MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel Force Probante des documents de santé

Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques

Version : V1.0 | Date : 22/03/2021

Documents de référence

1. Référence n° 1 : Référentiel force probante des documents de santé – Document introductif
2. Référence n° 2 : Référentiel Force Probante des documents de santé – Annexe 1 – Socle commun de principes techniques et organisationnels
3. Référence n° 3 : Référentiel Général de Sécurité V2 - Annexe B1 - Mécanismes cryptographiques (ANSSI) [https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs]
4. Référence n° 4 : eIDAS : Règlement du Parlement Européen et du Conseil n°910/2014 du 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
   [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR]
5. Référence n° 5 : Décision d'Exécution de la Commission n°2015/1506 du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public […]
   [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015D1506&from=FR]
6. Référence n°6 : Article 1367 du Code civil [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000032042456]
7. Référence n°7 : ETSI EN 319 411-1 : Policy and security requirements for Trust Service Providers issuing certificates [https://www.etsi.org/standards]
8. Référence n°8 : Référentiel Force Probante des documents de santé – Annexe 5 – Gestion des métadonnées
9. Référence n°9 : Référentiel Force Probante des documents de santé – Annexe 6 – Classification des documents de santé

Historique du document

Version	Date	Commentaires
V0.11	16/09/2019	Version diffusée pour la concertation
V1.0	22/03/2021	Version finale

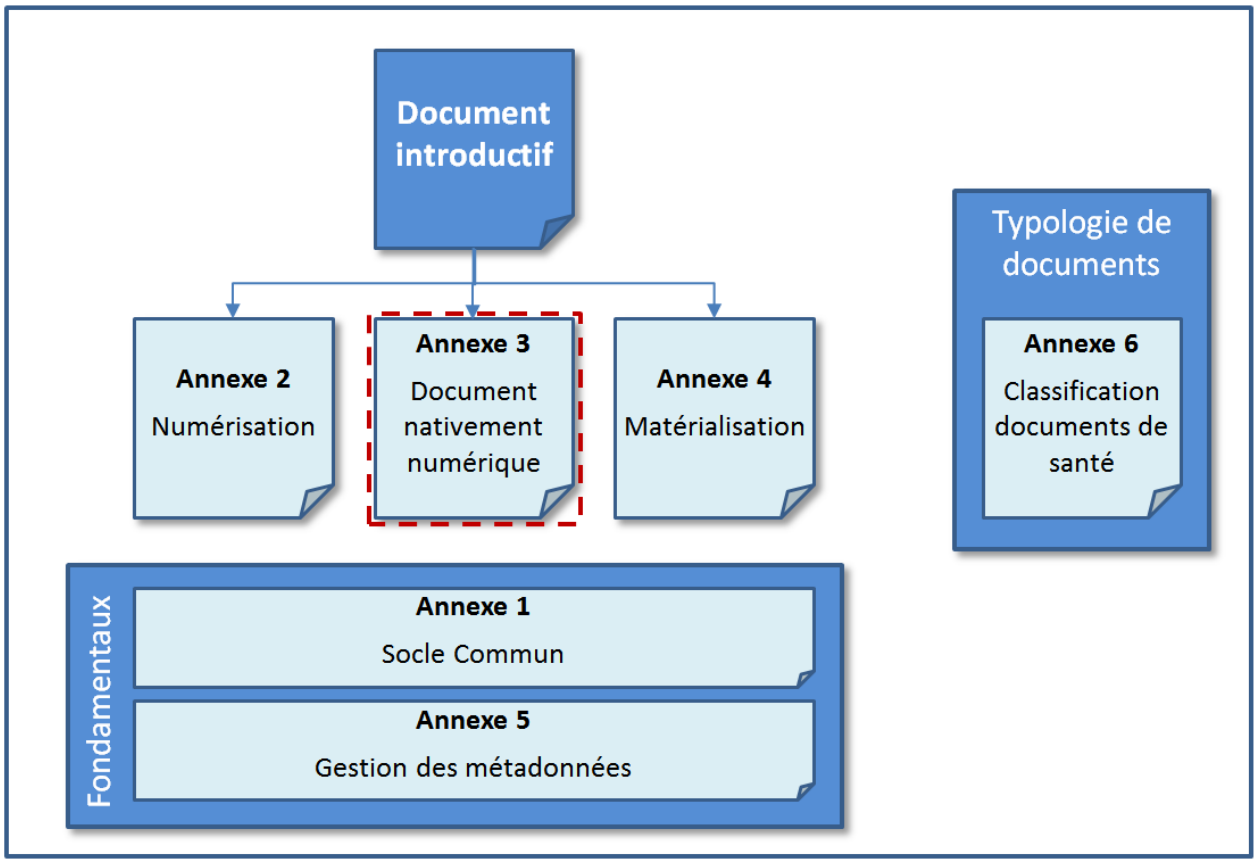
SOMMAIRE

1. INTRODUCTION

1.1. Objet du document

Ce document a pour objectif de préciser les mesures de sécurité à appliquer lors de la production de documents nativement numériques et comportant des données de santé à caractère personnel. Les règles définies dans ce document s'attachent en particulier à la force probante du document ainsi créé.

Ce document constitue l'une des annexes du référentiel « Force probante » ainsi structuré :



Structure du référentiel Force Probante

Le référentiel « Force probante » répond aux attendus des articles L.1111-25 à 31 du code de la santé publique concernant les documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique. Il comprend notamment :

- un document introductif qui présente la problématique, le périmètre et les enjeux **[document de référence n°1]** ;
- 3 annexes qui décrivent les exigences à appliquer dans les principaux cas d'usage
  - Cas de la dématérialisation (ou numérisation) de documents (présent document) ;
  - Cas de la production de documents nativement au format numérique ;
  - Cas de la matérialisation (ou impression) de documents ;
- 2 annexes présentant les principes fondamentaux à appliquer quel que soit le cas d'usage rencontré
  - Socle de principes communs à mettre en œuvre **[document de référence n°2]** ;
  - Explications relatives à la gestion des métadonnées **[document de référence n°8]** ;
- Une annexe qui propose une classification des documents de santé et fait correspondre à chaque classe de document de santé identifiée le niveau requis d'exigences de sécurité à appliquer **[document de référence n°9]**.

L'objet de cette annexe du référentiel est de définir des ensembles cohérents de règles de sécurité à appliquer lors de la création de documents nativement numériques, selon différents paliers clairement identifiés. Le niveau d'exigence des règles est adapté aux enjeux pour chacun des paliers définis.

Ce document s'adresse aux personnes impliquées dans la définition d'un processus de création de documents numériques. Il permet aux responsables de traitement d'identifier les mécanismes de sécurité exigés en fonction du palier requis.

1.2. Champ d'application

Le champ d'application de ce référentiel est précisé dans le document introductif du présent référentiel **[document de référence n°1]**.

De façon générale, ce référentiel s'applique aux documents comportant des données de santé à caractère personnel dans le domaine de la santé, du suivi social et du médico-social.

1.3. Enjeux et problématiques

Les enjeux et les problématiques de la production de documents nativement numériques et comportant des données de santé à caractère personnel sont rappelés dans le document introductif du présent référentiel **[document de référence n°1]**.

2. MECANISMES PROPRES AUX DOCUMENTS NATIVEMENT NUMERIQUES

2.1. Principes généraux relatifs aux documents nativement numériques

Le règlement eIDAS **[document de référence n°4]** indique dans son article 46 que « l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique ».

Ce principe est décliné dans le même texte pour la signature à l'article 26 : « L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée ». L'article 35 du règlement eIDAS applique le même principe pour le cachet.

2.2. La signature électronique

2.2.1. Finalité de la signature pour le domaine de la santé

Dans le domaine de la santé, la signature de documents comportant des données de santé peut être exigée de la part :

- du professionnel de santé (exemple : ordonnance délivrée dans le cadre de l'article R.5132-4 du code de la santé publique) ;
- du patient (exemple : Décharge pour sortie en cas de refus de soins dans le cadre de l'article R.1112-43 du code de la santé publique) ;
- des deux en même temps (exemple : Information concernant l'affection grave d'un enfant à naître et la prise en compte d'un délai de réflexion par la mère dans le cadre de l'article R.2131-18 du code de la santé publique).

Le code de la santé publique définit dans les termes suivants la signature :

Article L.1111-28 du code de la santé publique

La signature apposée sur un document mentionné à l'article L. 1111-25 signifie, selon le cas, que :

1° La personne prise en charge a pris acte du contenu du document et, le cas échéant, y consent ;

2° Le professionnel mentionné à l'article L. 1111-25 valide le contenu du document.

Lorsque le document sur lequel la signature est apposée est créé sur un support numérique, le procédé de signature respecte les conditions du second alinéa de l'article 1367 du code civil.

Lorsque le document comportant des données de santé établi par le professionnel de santé trace la réalisation de l'acte technique, intellectuel, qu'il a réalisé sur le patient, une signature est en général exigée. Que la signature soit manuscrite ou électronique, cette exigence juridique reflète l'importance du contenu du document pour la continuité des soins et dans une perspective de mise en cause de sa responsabilité. C'est pourquoi elle est définie comme la validation par le professionnel de santé du contenu du document.

S'agissant du patient, les cas dans lesquels il est tenu de signer un document relèvent de deux finalités :

- Il doit prendre acte qu'il doit assumer la situation décrite dans le document (exemple : signature d'un formulaire de sortie contre avis médical) ;
- Il doit attester qu'il a consenti à l'acte qu'il va subir dans le cadre de sa prise en charge.

2.2.2. Information du signataire

Le code de la santé publique fixe également dans l'article L.1111-28 les conditions juridiques et techniques à respecter pour recourir à des procédés électroniques permettant de répondre à l'exigence de validation d'un document de santé dans les cas exposés au paragraphe précédent :

Article L.1111-28 du code de la santé publique

Lorsque le document sur lequel la signature *[au sens juridique]* est apposée est créé sur un support numérique, le procédé de signature respecte les conditions du second alinéa de l'article 1367 du code civil.

Il en résulte que la nature de l'opération de signature électronique doit être portée à la connaissance du signataire avant sa décision de signer. Ceci se fait par la présentation au signataire des conditions générales d'utilisation de l'application ou du service de signature, et l'obtention explicite (à tracer) de son accord. Afin d'alléger le processus, cet accord ne sera demandé à l'occasion d'une prochaine signature que si les conditions générales d'utilisation ont été modifiées depuis le dernier accord donné.

2.2.3. Règlement eIDAS

Le règlement eIDAS clarifie les règles existantes et introduit un cadre juridique pour les cachets électroniques et signatures électroniques. Il prévoit d'accorder une meilleure garantie juridique au travers d'un système de présomption de preuve à ceux qui suivent les règles relatives aux dispositifs dits qualifiés dans le but d'améliorer la fiabilité de leurs services. Mais il ne contraint ni les prestataires de services ni leurs clients à recourir à ce type de dispositifs.

Le règlement eIDAS définit ainsi trois niveaux de sécurité pour la signature électronique :

- La signature électronique dite « simple » ;
- La signature électronique avancée ;
- La signature électronique qualifiée.

La signature électronique simple (SE) est constituée par un ensemble de données (sans format imposé) jointes ou associées aux données signées. En pratique, une structure de données comprenant les nom et prénom du signataire, l'identifiant unique du document signé et éventuellement une date, peut être considérée comme une signature simple. Cette simplicité n'apporte cependant que peu de garanties juridiques puisque la signature peut potentiellement être aisément falsifiée.

La signature électronique avancée (SEA) doit permettre d'identifier de façon sûre le signataire du document et de prouver l'intégrité des données signées. La preuve d'intégrité est apportée par le calcul d'une empreinte numérique des données signées puis la signature par le certificat du signataire de cette empreinte. Il est alors possible de détecter toute modification du document signé et d'identifier le signataire par le certificat. Le niveau de sécurité de la signature avancée est plus fort que la signature simple. Cependant, les garanties apportées dépendent beaucoup des méthodes de délivrance du certificat (processus sécurisé notamment) et du contexte de conservation du document (garantie d'intégrité identique pour chacune des parties concernées).

La signature électronique qualifiée (SEQ) est la seule à disposer de l'équivalence juridique avec la signature manuscrite. Les conditions d'obtention d'une signature électronique qualifiée sont logiquement très strictes : ce doit être une signature avancée réalisée avec des moyens (certificats et support de clé cryptographique) sécurisés et eux-mêmes qualifiés par l'ANSSI. En pratique, la signature électronique qualifiée n'est utilisée que dans un nombre restreint de domaines.

2.2.4. Valeur juridique des signatures électroniques non qualifiées

Les signatures qui ne remplissent pas les critères de la signature électronique qualifiée au sens du règlement eIDAS (SE ou SEA décrites au paragraphe précédent) ne se voient pas dénier toute valeur juridique mais elles ne bénéficient pas *a priori* de l'équivalence avec la signature manuscrite. En cas de litige, il sera nécessaire que celui qui s'en prévaut apporte la preuve que la signature non qualifiée permet effectivement d'assurer les fonctions revendiquées en l'occurrence (identifier le signataire, garantir l'intégrité de l'acte, etc.).

Toutefois, la validité d'une signature non qualifiée peut toujours être reconnue pour une utilisation spécifique, dans le cadre d'une convention de preuve. En effet, le règlement eIDAS dans son article 2-2 prévoit une dérogation pour « *les services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants* ». Ce qu'il faut entendre par « système fermé » n'est pas expressément défini par le règlement, mais il est précisé qu'il s'agit par exemple des « *systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance* […]. *Seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement* ».

En cas de contentieux, il appartiendra au juge d'arbitrer les conflits de preuve à défaut de convention valable entre les parties. Autrement dit, le juge appliquera la convention de preuve conclue entre les parties, en l'absence de clause pouvant être considérée comme abusive.

Pour plus d'informations sur la convention de preuve, se référer au document introductif de ce référentiel ***[document de référence n°1]****.*

2.3. Le cachet électronique, ou scellement

Techniquement très proche de la signature électronique, le cachet (ou scellement) a cependant une autre définition juridique, et pour seul objectif de garantir l'origine et l'intégrité de données. Ses effets juridiques sont donc sensiblement différents de ceux de la signature électronique. Toutefois, dans certains cas, une signature électronique « simple » peut être réalisée in fine par l'apposition d'un cachet électronique sur un document. Dans ce cas précis, c'est le processus de signature, l'authentification du signataire et son consentement explicite qui donne valeur de signature électronique à un document sur lequel est apposé techniquement un cachet.

La nature de l'opération de cachet électronique doit être portée à la connaissance de la personne qui déclenche le cachet, a fortiori lorsque le document concerné l'implique personnellement. Ceci se fait par la présentation au signataire des conditions générales d'utilisation de l'application ou du service de signature, et l'obtention explicite (à tracer) de son accord.

Un cachet électronique pourrait, selon le règlement eIDAS, être apposé par une personne physique ou une personne morale. Cependant, dans le cadre de ce référentiel, seuls les cachets électroniques réalisés au nom d'une personne morale (un organisme) sont envisagés. Le déclenchement de la création d'un cachet d'une organisation peut être interprété comme étant la validation du document par un représentant dûment autorisé au sein de cette organisation.

Comme pour la signature électronique, le règlement eIDAS définit trois niveaux de sécurité :

- Le cachet électronique dit « simple » ;
- Le cachet électronique avancé ;
- Le cachet électronique qualifié.

La définition de ces différents niveaux est équivalente à ceux de la signature, en remplaçant les termes « signature » par « cachet » et « signataire » par « créateur du cachet ». Un cachet électronique qualifié n'a pas d'équivalent manuscrit, il bénéficie simplement d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

2.4. L'horodatage

Au moment de la création d'une signature ou d'un cachet électronique, l'heure de la machine qui effectue l'opération est insérée dans la signature. L'exactitude de cette heure n'est pas toujours sûre, par exemple pour le cas de postes de travail utilisateur.

Afin d'ajouter une information fiable sur la date de création de la signature ou du cachet, une opération d'horodatage peut être déclenchée immédiatement après. Elle provoque l'ajout dans la signature de données nommées « jeton d'horodatage » qui apportent des garanties supplémentaires :

- Garantie d'antériorité : la datation des données électroniques permet de démontrer qu'elles existaient à partir de la date et heure certifiées ;
- Garantie d'exactitude : la date et l'heure attestées par le système émettant le jeton sont établies à partir de plusieurs sources de temps fiables, protégées contre des dérives temporelles ;
- Garantie d'intégrité des données : le jeton d'horodatage comprend l'empreinte des données horodatées, ce qui permet de prouver ensuite leur intégrité.

La confiance accordée à un jeton d'horodatage dépend des mesures de sécurité mises en place sur le service d'horodatage (contrôle des horloges, sécurité de l'infrastructure et de la clé de signature des jetons). Le règlement eIDAS permet au fournisseur d'un service d'horodatage de le faire qualifier lorsqu'il satisfait à un haut niveau de sécurité. Sur un plan juridique, un jeton d'horodatage émis par un service qualifié est présumé fiable.

L'horodatage électronique est un service bien distinct de celui de la signature (et du cachet), qui peut être déployé sur la même infrastructure que le service de signature ou chez un prestataire tiers. Il n'est pas forcément nécessaire d'envoyer un document dans sa totalité au service d'horodatage, la transmission d'une empreinte cryptographique (calculée dans le respect des standards PAdES et XAdES) peut suffire. Ceci permet de préserver la confidentialité des données (lorsque l'horodatage est réalisé par un tiers) et de limiter fortement le volume de données échangées. En particulier, le prestataire du service d'horodatage n'a pas à être certifié comme Hébergeur de Données de Santé.

2.5. Le dossier de preuve

Lorsqu'une signature électronique ou un cachet électronique est créé, il est nécessaire de conserver un ensemble de traces que l'on nomme « dossier de preuve ». L'objectif de ce dossier est principalement de pouvoir amener des éléments constituant un faisceau de preuves des opérations réalisées en cas de contentieux. Le dossier de preuve apporte des éléments factuels soutenant la non-répudiation de la signature : le signataire ne peut pas nier avoir signé un document donné à une date donnée, à moins d'apporter de nouveaux éléments contradictoires et probants.

En pratique, le dossier de preuve contient des traces logicielles et des documents (numériques ou papier) retraçant le processus de signature dans son ensemble :

- Traces de connexion du signataire à l'application ou au service de signature, et de l'éventuelle authentification réalisée à cette occasion ;
- Identification de la version des conditions générales d'utilisation en vigueur ;
- Actions du signataire, le plus souvent sous forme de cases à cocher ou boutons activés, en particulier pour consulter et accepter les conditions générales d'utilisation et déclencher la signature électronique ;
- Traces du processus d'authentification du signataire : Envoi au destinataire de mots de passe à usage unique (solution type OTP : « One Time Password ») par SMS par exemple, utilisation d'un moyen d'identification électronique, etc. ;
- Informations saisies ou documents fournis par le signataire, par exemple les documents fournis par le signataire pour prouver son identité.

Un dossier de preuve doit être constitué pour chaque signature électronique ou cachet électronique (ou chaque lot de signatures ou de cachets), quel que soit son niveau. Ces informations doivent être archivées aussi longtemps que le document signé conserve une valeur juridique, et tant que le document signé est archivé si tel est le cas. Cet

archivage doit garantir la disponibilité pendant la période de conservation, ainsi que l'intégrité et la confidentialité des données.

2.6. La conservation

La force probante d'un document électronique repose d'une part sur l'identification de la personne dont il émane (le signataire), et d'autre part sur la garantie d'intégrité du document sur toute sa durée de conservation. La conservation du document constitue donc une étape à considérer avec attention dans la production de tous les documents numériques.

Les mesures de sécurité dans la conservation d'un document doivent viser à garantir :

- La disponibilité : le système de conservation doit avant tout permettre de retrouver le document sur toute la durée prévue initialement ;
- L'intégrité des données : le document ne doit pas être modifié ou altéré durant sa conservation, et la force probante dépend entre autres du niveau de garantie d'intégrité du document dans le temps ;
- La confidentialité : La conservation du document ne doit pas remettre en question le niveau de confidentialité du document, et ce même sur une longue période de temps (qui peut impliquer des processus de copie, de transfert, etc.).

D'une façon générale, les mesures de sécurité mises en place pour la signature et la conservation d'un document sont d'autant plus exigeantes que le document est sensible. Dans cet esprit, et pour proposer des paliers cohérents, les exigences associées à la conservation sont croissantes avec les paliers successifs. Néanmoins, une étude menée sur un document spécifique pourrait conclure que le niveau de signature n'est pas forcément critique (car il peut exister d'autres preuves de l'origine du document, comme des pistes d'audit) alors que sa conservation doit être très sécurisée. Ainsi, les exigences associées à la conservation pour un palier donné sont des exigences minimales, qui peuvent être dépassés au cas par cas lorsqu'il existe une justification appropriée.

2.7. Choix du niveau de sécurité adapté

La sélection des signatures électroniques et des cachets à apposer sur un document, ainsi que des conditions et pratiques de mise en œuvre doit faire l'objet d'une étude approfondie. Comme indiqué dans le document introductif du présent référentiel **[document de référence n°1]**, il appartient aux responsables des systèmes d'information concernés par les procédés de production de document nativement au format numérique de :

- Identifier le palier minimum de mesures de sécurité à mettre en œuvre en fonction du type de document à l'aide de l'annexe 6 de ce référentiel « Classification des documents de santé » **[document de référence n°9]** ;
- Analyser le cadre légal associé aux documents métiers produits, les enjeux et les risques induits par les documents produits nativement au format numérique pour déterminer si des mesures complémentaires doivent être mises en œuvre ;
- Respecter les principes et règles de sécurité associés au palier identifié qui sont fixés au sein du présent document et les compléter de mesures additionnelles si ce besoin a été identifié.

Outre les mesures de sécurité correspondant au palier choisi et celles plus spécifiques au contexte décrites ci-dessus, il est indispensable de veiller au respect des recommandations plus générales citées dans l'annexe 1 du présent référentiel « Socle commun de principes techniques et organisationnels » **[document de référence nº 2]**.

3. PALIERS DE LA SIGNATURE ELECTRONIQUE

3.1. Signature électronique par un acteur de santé

3.1.1. Palier 1 : Signature électronique simple

Présentation de la signature électronique

Cette signature électronique, simple au sens du règlement eIDAS, consiste à apposer un cartouche graphique sur le document après recueil du consentement du signataire (par l'intermédiaire d'une case à cocher par exemple). Des métadonnées relatives à cette signature sont également ajoutées au document signé.

Lorsque le document ne peut pas être représenté graphiquement et donc recevoir un cartouche graphique de signature, il est nécessaire d'appliquer au minimum le palier 2 pour signer le document. A défaut, la validation du document par l'acteur de santé doit être consignées dans des traces comprenant au minimum le nom et le prénom de la personne et la date de validation.

Processus de signature électronique

L'application de signature affiche le document à signer et demande au signataire de déclencher la signature. L'application propose de vérifier visuellement le document obtenu après ajout du cartouche de signature.

La méthode d'identification n'est pas contrainte dans ce document, mais elle doit permettre d'obtenir au final le nom et prénom du signataire qui doivent apparaître de façon à identifier le signataire.

Description de la signature électronique

Le cartouche graphique contient :

- Le nom et le prénom de la personne signataire ;
- La date de signature ;
- Une image optionnelle (par exemple la représentation de la signature manuscrite du signataire) ;
- Une mention optionnelle, accompagnant la signature (par exemple « Document signé par »).

Le cartouche graphique ne doit cacher aucune information déjà présente sur le document. Son emplacement et sa taille doivent être choisis pour qu'il soit bien visible, dans une zone habituelle pour une signature manuscrite et sans risque de troncature des informations de la signature.

Les métadonnées doivent comprendre obligatoirement :

- Le nom et le prénom du signataire ;
- La date de signature.

Les métadonnées suivantes peuvent être ajoutées de façon optionnelle pour compléter ces informations :

- Des informations sur la personne morale à laquelle le signataire est rattaché.

Format du document signé

La signature peut être réalisée sur des documents de format :

- Document PDF. Les documents au format bureautique standard (suites Microsoft Office, Open office) devront être exportés vers le format PDF (PDF/A de préférence pour la pérennité du document) avant d'être signés. Le

document peut être utilisé seul ou intégré dans un document au format CDA. Les métadonnées sont au moins intégrées dans le document bureautique lui-même.
- Document de santé CDA. Le cartouche est intégré dans le corps du document tandis que les métadonnées de la signature sont ajoutées aux métadonnées du document.
- Tout autre type de document pour lequel il est possible de respecter les exigences de cette signature simple (par exemple une image). Les 2 premiers formats restent toutefois à privilégier dans un souci d'interopérabilité.

Horodatage

L'horodatage électronique du document ainsi signé n'est pas requis pour ce palier. L'horodatage d'un document PDF non signé électroniquement reste possible, et apporte une garantie d'intégrité et d'antériorité des données.

Conservation

La conservation du document vise à ce stade à garantir la disponibilité du document sur toute sa durée de vie (par exemple via une sauvegarde centralisée) et un contrôle d'accès à une version supposée intègre (afin d'éviter une suppression ou une modification non souhaitée).

Les mesures classiques de sécurité, en accord avec les pratiques générales de la politique de sécurité du système d'information et dépendant des informations contenues sur le document, restent à appliquer en tout état de cause.

3.1.2. Palier 2 : Signature électronique simple avec scellement

Présentation de la signature électronique

Cette signature est une signature simple au sens du règlement eIDAS. Elle se décompose en deux étapes :

- Réalisation d'une signature simple par le signataire, conforme aux exigences présentées au §3.1.1 (sauf en cas d'impossibilité de création du cartouche graphique) ;
- Scellement de cette signature par un certificat de personne morale.

Ce scellement garantit l'intégrité du document : toute modification des données du document casse le scellement effectué et est donc détectée par une application de vérification de signature. Par ailleurs, seule la réalisation du processus complet de signature permet d'activer le certificat de scellement, ce qui empêche un tiers de sceller un faux document.

Processus de signature électronique

Le processus de signature débute par la mise en œuvre de la signature simple.

Une fois la signature simple terminée, l'application déclenche immédiatement le scellement du document signé. L'affichage au signataire du document signé et scellé n'est pas requis puisqu'il n'y a pas de modification visuelle de celui-ci.

Description de la signature électronique

Le cartouche graphique apposé sur le document est conforme à celui de la signature simple. La mention accompagnant la signature peut toutefois avoir été rédigée de façon à indiquer que le document est scellé (la mention ne peut pas être modifiée après la signature par le signataire).

Les métadonnées du document signé sont à compléter par celles relatives au scellement :

- Le nom de l'organisation ;

- La date de scellement.

D'autres métadonnées peuvent être ajoutées de façon optionnelle pour compléter ces informations. Il faut dans ce cas veiller au respect des exigences de l'annexe 5 de ce référentiel **[document de référence n°8]** et au respect du cadre d'interopérabilité pour les systèmes d'information de santé.

Certificat de scellement

Le certificat de scellement est un certificat de cachet serveur correspondant à l'une des offres suivantes de l'IGC Santé :

- Offre « Certificat de personne morale Serveur » pour un usage de cachet ;
- Offre « Certificat de personne morale Organisation » pour un usage de cachet.

Format du document signé

Le format de signature dépend du type de document :

- Document PDF : La signature doit respecter le format PAdES pour le niveau Baseline B ;
- Document de santé CDA : La signature doit respecter le format de signature décrit dans le cadre d'interopérabilité ;
- Par dérogation, lorsque les données ne peuvent pas être formatées dans un document de type PDF ou CDA, la signature peut être réalisée au format XAdES, sur un document XML encapsulant les données à signer converties au format Base64 et intégrant les métadonnées de signature.

Horodatage

L'horodatage de la signature n'est pas obligatoire mais peut apporter des garanties supplémentaires sur la date de signature et donc l'antériorité des données. S'il est réalisé, la signature doit respecter le niveau Baseline T, ou Baseline-LT lorsque la durée de conservation est importante.

Conservation

La conservation du document signé, et du dossier de preuve associé, repose sur un espace de stockage centralisé et sécurisé, assurant :

- Disponibilité : les données bénéficient au minimum de sauvegardes sur des espaces distincts ou des supports matériels pour pallier les défaillances matérielles ou les incidents logiciels.
- Contrôles d'accès : L'accès aux données conservées est contrôlé, et interdit une modification ou une suppression des données aux personnes non autorisées.
- Intégrité : La preuve d'intégrité des données signées est apportée par le cachet apposé sur celles-ci. Le contrôle d'accès et les sauvegardes complètent les mesures de protection de l'intégrité des données.

L'espace de conservation n'est pas forcément un espace d'archivage, mais peut être une GED par exemple. Il faut cependant s'assurer que les données conservées ne puissent pas être modifiées ou supprimées, volontairement ou accidentellement, sauf à l'issue de la période de conservation prévue.

Dans le cas où la conservation des données est réalisée par un prestataire externe, une attention particulière doit être portée sur la contractualisation des mesures et de la veille de sécurité. Le prestataire doit disposer de la certification pour l'hébergement de données de santé (HDS). L'agrément du Ministère de la Culture est une obligation pour tout SAE destiné à conserver des archives publiques (cet agrément dispense dans ce cas de la certification HDS).

3.1.3. Palier 3 : Signature électronique avancée par certificat CPx[1]

Présentation de la signature électronique

Cette signature est une signature avancée au sens du règlement eIDAS. Elle est réalisée par l'acteur de santé (ou tout titulaire d'une carte de la famille CPx) soit en utilisant sa carte CPx (ou la version dématérialisée dite « e-CPS » de celle-ci), soit en utilisant un service de signature centralisé capable d'enrôler des certificats de signature délivrés par l'IGC Santé à des titulaires de cartes CPx. Des métadonnées relatives à cette signature sont également ajoutées au document signé.

Processus de signature électronique

L'application affiche le document à signer et demande au titulaire de la carte CPx de déclencher la signature. L'application de signature est garante de la représentation fidèle du document, elle doit interdire la signature d'un document qui ne serait pas complètement visualisable.

Le signataire doit pour chaque document ou lot de documents à signer, soit :

- saisir le code PIN personnel de sa carte CPx pour autoriser l'utilisation de son certificat,
- saisir son secret personnel pour activer l'utilisation de son certificat enrôlé dans le service centralisé de signature.

L'application vérifie la validité du certificat de signature avant de construire les données de signature.

L'application propose de vérifier le document signé obtenu, un cartouche graphique pouvant être ajouté sur le document par la signature.

Description de la signature électronique

La signature électronique doit suivre une politique de signature établie. Sur le plan cryptographique, les algorithmes utilisés doivent être compatibles avec les recommandations du RGS **[document de référence n°3]**.

Lorsqu'un cartouche graphique est apposé sur le document, celui-ci doit se conformer aux règles indiquées pour la signature simple.

Les métadonnées doivent comprendre obligatoirement :

- Le nom et le prénom du signataire ;
- La date de signature.

Les métadonnées suivantes peuvent être ajoutées de façon optionnelle pour compléter ces informations :

- Des informations sur la personne morale à laquelle le signataire est rattaché.

D'autres métadonnées peuvent être ajoutées de façon optionnelle pour compléter ces informations. Il faut dans ce cas veiller au respect des exigences de l'annexe 5 de ce référentiel **[document de référence n°8]** et au respect du cadre d'interopérabilité pour les systèmes d'information de santé.

Certificat de signature électronique

Le certificat utilisé est le certificat de signature présent sur la carte CPx du signataire ou le certificat de signature dérivé de l'identité numérique du titulaire de la carte CPx et fourni par l'IGC Santé au service centralisé de signature.

[1] Par CPx, il est fait référence ici et dans la suite du document à l'ensemble des cartes de la « famille CPS » : les cartes CPS (professionnel de santé) mais aussi CPE (personnel d'établissement), CPA (personnel autorisé) et CPF (personnel en formation) peuvent donc être utilisées pour réaliser une signature électronique avancée.

Format du document signé

Les formats de signature électronique avancée sont définis par le règlement eIDAS dans une décision d'exécution **[document de référence n°5]**. Ils doivent correspondre à des niveaux (Baseline) identifiés dans les formats PAdES, XAdES définis par l'ETSI.

Le format de signature est :

- Document PDF : La signature doit respecter le format PAdES pour le niveau Baseline B.
- Document de santé CDA : La signature doit respecter le format de signature décrit dans le cadre d'interopérabilité, de type XAdES ;
- Par dérogation, lorsque les données ne peuvent pas être formatées dans un document de type PDF ou CDA, la signature peut être réalisée au format XAdES, sur un document XML encapsulant les données à signer converties au format Base64 et intégrant les métadonnées de signature.

Horodatage

L'horodatage de la signature n'est pas obligatoire mais peut apporter des garanties supplémentaires sur la date de signature et donc l'antériorité des données. Il est ainsi conseillé en particulier lorsque la signature est réalisée avec une carte CPx sur un poste dont l'heure n'est pas forcément fiable. Si l'horodatage est réalisé, la signature doit respecter le niveau Baseline T, ou Baseline-LT lorsque la durée de conservation est de plusieurs années.

Pour ce palier de signature, qui apporte une garantie forte sur l'identité du signataire, il peut être utile de recourir à un service d'horodatage qualifié. Ce dernier apporte en effet une présomption de fiabilité de l'heure de signature, élément qui peut être important pour certaines catégories de documents.

Conservation

La conservation du document signé et du dossier de preuve associé est réalisé par un archivage de ces données, afin de garantir avec un haut niveau de sécurité leur intégrité dans le temps.

Les mesures de sécurité applicables pour la conservation de ces données sont les suivantes :

- Disponibilité : Pour éviter la perte accidentelle de données, la redondance du stockage des fichiers doit être assurée. Les modalités pratiques de cette redondance doivent prendre en compte la durée de conservation et les risques attachés aux documents (envisager la duplication hors site par exemple).
- Contrôles d'accès : L'accès aux données conservées doit être strictement restreint à un ensemble minimal d'acteurs. Une archive[2] n'est pas un document vivant, elle n'est consultée que de façon exceptionnelle pour retrouver un document détruit par ailleurs ou à titre de preuve. La modification d'une archive est interdite, sauf pour une opération de conversion nécessaire pour prolonger sa lisibilité dans le temps (voir ci-dessous le maintien de l'intégrité). La suppression d'une archive n'est possible qu'au terme de la durée de conservation fixée pour le document (par exemple une durée légale) et, dans le cas d'archives publiques, sous réserve de l'obtention du visa de l'administration des archives (cf. socle commun **[document de référence n°2]**).
- Confidentialité : Outre le contrôle d'accès, la confidentialité peut être renforcée par le chiffrement des données conservées avant leur écriture sur les supports de stockage. L'opportunité d'ajout de cette mesure doit être étudiée par l'analyse de risques, cela peut répondre par exemple à un risque lié à l'externalisation de cette conservation.
- Traçabilité : Toutes les opérations concernant les données conservées doivent être tracées. Les traces générées pour la création, la protection d'intégrité et la conservation des données conservées doivent être conservées aussi longtemps et dans les mêmes conditions que les documents concernés (cf. **[document de référence n°2]**).

[2] Le terme « archive » est employé dans ce paragraphe au sens d' « archive intermédiaire » décrit dans le code du patrimoine (voir article R212-11)

- Intégrité : L'intégrité des données conservées est garantie par une empreinte cryptographique calculée lors de la création de la signature ou au dépôt des données dans l'espace de conservation. Cette empreinte ne peut évoluer que dans trois situations :
  - Les données doivent être converties vers un nouveau format afin d'assurer leur lisibilité dans le temps ;
  - L'empreinte a été calculée ou protégée avec un algorithme devenu obsolète (ou simplement déprécié) et une nouvelle empreinte doit être calculée sur les données conservées ;
  - Les moyens cryptographiques (certificat électronique notamment) nécessaires à la vérification de la protection éventuelle de l'empreinte vont bientôt arriver à expiration.

  Cette évolution est autorisée, sans perte de valeur probante, dans la mesure où les conditions suivantes sont réunies :
  - L'intégrité des données conservées est vérifiée avec succès avant le calcul de la nouvelle empreinte ;
  - La nouvelle empreinte est calculée et protégée dans des conditions au moins équivalentes au calcul de la première empreinte ;
  - Cette opération est correctement tracée et l'intégrité des traces ne peut être remise en cause

  La preuve d'intégrité peut reposer par exemple sur un mécanisme de signature électronique ou de chainage d'empreinte, au choix du concepteur. Dans tous les cas, les mécanismes cryptographiques utilisés doivent satisfaire les exigences indiquées dans le socle commun du référentiel **[document de référence nº 2]**.
- Veille et maintien en condition de sécurité : Dans la mesure où le document signé doit être conservé sur une longue période de temps, les mesures de sécurité adoptées doivent régulièrement être auditées et remises à l'état de l'art si des faiblesses significatives sont relevées. Cela comprend les algorithmes cryptographiques liés à l'empreinte et au cachet ou à la signature électronique des documents (voir paragraphe « mécanismes cryptographiques » du socle commun **[document de référence nº 2]**), mais aussi les autres mesures participant à leur disponibilité et à leur confidentialité.

  La mise en œuvre de ces mesures peut être réalisée par l'emploi d'un Système d'Archivage Electronique (SAE) conforme à la norme NF Z 42-013 dans sa dernière version. Cette solution n'est cependant pas obligatoire, des espaces sécurisés d'archivage (intégrant l'ensemble des fonctions décrites ci-dessus mais pas nécessairement certifiés conformes à la norme) peuvent être mis en place au sein du SI de l'organisation.

  Dans le cas où la conservation des données est réalisée par un prestataire externe, une attention particulière doit être portée sur la contractualisation des mesures et de la veille de sécurité. En plus de la mise en œuvre des mesures propres à l'hébergement chez un prestataire externe décrites dans le document socle commun **[document de référence nº 2]**, la certification de conformité du prestataire à la norme NF Z 42-013 dans sa dernière version est une précaution conseillée.

3.1.4. Signature électronique qualifiée

Dans le règlement eIDAS, la signature qualifiée est une signature avancée réalisée avec un certificat de signature électronique qualifié en utilisant un dispositif local (carte à puce par exemple) ou centralisé (matériel cryptographique) de signature qualifié.

Les certificats de la carte CPx ne sont pas à ce jour qualifiés et les contraintes organisationnelles en particulier ne permettent pas d'envisager cette qualification à court ou moyen terme.

La signature qualifiée à distance est toutefois atteignable à condition de disposer :

- d'un moyen d'authentification à deux facteurs, remis en face à face au signataire et sécurisé (une application sécurisée d'authentification sur téléphone mobile, initialisée après un face à face, est susceptible de satisfaire à cette exigence) ;
- d'une application sécurisée de signature électronique embarquée dans un matériel cryptographique qualifié.

La solution doit être évaluée par l'ANSSI afin d'obtenir le statut de dispositif qualifié de signature électronique à distance. Bien qu'une telle solution n'existe pas encore sur le marché à l'heure de la publication de ce référentiel, elle est envisageable à moyen terme au moins.

La mise en œuvre de cette signature qualifiée à distance pourrait se faire dans des conditions similaires à celle de la signature électronique avancée par certificat dérivé de l'identité numérique du titulaire de la carte CPx. Le certificat délivré serait qualifié (sur la base de l'authentification à deux facteurs) et la signature obtiendrait le statut qualifié grâce au dispositif de signature à distance qualifié.

3.2. Signature par une personne prise en charge

Comme il est précisé dans le document introductif de ce référentiel **[document de référence n°1]**, les documents émis directement par des personnes prises en charge sont exclus du périmètre de ce référentiel. Ce paragraphe traite uniquement le cas des documents émis par des structures de santé dans le cadre de la prise en charge d'une personne et requérant la signature de celle-ci. Pour rappel, cette signature signifie que la personne prise en charge a pris acte du contenu du document et, le cas échéant, y consent (cf. §2.2.1).

3.2.1. Palier 1 : Signature électronique simple

La personne prise en charge peut signer un document par une signature simple, dans des conditions strictement identiques à celles exposées pour l'acteur de santé au §3.1.1.

3.2.2. Palier 2 : Signature électronique simple avec scellement par l'acteur de santé

La personne prise en charge peut signer un document par une signature simple avec scellement, dans des conditions strictement identiques à celles exposées pour l'acteur de santé au §3.1.2. Le scellement par certificat de personne morale est déclenché par l'acteur de santé.

La nature juridique de cette signature (signature électronique personnelle dite « simple ») doit être explicitement indiquée dans les conditions générales d'utilisation de l'application ou du service de signature. La présence du scellement n'impacte pas cette portée juridique, et ne modifie pas la signification de la signature comme rappelé au §2.1.

3.2.3. Palier 3 : Signature électronique avancée

Présentation de la signature

Cette signature est une signature électronique avancée au sens du règlement eIDAS. Elle est réalisée par la personne prise en charge préalablement identifiée par un acteur de santé et après authentification de la personne prise en charge. Des métadonnées relatives à cette signature sont également ajoutées au document signé.

Processus de signature

Un acteur de santé, en présence d'une personne prise en charge, lui demande :

- Son nom et prénom ;
- Son numéro de téléphone portable ;
- Sa pièce d'identité (optionnelle).

Selon le moyen d'authentification de la personne prise en charge, d'autres informations pourraient être nécessaires et leur obtention est sous la responsabilité de l'acteur de santé.

Si une pièce d'identité est fournie, l'acteur de santé la vérifie et en effectue une copie, au format papier ou électronique. La copie de la pièce d'identité doit être conservée à titre de preuve, de façon centralisée et dans le respect des exigences du RGPD (cf. annexe 1 du présent référentiel « Socle commun de principes techniques et organisationnels » **[document de référence n° 2]**).

L'acteur de santé saisit le nom, prénom et numéro de téléphone portable de la personne prise en charge dans l'application de signature. L'application affiche le document à signer. Elle est garante de la bonne représentation du document, et doit interdire la signature d'un document qui ne serait pas complètement visualisable.

Ce référentiel propose initialement l'OTP SMS (ou One Time Password, c'est-à-dire mot de passe à usage unique transmis par minimessage) comme mode d'authentification de la personne prise en charge. L'application envoie un code OTP par SMS à la personne prise en charge. Celui-ci saisit ce code dans l'application de signature et déclenche ainsi la signature électronique.

A terme, tout moyen d'identification électronique de niveau de garantie substantiel ou élevé au sens eIDAS pourra être utilisé, en particulier si la fiabilité de l'OTP SMS est remise en cause. Le catalogue croissant des offres disponibles et l'adoption progressive par les particuliers de ces identités en feront des solutions privilégiées pour l'authentification des personnes prises en charge.

Après authentification de la personne prise en charge, l'application propose de vérifier le document signé obtenu, un cartouche graphique pouvant être ajouté sur le document par la signature.

Description de la signature

Les exigences pour la description de la signature avancée de la personne prise en charge sont identiques à celles spécifiées pour l'acteur de santé au §3.1.3.

Certificat de signature

Le certificat utilisé pour la signature est un certificat éphémère (valide quelques minutes) émis au nom de la personne prise en charge par une Autorité de Certification selon une politique de certification de niveau LCP (vérification de titre d'identité sans face à face) selon le règlement eIDAS **[document de référence n°7]**.

Format du document signé

Les exigences concernant le format du document signé par la personne prise en charge avec une signature avancée sont identiques à celles spécifiées pour l'acteur de santé au §3.1.3.

Horodatage

Les exigences d'horodatage de la signature avancée de la personne prise en charge sont identiques à celles spécifiées pour l'acteur de santé au §3.1.3.

Conservation

Les exigences de conservation de la signature avancée de la personne prise en charge sont identiques à celles spécifiées pour l'acteur de santé au §3.1.3.

4. SYNTHESE DES MECANISMES DE PROTECTION PAR PALIER

Les différents mécanismes de protection pour chaque palier sont présentés de façon synthétique dans les tableaux suivants.

4.1. Signature par un acteur de santé

	Palier 1 : Signature simple	Palier 2 : Signature simple avec scellement	Palier 3 : Signature avancée avec certificat CPx
Description	▶ Cartouche graphique ▶ Métadonnées	▶ Cartouche graphique + cachet cryptographique ▶ Métadonnées	▶ Cartouche optionnel + signature cryptographique ▶ Métadonnées
Processus	▶ Identification non contrainte ▶ Affichage du document et ajout du cartouche ▶ Constitution et conservation du dossier de preuve	▶ Identification non contrainte ou application du référentiel d'authentification de la PGSSI-S ▶ Affichage du document ▶ Ajout d'un sceau après le cartouche ▶ Constitution et conservation du dossier de preuve	▶ Authentification par carte CPx, e-CPS ou authentification multifacteur ▶ Affichage du document et signature (PIN code de la carte ou secret personnel pour autoriser l'utilisation du certificat) ▶ Constitution et conservation du dossier de preuve
Certificat	Aucun	▶ Certificat de cachet « Serveur » ou « Organisation »	▶ Certificat de signature de la carte CPx ▶ Certificat de signature enrôlé par le service centralisé et délivré par l'IGC de l'ANS
Format du document	▶ PDF, CDA	▶ PAdES ou CDA signé (XAdES)	▶ PAdES ou CDA signé (XAdES)
Horodatage	Aucun	Optionnel	Conseillé, potentiellement qualifié
Conservation	▶ Sauvegarde ▶ Application de PGSSI-S	▶ Sauvegarde ou redondance centralisée ▶ Contrôle d'accès	▶ Archivage sécurisé mais non nécessairement certifié conforme à la norme NF Z 42 -013

4.2. Signature par une personne prise en charge

	Palier 1 : Signature simple	Palier 2 : Signature simple avec scellement	Palier 3 : Signature avancée
Description	▶ Cartouche graphique ▶ Métadonnées	▶ Cartouche graphique + scellement cryptographique ▶ Métadonnées	▶ Cartouche optionnel + signature cryptographique ▶ Métadonnées
Processus	▶ Identification non contrainte ▶ Affichage du document et ajout du cartouche ▶ Constitution et conservation du dossier de preuve	▶ Identification non contrainte ou application du référentiel d'authentification de la PGSSI-S ▶ Affichage du document ▶ Ajout d'un sceau après le cartouche ▶ Constitution et conservation du dossier de preuve	▶ Identification par acteur de santé ▶ Authentification par OTP SMS ou moyen d'identification électronique de niveau substantiel ▶ Affichage du document et signature ▶ Constitution et conservation du dossier de preuve
Certificat	Aucun	▶ Certificat de cachet « Serveur » ou « Organisation »	▶ Certificat de signature éphémère de niveau LCP
Format du document	▶ PDF, CDA	▶ PAdES ou CDA signé (XAdES)	▶ PAdES ou CDA signé (XAdES)
Horodatage	Aucun	Optionnel	Conseillé, potentiellement qualifié
Conservation	▶ Sauvegarde ▶ Application de PGSSI-S	▶ Sauvegarde ou redondance centralisée ▶ Contrôle d'accès	▶ Archivage sécurisé mais non nécessairement certifié conforme à la norme NF Z 42 -013

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante

AGENCE DU NUMÉRIQUE EN SANTÉ

Agence du Numérique en Santé
01 58 45 32 50
9, rue Georges Pitard
75015 PARIS