AGENCE
DU NUMÉRIQUE
EN SANTÉ

PGSSI-S

Référentiel d'identification électronique

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

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

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

Documents de référence

Réglementation

Renvoi	Document
[ART_L1470]	Articles L. 1470-1 à 1470-5 du code de la santé publique (issus de l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464
[eIDAS]	Règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23/07/2014 (« règlement eIDAS ») https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR
[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/
[ORDO_RGS]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/

Documents techniques

Renvoi	Document
[CI-SIS]	Cadre d'Interopérabilité des SI de Santé https://esante.gouv.fr/interoperabilite/ci-sis
[EBIOS RM]	EBIOS Risk Manager https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/#
[EN319411]	ETSI EN 319411 : Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates - Part 1 General requirements https://www.etsi.org/standards
[ENGAGEMENT]	Engagement sur la sécurisation des modalités d'identification électronique des utilisateurs des services numériques en santé https://esante.gouv.fr
[IGC]	Politiques de certification et gabarits des certificats de l'IGC Santé http://igc-sante.esante.gouv.fr/PC/#pcr
[IE-ASPP]	Référentiel d'identification électronique - Acteurs des secteurs sanitaire, médico-social et social [personnes physiques] https://esante.gouv.fr

[IE-Usagers]	Référentiel d'identification électronique - Usagers https://esante.gouv.fr
[IE-CA]	Référentiel de contrôle d'accès – *à paraître* *Consulter aussi le* Guide gestion des habilitations d'accès au SI https://esante.gouv.fr
[MOS-NOS]	CI-SIS - Modèle des Objets de Santé https://esante.gouv.fr/interoperabilite/mos-nos
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://tools.ietf.org/html/rfc5280

SOMMAIRE

1 PREAMBULE

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

1.1 Objet du référentiel

Pris en application des dispositions des articles L. 1470-2 et L. 1470-5 du code de la santé publique (voir [ART_L1470]), le présent document définit le niveau minimum de garanties attendu s'agissant des modalités d'identification électronique des personnes morales utilisant des services numériques en santé. Le référentiel est décomposé en trois volets, dédiés respectivement :

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

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

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

L'étape d'habilitation, ou de contrôle d'accès, dans laquelle des autorisations sont données au professionnel de santé est traitée dans un référentiel distinct (voir [IE-CA]). Outre les traits d'identité, des éléments de contexte complémentaires (ex : l'identité de la personne physique ou du processus déclenchant une opération, etc.) peuvent être fournis par l'utilisateur au fournisseur de service dans cette phase d'identification électronique afin que le fournisseur de service puisse automatiser ses contrôles d'accès et/ou renforcer la traçabilité.

1.2 Périmètre d'application du référentiel

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

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

Au sein de ce périmètre, le présent volet s'applique à l'identification électronique des acteurs, personnes morales, en charge d'activités relevant des secteurs sanitaire, médico-social et social. Ceci correspond donc à l'identification d'une application ou d'un serveur, agissant sous la responsabilité d'une de ces personnes morales, et ouvrant une connexion à un service numérique en santé objet de ce référentiel. Cette connexion peut être à l'initiative d'une personne physique ou déclenchée sans intervention humaine.

Le fournisseur d'un service numérique en santé peut décider de n'autoriser l'accès à son service, ou à certaines fonctions de son service, qu'après identification de la personne morale ou de la personne physique interagissant

avec l'application qui ouvre la connexion. Cette identification supplémentaire permet de renforcer l'imputabilité et la traçabilité des actions. Elle nécessite des mécanismes supplémentaires qui sont décrits dans une partie dédiée du référentiel.

L'authentification d'un site web, sous la responsabilité d'une personne morale et exposé via des navigateurs, est exclue du périmètre de ce référentiel.

2 DEFINITIONS ET CONCEPTS GENERAUX

2.1 Personne morale

Dans le cadre de ce référentiel, le terme **personne morale** est utilisé pour désigner une entité dotée d'une personnalité juridique rentrant dans le champ de ce référentiel. Il s'agit par exemple d'entités en charge d'activités relevant des secteurs sanitaire, médico-social et social, ou de fournisseurs de services numérique à destination de ces dernières. Une personne morale est aussi désignée dans ce document par le terme « structure », ainsi que cela est fait dans d'autres référentiels de l'ANS.

2.2 Services numériques et services numériques partagés

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

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

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

2.3 Identification électronique

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

Par exemple, l'ouverture d'une connexion avec authentification mutuelle par certificat, ou la signature d'un jeton d'authentification, constituent une identification électronique auprès du système cible.

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

2.4 Moyen d'identification électronique

Un **moyen d'identification électronique** est un dispositif matériel et/ou immatériel contenant un identifiant personnel et utilisé pour s'authentifier sur un service numérique, en santé dans le présent document. Dans le règlement eIDAS, un moyen d'identification électronique est associé à un niveau de garantie faible, substantiel ou élevé selon le niveau de sécurité qu'il offre.

Afin de préserver le niveau de sécurité déclaré d'un moyen d'identification électronique, son fournisseur et son détenteur sont tenus de respecter un ensemble de mesures de sécurité sur tout son cycle de vie. En particulier, des engagements concernant la conservation et l'utilisation de ce dispositif 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, un certificat logiciel de personne morale sont des exemples de moyens d'identification électronique.

2.5 Données d'identité

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

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

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

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

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

2.6 Identifiant

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

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

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

- Il y a collision d'identifiants lorsqu'un même identifiant a été attribué à deux personnes distinctes dans le répertoire d'identité ;
- Il y a doublon d'identifiants lorsque plusieurs identifiants différents sont attribués à une même personne physique ou morale dans le répertoire d'identité. Cette notion de « même personne » doit être considérée au regard des traits d'identité définis comme différenciants pour le répertoire. Par exemple, une même personne morale peut apparaître plusieurs fois dans un répertoire d'identité d'établissements (i.e. pour chaque établissement rattaché à cette personne morale).

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

2.7 Répertoires d'identité

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

Dans le cadre de la PGSSI-S, différents types de répertoires d'identité sont identifiés :

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

Le répertoire SIRENE enregistre toutes les entreprises et leurs établissements, quelle que soit leur forme juridique et quel que soit leur secteur d'activité. Les entreprises étrangères qui ont une représentation ou une activité en France y sont également répertoriées.

Le répertoire FINESS (Fichier national des établissements sanitaires et sociaux) recense l'ensemble des structures et équipements des domaines sanitaire, médico-social, social et de formation aux professions de ces secteurs actuellement soumis à autorisation préalable en application des dispositions du code de la santé publique ou du code de l'action sociale et des familles, et a vocation à être élargi à toutes les structures du secteur.

2.8 Fournisseurs de service et fournisseurs d'identité

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

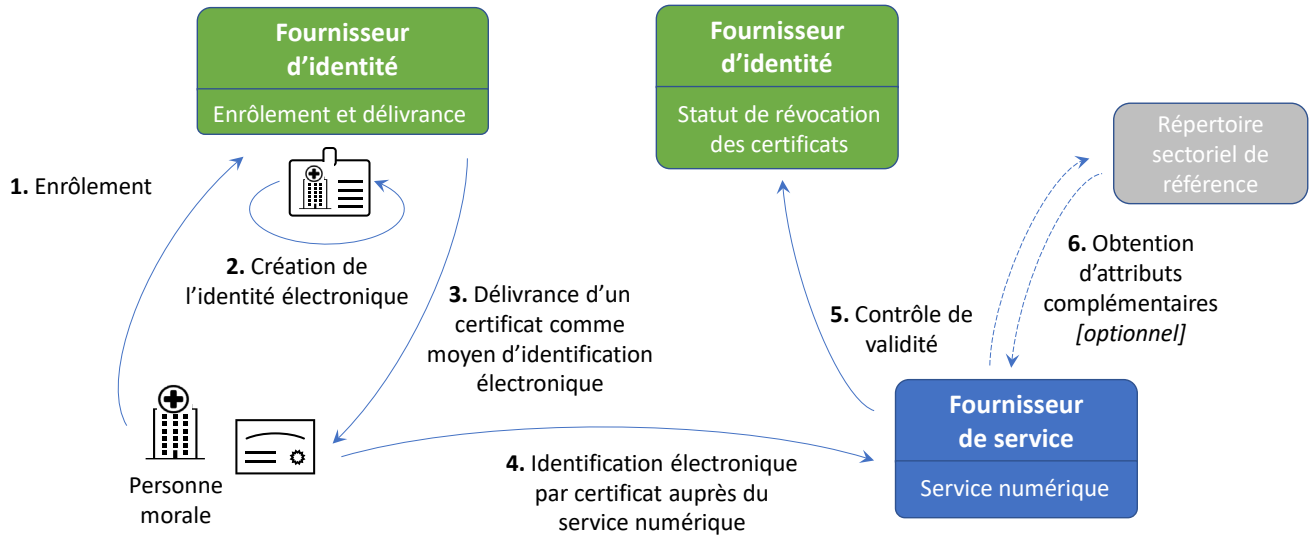
Un **fournisseur d'identité** est une entité qui délivre un moyen d'identification électronique à une personne physique ou morale (potentiellement elle-même) qui a demandé ce moyen et dont elle a établi une identité électronique fiable.

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

A titre d'exemple pour les personnes morales :
- L'Assurance Maladie est le fournisseur de service des API d'intégration du DMP dans des logiciels tiers ;
- L'ANS, en tant que responsable de l'IGC Santé, est un fournisseur d'identité délivrant des certificats comme moyens d'identification électronique.

2.9 Processus d'identification électronique

Les processus liés à l'identification électronique par certificat peuvent être schématisés ainsi :



Après s'être enregistrée et avoir obtenu un certificat x509 auprès d'un fournisseur d'identité, la personne morale initie une connexion vers le service numérique d'un fournisseur de service. Elle utilise son certificat pour s'identifier et s'authentifier.

Le service contrôle la validité du certificat en vérifiant notamment son statut de révocation auprès du fournisseur d'identité émetteur.

Le service peut obtenir des attributs supplémentaires d'identité de la personne morale connectée (tels que le type de structure, ses coordonnées, …) en interrogeant le répertoire sectoriel de référence sur la base de l'identifiant présent dans le certificat.

Une fois l'identification électronique vérifiée, le fournisseur de service octroie à la personne morale les accès correspondant à ses habilitations (se reporter au référentiel de contrôle d'accès [IE-CA]). Des éléments de contexte de cette connexion (tels que la personne physique ou le système initiant celle-ci) peuvent être transmis en complément de cette identification électronique pour préciser les habilitations à octroyer (cf. §5).

3 IDENTITE ELECTRONIQUE DES PERSONNES MORALES ACTEURS DE SANTE

3.1 Identifiants

Lors d'une demande d'identification électronique d'un acteur personne morale intervenant en santé, l'usage de l'identifiant national de cet acteur est obligatoire. Cet identifiant permet d'obtenir des données supplémentaires concernant la personne morale identifiée dans les répertoires d'identité nationaux régaliens ou sectoriels.

Exigence n°1
[EXI 01] Les identifiants nationaux à utiliser pour l'identification des personnes morales acteurs de santé sont[1] : - Le numéro FINESS juridique (FINESS EJ) ou géographique (FINESS ET) ; - Le numéro SIREN ou SIRET.

La valeur de l'identifiant sectoriel de référence est préfixée par un chiffre indiquant le type d'identifiant utilisé (cf. [MOS-NOS]), avec :

- « 1 » pour un identifiant FINESS juridique ou géographique ;
- « 2 » pour un identifiant SIREN ;
- « 3 » pour un identifiant SIRET ;
- « 4 » pour un identifiant RPPS-rang.

Un fournisseur de service doit explicitement indiquer quels sont les types d'identifiants qu'il accepte. Il peut être amené, selon ses contraintes et son appréciation des risques, à imposer certains types d'identifiants. Par exemple le FINESS géographique ou le numéro SIRET peuvent être préférés du fait de la meilleure traçabilité des accès qu'ils procurent et parce qu'ils permettent de retrouver la structure juridique à laquelle l'établissement est rattaché, mais à l'inverse ils peuvent être considérés comme générant trop de complexité de gestion pour les besoins du service.

3.2 Attributs d'identité

Les attributs d'identité d'un acteur de santé personne morale sont, entre autres :

- La raison sociale ;
- L'adresse postale ;
- La catégorie juridique ;
- Le secteur d'activité.

L'identité communiquée au fournisseur de service peut aussi intégrer d'autres informations relatives au contexte de la connexion auprès du fournisseur de service, par exemple :

- Le nom d'une entité interne de la personne morale ;
- Le nom du service applicatif (service médical, service de facturation…) ;
- Le nom de la machine ou le nom de domaine (FQDN) qui ouvre la connexion.

Un certificat émis par l'IGC Santé peut intégrer le nom d'un service applicatif dans l'attribut CommonName (CN) du sujet du certificat. Cette valeur n'est cependant pas vérifiée par l'IGC Santé, elle est uniquement sous la responsabilité de la personne morale demandant le certificat.

[1] L'identifiant RPPS-rang peut exceptionnellement être utilisé pour les cabinets individuels de radiologie organisés en SCM

Exigence n°2
[EXI 02] Un service numérique en santé ne doit pas imposer la présence d'un nom applicatif particulier ou d'un nom de machine spécifique dans les attributs du certificat utilisé pour l'identification électronique d'une personne morale.

Cette pratique conduirait en effet une entité à multiplier le nombre de certificats client avec l'augmentation du nombre de services auxquels ses applications se connectent. Pour favoriser l'évolutivité des moyens d'identification électronique présentés par une application cliente, un service numérique en santé devrait en règle générale n'extraire de l'identité présentée que l'identifiant du client, et compléter si nécessaire son contrôle d'accès sur des données supplémentaires acquises par ailleurs (cf. [IE-CA]).

4 MOYENS D'IDENTIFICATION ELECTRONIQUE

4.1 Sélection du moyen d'identification électronique

4.1.1 Analyse de risque

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

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

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

4.1.2 Moyens d'identification électronique exigés

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

Ce volet du référentiel s'applique à l'identification électronique de l'ensemble des acteurs personnes morales intervenant en santé qui utilisent des services numériques en santé, y compris les sous-traitants et prestataires impliqués.

Exigence n°3

[EXI 03] Les moyens d'identification électronique autorisés pour l'authentification d'une personne morale dépendent du **caractère partagé ou non du service** (voir au §2.2). Ce sont :
- Pour un service partagé : un certificat électronique x509 de personne morale émis par l'IGC Santé (voir au §4.2) ;
- Pour un service qui n'est pas un service partagé :
  - De préférence, un moyen d'identification électronique autorisé pour les services partagés ;
  - A défaut, un certificat électronique x509 respectant des contraintes minimales (voir au §4.3).

Le cas d'usage d'un service non partagé correspond à l'identification électronique d'une application (ou d'un serveur) se connectant à un service numérique de santé placés tous deux sous la responsabilité de la même personne morale.

Par exception, un service numérique d'un établissement membre d'un GHT, ouvert uniquement à des applications ou serveurs sous la responsabilité d'autres établissements du même GHT, n'est pas considéré comme un service partagé.

Exigence n°4
[EXI 04] Les services numériques partagés doivent avoir implémenté l'identification électronique des acteurs personnes morales intervenant en santé par un certificat émis par l'IGC Santé au plus tard au 1er juin 2022.

4.1.3 Exigences relatives aux certificats électroniques

Conformément à l'état de l'art, seuls les certificats x509 électroniques valides (au sens de la [RFC 5280]) doivent être acceptés lors de l'ouverture d'une connexion.

Exigence n°5
[EXI 05] Le fournisseur du service numérique doit vérifier la validité du certificat utilisé pour l'identification électronique d'une personne morale, et en particulier son statut de révocation en recourant aux listes de révocation (CRL) ou aux services en ligne (OCSP).

En cas de suspicion de compromission du certificat de l'un de ses clients, le fournisseur du service numérique doit en informer l'Autorité de Certification émettrice afin que celle-ci étudie la situation et procède le cas échéant à la révocation du certificat. Les procédures applicables sont décrites dans la Politique de Certification du certificat concerné.

Exigence n°6
[EXI 06] Le certificat utilisé par une personne morale pour son identification électronique sur un service numérique doit être dédié à cet usage.

Ce certificat ne doit pas être identique avec un potentiel certificat de cachet utilisé pour créer des cachets électroniques de documents, et qui peut être émis pour les mêmes personnes morales avec des identifiants identiques ou différents de ceux stipulés par ce document.

4.2 Certificat de personne morale de l'IGC Santé

4.2.1 Généralités

Les certificats de personne morale font partie de l'offre de certificats logiciels x509 de l'IGC Santé (voir [IGC]), agissant ici en tant que fournisseur d'identité. Les certificats d'authentification permettent d'initier une connexion TLS avec authentification mutuelle sur un service distant, et des certificats de cachet permettent de signer des jetons d'authentification. Le niveau de sécurité de l'identification et de l'authentification avec ces certificats est garanti par les processus de délivrance et de gestion des certificats de l'IGC Santé. Les certificats délivrés par l'IGC Santé sont conformes au RGS.

Les certificats de personne morale (nommée également « organisation ») émis par l'IGC Santé portent un identifiant de la structure permettant d'obtenir les données d'identité de cette structure dans un répertoire national de référence. Cet identifiant est contenu dans le champ OU (« Organizational Unit ») du certificat.

Une personne morale voulant accéder à un service numérique nécessitant un certificat de l'IGC Santé doit demander ce certificat auprès cette IGC[2]. Ces certificats sont valables 3 ans, et doivent être renouvelés avant d'atteindre leur date d'expiration pour prolonger le fonctionnement de l'identification électronique.

4.2.2 Identifiant et données d'identité

Le certificat porte, dans le sujet du certificat, certains attributs d'identité de la structure pour laquelle il a été émis, dont :

- Un identifiant issu d'un répertoire sectoriel de référence ou d'un répertoire d'identité national régalien (voir §3.1) ;
- La raison sociale de la structure ;
- Pour les certificats d'authentification serveur uniquement : le nom FQDN (nom de domaine pleinement qualifié) du serveur pour lequel le certificat est émis.

L'exactitude et l'authenticité de l'ensemble de ces données ont été vérifiées lors de l'enregistrement de la demande de certificat.

L'identifiant national permet de retrouver les données d'identité de la structure dans un répertoire sectoriel de référence. Cette recherche aux couches d'exposition des répertoires de référence est à la charge du service numérique cible de l'identification électronique ou du fournisseur d'identité auquel a été déléguée cette identification électronique.

Le répertoire sectoriel de référence intègre les données d'identité de la structure concernée, dont son secteur d'activité et son adresse postale.

4.2.3 Certificats requis

Il est recommandé d'utiliser, pour favoriser l'interopérabilité et la généricité, un certificat d'authentification permettant d'initier une authentification mutuelle TLS. Des certificats de cachet peuvent aussi être utilisés pour signer des jetons d'authentification, pour des cas d'usage plus spécifiques. Il est alors recommandé de recourir à des protocoles et formats interopérables, tels que des jetons VIHF ou le protocole OpenID Connect.

Exigence n°7
[EXI 07] Les certificats de personne morale émis par l'IGC Santé et utilisés pour l'identification électronique doivent respecter les exigences suivantes : - Lorsqu'il s'agit d'un certificat d'authentification, ce doit être un certificat d'authentification d'une « Organisation » (offre « ORG-CL-AUTH_CLI ») ou un certificat d'authentification « Serveur » (offre « ORG-CL-SSL_SERV ») ; - Lorsqu'il s'agit d'un certificat de cachet, ce doit être un certificat de cachet d'une « Organisation » (offre « ORG-CL-SIGN ») ; - Le certificat doit être émis par une AC de niveau « Elémentaire » ou supérieur.

Les certificats émis par l'IGC Santé au niveau « Elémentaire » visent une conformité au niveau RGS*.

4.3 Certificat de personne morale hors IGC Santé

4.3.1 Généralités

Comme pour les services partagés, des certificats d'authentification ou de cachet peuvent être utilisés pour l'identification électronique de personnes morales sur des services numériques non partagés. Le niveau de sécurité

[2] En ligne : https://esante.gouv.fr/securite/cartes-et-certificats/commandes

de l'identification et de l'authentification ainsi réalisées dépend en partie des processus de délivrance et de gestion des certificats utilisés. Ce chapitre fixe des exigences minimales concernant ces certificats afin qu'ils puissent être acceptés dans les cas identifiés au chapitre 4.1.

Ces exigences concernent :

- L'organisation mise en place pour gérer l'identification électronique ;
- Le choix de l'identifiant des personnes morales ;
- Les attributs d'identité associés aux personnes morales ;
- Les caractéristiques techniques du certificat.

Lorsque ce type de certificat est autorisé, le fournisseur du service numérique est responsable de la vérification de conformité de l'ensemble de ces exigences avant d'autoriser la connexion d'un client au service.

4.3.2 Gestion de l'identification électronique

Exigence n°8

[EXI 08] Le fournisseur du service numérique acceptant l'identification électronique de personne morale avec un certificat hors IGC Santé doit définir :

- La nature et les critères de sélection des personnes morales qui peuvent accéder à son service en utilisant un certificat ;
- La méthode de construction de l'identifiant de chaque personne morale autorisée à accéder au service ;
- Les attributs d'identité associés à une personne morale ;
- Les processus de délivrance et de gestion des certificats des clients du service ;
- Les caractéristiques des certificats autorisés pour authentifier les clients du service ;
- Les modalités de conservation et de protection des données d'identité.

De façon plus générale, le fournisseur de service est responsable de la définition des mesures de sécurité minimales à mettre en œuvre en fonction des résultats de l'analyse de risque portant sur le service fourni.

Des exigences favorisant l'interopérabilité et garantissant un niveau minimal de sécurité sont définies ci-après dans le présent référentiel.

Le fournisseur des certificats représente le fournisseur d'identité selon le schéma d'organisation décrit au chapitre 2.8.

Exigence n°9

[EXI 09] Le fournisseur d'un service acceptant l'identification électronique de personne morale avec un certificat hors IGC Santé doit choisir et identifier explicitement le ou les fournisseurs de certificats qui conviennent à son cas d'usage et qui respectent les exigences qu'il a fixées conformément à ce référentiel. Il peut endosser lui-même ce rôle.

Le recours à des certificats autosignés n'est pas autorisé du fait des risques trop importants liés à leur utilisation.

Les certificats peuvent ainsi être émis par une Autorité de Certification du marché ou par exemple par une IGC interne du fournisseur du service

Il est recommandé que ces dispositions soient rassemblées dans un document de définition des modalités d'accès au service et de description des certificats autorisés. La protection des données à caractère personnel, s'il y en a, doit être traitée par le fournisseur du service et par le fournisseur des certificats.

4.3.3 Identifiant et données d'identité

4.3.3.1 Identifiant

Exigence n°10
[EXI 10] L'identifiant de personne morale fourni par un certificat hors IGC Santé doit être : - Soit, s'il existe, le numéro FINESS juridique (EJ) ou géographique (ET) ; - Soit le numéro SIREN ou SIRET ; - Soit, à défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.), établi sous la responsabilité du fournisseur du service ou des certificats.

Dans ce cas, il n'est pas imposé de structuration ni de codage spécifique des identifiants. Néanmoins, il est fortement recommandé d'utiliser, chaque fois que c'est possible, une structuration et un codage conformes au Modèle des Objets de Santé [MOS] défini par le Cadre d'Interopérabilité des SI de Santé [CI-SIS].

Exigence n°11
[EXI 11] Le certificat hors IGC Santé doit porter au minimum l'identifiant de la personne morale à laquelle il a été attribué.

4.3.3.2 Données d'identité

Le fournisseur du service numérique est libre de choisir des attributs d'identité qui seront associés aux personnes morales. Ces attributs devront être adaptés au cadre d'utilisation prévu par le service.

Les attributs suivants sont proposés à titre d'exemple :

- Identifiant unique pour chaque personne morale du périmètre ;
- Raison sociale de l'organisation ;
- Adresse postale ;
- Secteur d'activité.

4.3.4 Certificats requis

Exigence n°12
[EXI 12] Les certificats hors IGC Santé utilisés pour l'identification électronique d'une personne morale doivent respecter les exigences suivantes : - Le certificat doit être émis par une Autorité de Certification considérée de confiance par le fournisseur du service ; - Le gabarit du certificat doit être conforme à la RFC 5280, et, si possible, à l'annexe 4 du RGS ; - Les clés publiques de type RSA doivent avoir une longueur minimale de 2048 bits. Pour les autres algorithmes, les clés publiques doivent offrir un niveau de sécurité équivalent ; - Le certificat doit être signé en utilisant une empreinte calculée par un algorithme SHA-2 ou SHA-3 ; - La clé privée doit toujours être conservée et transportée de manière chiffrée ; - L'utilisation de la clé privée doit être protégée contre toute utilisation par des tiers.

A titre de référence, la conformité aux standards suivants apporte des garanties minimales compatibles avec ces exigences :

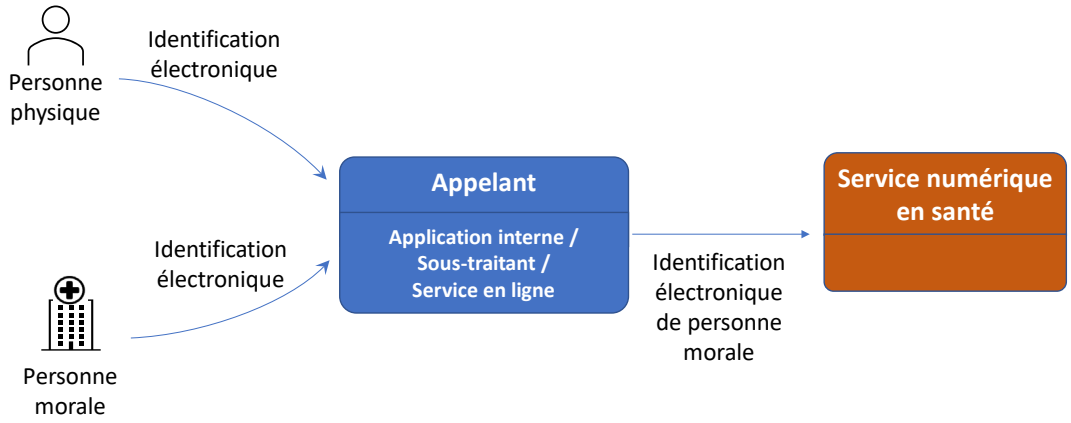
- RGS 1 étoile (voir [RGS]);
- ETSI 319 411-1 niveau LCP ou supérieur (voir [EN319411]).

5 IDENTIFICATION ELECTRONIQUE INDIRECTE

5.1 Présentation du contexte

L'identification électronique d'une personne morale permet à un service numérique en santé d'identifier et d'authentifier une application (ou un serveur) et la personne morale responsable de celle-ci. Dans de nombreuses situations, le service numérique en santé a besoin de connaître précisément l'utilisateur de cette application appelante, par exemple pour avoir une traçabilité nationale et/ou pouvoir exercer un contrôle d'accès à la personne physique. Ce peut être le cas pour :

- Des professionnels de santé utilisant une application interne de sa structure, cette application sollicitant elle-même un service numérique en santé déployé au niveau national ;
- Des professionnels de santé utilisant, directement ou via leur établissement, des services proposés par des tiers, agissant généralement comme sous-traitants. Ces services tiers, typiquement accessibles en mode « Software as a Service » (SaaS), sont mutualisées avec d'autres personnes morales ou physiques également clientes du sous-traitant. Ce sont par exemple :
  - Certains systèmes qui ont été mutualisés par des GHT ;
  - Des solutions de e-parcours proposées par les GRADeS ;
- Des citoyens utilisant un service en ligne, ce service devant accéder à leurs données dans l'espace numérique patient (« Mon espace santé »).



L'identification électronique indirecte est une solution proposée pour répondre au besoin d'identification d'un utilisateur par un service numérique lorsque cet utilisateur, que l'on nomme ci-dessous utilisateur final, n'est pas connecté directement sur ce service mais uniquement à travers une application appelante.

5.2 Modalités d'identification électroniques applicables

Afin d'éviter d'exiger une identification électronique nominale de l'utilisateur directement sur le service numérique en santé, le principe de l'identification électronique indirecte est que :

- L'application appelante réalise l'identification électronique de son utilisateur conformément au référentiel en vigueur (volets [IE-ASPP], [IE-Usagers] et le présent document) ;
- Le service numérique en santé réalise l'identification électronique de l'application appelante (en tant que personne morale), en conformité avec le présent document ;
- L'application appelante transmet l'identité de son utilisateur au service numérique en santé.

Exigence n°13

[EXI 13] L'identification électronique indirecte d'un utilisateur sollicitant un service numérique via une application appelante doit respecter les règles suivantes :

- L'application appelante s'authentifie auprès du service numérique en santé à l'aide d'un moyen d'identification électronique conforme au présent référentiel, et s'identifie en tant que personne morale ;
- L'identification de l'utilisateur (personne physique ou morale) pour lequel est effectuée cette connexion est traitée selon l'une des modalités suivantes :

1. L'application appelante communique au service numérique en santé l'identifiant de son utilisateur et une preuve de l'identification électronique de celui-ci, en utilisant des mécanismes techniques adéquats (signature électronique de l'utilisateur, transmission de jeton OpenID/SAML/VIHF/OAuth, etc.). Cette méthode fournit la meilleure garantie de sécurité mais est en pratique limitée par les développements nécessaires et les contraintes d'interopérabilité entre les services ;

2. L'application appelante communique uniquement au service numérique en santé l'identifiant de son utilisateur. Cette méthode correspond au cas général attendu ;

3. Uniquement dans le cas où l'application appelante n'est pas sollicitée par une personne physique (elle se déclenche de façon programmée par exemple), elle n'a pas à communiquer d'identifiant d'utilisateur au service numérique en santé.

Dans les deux premiers cas, le service numérique en santé est capable de mettre en place un contrôle d'accès tenant compte de l'identité de l'utilisateur de l'application appelante. Sinon, la personne morale responsable de l'application appelante devient seule responsable du respect des exigences de traçabilité et de contrôle d'accès aux données obtenues.

Exigence n°14

[EXI 14] Dans tous les cas d'identification électronique indirecte, l'application appelante conserve en interne les éléments de preuve de l'identification électronique de son utilisateur (s'il existe).

L'application appelante sera ainsi en mesure de communiquer les preuves nécessaires sur demande du service numérique en santé, en cas de litige par exemple.

Il revient au fournisseur d'un service numérique en santé de décider, au regard de son analyse de risque, d'autoriser ou non l'identification électronique indirecte et, le cas échéant, de :

- définir les modalités autorisées pour identifier les utilisateurs pour lesquels sont effectuées les connexions ;
- restreindre si nécessaire les moyens d'identification électronique autorisés pour l'identification électronique des utilisateurs du service appelant (par exemple imposer un dispositif d'authentification à deux facteurs). Le fournisseur du service numérique sensible peut, dans ce cas, demander au fournisseur du service appelant de lui communiquer son engagement de sécurisation de l'identification électronique.

Le niveau de confiance accordé à l'appelant fait partie de l'évaluation du risque, ce qui peut amener à restreindre l'accès ou différencier les exigences pour certains types d'entités (aux GRADeS par exemple, etc.).

Les utilisateurs finaux (ceux de l'application appelante) doivent être clairement informés des accès réalisés en leur nom par identification indirecte.

Exigence n°15
[EXI 15] Le contrat convenu entre les utilisateurs finaux et une application appelant un service numérique en santé doit intégrer explicitement : - L'autorisation donnée par l'utilisateur à cette application pour que celle-ci se connecte à des services numériques en santé pour son compte, en précisant les services concernés, les situations et conditions dans lesquelles ceci peut se faire ; - L'obligation faite à cette application de respecter les référentiels de sécurité relatifs à l'identification électronique, aussi bien dans l'identification électronique de l'utilisateur sur l'application, qu'à l'identification électronique de l'application auprès des services numériques en santé ; - L'obligation faite à cette application de communiquer à l'utilisateur le récapitulatif des accès effectués pour son compte auprès des services numériques en santé, en précisant les modalités de restitution.

Ce contrat peut prendre la forme de CGU signées par l'usager ou le professionnel recourant à un service tiers.

Par ailleurs, ce référentiel déconseille vivement aux utilisateurs de fournir à l'application appelante l'un de leurs propres moyens d'identification électronique (par exemple un certificat d'authentification de personne morale acteur de santé confié à un sous-traitant). Ce choix comporte en effet des risques importants quant à la confidentialité et au bon usage des moyens d'identification électronique confiés.

6 ENGAGEMENT DE SECURISATION DE L'IDENTIFICATION ELECTRONIQUE

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

Cette démarche permet en outre d'informer les tiers, utilisateurs et partenaires du service par exemple, des modalités d'identification électronique mises en place et de leur donner ainsi un élément d'appréciation du niveau de sécurité atteint. Cet engagement pourra notamment être demandé par un autre fournisseur de service numérique en santé avec lequel serait établie une identification électronique indirecte (cf. §5).

Exigence n°16
[EXI 16] Les fournisseurs de services numériques en santé doivent produire un engagement de sécurisation de l'identification électronique des personnes morales à leurs services numériques, dès la date d'entrée en vigueur du présent référentiel.

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

L'engagement est décomposé en deux parties :

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

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

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

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

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

Exigence n°17
[EXI 17] L'engagement de sécurisation de l'identification électronique doit suivre le modèle proposé par l'ANS et être signé par un responsable légal du fournisseur des services numériques concernés, ou, à défaut, par un délégataire dument habilité.

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

Exigence n°18
[EXI 18] L'engagement de sécurisation de l'identification électronique doit être renouvelé à chaque modification des modalités d'identification électronique d'un service numérique en santé, et a minima une fois par an.

7 SYNTHESE DES EXIGENCES

7.1 Identité électronique des personnes morales acteurs de santé

[EXI 01] Les identifiants nationaux à utiliser pour l'identification des personnes morales acteurs de santé sont :

- Le numéro FINESS juridique (FINESS EJ) ou géographique (FINESS ET) ;
- Le numéro SIREN ou SIRET.

[EXI 02] Un service numérique en santé ne doit pas imposer la présence d'un nom applicatif particulier ou d'un nom de machine spécifique dans les attributs du certificat utilisé pour l'identification électronique d'une personne morale.

7.2 Sélection du moyen d'identification électronique

[EXI 03] Les moyens d'identification électronique autorisés pour l'authentification d'une personne morale dépendent du **caractère partagé ou non du service** (voir au §2.2). Ce sont :

- Pour un service partagé : un certificat électronique x509 de personne morale émis par l'IGC Santé (voir au §4.2) ;
- Pour un service qui n'est pas un service partagé :
  - De préférence, un moyen d'identification électronique autorisé pour les services partagés ;
  - A défaut, un certificat électronique x509 respectant des contraintes minimales (voir au §4.3).

[EXI 04] Les services numériques partagés doivent avoir implémenté l'identification électronique des acteurs personnes morales intervenant en santé par un certificat émis par l'IGC Santé au plus tard au 1er juin 2022.

[EXI 05] Le fournisseur du service numérique doit vérifier la validité du certificat utilisé pour l'identification électronique d'une personne morale, et en particulier son statut de révocation en recourant aux listes de révocation (CRL) ou aux services en ligne (OCSP).

[EXI 06] Le certificat utilisé par une personne morale pour son identification électronique sur un service numérique doit être dédié à cet usage.

7.3 Certificat de personne morale de l'IGC Santé

[EXI 07] Les certificats de personne morale émis par l'IGC Santé et utilisés pour l'identification électronique doivent respecter les exigences suivantes :

- Lorsqu'il s'agit d'un certificat d'authentification, ce doit être un certificat d'authentification d'une « Organisation » (offre « ORG-CL-AUTH_CLI ») ou un certificat d'authentification « Serveur » (offre « ORG-CL-SSL_SERV ») ;
- Lorsqu'il s'agit d'un certificat de cachet, ce doit être un certificat de cachet d'une « Organisation » (offre « ORG-CL-SIGN ») ;
- Le certificat doit être émis par une AC de niveau « Elémentaire » ou supérieur.

7.4 Certificat de personne morale hors IGC Santé

[EXI 08] Le fournisseur du service numérique acceptant l'identification électronique de personne morale avec un certificat hors IGC Santé doit définir :

- La nature et les critères de sélection des personnes morales qui peuvent accéder à son service en utilisant un certificat ;
- La méthode de construction de l'identifiant de chaque personne morale autorisée à accéder au service ;
- Les attributs d'identité associés à une personne morale ;
- Les processus de délivrance et de gestion des certificats des clients du service ;
- Les caractéristiques des certificats autorisés pour authentifier les clients du service ;
- Les modalités de conservation et de protection des données d'identité.

De façon plus générale, le fournisseur de service est responsable de la définition des mesures de sécurité minimales à mettre en œuvre en fonction des résultats de l'analyse de risque portant sur le service fourni.

[EXI 09] Le fournisseur d'un service acceptant l'identification électronique de personne morale avec un certificat hors IGC Santé doit choisir et identifier explicitement le ou les fournisseurs de certificats qui conviennent à son cas d'usage et qui respectent les exigences qu'il a fixées conformément à ce référentiel. Il peut endosser lui-même ce rôle.

Le recours à des certificats autosignés n'est pas autorisé du fait des risques trop importants liés à leur utilisation.

[EXI 10] L'identifiant de personne morale fourni par un certificat hors IGC Santé doit être :

- Soit, s'il existe, le numéro FINESS juridique (EJ) ou géographique (ET) ;
- Soit le numéro SIREN ou SIRET ;
- Soit, à défaut, un identifiant privé à l'état de l'art (absence de collisions, autorité d'affectation définie, etc.), établi sous la responsabilité du fournisseur du service ou des certificats.

[EXI 11] Le certificat hors IGC Santé doit porter au minimum l'identifiant de la personne morale à laquelle il a été attribué.

[EXI 12] Les certificats hors IGC Santé utilisés pour l'identification électronique d'une personne morale doivent respecter les exigences suivantes :

- Le certificat doit être émis par une Autorité de Certification considérée de confiance par le fournisseur du service ;
- Le gabarit du certificat doit être conforme à la RFC 5280, et, si possible, à l'annexe 4 du RGS ;
- Les clés publiques de type RSA doivent avoir une longueur minimale de 2048 bits. Pour les autres algorithmes, les clés publiques doivent offrir un niveau de sécurité équivalent ;
- Le certificat doit être signé en utilisant une empreinte calculée par un algorithme SHA-2 ou SHA-3 ;
- La clé privée doit toujours être conservée et transportée de manière chiffrée ;
- L'utilisation de la clé privée doit être protégée contre toute utilisation par des tiers.

7.5 Identification électronique indirecte

[EXI 13] L'identification électronique indirecte d'un utilisateur sollicitant un service numérique via une application appelante doit respecter les règles suivantes :

- L'application appelante s'authentifie auprès du service numérique en santé à l'aide d'un moyen d'identification électronique conforme au présent référentiel, et s'identifie en tant que personne morale ;
- L'identification de l'utilisateur (personne physique ou morale) pour lequel est effectuée cette connexion est traitée selon l'une des modalités suivantes :

1. L'application appelante communique au service numérique en santé l'identifiant de son utilisateur et une preuve de l'identification électronique de celui-ci, en utilisant des mécanismes techniques adéquats (signature électronique de l'utilisateur, transmission de jeton OpenID/SAML/VIHF/OAuth, etc.). Cette méthode fournit la meilleure garantie de sécurité mais est en pratique limitée par les développements nécessaires et les contraintes d'interopérabilité entre les services ;

2. L'application appelante communique uniquement au service numérique en santé l'identifiant de son utilisateur. Cette méthode correspond au cas général attendu ;

3. Uniquement dans le cas où l'application appelante n'est pas sollicitée par une personne physique (elle se déclenche de façon programmée par exemple), elle n'a pas à communiquer d'identifiant d'utilisateur au service numérique en santé.

[EXI 14] Dans tous les cas d'identification électronique indirecte, l'application appelante conserve en interne les éléments de preuve de l'identification électronique de son utilisateur (s'il existe).

[EXI 15] Le contrat convenu entre les utilisateurs finaux et une application appelant un service numérique en santé doit intégrer explicitement :

- L'autorisation donnée par l'utilisateur à cette application pour que celle-ci se connecte à des services numériques en santé pour son compte, en précisant les services concernés, les situations et conditions dans lesquelles ceci peut se faire ;
- L'obligation faite à cette application de respecter les référentiels de sécurité relatifs à l'identification électronique, aussi bien dans l'identification électronique de l'utilisateur sur l'application, qu'à l'identification électronique de l'application auprès des services numériques en santé ;
- L'obligation faite à cette application de communiquer à l'utilisateur le récapitulatif des accès effectués pour son compte auprès des services numériques en santé, en précisant les modalités de restitution.

7.6 Engagement de sécurisation de l'identification électronique

[EXI 16] Les fournisseurs de services numériques en santé doivent produire un engagement de sécurisation de l'identification électronique des personnes morales à leurs services numériques, dès la date d'entrée en vigueur du présent référentiel.

[EXI 17] L'engagement de sécurisation de l'identification électronique doit suivre le modèle proposé par l'ANS et être signé par un responsable légal du fournisseur des services numériques concernés, ou, à défaut, par un délégataire dument habilité.

[EXI 18] L'engagement de sécurisation de l'identification électronique doit être renouvelé à chaque modification des modalités d'identification électronique d'un service numérique en santé, et a minima une fois par an.

Annexe 1 : Abréviations

Sigle / Acronyme	Signification
AC	Autorité de Certification
ADELI	Automatisation DEs Listes
ANS	Agence du Numérique en Santé
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé
CPS	Carte de Professionnel de Santé
CRL	Certificate Revocation List : Liste de certificats révoqués par un AC
FINESS	FIchier National des Etablissements Sanitaires et Sociaux
FQDN	Fully Qualified Domain Name
GHT	Groupement hospitalier de territoire
GRADeS	Groupements d'appui au développement de la e-santé
IGC	Infrastructure de Gestion de Clés
MOS	Modèle des Objets de Santé
OCSP	Online Certificate Status Protocol
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
RGS	Référentiel Général de Sécurité
RNIPP	Répertoire National d'Identification des Personnes Physiques
RPPS	Répertoire Partagé des Professionnels de Santé
SaaS	Software as a Service
SCM	Société Civile de Moyens
SIREN	Système d'Identification du Répertoire des ENtreprises
SIRENE	Système Informatique pour le Répertoire des ENtreprises et des Etablissements
SIRET	Système Informatique pour le Répertoire des Entreprises sur le Territoire
SIS	Système d'Information de Santé
SNGI	Système National de Gestion des Identifiants
TLS	Transport Layer Security