easy.brussels
SERVICE PUBLIC RÉGIONAL DE BRUXELLES
GEWESTELIJKE OVERHEIDSDIENST BRUSSEL

LA SIGNATURE électronique

Guide de référence

BRUXELLES CONNECTIT
BRUSSEL CONNECTIT
SERVICE PUBLIC RÉGIONAL DE BRUXELLES
GEWESTELIJKE OVERHEIDSDIENST BRUSSEL

TABLE DES MATIÈRES

CONTACTEZ-NOUS

Pour toute question relative au contenu de ce guide, à la simplification administrative ou à la relation usager, contactez **l'agence easy.brussels** :

info@easy.brussels

Pour contacter Bruxelles ConnectIT, l'administration chargée de la stratégie informatique pour les administrations du Service public régional de Bruxelles, et centre de compétence régional SAP :

connectit@sprb.brussels

Pour contacter ConnectMemory, le Service Régional des Archives :

connectmemory@sprb.brussels

Attention, ce guide ne se substitue pas à l'avis et aux directives de votre administration. Renseignez-vous toujours en interne, auprès de votre service juridique par exemple.

Vous trouverez dans ce guide de nombreux termes juridiques ou techniques qui peuvent sembler plus compliqués. Pas de panique ! Nous vous expliquons toutes ces notions dans le lexique en page 37.

COLOPHON

Comité de rédaction :

Cathy Marcus, Directrice d'easy.brussels
Florence Biston • Sarah De Cock • Koen De Pauw • Stéphanie Dheur • Roxana Dragomir • Julie Etienne

Coordination : easy.brussels

Mise en page : Florence Biston - easy.brussels

Traduction : Direction Traduction, Service public régional de Bruxelles

Éditeur responsable : Baptiste Daveau • Directeur général A.I. de Bruxelles ConnectIT, Service public régional de Bruxelles
Iris Tower, Place Saint-Lazare 2, 1035 Bruxelles

ISBN : 2026/14.404/08

PRÉAMBULE

Aujourd'hui, la digitalisation des services administratifs est devenue une nécessité pour améliorer l'efficacité des administrations, renforcer la transparence et simplifier les démarches.

Cette transformation ne se limite toutefois pas à remplacer le papier par des outils numériques. Elle offre l'opportunité de repenser les services publics pour les rendre plus simples, accessibles et mieux adaptés aux besoins des citoyens, des entreprises et des organisations.

En Région de Bruxelles-Capitale, cette évolution est encadrée par la réglementation **Bruxelles Numérique**[1], qui encourage la digitalisation des procédures administratives tout en garantissant l'inclusion de tous les usagers. Chacun doit pouvoir accéder aux services publics en fonction de ses capacités, ses besoins et ses préférences.

> Le numérique doit faciliter les démarches, jamais devenir un obstacle.

Dans ce contexte, les administrations bruxelloises sont amenées à faire évoluer leurs méthodes de travail, leurs processus décisionnels et leurs interactions avec les usagers. Elles digitalisent progressivement leurs procédures et les communications qui en découlent, tout en offrant un support hors ligne pour les usagers en difficulté avec les outils numériques.

Cette transformation implique parfois l'utilisation de **la signature électronique**... ce qui soulève de nombreuses questions : tous les documents doivent-ils être signés ? Quel type de signature électronique utiliser ? Une signature électronique a-t-elle la même valeur légale qu'une signature manuscrite ? Comment garantir la valeur légale tout au long du cycle de vie d'un document ?

Ce guide a pour objectif d'accompagner les administrations publiques bruxelloises dans la compréhension et la mise en œuvre de la signature électronique.

A travers ce guide, nous souhaitons apporter des explications et repères concrets pour évaluer les besoins et faire un choix éclairé dans l'utilisation de la signature électronique et des solutions technologiques adaptées.

La première partie du guide explique les principes et notions liés à la signature électronique. La seconde partie est constituée de fiches pratiques qui visent à répondre rapidement et clairement aux questions fréquemment posées par les administrations. Cette seconde partie est susceptible d'évoluer dans le temps.

Une version digitale de ce guide est disponible sur notre site internet https://easy.brussels.

[1] Décret et ordonnance conjoints du 25 janvier 2024 de la Commission communautaire française, la Région de Bruxelles-Capitale et la Commission communautaire commune relatifs à la transition numérique des autorités publiques, M.B. 21/02/2024.

Rendez-vous sur notre site https://easy.brussels pour consulter le guide complet « Bruxelles numérique ».

DÉFINITION USUELLE DE LA SIGNATURE

> *« Un signe ou une suite de signes tracés à la main, par voie électronique ou par un autre procédé, par lesquels une personne s'identifie et manifeste sa volonté[2]. »* (Code civil belge)

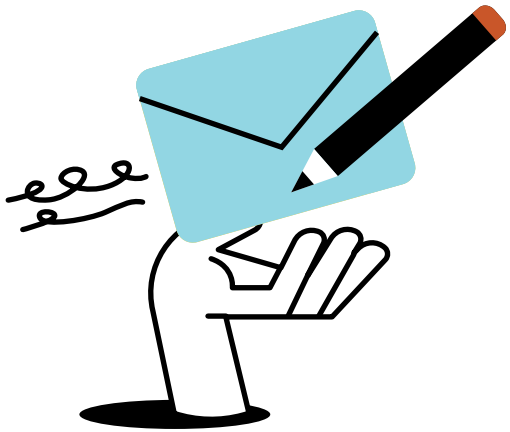
DÉFINITION JURIDIQUE DE LA SIGNATURE

La définition juridique de la signature désigne «*l'inscription qu'une personne appose de son nom sous une forme particulière et constante, dans le but de certifier l'exactitude ou l'authenticité d'un document, et d'engager sa responsabilité*».

Par cet acte volontaire, le signataire **atteste de son identité et reconnaît avoir pris connaissance du contenu** du document **et/ou y avoir donné son consentement**. La signature joue ainsi un rôle indispensable dans les échanges juridiques : elle permet d'établir la **preuve de l'accord**, de **sécuriser** les relations entre les parties, et de donner une **valeur probante** aux documents. Sauf exception prévue par la loi, la signature est exigée sur des actes juridiques. Elle assure **l'intégrité** du document tout en permettant d'identifier le signataire avec certitude. C'est pourquoi elle occupe une place centrale en droit civil et commercial, où elle participe à la validité des actes et à leur force probante.

LE SAVIEZ-VOUS ?

Sur papier, l'intégrité du document est assurée par le support matériel lui-même... Impossible de le modifier sans que cela se voie. Au format numérique, c'est un **système de sécurité, la cryptographie**, qui garantit cette intégrité : il permet de vérifier que le document n'a pas été altéré après sa signature.



2. Code civil belge, Livre 8 « La preuve », article 8.1, 2° (Définitions)
https://www.ejustice.just.fgov.be/eli/loi/2019/04/13/2019A12168/justel

DÉFINITION JURIDIQUE DE LA SIGNATURE ÉLECTRONIQUE

Au sens du règlement (UE) n° 910/2014 (« eIDAS* »), une signature électronique est définie comme étant « *données sous forme électronique, jointes ou associées logiquement à d'autres données sous forme électronique, et utilisées par le signataire pour signer* ».

En d'autres termes, une signature électronique est un ensemble d'informations numériques « attachées » à un document de manière à :

- identifier (ou authentifier) le signataire,
- garantir l'intégrité du document signé, c'est-à-dire permettre de vérifier que ce document n'a pas été modifié après la signature.

RÔLE D'UNE SIGNATURE ÉLECTRONIQUE

La signature électronique remplit **3 fonctions essentielles** :

1. identifier le signataire (**authentification**),
2. confirmer son accord ou prise de connaissance sur le contenu du document (**consentement**),
3. garantir que le document n'a pas été modifié après la signature (**intégrité**).

Elle assure également la **sécurité juridique** en donnant une valeur probante aux documents électroniques, équivalente à celle des documents papier. Par ailleurs, elle **engage la responsabilité** de la personne qui signe.

Reconnue légalement dans l'ensemble de l'Union européenne, la signature électronique facilite la dématérialisation des procédures tout en assurant la sécurité et la confiance dans les échanges électroniques.

Si l'évolution technologique a permis de dématérialiser la signature, notamment par le biais de solutions électroniques, il ne faut pas perdre de vue que les fonctions essentielles de la signature demeurent inchangées à travers les époques. Qu'il s'agisse d'une inscription manuscrite ou d'une empreinte numérique, la signature vise toujours à authentifier l'identité du signataire, à engager sa responsabilité si nécessaire et à garantir l'intégrité du document signé.

En résumé, la forme peut évoluer, mais le fond reste identique. Elle matérialise l'accord, la volonté ou l'engagement, tout en assurant la sécurité juridique des échanges. Cette continuité témoigne de l'importance universelle de la signature, quel que soit le support utilisé.

**Que signifie eIDAS ?*

Le règlement 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS) est la référence clé dans l'Union Européenne en ce qui concerne la signature électronique et l'archivage électronique. Il offre un cadre juridique commun et normalisé pour que les signatures électroniques soient reconnues et acceptées juridiquement dans tous les états membres de l'UE.

Ce règlement a été transposé en droit belge par la loi du 21 juillet 2016 (« Digital Act »).

LE SAVIEZ-VOUS ?

En 2026, le Service public fédéral Intérieur a procédé à des **adaptations du certificat de signature de la carte d'identité électronique belge (eID)**.

Ces modifications s'inscrivent dans le cadre de la modernisation de l'infrastructure eID en Belgique et de la préparation aux futures évolutions européennes. **Depuis le 21 mai 2026, les cartes d'identité délivrées avant juillet 2016 ne permettent plus de réaliser des signatures électroniques qualifiées**. Les utilisateurs concernés doivent renouveler leur eID ou utiliser d'autres solutions de signature qualifiée conformes au règlement eIDAS.

Plus d'informations : https://www.ibz.rrn.fgov.be/fr/actualites/signature-electronique-avec-leid-modification-a-partir-du-21-mai-2026

Par ailleurs, la loi du 16 juillet 2026 relative à un service de signatures électroniques qualifiées confère une base légale au système de création de signatures mis en place par le SPF.

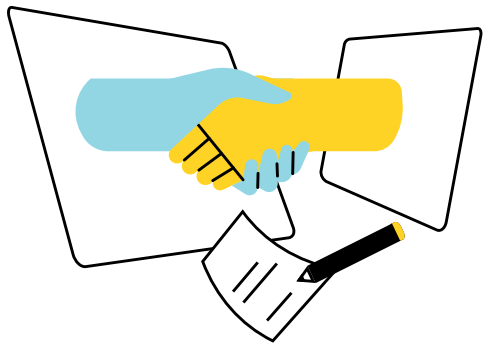
Plus d'informations : https://www.ejustice.just.fgov.be/eli/loi/2026/07/16/2026005829/justel

UNE SIGNATURE ÉLECTRONIQUE A-T-ELLE LA MÊME VALEUR LÉGALE QU'UNE SIGNATURE MANUSCRITE ?

Tout dépend du cadre légal et du niveau de sécurité offert par la technologie utilisée.

En Belgique, la signature électronique bénéficie d'une reconnaissance légale équivalente à la signature manuscrite, pour autant qu'elle respecte certaines exigences de fiabilité et d'identification du signataire. De plus, selon le principe de **non-discrimination**, une signature électronique ne peut être rejetée ou privée d'effets juridiques uniquement parce qu'elle est au format électronique.

La signature manuscrite, traditionnellement perçue comme plus «tangible», n'est pas nécessairement supérieure ni davantage valable : une signature électronique avancée ou qualifiée **garantit l'intégrité du document et l'identité du signataire**, tout en **assurant la non-répudiation** (garantie qu'un signataire ne peut pas contester valablement avoir signé un document). Ainsi, dans de nombreux cas, **la signature électronique offre des garanties au moins équivalentes, voire supérieures**, notamment en matière de traçabilité et de sécurité, à condition que le procédé utilisé soit conforme aux normes en vigueur.



LES DIFFÉRENTS TYPES DE SIGNATURES ÉLECTRONIQUES

Selon la réglementation européenne (eIDAS), il existe **trois types de signatures électroniques**, offrant un niveau de sécurité et de reconnaissance juridique différent.

1. LA SIGNATURE ÉLECTRONIQUE SIMPLE

C'est le niveau le plus basique de signature électronique. Elle est facile à mettre en œuvre car elle ne nécessite pas de technologie spécifique. Son usage est courant pour des démarches peu risquées, mais elle offre un niveau de sécurité limité.

En pratique : elle est surtout utilisée lorsque le document n'a pas ou peu d'enjeu juridique, et que les risques de contestation sont faibles. **Elle suffit donc pour des démarches simples et/ou internes** (formulaire, demandes mineures) mais est à éviter pour des contrats/engagements plus importants ou lorsqu'un niveau de signature plus fort est imposé pour une loi.

Exemples :

- ✓ image scannée d'une signature manuscrite apposée sur un document,
- ✓ case à cocher sur un document en ligne,
- ✓ signature en bas d'un e-mail,
- ✓ code secret d'une carte de crédit.

2. LA SIGNATURE ÉLECTRONIQUE AVANCÉE

Elle repose sur des **critères plus stricts d'identification et d'authentification et doit répondre à des exigences eIDAS spécifiques** : elle fait le lien entre le signataire, sa signature et les données signées. Ce lien vise à garantir l'intégrité des données (document n'a pas été modifié après signature), l'identification du signataire et la non-répudiation (la personne ne peut pas nier avoir signé). Toutes les administrations n'offrent pas ce niveau de signature.

En pratique : la signature électronique avancée offre un **bon équilibre entre sécurité et simplicité, sans nécessiter un certificat officiel.** Elle impose toutefois l'utilisation d'une technologie plus spécifique.

Exemples :

- ✓ signature via votre nom et mot de passe ;
- ✓ signature dans une application bancaire ;
- ✓ signature validée par OTP (One Time Password) : MFA[3] (Multi-Factor Authentication), code unique par SMS, e-mail ou application mobile,
- ✓ signature biométrique (signature manuscrite faite sur une tablette ou via un autre dispositif qui enregistre le tracé, la pression et la vitesse, afin d'identifier le signataire).

3. Mécanisme de sécurité qui consiste à vérifier l'identité d'un utilisateur au moyen d'au moins deux facteurs d'authentification de nature différente avant de lui accorder l'accès à un système ou à un service. Par exemple, un utilisateur qui se connecte à une plateforme de signature électronique à l'aide de son mot de passe (premier facteur), puis saisit un code reçu sur son téléphone mobile (deuxième facteur), ou l'utilisation de l'eID combinée à un code PIN.

LE SAVIEZ-VOUS ?

Une signature qualifiée appose une marque visuelle, un tampon, sur votre document. Cette marque contient parfois une date et une heure (**un horodatage**), afin d'ajouter une preuve supplémentaire, qui ne pourra être ni supprimée ni modifiée par la suite.

Principe	signature simple	signature avancée	signature qualifiée
Identification du signataire	-	✓	✓
Intégrité du document[1]	-	✓	✓
Non-discrimination[2]	✓	✓	✓
Non-répudiation[3]	-	✓	✓
Certification agréée[4]	-	-	✓
Sécurité et reconnaissance juridique	+	++	+++

1. **Intégrité :** garantit que le document n'a pas été modifié après la signature.
2. **Principe de non-discrimination :** une signature ne peut pas être rejetée ou privée d'effets juridiques uniquement parce qu'elle est électronique.
3. **Principe de non-répudiation :** le signataire ne peut pas valablement contester avoir signé le document.
4. **Certification :** opération consistant à attester du lien entre l'identité d'une personne et les données utilisées pour créer sa signature électronique.

3. LA SIGNATURE ÉLECTRONIQUE QUALIFIÉE

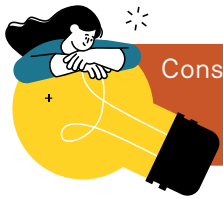
C'est le **niveau le plus élevé de sécurité et de valeur juridique, assimilée à une signature manuscrite**. La signature électronique qualifiée cumule toutes les garanties de la signature avancée, en plus d'une **certification par un prestataire qualifié, agréé par le SPF Économie (ou reconnu au sein de l'UE)**. Le certificat qui authentifie le signataire repose sur des procédures strictes. Elle est donc plus complexe, et a un coût plus élevé pour l'administration.

Dans certains cas, elle peut être accompagnée d'un **horodatage électronique**. Celui-ci permet d'attribuer à un document une date - et parfois une heure - qui ne peut pas être modifiée. Il sert à prouver qu'un document ou une action (comme une signature) existait bien à un moment précis. Cette fonction est particulièrement utile lorsque l'ordre chronologique compte, par exemple pour une demande de prime ou pour vérifier qu'une démarche a été faite avant une échéance.

En pratique : utilisez cette signature lorsque c'est **absolument nécessaire**, c'est-à-dire si l'authentification doit être irréprochable, ou si une règlementation l'exige. Elle doit être créée à l'aide d'un dispositif qualifié de création de signature.

Exemples :

- ✓ signature via un lecteur de carte d'identité et logiciel spécifique (eID),
- ✓ clé numérique en ligne,
- ✓ méthode permettant aux citoyens de s'authentifier de manière sécurisée telles que Itsme, myGov.be, etc.
- ✓ signature via un logiciel ou solution dédiée (Adobe Acrobat, Microsoft Word, etc.).



Consultez la fiche pratique **« Les 3 types de signature électronique »**

CONCRÈTEMENT : LES ÉLÉMENTS D'UNE SIGNATURE ÉLECTRONIQUE

La signature simple peut être une simple image, un nom ou une case à cocher, les signatures avancées ou qualifiées sont plus complexes. **Il s'agit d'un ensemble d'éléments techniques et juridiques qui permettent de garantir l'identité du signataire et l'intégrité du document.**

Les signatures avancées et qualifiées sont généralement constituées des éléments suivants :

- ✓ **les données du document signé :** la signature est liée au document lui-même. Un mécanisme cryptographique (*calcul mathématique appelé aussi hachage*) crée une empreinte numérique unique (*hash*) pour le contenu du document. Lors de la vérification, une nouvelle empreinte sera recalculée et comparée à l'empreinte d'origine, pour garantir que le document n'a pas été modifié après la signature.
- ✓ **Les données de la signature :** il s'agit d'informations cryptographiques produites lors de la signature à l'aide de la clé privée du signataire. Elles créent un lien unique entre le signataire et le document.
- ✓ **Le certificat électronique :** sorte de «carte d'identité numérique» qui contient notamment l'identité du signataire, la clé publique associée, un numéro de série (*code du certificat*), la période de validité, et l'identité de l'autorité qui délivre ce certificat. Il permet d'attester que le document n'a pas été falsifié, de confirmer l'identité du signataire, et de retracer l'itinéraire du document en ligne. **Dans le cas d'une signature électronique qualifiée**, l'autorité qui délivre le certificat est spécialement agréée par l'Union européenne et régulièrement contrôlée, avec des exigences renforcées.
- ✓ **L'horodatage** (le cas échéant) **:** atteste la date et l'heure exactes de la signature. L'horodatage ne peut être modifié sous peine d'invalider la signature… et le document !
- ✓ **Les preuves de signature :** selon la solution technologique utilisée, des éléments complémentaires peuvent être conservés tels que l'adresse IP, la méthode d'authentification, la preuve de validation par SMS, eID, itsme®, etc. Ces preuves permettent de renforcer la non-répudiation[4] et la valeur probante du document.

En résumé, une signature électronique fonctionne comme un «sceau» numérique. Le système crée une empreinte numérique du document, comparable à votre empreinte digitale. Si le document est modifié après la signature, même très légèrement, son empreinte changera. Il sera alors possible de détecter toute altération du document, le rendant potentiellement invalide.

LE SAVIEZ-VOUS ?

Le cachet électronique est similaire à une signature électronique mais pour une personne morale. Il est l'équivalent numérique du tampon d'une organisation et permet à une entreprise ou une administration d'authentifier un document.

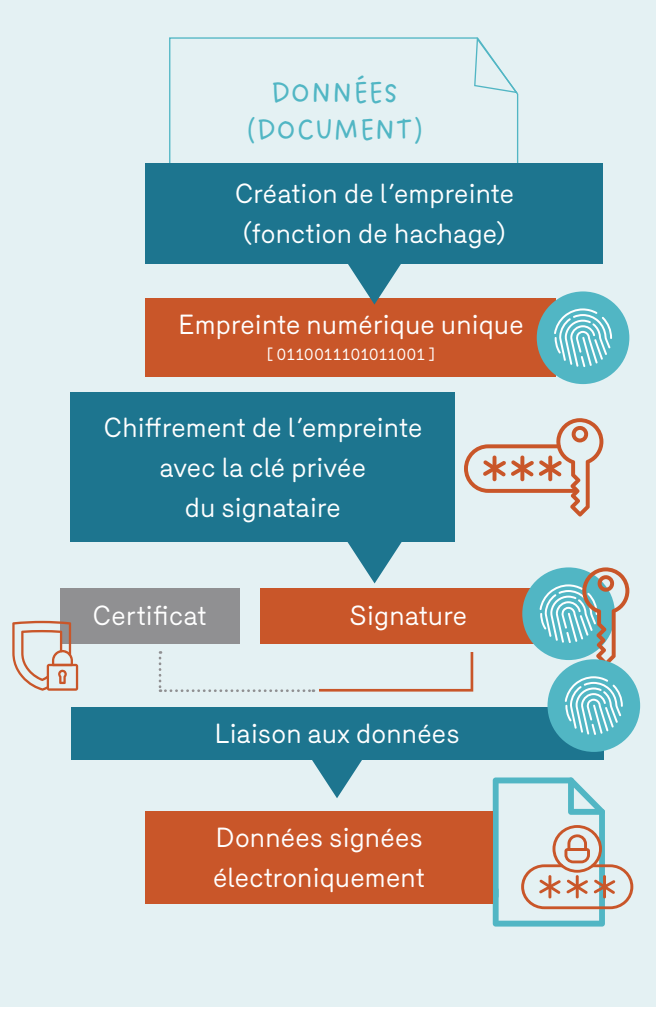
4. Non-répudiation : capacité à fournir des preuves fiables qu'une signature électronique a été réalisée par une personne déterminée, de sorte qu'elle ne puisse raisonnablement contester avoir signé le document.

POINT D'ATTENTION

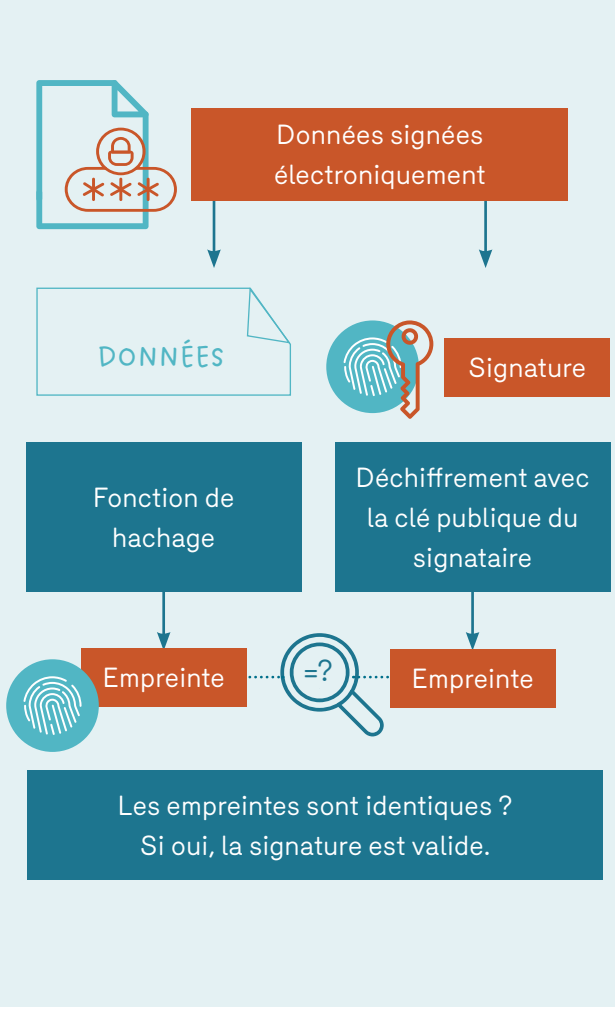
L'image d'une signature manuscrite, apposée sur un document papier ou numérique, ne constitue pas en soi une garantie de validité ou d'authenticité.

Ce qui confère une **valeur juridique** à une signature, ce sont les **critères vérifiés lors du processus de signature** : l'identification du signataire, l'intégrité du document et la capacité à prouver l'acceptation du contenu. Ainsi, la simple reproduction graphique d'une signature ne suffit pas pour attester de la volonté du signataire ou pour assurer la sécurité du document. Les mécanismes de contrôle associés à la signature (qu'elle soit électronique ou manuscrite) sont essentiels pour garantir sa validité et sa force probante.

CRÉATION DE LA SIGNATURE ÉLECTRONIQUE



VÉRIFICATION DE LA VALIDITÉ D'UNE SIGNATURE ÉLECTRONIQUE



Source : https://fr.wikipedia.org/wiki/Signature_numérique

QUEL TYPE DE SIGNATURE ÉLECTRONIQUE UTILISER ? ARBRE DÉCISIONNEL

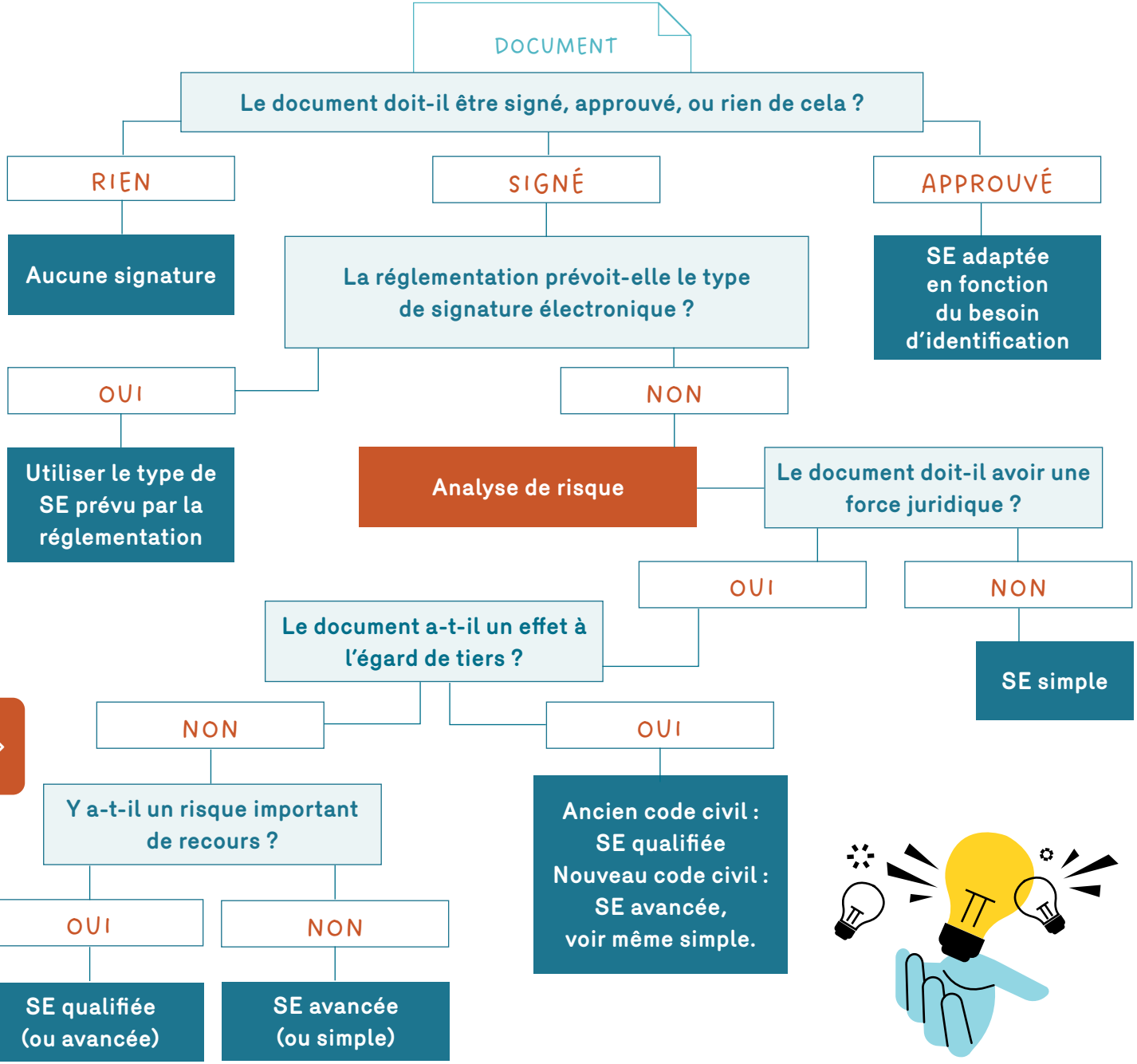
Le choix du type de signature dépend de l'usage et de l'enjeu du document à signer. En cas de litige, plus votre signature aura un niveau de fiabilité fort, plus il sera difficile de contester la validité du document signé et les engagements qu'il contient.

Privilégiez les signatures avancées (si disponibles) et qualifiées pour les contrats commerciaux, les actes juridiques ou les transactions sensibles. Utilisez la signature simple pour des procédures administratives ou des échanges quotidiens moins critiques.

Ci-contre : un arbre décisionnel vous aidera à choisir le type de signature adapté.

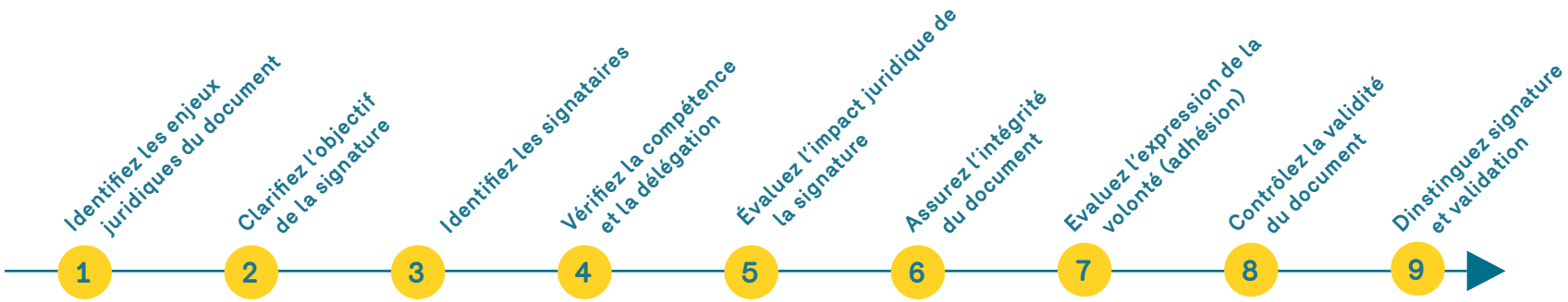
SE = signature électronique

Consultez la fiche pratique
« Quel type de signature choisir »



AVANT DE (FAIRE) SIGNER UN DOCUMENT : QUELQUES ÉTAPES DE RÉFLEXION.

1. **Déterminez la nature et le cadre juridique (droit administratif) du document.** Est-ce une décision unilatérale, une notification, une pièce interne, ou autre ? Quel est le cadre juridique ? Cela permettra de vérifier les exigences à respecter, tant sur le fond (compétence, base légale, motivation, procédure) que sur la forme, notamment en matière de signature.
2. **Clarifiez l'objectif recherché.** La signature servira-t-elle à …
   - identifier la personne qui intervient ?
   - marquer un accord (ou non) sur le contenu ?
   - garantir l'intégrité du document ?
   - organiser un workflow (relecture, validation) ?
   - assurer la crédibilité du document ?
3. **Identifiez le ou les signataires.** Qui doit signer (identité), et à quel titre (autorité compétente, mandataire, agent habilité) ? Quel est le niveau de certitude nécessaire sur cette identité, en fonction du document et de ses effets ?
4. **Vérifiez la compétence et la délégation de signature.** L'autorité compétente a-t-elle bien décidé du document ? La délégation de signature (autorisation de signer « pour ordre ») est-elle valable, traçable et compatible avec l'organisation interne ?
5. **Identifiez les questions juridiques posées par la signature.** Vérifiez si la signature peut avoir un impact sur la régularité externe et/ou interne, la compétence de l'auteur, la traçabilité, la preuve, l'opposabilité, les voies de recours, l'archivage de l'original électronique, etc.
6. **Assurez l'intégrité du document.** Définissez ce que vous devez pouvoir prouver : que le document n'a pas été modifié après signature, ou que toute modification est détectable ?
7. **Évaluez l'adhésion.** La signature doit-elle exprimer une volonté d'engagement, de consentement, de refus du contenu, ou une décision ? Précisez à quel moment cette signature est exigée (signature finale, contreseing, etc.).
8. **Contrôlez la validité du fond et de la forme.** Le document doit réunir deux types de condition :
   - *validité de fond :* compétence et respect des règles,
   - *validité de forme :* formalités, mention de l'auteur, signature, etc. La signature fait partie des éléments de forme, mais elle ne suffit pas à elle seule pour garantir la validité du document.
9. **Distinguez signature et validation.** Une validation ne nécessite pas toujours une signature, et peut prendre d'autres formes : un visa dans un workflow, un bouton d'approbation, un login, etc. Une analyse de risques vous aidera à choisir le mécanisme le plus adapté.



LES ENJEUX DE LA SIGNATURE ÉLECTRONIQUE

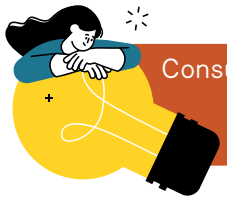
QUELLES RESPONSABILITÉS LA SIGNATURE ENGAGE-T-ELLE ?

- **Sur la forme (régularité externe)** : la signature permet d'identifier le signataire et de confirmer sa compétence, de vérifier l'existence d'une délégation en règle, le respect des formalités (mentions, dates, modalités de notification), ainsi que l'intégrité et à la traçabilité du document.
    - › Une défaillance à ce niveau peut fragiliser le document, même si le contenu est correct.
- **Sur le fond (régularité interne)** : la signature ne suffit pas à rendre un document légal ou incontestable. Un document valablement signé peut toujours être contesté s'il repose sur une décision irrégulière, une erreur manifeste, une violation de la loi, un défaut de motivation, ou un usage abusif de pouvoir, etc.

En résumé, en cas de contestation, ce n'est pas seulement le type de signature qui compte, mais aussi la capacité à démontrer qui a signé, quand, et dans quelles conditions, au moyen de preuves.

A quoi faire attention ?

Lors du choix du type de signature approprié pour la démarche, demandez-vous également quelles preuves peuvent être produites si la signature est contestée, et assurez-vous que ce niveau de preuve est en adéquation avec l'enjeu du document.



Consultez la fiche pratique **« Le document doit-il être signé ? »**

LE SAVIEZ-VOUS ?

Le droit reconnaît plusieurs formes de signature, peu importe le visuel, tant qu'elles permettent d'identifier le signataire, de confirmer son accord ou sa volonté, et de garantir l'intégrité du document.

Toutefois, toutes les signatures n'offrent pas le même niveau de sécurité ni la même valeur juridique.

LE SAVIEZ-VOUS ?

La **signature électronique qualifiée** est reconnue dans toute l'Union européenne. Contrairement aux autres types de signatures, en cas de litige, c'est à la partie adverse de démontrer qu'elle n'est pas valable. Pour la signature simple ou avancée, c'est au signataire qu'il revient d'apporter la preuve de sa validité.

QUE SE PASSE-T-IL SI UN DOCUMENT N'EST PAS (VALABLEMENT) SIGNÉ ?

Le principal risque, pour une administration, est qu'un document non signé, signé par une personne non compétente, ou au moyen d'un procédé insuffisamment fiable peut être contesté et entraîner un litige (annulation, suspension, contestation de preuve, litige contractuel, etc.).

En pratique, l'absence ou le défaut de signature ne rend pas systématiquement le document non valide. En cas de litige, le juge vérifie souvent si le mécanisme utilisé remplit les fonctions attendues d'une signature : identifier le signataire, exprimer l'adhésion/volonté, garantir l'intégrité du document, assurer la traçabilité.

- **Ce qui est en jeu :**
  - la validité de l'acte (forme/fond), son opposabilité, et la possibilité d'en rapporter la preuve en cas de contestation.
- **Ce que le juge examinera :**
  - la compétence de l'auteur, la réalité de la décision/consentement, l'intégrité du document, et la qualité des traces (journal d'événements, horodatage, conservation).

En résumé, ce n'est pas seulement la présence d'une signature qui compte, mais la capacité à prouver l'identité du signataire, son accord, l'intégrité du document et sa traçabilité.

Comment réduire le risque ?

En documentant votre analyse (choix du canal, niveau de signature ou validation, mesures d'identification et de conservation) et en adaptant la solution aux enjeux du document.

Les conséquences d'un défaut de signature (ou d'un mécanisme de signature inadapté) varient selon la nature du document et la juridiction susceptible d'être saisie.

- **Actes administratifs (notamment individuels) :** une contestation peut porter sur la légalité (forme et/ou fond). Elle peut entraîner l'annulation ou suspension, avec des conséquences concrètes : réédition des documents, reprise de procédure, retards dans le traitement et coûts administratifs supplémentaires.
- **Contentieux civil :** la signature est souvent abordée sous l'angle de la preuve. Il peut s'agir de démontrer l'existence d'un accord, l'acceptation d'un engagement, une date ou l'identité de l'auteur. Un mécanisme de signature insuffisant peut compliquer cette démonstration et augmenter le risque de contestation.
- **Contentieux pénal :** certaines situations peuvent soulever des questions liées à l'altération de documents, à l'usurpation d'identité ou à un accès non autorisé. Ces risques rappellent l'importance de garantir la traçabilité, l'intégrité et la sécurité des accès.

En résumé : les conséquences d'un défaut de signature dépendent du contexte, mais elles peuvent affecter la validité d'un document, sa force probante, et engendrer des coûts ou des retards.

Posez-vous les bonnes questions...

Qui peut contester ? Devant quel juge ? Quelles conséquences (annulation, réparation, sanction) ? Quels coûts directs et indirects ?

LA FORCE PROBANTE EN JUSTICE

Au-delà de la validité du document, l'enjeu est souvent de pouvoir démontrer que la signature est fiable et que le document peut être retenu comme preuve (force probante).

En cas de contestation, l'administration doit pouvoir établir que :

- ✓ le signataire est bien la personne qui a apposé la signature,
- ✓ le signataire a exprimé son accord et/ou sa décision,
- ✓ le document présenté est celui qui a été signé (intégrité),
- ✓ les circonstances de la signature (date, chaîne de conservation) peuvent être démontrées.

Le règlement eIDAS prévoit la reconnaissance des signatures électroniques et accorde, pour certaines, une présomption de fiabilité. Toutefois, la valeur de la preuve repose sur la qualité des éléments (traces) disponibles : journaux d'événements, horodatage, journal des logs et des actions, certificat, ainsi que sur les modalités de conservation.

En résumé : en cas de contestation, ce n'est pas seulement le type de signature qui compte, mais aussi la capacité à démontrer qui a signé, quand, est dans quelles conditions, au moyen de preuves.

A quoi faire attention ?

Lors du choix du type de signature approprié pour la démarche, demandez-vous également quelles preuves peuvent être produites si la signature est contestée, et assurez-vous que ce niveau de preuve est en adéquation avec l'enjeu du document.

NUANCES ET PRÉCISIONS DES NOTIONS

Dans la pratique, on mélange souvent plusieurs termes : signer, valider, viser, parapher, contresigner… alors qu'ils ne renvoient pas aux mêmes effets juridiques ni aux mêmes exigences de preuve.

Les distinctions ci-dessous vous aideront à choisir le bon geste (signature ou simple validation), à comprendre ce que cela prouve, et à organiser la conservation du document.

VALIDATION OU SIGNATURE ?

Validation : action par laquelle une personne confirme qu'un document peut « passer à l'étape suivante » (relecture effectuée, accord interne, feu vert). Une validation peut être matérialisée par un clic, un statut dans un workflow, un e-mail, un ticket, un login, etc.

Signature : action par laquelle une personne s'engage (décision, consentement, accord sur le contenu) et permet d'imputer le document à un signataire identifié, avec une attente forte d'intégrité du document signé.

✘ **Erreur fréquente :** utiliser une « validation » (par exemple un simple login) alors qu'il faut pouvoir démontrer, en cas de contestation, qui a pris la décision, sur quel document et à quelle date.

SIGNATURE, VISA OU CONTRESEING ?

Visa : marque d'examen ou de contrôle (par exemple visa budgétaire, visa juridique). Le visa atteste généralement qu'une étape de vérification a eu lieu, sans nécessairement exprimer la décision finale.

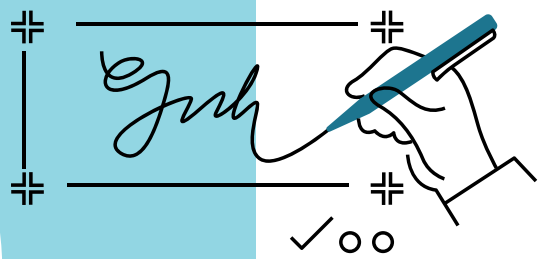
Contreseing (ou « contre-signature) : signature « additionnelle » apposée en plus de la signature principale, pour, par exemple, attester une vérification, une responsabilité partagée, ou l'intervention d'une autre autorité. Selon les cas, cette contre-signature peut avoir une portée juridique spécifique.

Signature : acte par lequel l'autorité ou la personne compétente prend la décision ou exprime son engagement.

✘ **Erreur fréquente :** traiter un visa comme une signature (ou l'inverse) alors que les responsabilités et la compétence attendue ne sont pas les mêmes.

À RETENIR :

Adoptez le bon réflexe : demandez-vous ce que vous devriez prouver : adhésion, identité, intégrité, date ou autre ? Si le risque est faible, une validation peut suffire ; si le risque est élevé, une signature (et une conservation renforcée) est préférable.



SIGNATURE OU PARAPHE ?

Paraphe : marque courte, souvent des initiales, apposée sur une page, généralement pour indiquer qu'elle a été lue/validée, ou pour limiter le risque de substitution de pages dans un dossier .

Signature : marque (manuscrite ou électronique) qui identifie le signataire et matérialise son engagement/adhésion au contenu.

LOGIN, CLIC, PARAPHE ?

Login/compte utilisateur : peut prouver qu'un compte a réalisé une action, mais pas toujours quelle personne était derrière l'écran (compte partagé, vol d'identifiants, absence de double facteur).

Clic « approuver » : utile dans un processus interne, à condition que le système conserve des traces (qui, quoi, quand) et que les droits d'accès soient maîtrisés.

Paraphe : utile pour « figer » un dossier page par page, mais ne garantit pas l'identité avec le même niveau de preuve qu'une signature.

SIGNATURE PHOTOCOPIÉE, SCANNÉE, OU SIGNATURE ORIGINALE ?

Signature originale manuscrite : signature apposée physiquement par la personne sur le document papier.

Signature scannée ou photocopiée : l'image de la signature ne prouve pas, à elle seule, que la personne a effectivement signé ou que le document n'a pas été modifié.

À ne pas confondre avec une signature électronique (avancée ou qualifiée) : une signature électronique avancée ou qualifiée repose sur un procédé qui vise à lier un signataire au document et à garantir l'intégrité, ce qu'une image ne fait pas. Une image apposée sur un document constitue une signature électronique simple, elle ne lie pas le signataire au document de façon sûre, et ne garantit pas l'intégrité du document.

✘ **Erreur fréquente :** croire qu'un PDF avec une image de signature « vaut signature manuscrite ». En cas de contestation, il faut des éléments complémentaires (processus, e-mails, traces, etc.), souvent plus fragiles qu'un mécanisme de signature électronique.

À RETENIR :

Un paraphe ne remplace pas la signature lorsqu'elle est requise. Il a une utilité pratique, mais une portée juridique et probatoire plus limitée.

À RETENIR :

Si l'on retient une validation plutôt qu'une signature, il est utile de documenter l'analyse de risques et de renforcer, si nécessaire, l'identification (p. ex. authentification forte), la traçabilité (journal d'audit) et la conservation.

À RETENIR :

L'image d'une signature ne lie pas le signataire au document de façon sûre.

ACTE AUTHENTIQUE, AUTHENTICITÉ EN MATIÈRE DE CONSERVATION ET ORIGINAL

QU'EST-CE QU'UN ACTE « AUTHENTIQUE » ?

Au sens juridique, un acte authentique est un document reçu (ou établi) par un officier public[5] compétent (par exemple un notaire) selon des règles précises définies par la loi. Il s'agit donc d'une notion juridique précise, et pas juste d'un document considéré comme étant « fiable ».

Au sens de la conservation (gestion documentaire/archivage), on parle plutôt **d'authenticité**.

Ceci signifie que le document est bien celui qu'il prétend être, qu'il provient de la bonne source et qu'il a été conservé sans modification indétectable (traçabilité, intégrité, chaîne de conservation).

QU'EST-CE QU'UN « ORIGINAL » ?

Original papier : document papier qui constitue la version d'origine, éventuellement signé à la main.

Original électronique : version numérique dont l'intégrité et la provenance sont prouvées (signature, horodatage, conservation). C'est cette version qui « fait foi ».

Original hybride : dossier qui combine papier et numérique (document signé sur papier puis numérisé, par exemple). Dans ce cas, la difficulté est d'identifier clairement quelle version est considérée comme l'original.

✘ **Erreur fréquente** : croire que les documents rédigés par des fonctionnaires de l'administration sont des actes authentiques. En réalité, seuls certains documents rédigés par des officiers publics désignés (notaires, huissiers, etc.) sont des actes authentiques (ex : actes d'achat-vente ou des actes de l'état civil (acte de naissance, de mariage, etc.)). Les agents publics peuvent rédiger des actes administratifs, qui ont leur propre régime. Nous vous conseillons de contacter vos services juridiques pour qualifier chaque document rédigé, et connaître le régime légal applicable.

À RETENIR :

Adoptez le bon réflexe : pour votre procédure, identifiez quelle version fait foi (quel est l'original) et comment l'administration peut le démontrer dans la durée.

5. Un officier public est un fonctionnaire public, mais tout fonctionnaire public n'est pas officier public. Cette responsabilité est accordée par un texte légal.

FAUX EN ÉCRITURE

Un faux en écriture est une infraction qui consiste à créer, modifier ou utiliser un écrit de manière frauduleuse dans le but de tromper.

Exemples : altération du contenu, fausse signature, usurpation d'identité, substitution de pages, antidatage, etc.

Quel est le lien avec la signature ?

› Plus le document est sensible, plus un mécanisme qui rend toute modification détectable est important. Il permettra également de lier le document à son signataire.

À RETENIR :

Raisonnez en « chaine de confiance » : qui a accès au document, qui peut le modifier, le valider ou le signer ? Quelles preuves sont conservées ? Où et comment l'original est-il conservé ?

SOLUTIONS TECHNOLOGIQUES

POUR LES CITOYENS

Pour un citoyen, signer électroniquement signifie généralement s'engager sur une décision ou un consentement dans le cadre d'une procédure administrative. Cela peut se faire à l'aide d'un moyen d'identification numérique (carte d'identité électronique, Itsme, ou autre).

Il existe plusieurs solutions technologiques qui n'offrent pas toutes le même niveau de garantie (identification du signataire, détection des modifications, preuve en cas de contestation).

Le choix dépend donc de plusieurs facteurs : nature du document, risques liés à son utilisation, niveau de preuve recherché, mais aussi la simplicité d'utilisation et l'accessibilité de l'outil.

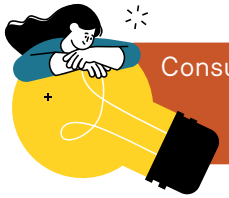
POUR LES ADMINISTRATIONS PUBLIQUES

De nombreuses solutions existent pour signer (ou valider) un document électronique. Certaines prennent la forme de plateformes de signature intégrées aux processus administratifs (circuits de validation, signature en série, suivi des dossiers), tandis que d'autres fournissent des fonctions plus spécifiques comme l'authentification, l'horodatage, le scellement électronique ou la conservation des preuves.

Le marché évolue rapidement et les besoins varient d'une administration à l'autre : volume de documents, profil des utilisateurs, contraintes techniques, politiques de sécurité, etc.

À RETENIR :

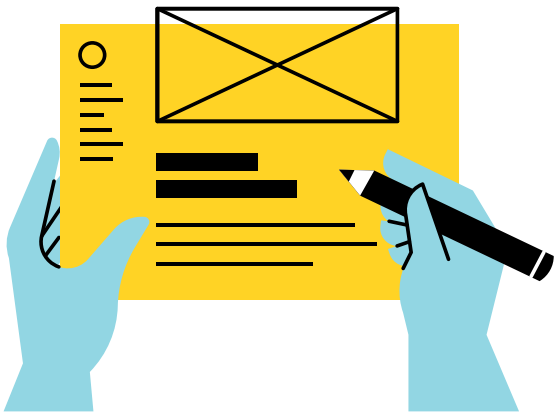
Adoptez le bon réflexe : l'utilisation d'une technologie numérique est parfois difficile d'accès pour les personnes en situation de fracture numérique. Assurez-vous donc qu'une signature qualifiée est réellement nécessaire et, si oui, pensez à proposer une alternative physique.



Consultez la fiche pratique **« Quel outil technologique utiliser ? »**

Dans un souci de neutralité technologique*, nous ne privilégions aucune solution spécifique. L'essentiel est de s'assurer que la solution retenue répond aux besoins de l'administration et offre des garanties en matière :

- d'identification et d'authentification des signataires ;
- d'intégrité des documents ;
- de traçabilité des actions réalisées ;
- de valeur probante en cas de contestation ;
- de conservation des documents et des preuves associées.



Avant d'opter pour une solution, il est donc nécessaire de définir vos besoins :

- ✓ Quels types de documents devez-vous signer ? Quel niveau de signature requièrent-ils ?
- ✓ Qui sont les personnes qui devront signer, quel rôle auront-elles ?
- ✓ Les coûts de la solution sont-ils clairement indiqués et maîtrisés ?
- ✓ La solution est-elle facile à utiliser, tant pour les agents que pour les usagers ?
- ✓ La solution peut-elle s'intégrer aux outils et processus internes ?

↬ Aidez-vous de l'arbre décisionnel ou de la fiche pratique pour valider le type de signature nécessaire.

POINT D'ATTENTION

Toute technologie a un coût : licences et exploitation, coûts par signature apposée, accompagnement (support, formation), et intégration (connecteurs, API, interfaçage avec les applications métiers et, le cas échéant, avec l'archivage électronique). Le recours à une signature électronique qualifiée suppose l'intervention d'un prestataire qualifié, peut donc limiter les options et augmenter les coûts unitaires. Si le cadre légal ou contexte n'impose pas une signature électronique qualifiée, envisagez d'autres types de signatures électroniques, ou même une validation alternative (validation dans un processus, accord via un outil interne, mécanisme d'authentification/login).

À RETENIR :

Adoptez le bon réflexe : après avoir défini vos besoins, collecter l'avis des autres administrations sur les solutions qu'elles utilisent. Les administrations régionales de support informatique et technologique peuvent également vous aider dans ce choix.

*Principe de ne pas privilégier une technologie, un produit, un fournisseur, ou un support spécifique, mais de définir les résultats ou fonctionnalités attendues et de laisser les administrations choisir la solution la plus adaptée.

FICHES PRATIQUES

Ces fiches pratiques ont pour objectif de répondre rapidement à quelques questions précises et récurrentes.

1. **Le document doit-il être signé ?**
2. **Les 3 types de signature électronique**
3. **Quel type de signature choisir ?**
4. **Quelle est la durée de validité d'une signature électronique ?**
5. **Comment archiver un document signé électroniquement ?**
6. **Quel outil technologique utiliser ?**
7. **Envoi et impression d'un document signé électroniquement**
8. **Signatures multiples**
9. **Signature par lot**
10. **Puis-je modifier un document après signature ? (contenu ou horodatage)**

1. Le document doit-il être signé ?

Dans le cadre de la simplification administrative, il est pertinent de s'interroger sur l'intérêt réel de la signature. Avant de signer un document, posez-vous cette question simple : la signature est-elle vraiment nécessaire ? Dans beaucoup de cas, elle n'est pas indispensable : une validation suffit.

Signature ou validation ?

- **Une signature engage** une personne, **confirme** un accord ou une décision, et a une **valeur** juridique.
- **Une validation** donne un **accord** (un «ok») ; sert souvent dans un processus interne et n'implique pas toujours un engagement juridique.

  Exemples de validation : répondre «ok» par e-mail, ou cliquer sur «approuver» dans un outil numérique.

Cas fréquents où la signature n'est PAS nécessaire

Beaucoup de documents sont signés «par habitude» alors que ce n'est pas utile : notes internes, validations RH simples, échanges entre collègues, documents sans impact juridique. Dans ces cas, une validation suffit.

3 questions à se poser

1. Le document crée-t-il un droit, une obligation ou une décision ?

▻ **Oui :** signature nécessaire.

► **Non :** validation souvent suffisante.

2. Le document doit-il servir de preuve en cas de problème ?

▻ **Oui :** signature recommandée.

► **Non :** validation possible.

3. Est-ce une exigence légale ou interne ?

▻ **Oui :** respectez le type de signature demandé.

► **Non :** adaptez en fonction du besoin, une validation peut suffire.

✓ *Pour aller plus loin dans ce choix, consulter l'arbre décisionnel en page 13 du guide de réference.*

À RETENIR

- ✓ La signature n'est pas automatique.
- ✓ Elle doit être utilisée uniquement lorsque c'est nécessaire.
- ✓ Une validation peut souvent suffire et simplifier les procédures.

LE BON RÉFLEXE

Posez-vous toujours la question : que dois-je pouvoir prouver ?

- ✓ un accord formel = **une signature**
- ✓ un simple feu vert ou une prise de connaissance = **une validation**

2. Les 3 types de signature électronique (SE)

Toutes les signatures n'offrent pas le même niveau de sécurité. Il en existe 3 types, à utiliser en fonction du risque et de l'importance du document à signer.

SE simple

Forme de signature facile à utiliser, sans technologie particulière, et à faible enjeu juridique.

Exemples : case à cocher en ligne, signature d'un e-mail, image d'une signature scannée.

- ✔ **On l'utilise pour :** signer des documents internes, des demandes simples, sans réel enjeu juridique.
- **Bon à savoir :** son niveau de sécurité est limité, et le risque de contestation est plus élevé.

SE avancée

Permet d'identifier clairement le signataire et de garantir que le document n'a pas été modifié après signature.

Exemples : signature via code SMS (OTP), via une application, ou dans certaines plateformes en ligne.

- ✔ **On l'utilise pour :** signer des documents importants ou des procédures administratives à risque modéré.
- **Bon à savoir :** la signature avancée est un bon compromis entre sécurité et simplicité. Cette signature nécessite un outil spécifique et n'est pas systématiquement proposée au sein des administrations publiques.

SE qualifiée

Le niveau le plus élevé de sécurité, équivalent à une signature manuscrite, reconnue dans toute l'Union européenne. **Elle est validée par un certificat qui garantit l'intégrité du document et l'identité du signataire.**

Exemples : signature avec carte d'identité électronique, itsme®, ou un autre type de certificat qualifié.

- ✔ **On l'utilise pour :** signer des documents sensibles, des décisions officielles, dans des situations à fort risque juridique, ou simplement quand la loi l'exige.
- **Bon à savoir :** plus complexe à mettre en oeuvre, ce niveau peut engendrer des coûts et l'utilisation d'un outil spécifique.

Principe	SE simple	SE avancée	SE qualifiée
Identification	-	✔	✔
Intégrité	-	✔	✔
Non-discrimination	✔	✔	✔
Non-répudiation	-	✔	✔
Certification	-	-	✔

À RETENIR

- ✓ Plus le niveau de sécurité est élevé, plus la signature est fiable... mais aussi plus contraignante et coûteuse.
- ✓ Le choix du niveau de signature doit être adapté au contexte et au niveau de risque de votre document.

LE BON RÉFLEXE

Utilisez la fiche « quel type de signature choisir » pour vous aider, ainsi que l'arbre décisionnel à la page 13 du guide de référence.

3. Quel type de signature choisir ?

Le choix du niveau de signature (simple, avancé ou qualifié) dépend du niveau de risque et de l'importance du document. Plus le risque est élevé, plus le niveau de signature doit l'être également.

Pour évaluer le ou les risque(s), analysez les questions suivantes :

Le document a-t-il un effet juridique ?

Crée-t-il des droits ou des obligations ?

Non ▶ une **signature simple** est suffisante.

Oui ▼

Le document concerne-t-il ou implique-t-il des tiers ?

A-t-il un impact en dehors de votre organisation, implique-t-il une autre partie (personne, organisation, etc.) ?

Non ▶ optez pour une signature **simple** ou **avancée**.

Oui ▼

Y a-t-il un risque de recours ou de contestation ?

Le document pourrait-il être remis en cause ?

Non ▶ optez pour une **signature avancée** (si disponible).

Oui ▶ choisissez une **signature qualifiée.**

	Quand l'utiliser ?
SE simple	Documents internes, faible enjeu
SE avancée	Documents importants, risque modéré
SE qualifiée	Documents sensibles, risque élevé, exigence légale. *= Pouvoir prouver identité et intégrité.*

SE = signature électronique

À RETENIR

- ✓ Si une réglementation impose le type de signature, respectez-la.
- ✓ Une signature plus forte garantit plus de sécurité mais aussi plus de contraintes (coût, complexité).
- ✓ Une signature qualifiée n'est pas toujours le meilleur choix, elle doit être utilisée uniquement si nécessaire.

LE BON RÉFLEXE

Demandez-vous quels sont les risques si ce document est contesté, c'est ce qui détermine le bon niveau de signature.

4. Quelle est la durée de validité d'une signature électronique ?

Pouvez-vous signer électroniquement un document qui devra être archivé pendant plusieurs années ? La signature électronique a-t-elle une validité limitée dans le temps ?

La durée de validité d'une signature électronique ne dépend pas de la signature elle-même, mais de celle des éléments qui permettent de la vérifier :

- le certificat lié à la signature, qui doit être valable au moment de la signature ;
- la ou les preuve(s) d'intégrité du document : un horodatage fiable, le scellement, etc.

Une signature n'expire pas automatiquement, elle reste valable aussi longtemps que les preuves qui permettent de la valider sont conservées !

Un certificat de signature électronique a une durée de validité limitée dans temps. Une fois expiré, il n'est plus possible de créer de nouvelles signatures avec ce même certificat, mais les signatures déjà apposées restent valables tant que vous pouvez prouver :

- ✓ qu'elles ont été créées pendant la période de validité du certificat,
- ✓ que le document n'a pas été modifié.

L'important est donc que le certificat soit valable au moment de la signature.

Comment prolonger la durée de validité d'une signature ?

Pour garantir la validité sur plusieurs années ou décennies, on utilise souvent :

- l'horodatage qualifié ;
- l'archivage électronique qualifié (prévu par la loi belge du 21 juillet 2016).

Ces mécanismes permettent de maintenir la valeur probante même après l'expiration du certificat.

À RETENIR

- ✓ Une signature électronique n'a pas de durée de validité fixe. C'est le certificat qui expire, pas la signature apposée.
- ✓ Votre signature restera valable tant que vous pourrez prouver son authenticité et l'intégrité du document.

LE BON RÉFLEXE

Conservez toutes les preuves qui permettront de prouver la validité de votre signature au moment où elle a été faite. Consultez la fiche « Comment archiver un document signé électroniquement ? » pour plus d'informations !

5. Comment archiver un document signé électroniquement ?

Pour qu'un document signé électroniquement, particulièrement avec signature qualifiée, reste valable dans le temps, il doit être conservé dans de bonnes conditions afin d'éviter toute modification.

Les bons réflexes :

1. **Archivez l'original (numérique ou papier)** et évitez de multiplier des copies non maîtrisées :
   - L'impression d'un original numérique est une copie, de même que la numérisation d'un original au format papier. (sauf utilisation d'un service d'archivage qualifié.)
   - Un document hybride nécessitera de conserver les deux formats.
2. **Conservez les preuves** qui permettent la vérification : le document signé, la signature et les preuves techniques qui l'accompagnent (horodatage, certificat, etc.)
3. **Ne « cassez » pas la signature :** certaines opérations (ré-enregistrer, retransformer, « imprimer en PDF ») peuvent invalider les mécanismes de signature ou faire perdre des informations utiles à la preuve.
4. **Prévoyez la durée :** les délais de conservation proposés par la plupart des prestataires de signature électronique sont limités. Si cette durée est insuffisante, archivez les documents dans votre propre système d'archivage électronique.
5. **Pour conserver une signature électronique qualifiée**, utilisez un service d'archivage qualifié pour conserver la valeur juridique de la signature.

Si vous souhaitez prolonger la durée de validité d'une signature électronique qualifiée :

- **L'archivage électronique à valeur probatoire :** système de stockage permettant de garder un document numérique comme preuve fiable dans le temps, comme un « coffre-fort » numérique certifié.
- **La sur-signature** : ajouter une nouvelle signature ou un nouvel horodatage permet de maintenir la preuve dans le temps.

Prestataires régionaux

Deux prestataires sont en charge de conserver tant les documents papier que les documents électroniques des administrations.

Au niveau régional :
ConnectMemory, le Service régional des Archives
✉ **connectmemory@sprb.brussels**

Au niveau local/communal :
Archives générales du Royaume
✉ **archives.generales@arch.be**

À RETENIR

- ✓ Un document signé électroniquement comprend : le document + la signature + les preuves de la signature.
- ✓ Un bon archivage est indispensable pour conserver la valeur juridique de votre document.

LE BON RÉFLEXE

Posez-vous toujours la question : serai-je capable de prouver la validité du document dans 5 ou 10 ans ?

6. Quel outil technologique utiliser ?

Il existe de nombreux outils dédiés à la signature électronique. Par souci de neutralité technologique et parce que les besoins varient d'une administration à l'autre, cette fiche ne privilégie aucun outil en particulier. Le choix dépendra de vos besoins, que cette checklist vous aidera à identifier.

Besoins

- ☐ Quels types de documents devez-vous signer ?
- ☐ Qui doit signer (interne ou externe) ?
- ☐ Quels sont les niveaux de signature requis pour les différents types de documents?

Fonctionnalités

- ☐ La solution permet-elle les différents niveaux de signature requis par le règlement eIDAS ?
- ☐ Est-elle compatible avec vos outils internes ?
- ☐ Est-elle compatible avec d'autres fournisseurs d'identité numérique (ex: itsme®) ?
- ☐ Permet-elle de signer et/ou de charger des documents par lot ?
- ☐ Faut-il parcourir toutes les pages ou tous les documents avant de signer ?
- ☐ Permet-elle de gérer un flux de signature (ordre des signataires, modification en cas d'absence, etc.) ?
- ☐ Est-elle utilisable sur mobile ?
- ☐ Permet-elle l'intégration avec d'autres systèmes (API) ?
- ☐ Est-elle personnalisable ?

Expérience utilisateur

- ☐ La solution est-elle simple à utiliser ?
- ☐ Permet-elle à des personnes externes de signer facilement ?
- ☐ Offre-t-elle un helpdesk ?

Sécurité et conformité

- ☐ La solution respecte-t-elle le RGPD[1] ?
- ☐ Garantit-elle l'identification, l'intégrité et la traçabilité ?

Archivage

- ☐ La solution prévoit-elle un archivage adapté ?
- ☐ Pendant combien de temps les documents sont-ils conservés ?
- ☐ Permet-elle d'utiliser des API avec vos systèmes d'archivages internes ?

Organisation & coûts

- ☐ Les coûts sont-ils clairement identifiés ?
- ☐ La solution nécessite-t-elle une formation du personnel ?

À RETENIR

- ✓ La solution retenue doit répondre à vos besoins internes, qu'il convient d'identifier.
- ✓ Le bon outil doit vous garantir la preuve de la signature ainsi que la sécurité de vos documents.
- ✓ Avant de digitaliser une procédure existante, assurez-vous qu'elle corresponde au mieux aux attentes et besoins des usagers. easy.brussels peut vous y aider.

LE BON RÉFLEXE

Définissez d'abord vos besoins avant de choisir un outil adapté. Renseignez-vous auprès d'institutions similaires à la vôtre pour connaître leurs retours et expériences.

1 - Règlement Général sur la Protection des Données : réglementation européenne qui encadre le traitement et la libre circulation des données personnelles.

7. Envoi et impression d'un document signé électroniquement

Lorsqu'un document est signé avec une signature électronique qualifiée, un certificat y est automatiquement associé. Selon le logiciel utilisé, une mention visuelle apparaît sur le document (par exemple : une image, un texte « Signé (eID) le xx-xx-xx par Xavier Dupont »). Cette mention n'a pas de valeur légale en elle-même, mais elle permet d'accéder au certificat, en un simple clic.

Peut-on envoyer un document signé électroniquement par e-mail, via eBox, ou tout autre canal digital ?

Oui. Tant que le document reste au format électronique, la signature qualifiée suit et reste liée au document. Sa valeur légale reste inchangée car le certificat peut toujours être téléchargé pour vérification.

Peut-on imprimer un document signé électroniquement ?

Si votre document signé électroniquement doit être imprimé (*par exemple si le destinataire n'a pas donné son consentement pour recevoir du courrier via eBox*), **la mention « Signé le xx par xx » restera visible mais perdra sa valeur légale, puisque non cliquable.** Il ne sera plus possible de télécharger le certificat lié, retracer la signature en ligne afin d'en vérifier la validité (qui a signé et quand ?), ou prouver que le document n'a pas été modifié.

Un document signé électroniquement puis imprimé est légalement considéré comme une « copie ». L'original reste le format électronique.

Pour conserver la validité de votre signature, vous pouvez :

- ✓ **Apposez un lien de téléchargement** du document en bas de page (lien de vérification) et précisez le délai de disponibilité. Ce lien de vérification est en général prévu par les applications ou plateformes dédiées. Prévoyez un délai suffisant pour permettre au destinataire de consulter ou télécharger son document.
- ✓ Donnez au destinataire la possibilité de contacter l'administration pour **obtenir ou consulter une copie du document original.**
- ✓ À défaut, si votre solution technologique n'offre pas la possibilité de vérifier ou télécharger le document en ligne, ajoutez une **mention plus générique** telle que : « *la signature de ce document a été certifiée par notre administration via un dispositif reconnu par le SPF BOSA* ».

À RETENIR

- ✓ Une signature électronique doit pouvoir être retracée en ligne pour rester valable.

LE BON RÉFLEXE

Prévoyez toujours un lien de consultation et/ou de téléchargement sur le document original, ou une mention informant que l'original est disponible sur demande.

8. Signatures multiples

Le concept de signature multiple comprend le fait de signer plusieurs pages par un même signataire, ou de signer un même document par plusieurs personnes.

Faut-il signer ou parapher toutes les pages d'un document ?

Non. Une seule signature, quel que soit son niveau, suffit pour engager le signataire sur l'ensemble d'un même document, peu importe sa longueur. Inutile donc de parapher ou signer chaque page !

Un même document peut-il être signé par plusieurs personnes ?

Oui. Pour garantir la validité de l'ensemble des signatures, il est recommandé d'intégrer tous les signataires dans un même processus de signature. Les solutions de signature électronique permettent généralement d'ajouter plusieurs signataires, de définir l'ordre de signature, de suivre l'avancement du processus et de garantir la validité juridique de chaque signature.

Avant l'envoi du document, il est utile de définir :

- ✓ Les signataires : nom, prénom, adresse e-mail et rôle (signataire, observateur, approbateur) ;
- ✓ l'ordre de signature :
  - séquentiel : A signe, puis B, puis C... idéal pour des contrats par exemples,
  - en parallèle : tout le monde peut signer dès la réception du document... idéal pour les documents internes ;
- ✓ les zones à compléter ou à signer ;
- ✓ les méthodes d'authentification.

Attention : toute modification ou réintroduction d'un document déjà signé invalide les signatures existantes.

Lorsque plusieurs personnes ne peuvent pas signer dans le même processus, chacune signe sa propre version, à conserver avec les autres.

Les mentions de signature ne sont qu'indicatives ! Seul le certificat de signature possède une valeur juridique.

À RETENIR

- ✓ Une seule signature suffit pour engager le signataire sur l'ensemble du document.
- ✓ Il est tout à fait possible de faire signer électroniquement un même document par plusieurs personnes.

LE BON RÉFLEXE

Posez-vous les bonnes questions : qui doit signer votre document ? L'ordre des signatures est-il important ?

9. Signature par lots

Pour gagner du temps, il est possible de signer électroniquement plusieurs documents à la fois. Selon la solution de signature électronique utilisée, il est possible de :

Signer plusieurs documents en une seule opération (signature par lots)

Certains logiciels permettent d'apposer automatiquement une signature électronique certifiée sur plusieurs documents simultanément. Le signataire ne validera qu'une seule fois l'opération via son certificat, sa carte eID ou son token.

Même si l'utilisateur ne signe qu'une fois, le système génère autant de signatures numériques que de documents :

- ✓ chaque document reçoit une empreinte numérique unique (hash) qui garantit l'intégrité du document) ;
- ✓ chaque empreinte contient le certificat du signataire (identification du signataire) ;
- ✓ chaque fichier devient indépendamment vérifiable (non-répudiation).

Chaque document est signé séparément, avec une signature juridiquement valable.

✗ On ne signe jamais un fichier .zip !

Signer un fichier .zip ne donne aucune valeur juridique aux documents qu'il contient. Un fichier .zip est comparable à une enveloppe contenant plusieurs documents : apposer une signature sur l'enveloppe ne signifie pas que l'on a signé les documents qu'elle renferme.

Signer plusieurs documents dans une même session de manière séquentielle.

Certains logiciels permettent de signer plusieurs documents consécutivement : après avoir signé un premier document, la plateforme propose automatiquement le suivant.

Regrouper plusieurs documents dans une seule demande de signature.

Des solutions permettent d'envoyer une seule demande contenant plusieurs documents à signer. Les signataires peuvent alors parcourir et signer tous les documents dans un flux unique.

À RETENIR

- ✓ La signature par lots permet, en une seule action du signataire, d'appliquer automatiquement la signature à plusieurs documents. Tout dépend de la solution technologique utilisée.
- ✓ Lors d'une signature par lots, chaque document est signé et vérifiable individuellement.
- ✓ Ne signez jamais un fichier .zip : il s'agit d'un conteneur, pas du document final.

LE BON RÉFLEXE

Chaque solution de signature électronique a ses propres caractéristiques. Vérifiez ce que vous offre celle dont vous disposez.

10. Puis-je modifier un document après signature ? (contenu ou horodatage)

Puis-je modifier le contenu d'un document après signature ?

Non. Même si la modification du contenu est techniquement possible, **cela invaliderait la signature** (avancée ou qualifiée), car :

- ✓ le lien cryptographique entre la signature et le document serait rompu ;
- ✓ les outils de vérification indiqueront que le document a été modifié après signature.

L'un des rôles de la signature électronique est de garantir l'intégrité du document, donc de démontrer qu'il n'a pas été modifié après sa signature.

Si une modification est nécessaire après la signature, certains formats (notamment les PDF), permettent l'ajout d'une nouvelle signature électronique, d'un horodatage ou d'annotations sans remettre en cause les signatures précédentes. Vérifiez donc si le format et le processus de signature vous autorise cette modification.

Puis-je adapter l'horodatage de la signature électronique ?

Non. Dans un système de signature électronique correctement mis en œuvre, l'horodatage ne peut pas être modifié sans que cela soit détecté.

L'horodatage est intégré à la signature et est lié à une empreinte (hachage) du document à un instant précis.

Le modifier impliquerait d'adapter les données signées et donc de ne plus pouvoir garantir l'intégrité du document.

La signature deviendrait alors invalide.

Si un nouvel horodatage est nécessaire (par exemple pour prolonger la valeur probante d'une signature ou lors d'un archivage électronique), il est ajouté au document sans remplacer l'horodatage d'origine. L'horodatage d'origine n'est pas modifié ; un horodatage supplémentaire est ajouté et la trace de cette opération est conservée.

À RETENIR

- ✓ Modifier le contenu d'un document signé électroniquement rendra invalide la signature.
- ✓ Toute modification de l'horodatage invalidera également la signature électronique.

LE BON RÉFLEXE

Si le contenu doit être modifié après la signature (erreur, ajout d'information, etc.) :

- créez une nouvelle version du document,
- faites signer cette nouvelle version,
- conservez l'ancienne version signée à titre de preuve ou pour l'archivage.

LEXIQUE

LEXIQUE

Acte administratif : décision, document ou mesure pris par une autorité administrative dans l'exercice de ses missions de service public et produisant des effets juridiques à l'égard d'une ou plusieurs personnes (par exemple : autorisation, permis, décision d'octroi ou de refus d'une prime, etc.)

Acte authentique : document rédigé ou validé par un officier public (notaire, officier d'état civil...) dans le cadre de ses compétences légales. Il bénéficie d'une force probante renforcée : son contenu fait foi jusqu'à inscription de faux, et sa date est certaine. Lorsqu'il est signé électroniquement, les exigences légales propres sont applicables.

Acte juridique : manifestation de volonté destinée à produire des effets juridiques, tels que la création, la modification, la transmission ou l'extinction de droits et d'obligations (par exemple : signature d'un contrat, procuration, acte administratif pris par une administration, etc.)

Adresse IP (Internet Protocol) : identifiant numérique attribué à un appareil connecté à un réseau utilisant le protocole Internet. Elle permet d'identifier l'appareil et de l'acheminer lors des échanges de données sur Internet ou sur un réseau privé. Par exemple, lorsqu'un utilisateur signe un document en ligne, son adresse IP peut être enregistrée dans les journaux de preuve de l'opération.

Analyse de risque : processus consistant à identifier, évaluer et hiérarchiser les risques susceptibles d'affecter un système, un processus ou une activité, afin de déterminer les mesures appropriées pour les prévenir, les réduire ou les gérer. Par exemple : réaliser une analyse de risque avant de mettre en place une solution de signature électronique afin d'évaluer les risques de contestation de signature.

Antidatage : action consistant à attribuer à un document, un acte ou une signature une date antérieure à sa date réelle de création, de signature ou de validation. Par exemple, si une personne signe un document le 15 mars mais indique volontairement la date du 1er mars afin de faire croire que la signature est intervenue plus tôt.

API (Application Programming Interface) : ensemble de règles, de protocoles et de fonctions permettant à différentes applications ou systèmes informatiques de communiquer entre eux et d'échanger des données de manière automatisée. Par exemple, une plateforme de signature électronique peut utiliser une API pour recevoir automatiquement des documents à signer depuis une application métier, ou une administration peut intégrer un service de signature électronique à son système de gestion documentaire grâce à une API.

Archivage : action de conserver, d'organiser et de protéger des documents ou des données pendant une durée déterminée, afin de garantir leur disponibilité, leur intégrité, leur lisibilité et, le cas échéant, leur valeur probante dans le temps.

Archivage électronique à valeur probatoire : dispositif d'archivage conçu pour conserver des documents électroniques de manière à maintenir leur valeur juridique dans le temps.

Authenticité en matière de conservation : garantie qu'un document conservé est bien celui qui a été créé, reçu ou signé à l'origine, et qu'il peut être attribué de manière fiable à son auteur ou à son émetteur tout au long de sa durée de conservation.

Authentification : processus qui permet de vérifier que la personne est bien celle qu'elle prétend être.

Batch signing (signature par lots) : procédé permettant de signer électroniquement plusieurs documents en une seule opération, sans devoir effectuer une action de signature distincte pour chaque document.

Bruxelles Numérique : cadre réglementaire de la Région de Bruxelles-Capitale visant à encadrer la transition numérique des administrations publiques, à développer les services publics numériques et à garantir leur accessibilité, leur inclusivité et leur disponibilité pour l'ensemble des usagers.

Cachet électronique : équivalent numérique du tampon d'une organisation. Il permet à une entreprise ou une administration d'authentifier un document, comme une signature électronique mais pour une personne morale.

Carte d'identité belge (eID) : carte d'identité électronique officielle délivrée par les autorités belges. Elle permet de prouver l'identité de son titulaire, aussi bien en personne qu'en ligne, grâce à une puce électronique contenant des certificats numériques.

Certificat électronique : sorte de "carte d'identité numérique" utilisée pour signer électroniquement. Il permet de vérifier l'identité du signataire et de sécuriser la signature.

Certificat qualifié : certificat utilisé pour les signatures qualifiées, délivré par un prestataire qualifié,agréé par le SPF Economie ou au sein de l'UE.

Certification : procédure par laquelle un organisme compétent atteste qu'une personne, un produit, un service, un système ou un processus respecte des exigences, des normes ou des critères définis.

Clé privée du signataire : donnée cryptographique confidentielle détenue exclusivement par le signataire et utilisée pour créer une signature électronique. Elle est associée à une clé publique correspondante et permet d'établir un lien fiable entre le signataire et le document signé. Lorsqu'un utilisateur signe électroniquement un document, sa clé privée est utilisée pour générer la signature électronique. La clé privée peut être conservée dans une eID, un token cryptographique, un dispositif sécurisé de création de signature ou une infrastructure de signature à distance sécurisée. Seul le titulaire légitime de la clé privée est censé pouvoir l'utiliser.

Clé publique : donnée cryptographique associée à une clé privée, utilisée pour vérifier une signature électronique ou pour chiffrer des données. Elle peut être communiquée à des tiers sans compromettre la sécurité du système.

Clic : action réalisée par un utilisateur consistant à appuyer sur un bouton d'une souris, à toucher un élément d'une interface numérique ou à sélectionner une commande afin d'exécuter une action dans un système informatique. Par exemple, un utilisateur clique sur le bouton «Signer» pour lancer le processus de signature électronique.

Contentieux civil : ensemble des litiges relevant du droit civil et soumis aux juridictions civiles. Il concerne principalement les différends entre personnes physiques ou morales portant sur des droits et obligations de nature privée, tels que les contrats, la responsabilité civile ou les relations patrimoniales. Par exemple, une partie remet en cause l'authenticité d'un document produit comme preuve devant un tribunal

Contentieux pénal : ensemble des procédures et des litiges relatifs à des infractions prévues par la loi pénale et poursuivies devant les juridictions répressives. Il vise à déterminer si une infraction a été commise, à identifier son auteur et, le cas échéant, à prononcer une sanction. Par exemple, une personne falsifie un document signé électroniquement afin de tromper un tiers.

Contresigner : action consistant pour une personne à apposer sa signature sur un document déjà signé par une autre personne, afin de confirmer, d'approuver, d'attester ou de valider l'acte dans le cadre de ses compétences ou responsabilités.

Contreseing ou contre-signature : signature apposée par une seconde personne, généralement habilitée, pour valider, confirmer ou authentifier la première signature. Elle engage la responsabilité du contre signataire et renforce la valeur juridique du document.

Cryptographie : ensemble des techniques mathématiques et informatiques permettant de protéger des informations en garantissant leur confidentialité, leur intégrité, leur authenticité et, dans certains cas, leur non-répudiation. Par exemple, lorsqu'un document est signé électroniquement, des mécanismes cryptographiques sont utilisés pour créer et vérifier la signature.

Délégation de signature : acte par lequel une autorité habilitée autorise une autre personne à signer, en son nom et dans des limites déterminées, certains documents, actes ou décisions relevant de ses compétences.

Digitalisation : processus consistant à utiliser les technologies numériques pour transformer, simplifier ou automatiser des activités, des processus, des services ou des documents auparavant gérés de manière non numérique ou partiellement numérique. Par exemple, une administration remplace un formulaire papier par un formulaire en ligne.

eIDAS : acronyme de « electronic IDentification, Authentication and Trust Services ». Il s'agit du règlement européen qui établit un cadre juridique commun pour l'identification électronique et les services de confiance au sein de l'Union européenne. Il vise à garantir la sécurité, la fiabilité et la reconnaissance transfrontalière des transactions électroniques.

Enveloppe de signature : fichier technique qui contient le document signé et les preuves associées.

Empreinte numérique (hash) : valeur unique générée à partir d'un document grâce à un algorithme cryptographique. Elle permet de vérifier l'intégrité d'un document : si le document est modifié, l'empreinte l'est également.

Faux en écriture : infraction consistant à altérer la vérité dans un écrit, un document ou un acte, par création, modification, falsification ou usage de fausses informations, dans l'intention de produire des effets juridiques ou de tromper autrui. Par exemple, modifier le contenu d'un contrat après sa signature sans l'accord des parties.

Force juridique : aptitude d'un acte, d'un document ou d'un élément de preuve à produire des effets de droit, à être reconnu par l'ordre juridique et à pouvoir être invoqué dans un cadre administratif, contractuel ou judiciaire.

Force (valeur) probante : capacité d'un document, d'un acte ou d'un élément de preuve à démontrer un fait ou une situation et à être reconnu comme preuve fiable dans un cadre administratif ou judiciaire.

Hachage (ou empreinte numérique) : technique permettant de créer une empreinte numérique unique à partir d'un document afin de vérifier qu'il n'a pas été modifié. Par exemple, avant de créer une signature électronique, le système calcule l'empreinte du document à signer. Si un seul caractère est modifié dans le document après la signature, la valeur de hachage change, ce qui permet de détecter l'altération.

Horloge de confiance : source officielle utilisée pour donner une date et une heure fiables, principalement pour l'horodatage.

Horodatage : système qui associe une date (et parfois une heure) à un document pour prouver qu'il existait à ce moment précis et qu'il n'a pas été modifié depuis.

Horodatage qualifié : mécanisme d'horodatage certifié qui permet de prouver de manière fiable à quelle date et à quelle heure un document électronique existait ou a été signé.

Identité du signataire : ensemble des informations permettant d'identifier de manière fiable la personne physique ou morale qui a apposé une signature sur un document.

Identité numérique : ensemble de données et moyens électroniques permettant d'identifier de manière fiable une personne dans un environnement numérique.

Inclusion : principe visant à garantir que toutes les personnes, quelles que soient leurs capacités, leur situation sociale, leur âge, leur niveau de compétences ou leur maîtrise des outils numériques, puissent accéder aux services, participer aux démarches et exercer leurs droits dans des conditions équitables.

Intégrité : garantie qu'un document n'a subi aucune modification depuis sa création ou sa signature. Dans le cadre de la signature électronique, l'intégrité d'un document est assurée par des mécanismes de cryptographie qui rendent toute altération détectable.

itsme® : application mobile permettant de prouver son identité, de se connecter à des services en ligne et de signer des documents électroniques de manière sécurisée.

Journal d'audit : historique technique qui prouve comment et quand la signature a été réalisée.

Journal de logs : ensemble des enregistrements chronologiques générés automatiquement par un système informatique afin de conserver la trace des événements, actions et opérations qui y sont réalisés.

Lien de téléchargement : adresse ou hyperlien permettant d'accéder à un fichier électronique afin de le consulter, de le récupérer ou de l'enregistrer sur un appareil.

Lien de consultation : adresse ou hyperlien permettant à une personne autorisée d'accéder à un document électronique afin de le visualiser ou de le consulter, sans nécessairement pouvoir le modifier ou le télécharger.

Login : identifiant utilisé par une personne pour accéder à un système informatique, une application ou un service en ligne. Le login permet de reconnaître l'utilisateur et est généralement associé à un ou plusieurs mécanismes d'authentification, tels qu'un mot de passe, un code de sécurité ou une authentification multifacteur.

MFA (Multi-Factor Authentication ou authentification multifacteur) : mécanisme de sécurité qui consiste à vérifier l'identité d'un utilisateur au moyen d'au moins deux facteurs d'authentification de nature différente avant de lui accorder l'accès à un système ou à un service. Par exemple, un utilisateur qui se connecte à une plateforme de signature électronique à l'aide de son mot de passe (premier facteur), puis saisit un code reçu sur son téléphone mobile (deuxième facteur), ou l'utilisation de l'eID combinée à un code PIN.

myGov.be : application et portail numériques officiels du gouvernement fédéral belge permettant aux citoyens d'accéder à différents services publics en ligne, à leurs documents administratifs, à leur eBox et à certaines données personnelles au moyen d'une identification sécurisée.

Non-répudiation : une personne ne peut pas nier avoir réalisé une action, notamment une signature électronique. Des éléments techniques et juridiques permettent d'attribuer la signature à un signataire identifié et d'en démontrer la validité.

Non-discrimination : principe selon lequel un document, une signature ou une opération ne peut être refusé, déclaré irrecevable ou privé d'effet juridique au seul motif qu'il est sous forme électronique. Par exemple, un contrat ne peut pas être rejeté uniquement parce qu'il a été signé électroniquement plutôt que manuscritement.

Original : document ou acte dans sa version faisant foi, c'est-à-dire celle qui constitue la référence authentique et sur laquelle reposent les droits, obligations ou effets juridiques qui en découlent.

Opposabilité : période pendant laquelle un document peut servir de preuve.

OTP (one time password): code de sécurité à usage unique utilisé pour vérifier l'identité d'un utilisateur et renforcer la sécurité d'une opération électronique, telle qu'une signature électronique.

Paraphe : signe ou ensemble d'initiales apposé sur un document pour montrer qu'il a été lu, vérifié ou validé à une étape donnée.

Présomption de fiabilité : principe selon lequel un système ou un procédé est considéré comme fiable tant qu'il n'est pas démontré qu'il ne l'est pas.

Prestataire de services de confiance : acteur certifié et contrôlé, chargé de garantir la fiabilité, l'intégrité et la valeur juridique des services de confiance utilisés dans les démarches électroniques. En Belgique, ces prestataires doivent respecter le règlement eIDAS.

Prestataire qualifié : organisme officiellement reconnu qui fournit des services de confiance numériques, comme la signature électronique ou l'horodatage, en respectant les exigences du règlement eIDAS.

Reconnaissance juridique : fait, pour un document, un acte, une signature ou un procédé, d'être admis par le droit comme produisant des effets juridiques et pouvant être invoqué valablement devant une administration, une autorité ou une juridiction.

Recours : action permettant à une personne de demander la révision ou l'annulation d'une décision qu'elle conteste.

Responsabilité : obligation pour une personne physique ou morale de répondre de ses actes, de ses décisions ou de ses engagements, et d'en assumer les conséquences juridiques, administratives, civiles ou pénales.

Risque contentieux : risque qu'un acte, un document ou une décision fasse l'objet d'une contestation susceptible de donner lieu à une procédure administrative ou judiciaire.

Scellement : action consistant à protéger un document électronique au moyen d'un sceau afin de garantir son origine et de détecter toute modification ultérieure.

Signataire : personne physique ou, dans certains cas, représentant d'une personne morale, qui appose une signature sur un document afin de manifester son accord, son approbation, son engagement ou son intervention dans l'acte concerné.

Signature : marque apposée par une personne sur un document afin de manifester son identité, son consentement au contenu du document et, le cas échéant, son engagement à l'égard des effets juridiques qui en découlent.

Signature biométrique : type de signature électronique reposant sur la capture et l'analyse de caractéristiques comportementales du signataire lors de l'apposition de sa signature, telles que la vitesse d'écriture, la pression exercée, l'accélération, l'inclinaison du stylet ou le rythme du geste.

Signature électronique : procédé permettant de signer un document numérique afin d'identifier le signataire, de marquer son accord sur le contenu du document et de sécuriser celui-ci contre toute modification ultérieure.

Signature électronique simple : forme de signature électronique consistant en des données sous forme électronique utilisées par une personne pour manifester son accord sur un document ou une opération. Elle ne doit pas répondre aux exigences supplémentaires applicables aux signatures électroniques avancées ou qualifiées. Le règlement eIDAS la reconnaît comme le niveau le plus élémentaire de signature électronique.

Signature électronique avancée : signature électronique qui répond à des exigences spécifiques permettant d'établir un lien fiable avec le signataire. Elle doit être liée de manière univoque au signataire, permettre son identification, être créée à l'aide de données que le signataire peut utiliser sous son contrôle exclusif et être liée au document de telle sorte que toute modification ultérieure soit détectable.

Signature électronique qualifiée : signature électronique avancée créée au moyen d'un dispositif qualifié de création de signature électronique et reposant sur un certificat qualifié délivré par un prestataire de services de confiance qualifié. Elle constitue le niveau de signature électronique offrant les garanties les plus élevées prévues par le règlement eIDAS.

Signature en masse : procédé permettant de signer électroniquement un grand nombre de documents de manière automatisée ou semi-automatisée, sans devoir réaliser une opération de signature distincte pour chaque document.

Signature manuscrite : signature réalisée à la main sur un document papier pour identifier son auteur et marquer son accord sur son contenu.

Signatures multiples : apposition de plusieurs signatures sur un même document par différentes personnes.

Signature par lot : méthode permettant de signer plusieurs documents électroniques au moyen d'une seule opération de signature.

Sur signature : nouvelle signature ou un nouvel horodatage servant à prolonger la valeur juridique de la signature précédente ou de l'horodatage précédent.

Token : méthode permettant de signer plusieurs documents électroniques au moyen d'une seule opération de signature.

Valeur légale : effet reconnu par la loi à un document, une signature ou un acte, lui permettant de produire des conséquences juridiques.

Validation : action consistant à vérifier et à approuver un document, une information ou une étape d'un processus.

Visa : mention apposée sur un document pour attester qu'il a été vu, vérifié ou contrôlé par une personne habilitée. Le visa ne vaut pas signature : il confirme un examen, pas un engagement juridique.

Zip : format de fichier compressé permettant de regrouper un ou plusieurs fichiers dans une seule archive tout en réduisant leur taille afin de faciliter leur stockage, leur transmission ou leur téléchargement.