Signature électronique et bonnes pratiques

eSignFlow
signer autrement

Table des matières

Depuis la crise du Covid-19, **la transition digitale** au sein des administrations s'est encore accélérée, ce qui permet aux personnes de travailler de manière asynchrone.

Les services se multiplient et les flux de documents sont gérés plus efficacement, voire automatiquement dans certains cas.

Les e-guichets, qui connaissent un essor depuis 2020, en sont un bel exemple.

Ce contexte actuel a par ailleurs des répercussions très positives sur le fonctionnement interne des organisations. Comme les collaborateurs et les signataires peuvent travailler indépendamment du lieu et du temps, les processus décisionnels sont plus efficaces, ce qui se traduit par une prise de décision plus rapide.

La transition digitale présente donc des **avantages** indéniables, mais ce monde en mutation rapide engendre également davantage d'**incertitudes**. Toutes les administrations ne sont pas aussi bien informées quant aux différentes réglementations et conséquences juridiques relatives aux **signatures électroniques**.

Dans ce whitepaper, nous fournissons plus d'informations sur les différents types de signatures numériques, la différence entre une signature électronique et un cachet électronique, des précisions sur la manière de traiter les documents imprimés signés numériquement, ainsi qu'une checklist pour choisir la meilleure solution de signature.

Qu’est-ce qu’une signature en ligne ?

En pratique, on confond souvent trois termes différents : la signature **électronique**, la signature **numérique** et la signature **numérisée**.
Ces trois types de signatures ne sont pas identiques..

Signature électronique

Signature numérique

Signature numérisée

Qu’est-ce qu’une signature électronique ?

Le règlement eIDAS définit la signature électronique comme :

> **« des données sous forme électronique qui sont jointes ou liées logiquement à d’autres données sous forme électronique et qui sont utilisées par le signataire pour signer ».**

La signature électronique est constituée de données électroniques associées à certaines informations (également sous forme électronique). Par ailleurs, la signature électronique est un **concept juridique** qui équivaut à la signature manuscrite et qui a pour **but d’exprimer la volonté du signataire.**

Cela inclut donc toutes les formes possibles : une signature numérisée, une signature numérique (via eID, Itsme), un SMS, un e-mail, etc.

Il existe trois types de signatures électroniques :

- Signature électronique simple
- Signature électronique avancée
- Signature électronique qualifiée

Les différences entre ces trois types de signatures électroniques concernent principalement le **niveau de sécurité**, la garantie de **l'intégrité du document signé** et la capacité à **identifier le signataire**. Nous y reviendrons plus loin dans ce whitepaper.

Qu'est-ce qu'une signature numérique ?

Une signature numérique repose sur **l'application de techniques cryptographiques** au contenu d'un document. Cela permet d'offrir un niveau supplémentaire de sécurité et d'intégrité.

Cette méthode est utilisée pour les signatures électroniques **avancées** et **qualifiées**. On peut citer comme exemple la signature avec votre eID belge ou avec Itsme. Dans le cas d'une signature électronique simple, cette méthode n'est pas utilisée, ce qui lui confère par conséquent le niveau de sécurité le plus bas.

Qu'est-ce qu'une signature numérisée ?

Il s'agit simplement **d'une image d'une signature** au format jpg ou png, par exemple. Vous pouvez l'obtenir, par exemple, en scannant une signature. Cela vous permet d'utiliser la signature dans n'importe quel document par simple copier-coller.

Selon la législation européenne, il s'agit d'une signature électronique **simple**.

Quels sont les différents types de signatures électroniques et leurs effets juridiques ?

Dans le cadre de l'eIDAS, une signature électronique ne peut être déclarée **non valide** et **irrecevable** au seul motif qu'elle est électronique.

Le règlement reconnaît toutefois que, selon la technologie et la validation sous-jacentes à la signature, certains types de signatures sont intrinsèquement **plus fiables** que d'autres et résistent donc mieux à un examen juridique.

Cela signifie qu'elles peuvent être associées de manière fiable à la personne qui a signé le document, qu'elles peuvent protéger l'intégrité du document et qu'elles peuvent avoir les mêmes effets juridiques qu'une signature manuscrite.

La signature électronique simple

eiDAS la définit comme :

> **« des données sous forme électronique qui sont jointes à d'autres données sous forme électronique ou qui y sont logiquement associées, et qui sont utilisées par le signataire pour signer ».**

Et comme :

> **« des données sous forme électronique qui sont jointes ou liées logiquement à d'autres données sous forme électronique et qui sont utilisées pour garantir leur origine et leur intégrité ».**

Si l'on prend cette définition au pied de la lettre, il est possible de signer un document en scannant sa signature ou en cochant une case dans un document ouvert sur l'appareil de son choix. Techniquement parlant, il s'agit de données sous forme électronique, associées à un document.

Avec ce type de signature, il n'y a toutefois **aucune certitude** que le contenu du document n'ait pas été falsifié, ni aucune preuve que la « signature » ne soit pas un faux (c'est-à-dire que nous ne pouvons pas être sûr, par exemple, de l'identité de la personne qui a effectivement coché la case pour confirmer les conditions).

- Ce type de signature peut être utilisé à de nombreuses fins, mais il est important de garder à l'esprit qu'il ne garantit ni l'intégrité ni l'authenticité d'un document. Il bénéficie toutefois du principe de non-discrimination.
- Le juge doit examiner la signature, mais n'est pas tenu de lui attribuer automatiquement les mêmes effets qu'à une signature manuscrite. Il ne le fera que s'il constate que ce mécanisme, après en avoir vérifié la fiabilité, permet d'identifier de manière raisonnable le signataire et de déterminer l'expression de sa volonté véritable.

EN PRATIQUE

- On parle de tout type d'élément numérique attestant de l'acceptation ou de l'approbation par le signataire au moyen d'un certificat. Il peut s'agir d'une signature apposée manuellement sur un écran (et enregistrée numériquement), d'un clic sur un bouton « J'accepte », d'une signature électronique, d'une numérisation d'une signature manuscrite, etc.

- Se connecter via Active Directory, puis cliquer sur le bouton « Confirmer ».
- Se connecter via eID ou Itsme, puis cliquer sur le bouton « Confirmer ».
- Saisir son nom d'utilisateur et son mot de passe, puis cliquer sur le bouton « Confirmer ».

La signature électronique avancée

Celle-ci offre **un niveau de sécurité supérieur** à celui de la signature électronique simple : elle garantit que l'identité du signataire peut être établie avec certitude, tout en réduisant considérablement le risque de contrefaçon et d'usurpation d'identité.

Pour être considérée comme une signature électronique avancée, les conditions suivantes doivent être remplies :

- elle est liée de manière unique au signataire ;
- elle permet d'identifier le signataire ;
- elle est générée à l'aide de données de création de signatures électroniques
- que le signataire peut utiliser, avec un niveau de confiance élevé, sous son contrôle exclusif ;
- elle est liée aux données ainsi signées de telle manière que toute modification ultérieure des données puisse être détectée.

L'utilisation de signatures numériques basées sur une infrastructure à clé publique (PKI - Public Key Infrastructure) répond à toutes les exigences ci-dessus. Consultez la partie « Comment fonctionne une signature électronique ? » pour plus d'informations à ce sujet.
Étant donné que le signataire est le seul détenteur de la clé privée utilisée pour apposer la signature, vous avez la certitude que le signataire est bien la personne qu'il prétend être.
Lorsqu'une personne ouvre le document signé, du moins lorsqu'il s'agit d'un PDF signé, des contrôles automatiques sont effectués pour vérifier l'identité du signataire et détecter d'éventuelles modifications apportées au document après la signature.

À RETENIR

- L'intégrité et l'authenticité sont toutes deux garanties dès lors que les exigences relatives à la signature électronique avancée sont respectées.
  Une signature électronique avancée ne peut être rejetée sur le plan juridique au seul motif qu'elle se présente sous forme électronique, ce qui signifie que les signatures électroniques avancées correctement exécutées ont la même valeur qu'une signature manuscrite traditionnelle (voire davantage).
  Toutefois, si la validité des signatures électroniques avancées est remise en cause, la charge de la preuve que tous les critères nécessaires sont remplis incombe à la partie signataire.

EN PRATIQUE

- Les exemples repris ci-dessus pour une signature électronique simple sont les mêmes MAIS si le processus garantit l'authenticité de la signature, il peut s'agir d'une signature électronique avancée. Le processus par lequel la signature est créée est donc **très important**.

BON À SAVOIR :

- Lorsque vous utilisez cette fonctionnalité dans eSignFlow, vous n'avez pas à vous soucier de la charge de la preuve. Pour chaque signature effectuée à l'aide d'un certificat avancé, nous fournissons un **rapport de preuve**. Vous disposez ainsi immédiatement de la documentation nécessaire si quelqu'un venait à contester la signature.

La signature électronique qualifiée

La législation européenne la définit comme :

> **« une signature électronique avancée qui a été créée à l'aide d'un dispositif qualifié de création de signatures électroniques et qui repose sur un certificat qualifié pour les signatures électroniques ».**

Les exigences relatives aux dispositifs qualifiés pour la création de signatures électroniques sont donc beaucoup plus strictes. Elles sont énumérées à l'annexe II du règlement eIDAS. Concrètement, il s'agit de logiciels (pour la cryptographie, par exemple) et/ou de matériel (une carte à puce, par exemple), configurés pour créer une signature électronique. Celle-ci est assimilée à la signature manuscrite et a donc les mêmes effets juridiques.

À RETENIR

- Les États membres de l'UE sont tenus de reconnaître la validité d'une signature électronique qualifiée créée à l'aide d'un certificat qualifié délivré par un autre État membre. En outre, une signature électronique qualifiée est considérée comme l'équivalent juridique de la signature manuscrite traditionnelle, sauf s'il existe des raisons de soupçonner un usage abusif des certificats sous-jacents. La charge de la preuve incombe à la partie qui conteste la validité de la signature qualifiée.

EN PRATIQUE

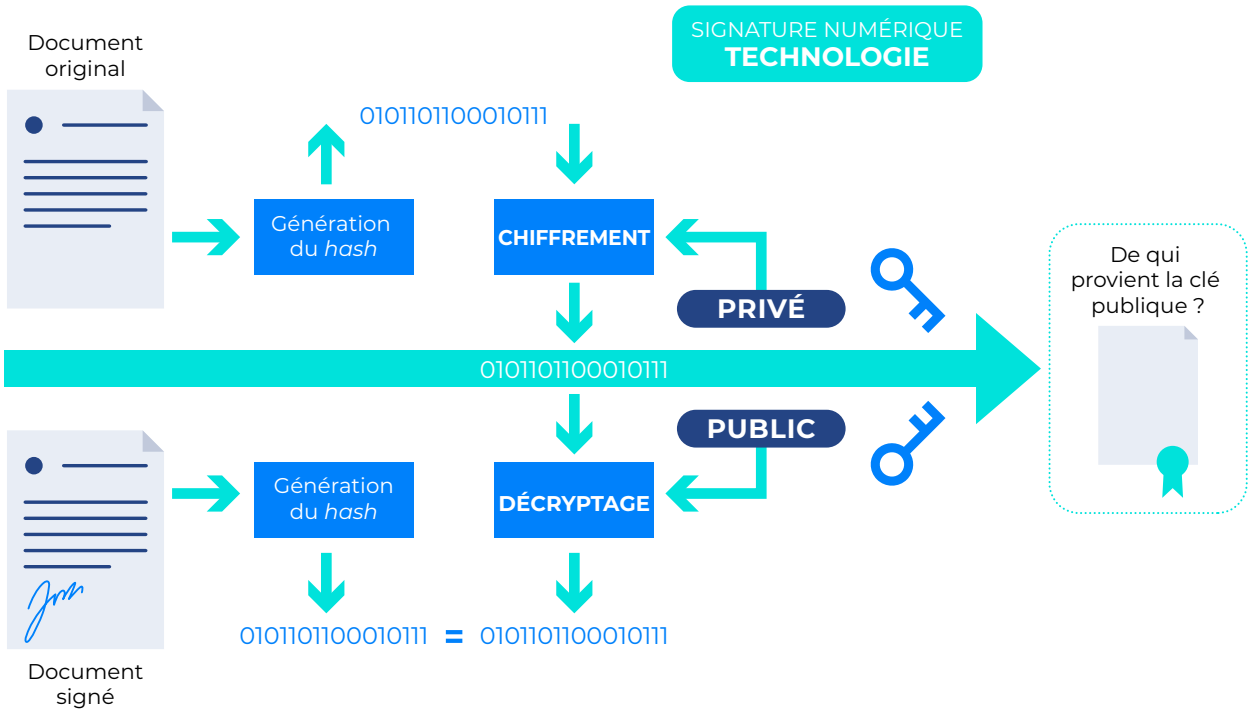
- Quand parle-t-on de signature qualifiée ? Quand vous signez un document avec votre eID belge ou Itsme.

Comment fonctionne la signature électronique ?

Une signature électronique fonctionne selon **un protocole appelé PKI** (acronyme de Public Key Infrastructure), une technique de chiffrement qui utilise des clés publiques et privées à des fins d'identification et d'authentification. Les certificats de clé publique, souvent appelés certificats numériques, ne sont délivrés qu'après une vérification approfondie de votre identité par un tiers de confiance, appelé autorité de certification (ou CA). Chaque certificat contient des informations importantes telles que l'identité de l'émetteur du certificat, la date de création et la durée de validité.

Ce qui rend une signature numérique plus sûre qu'une simple signature électronique, c'est le fait qu'elle est associée à **un certificat numérique**, ce qui permet de garantir et de prouver que la signature a bien été apposée par la personne à laquelle le certificat a été délivré.

Les certificats numériques, et les signatures qui en découlent, sont propres à chaque personne et pratiquement impossibles à falsifier. L'eID belge en est un excellent exemple.



Le cachet électroniquel

Le cachet électronique a été créé pour garantir le lien entre **les données électroniques** scellées et **une personne morale**.
Il sert donc de **preuve** qu'un document électronique a été émis par une personne morale, en garantissant l'origine et l'intégrité du document

Les cachets électroniques sont comparables aux signatures électroniques, mais la différence réside dans **l'identité** qui se cache derrière. Un cachet garantit **l'intégrité** et **l'authenticité** de la même manière qu'une signature électronique le ferait, mais au lieu d'un particulier, c'est une personne morale qui remplace le signataire.

La nécessité d'en utiliser un dépend du fait que vous signiez en tant que particulier ou en tant qu'entité juridique. Les cachets sont généralement plus adaptés aux besoins de signature automatisés ou à grande échelle.

Quelle est la différence entre une signature électronique et un cachet électronique ?

Le cachet électronique se distingue de la signature électronique principalement en ce que cette dernière (selon le règlement) est réservée aux **personnes physiques**, tandis que le cachet est destiné aux **personnes morales**.

Le règlement stipule que la signature électronique est utilisée par une personne physique « pour signer » (articles 3.9 et 3.10 du règlement eIDAS). Elle peut donc « engager » cette personne. Le règlement ne prévoit en revanche pas que le cachet électronique puisse en soi engager juridiquement une personne morale. L'article 3.25 stipule que le cachet électronique sert « à garantir l'origine et l'intégrité des données scellées ».

Chaque État membre reste toutefois libre de prévoir, au niveau national, que l'utilisation de la signature électronique peut engager directement la personne morale sur le plan juridique. La Belgique a inscrit cette possibilité dans la loi du 21 juillet 2016.

Les différentes possibilités de cachet

Un cachet **peut être demandé** pour une organisation (par exemple, la Ville de Bruxelles) ou pour une entité d'une organisation (par exemple, le service environnement de la Ville de Bruxelles) mais **pas** pour une fonction (par exemple, bourgmestre).

Ville de Bruxelles

Service environnement

Bourgmestre

Quels sont les différents types de cachets électroniques et leurs effets juridiques ?

Une signature électronique peut être soit avancée, soit qualifiée. Les deux sont émises par **une autorité de certification** (CA). Nous vous renvoyons à la partie « Comment fonctionne une signature électronique ? » pour plus d'informations à ce sujet.

En ce qui concerne les effets juridiques, ceux-ci sont identiques à ceux d'une signature électronique.

Qu'en est-il d'un document imprimé et signé numériquement ?

Un document imprimé n'est pas un document signé numériquement ayant force de loi. Vous devez le considérer comme une **copie non équivalente** sur le plan juridique de l'original. Cela est logique, puisque la signature numérique est en fait un calcul mathématique qui ne peut être reproduit sur papier.

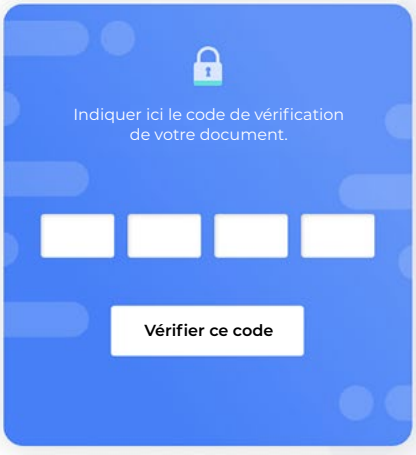
Il existe toutefois des moyens de considérer les documents imprimés comme ayant une valeur juridique. Pour ce faire, il faut pouvoir établir un lien entre le document imprimé et le document signé numériquement. Cela est possible grâce à **un code imprimable** ou à **un QR code**. De cette manière, il est possible de vérifier si la copie est conforme à l'original.

Comment eSignFlow résout-il cela ?

eSignFlow est une **plateforme de signature numériqu**e qui assure, au sein de votre organisation, la signature numérique juridiquement valable aussi bien des documents papier (numérisés) que des documents numériques.

Les documents signés numériquement restent **valides même après impression**, grâce au code de vérification unique attribué à chaque document signé numériquement. À l'aide de ce code, le document signé électroniquement de manière authentique peut être rouvert et vérifié en ligne. Vous avez ainsi la certitude que le document imprimé correspond au document signé numériquement.

D'un point de vue juridique, une signature électronique qualifiée est apposée sur une version PDF/A d'un document. Cette signature numérique est, en vertu de la loi, **assimilée à une signature sur papier.**



Pourquoi tombez-vous sur cette page ?

Vous vous retrouvez sur cette page web car vous avez très probablement en votre possession un document qui a été signé et sécurisé avec eSignFlow.

Celui qui reçoit des documents d'eSignFlow par mail peut dormir sur ses deux oreilles. C'est aussi le cas si vous les imprimer, les documents restent juridiquement valides.

Vérifier

Avec le **code unique** disponible sur le document que vous avez reçu, vous pouvez le vérifier et, si vous le souhaitez, récupérer à nouveau le document original. Il se peut que vos données d'identification soient encore demandées (par exemple via eID) avant de vous donner accès au document.

Besoin d'aide ?

Contactez-nous par mail via helpdesk@esignflow.be ou par téléphone au 023 082 838.

Checklist pour choisir une solution de signature

Retrouvez-ci dessous notre checklist élaborée rien que pour vous. Elle vous aide à sélectionner la solution de signature électronique la plus adaptée à vos besoins et à ceux de votre organisation.

Juridique

1

- ◯ La solution de signature est-elle conforme à la directive eIDAS ?
- ◯ La solution de signature est-elle conforme au RGPD ?
- ◯ Un contrat de niveau de service (SLA) est-il disponible ?
- ◯ Existe-t-il une distinction entre les signatures avancées et les signatures qualifiées ?
- ◯ Le document reste-t-il utilisable et vérifiable quant à son authenticité
- ◯ et son intégrité après la signature numérique ?
- ◯ L'application utilise-t-elle un code QR ou un code de vérification unique ?

Efficacité

- ◯ Existe-t-il un système permettant un flux de signature automatique ?
- ◯ Existe-t-il un système permettant un remplacement automatique en cas d'absence du signataire ?
- ◯ Est-il possible de télécharger des documents en masse ?
- ◯ Est-il possible de signer en masse ?
- ◯ Le logiciel est-il ouvert à des intégrations avec d'autres logiciels que votre organisation utilise ?
- ◯ Est-il possible de l'intégrer à Active Directory ?
- ◯ ...

2

Expérience d'utilisation

3

- ◯ Est-il facile de télécharger des documents à signer ?
- ◯ Est-il facile de définir des flux de signature ?
- ◯ Est-il facile de signer des documents ?
- ◯ Est-il possible de déterminer l'ordre de signature ?
- ◯ Est-il possible de faire signer des personnes externes à l'organisation ?
- ◯ Pouvez-vous choisir librement ce qui apparaîtra dans le champ de signature ?
- ◯ Pouvez-vous ajouter des approbateurs avant qu'un document ne soit soumis à la signature ?
- ◯ Existe-t-il une possibilité de signer depuis un appareil mobile ?
- ◯ Le service d'assistance est-il facilement joignable ?
- ◯ L'application a-t-elle fait ses preuves ?
- ◯ L'application bénéficie-t-elle d'un bon taux de satisfaction client ?

Exigences techniques

4

- ◯ Existe-t-il un API permettant à vos autres applications logicielles d'utiliser le logiciel de signature pour l'approbation, la signature et l'envoi de documents ?
- ◯ Existe-t-il une description claire de l'API ?
- ◯ Est-il possible d'utiliser des marqueurs de signature dans les documents, afin que le logiciel insère automatiquement le champ de signature à cet endroit ?
- ◯ L'envoi en recommandé est-il possible ?
- ◯ Existe-t-il une connexion avec l'eBox fédérale ?
- ◯ Est-il possible de disposer d'une piste d'audit des étapes clés d'un dossier ?
- ◯ ...

Prix

- ◯ Le coût est-il clair (avez-vous une idée approximative des frais) ?
- ◯ ...

5

Sources

- → https://economie.fgov.be/fr/themes/line/commerce-electronique/signature-electronique-et
- → https://economie.fgov.be/sites/default/files/Files/Online/FAQ-services-de-confiance.pdf

Envie d’en savoir plus ?

Si vous souhaitez en savoir plus sur **eSignFlow** et sur la manière dont nous transformons les processus en flux numériques intelligents grâce à la signature électronique n’hésitez pas à nous contacter à l’adresse helpdesk@esignflow.be.

eSignFlow

Transformez vos processus en flux numériques intelligents. Avec une signature et un envoi électroniques sécurisés et juridiquement conformes.

1. Soumettre

Présentez les bons documents à la bonne personne sans problème.

2. Valider

Gardez toujours une vue d’ensemble des documents en circulation.

3. Signer

Signez tous vos documents en quelques clics, où et quand vous le souhaitez.

4. Envoyer

Envoyez les documents signés numériquement par le canal de votre choix (courrier, e-mail, eBox, etc.).

5. Vérifier

Utilisez un code unique pour vérifier rapidement et facilement la validité juridique d’un document.

Rendez-vous sur : www.esignflow.be