La présente décision d'homologation est valable à compter du *JJ/MM/AAAA*, et pour une durée de *4* ans, soit jusqu'au *JJ/MM/AAAA*.

Toute modification significative du système et / ou de son environnement annule la présente décision.

ATTACHE ET SIGNATURE

»

4.8.6 Communication de la décision d'homologation à l'ANS

Une fois la décision d'homologation signée, l'autorité d'homologation transmet à l'ANS :

- Le document de décision d'homologation ;
- L'analyse de risque du système d'information de gestion du MIE ;
- Le rapport d'audit de conformité du MIE au référentiel européen d'exigences pour les identités électroniques de niveau substantiel (dont l'évaluation technique de la sécurité du dispositif d'authentification) et au référentiel [IE-ASPP] ;
- [Optionnel] L'analyse de risque du ou des services numériques en santé sur lesquels le MIE sera utilisable, comprenant le cas échéant l'évaluation du risque induit par l'utilisation du MIE avec un seul de ses deux facteurs.

Les pièces doivent être transmises de façon chiffrée après validation de la méthode utilisée par le correspondant ANS.

4.9 Étape n°9 : Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?

4.9.1 Suivi de l'homologation

Après homologation, les éléments du dossier d'homologation doivent être maintenus avec une fréquence au moins annuelle.

La commission d'homologation se réunit chaque année et vérifie, sur la base du dossier à jour, que les conditions énoncées dans la décision d'homologation sont toujours satisfaites. Elle saisit l'autorité d'homologation si une nouvelle décision doit être prise du fait de changements invalidant la dernière décision en vigueur.

La commission s'assure de plus que la décision d'homologation est renouvelée avant sa fin de validité, et au maximum 2 ans après tout changement du référentiel européen d'exigences pour les identités électroniques de niveau eIDAS substantiel.

4.9.2 Maintien en condition de Sécurité

Le maintien du niveau de sécurité du MIE doit rester une préoccupation continue de l'ensemble des acteurs du système (utilisateurs, opérateurs, responsables, commission et autorité d'homologation).

A ce titre, les actions suivantes doivent être mises en œuvre :

- Assurer la supervision fonctionnelle et de sécurité du système ;
- Effectuer une veille de sécurité régulière sur les composantes du système d'information ;
- Effectuer une veille de sécurité régulière sur le dispositif d'authentification, et s'assurer du maintien de la validité de son évaluation technique de sécurité ;
- Revoir les analyses de risques des systèmes d'information, et les amender si nécessaire, à chaque modification significative sur le périmètre homologué, et a minima tous les deux ans ;

L'autorité d'homologation doit s'assurer que tout incident de sécurité majeur impactant le moyen d'identification électronique homologué soit notifié au [CERT Santé] selon les procédures en vigueur.

Annexe 1 : Abréviations

Sigle / Acronyme	Signification
AH	Autorité d'homologation
ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de Sécurité des Systèmes d'Information
CSPN	Certification de Sécurité de Premier Niveau
DPO	Data Protection Officer
FIDO	Fast Identity Online
MIE	Moyen d'Identification Electronique
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
RSSI	Responsable de la Sécurité des Systèmes d'Information
SSI	Sécurité des Systèmes d'Information
OTP	One Time Password
TLS	Transport Layer Security
TOTP	Time-based One Time Password ([RFC 6238])
UE	Union Européenne