Préserver la validité de vos signatures électroniques

eSignFlow
signer autrement

Les signatures électroniques basées sur un certificat sont considérées par l'UE, et même à l'échelle mondiale, comme une alternative **juridiquement valide** aux signatures manuscrites. Elles servent souvent à prouver ou à garantir qui a signé un document, à quel moment, et à s'assurer que son contenu n'a pas été modifié depuis la signature.

Cependant, certains utilisateurs commettent une **erreur fréquente** : ils modifient un document après qu'il a déjà été (partiellement) signé.

Pensez par exemple à une modification de texte, de la mise en page, ou encore à la suppression ou l'ajout d'une page.

Ces actions rendent par conséquent les signatures précédentes **invalides**, comme le signalent des logiciels tels qu'Adobe Acrobat Reader et les outils de validation de signature du SPF BOSA ou de la Commission européenne.

Ne signez pas digitalement un document si vous comptez le modifier ensuite, même pour le faire re-signer par la suite.
Si une modification est nécessaire, repartez toujours du document original sans aucune signature et faites-le (re-)signer par tous les signataires. Si vous ne pouvez pas préserver la validité des signatures, conservez soigneusement chaque exemplaire signé.

Après avoir parcouru ce whitepaper, vous en saurez davantage sur :

- comment fonctionnent les signatures électroniques ;
- pourquoi des signatures peuvent être invalides ;
- ce que vous pouvez ou non faire avec un document signé ;
- comment vérifier vous-même la validité d'une signature.

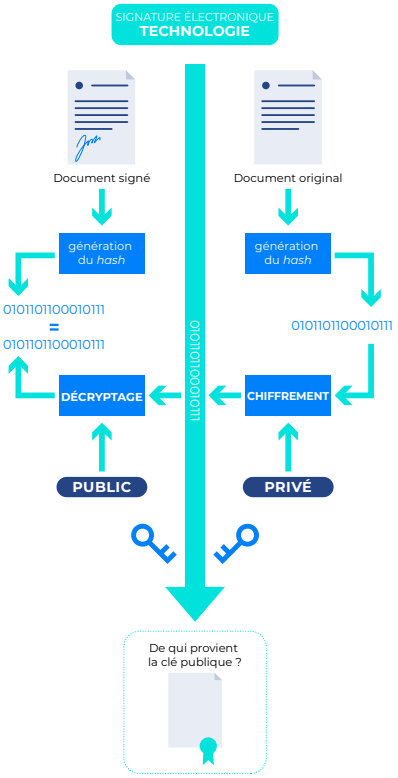
Table des matières

Qu’est-ce qu’une signature électronique ?

Une signature électronique peut être vue comme une sorte de **cachet numérique** apposé sur un document. Elle prouve qui a signé le document et garantit qu’il ne peut pas être modifié après la signature.

Voici comment cela fonctionne d’un point de vue technique :

- Une **« empreinte numérique » unique du document** est générée : on appelle cela un ***hash***. Il s’agit d’une courte suite de chiffres et de lettres calculée de façon unique à partir du contenu intégral du document. Le moindre changement de texte ou de mise en page produit un *hash* totalement différent.
- Ce *hash* est chiffré avec la clé secrète (« privée ») du signataire.
- Le *hash* chiffré et la « clé publique » correspondante sont intégrés au document en tant que signature électronique.



Les propriétés essentielles d’une signature électronique sécurisée :

- **Garantie d’identité** : vous savez qui a signé le document.
- **Garantie d’horodatage** : vous savez quand le document a été signé.
- **Garantie d’intégrité** : vous savez que le document n’a pas été modifié depuis la signature.
- **Non-répudiation** : le signataire ne peut pas nier sa signature, car il ou elle l’a apposée avec un moyen de signature sécurisé qui prouve son identité.
- **Validation à long terme** : les preuves nécessaires relatives aux identités des signataires, aux moments de signature et aux autres éléments de preuve, sont intégrées dans le document (LTV ou « Long Term Validation »).

2. Comment savoir si une signature est (toujours) valide ?

Un logiciel peut vérifier si une signature électronique est encore **valide**. Il contrôle :

- si le contenu du document est exactement le même qu'au moment de la signature (contrôle du *hash*) ;
- si le certificat utilisé pour signer est toujours valide (chaîne de confiance) ;
- si un horodatage valide est présent.

Outils gratuits pour vérifier la validité d'une signature

- **Adobe Acrobat Reader DC**

  Ce logiciel affiche automatiquement si une signature est valide à l'ouverture d'un PDF contenant une ou plusieurs signatures électroniques.

  Adobe reconnaît automatiquement les signatures dont le certificat figure dans l'Adobe Acrobat Trusted List (AATL) ainsi que dans la liste de confiance de l'Union européenne (EUTL).

- **EU DSS Demonstration Tool** (Commission européenne)

  Cet outil teste si une signature électronique est « qualifiée » (c'est-à-dire équivalente à une signature manuscrite).

  L'outil de validation est disponible en ligne via ce lien : *https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation*.

- **SPF BOSA Validator** (Belgique)

  Cet outil détermine si une signature électronique apposée avec la carte d'identité électronique belge (eID) est toujours valide.

  Ce dernier est disponible en ligne via ce lien : *https://signing.fts.bosa.belgium.be/validate?language=fr#*.

3. Qu'est-ce qui rend une signature électronique invalide ?

Dès qu'un document est signé, il est considéré comme **« figé »**. Si vous y apportez la moindre modification — même la plus infime — l'empreinte numérique (*hash*) du document change. La signature ne correspond alors plus au nouveau contenu et devient **invalide**.

Quelques actions à ne pas effectuer :

- Modifier ou ajouter du texte (attention : ajouter ou supprimer un espace est une modification).
- Changer la mise en page (par exemple : modifier la police, la couleur, etc.).
- Ajouter, supprimer ou réorganiser des pages.
- Remplir des champs de formulaire après que le document a été signé.
- Recharger un document déjà signé pour le faire signer à nouveau, si le logiciel de signature modifie quelque chose dans le texte du document à cette occasion.

Dans le cadre de l'utilisation de notre logiciel de signature électronique eSignFlow, les actions suivantes sont concernées :

- eSignFlow appose (ou réappose) une règle de vérification sur le document.
- eSignFlow ajoute une page de signatures à la fin du document.
- eSignFlow place des signatures sur des « *signmarkers* » (des repères textuels indiquant l'emplacement des zones de signature). eSignFlow commence par supprimer ces repères, ce qui constitue une modification du texte…

CONSÉQUENCE : les outils de validation signaleront la signature comme « invalide » ou « rompue ».

Voici un exemple d'actions incorrectes

Le déposant X charge un document **A** (via un logiciel quelconque) pour signature par le signataire Y. Y signe. X télécharge le document signé par Y et le modifie.

Cette modification invalide la signature de Y. X recharge le document modifié **A**' pour signature par le signataire Z. Z signe. Le document **A**' est désormais valablement signé par Z, mais contient aussi la signature invalidée de Y !

➔ **Les outils de validation considèreront ce document comme invalide.**

Remarque : si le déposant X soumet à nouveau la version **A**' du document au même signataire Y, le document **A**' contiendra deux fois la signature de Y — dont une signature invalide et une signature valide.

➔ **Les outils de validation considèreront également ce document comme invalide.**

Remarque : des signatures invalidées apparaissent parfois aussi dans des documents préalablement signés avec Adobe Acrobat Reader, puis re-soumis via eSignFlow pour une signature complémentaire. Restez attentif à ce genre de situation dans Adobe.

4. Combiner les signatures électroniques et manuscrites ?

En règle générale, nous **déconseillons de signer** un même document à la fois de façon manuscrite et numérique (ce cas se présente souvent lorsqu'un des signataires se trouve dans l'incapacité de signer électroniquement). Dans la mesure du possible, faites signer un document entièrement en numérique ou entièrement sur papier.

Pourquoi ? Parce qu'une signature électronique ne peut être prouvée que numériquement, tandis qu'une signature manuscrite ne peut être prouvée que sur papier. Lequel des deux documents conserverez-vous alors comme pièce justificative ?

Solution acceptable : conservez soigneusement les deux documents afin de pouvoir les présenter ensemble devant un tribunal en cas de litige.

ATTENTION : n'utilisez cette méthode combinée qu'en dernier recours, lorsqu'il n'y a vraiment pas d'autre option.

5. Que peut-on encore faire avec un document signé ?

Tant que vous ne modifiez pas le contenu du document signé, vous pouvez encore effectuer les **opérations suivantes**, pour autant que le logiciel de signature le permette :

- **ajouter des signatures supplémentaires** : par exemple, faire signer une deuxième personne, à condition que le contenu original ne soit pas modifié ;
- **ajouter un horodatage** : via un service officiel (une « autorité d'horodatage ») pour prouver à quel moment le document a été signé ;
- **ajouter des annotations visuelles** et des **commentaires textuels.**

ATTENTION : ces opérations doivent être effectuées avec un logiciel fonctionnant selon le principe de l'« ajout uniquement » (*append-only*) : les nouvelles informations sont ajoutées en couche supplémentaire sans modifier le document original.

6. Quelques bonnes pratiques pour travailler avec la signature électronique

- Ne signez qu'une fois le document entièrement finalisé.
- Établissez une procédure claire séparant strictement la phase d'édition de la phase de signature.
- Évitez de signer numériquement un document si vous comptez le modifier ensuite, même pour le faire re-signer.
- En cas de modification nécessaire, repartez toujours du document original (sans aucune signature) et faites-le (re-)signer.
- Utilisez des logiciels fiables pour les PDF et les signatures électroniques.
- Enregistrez de préférence les documents au format PDF/A. Ce format garantit un archivage stable des documents signés et assure leur intégrité et leur authenticité essentielles à des fins juridiques et administratives.
- Informez vos collaborateurs de l'importance de ne pas modifier les documents signés.
- Conservez les documents signés dans un espace où ils ne peuvent plus être modifiés.
- Si vous avez malgré tout plusieurs versions d'un document avec des signatures différentes, conservez absolument chaque version signée.

7. Le règlement eIDAS et les exigences relatives aux signatures électroniques

eIDAS signifie : electronic IDentification, Authentication and trust Services. Il s'agit d'un règlement européen (n° 910/2014) qui fournit **un cadre juridique** pour les services d'identification électronique et de confiance au sein du marché des États membres de l'UE. Son objectif est de permettre des transactions numériques transfrontalières sécurisées, avec des signatures, cachets, horodatages, et documents électroniques juridiquement valides.

Le règlement eiDAS distingue trois types de signature électronique :

1. **Signature électronique simple** : toute forme de signature électronique, comme un nom en bas d'un e-mail ou une image de signature scannée.
2. **Signature électronique avancée** : cette signature est liée de façon unique au signataire, elle utilise un certificat et permet de détecter toute modification ultérieure du document.
3. **Signature électronique qualifiée** : répond à toutes les exigences d'une signature avancée ET est créée à l'aide d'un dispositif de signature qualifié.

Une signature électronique qualifiée a la **même valeur juridique** qu'une signature manuscrite dans tous les États membres de l'UE.

Les différences entre signature avancée et signature qualifiée

Caractéristique	Avancée	Qualifiée
Certificat requis	Oui	Oui
Lien unique avec le signataire	Oui	Oui
Détecte les modifications	Oui	Oui
Émise par	PSC (*)	QPSC (*)
Valeur juridique	Preuve solide	Équivalente à la signature manuscrite

(*) (Q)PSC : Prestataire de Services de Confiance (Qualifié) — voir aussi plus loin.

8. La signature qualifiée en Belgique

En Belgique, plusieurs moyens fiables permettent d'apposer une **signature qualifiée**.

- **La carte d'identité électronique belge** (eID) : elle contient un certificat qualifié, délivré par l'État (via le SPF Intérieur). Lorsque vous signez avec votre eID, la signature est confirmée par votre code PIN et un lecteur de carte sécurisé. La carte de séjour électronique (eCarte) est fonctionnellement identique à l'eID et peut donc aussi être utilisée pour les signatures qualifiées.
  Remarque : les signatures apposées avec une « ancienne » eID belge ne sont plus considérées comme qualifiées par l'outil de validation de la Commission européenne, car elles reposent sur un chiffrement obsolète (SHA1). La seule solution est de demander à la personne concernée de renouveler son eID auprès du service population de sa commune. Adobe et l'outil de validation du SPF BOSA reconnaissent néanmoins encore (provisoirement) ces signatures.
- **L'application Itsme** : reconnue en 2020 comme méthode de signature qualifiée. L'utilisateur signe avec une combinaison de son smartphone, d'une vérification dans l'application et d'un code PIN ou de la biométrie (comme la reconnaissance faciale). En arrière-plan, Itsme utilise un certificat personnel qualifié d'un QPSC.
- **Un certificat personnel qualifié** ou **un cachet électronique qualifié d'organisation** : en tant que mandataire ou collaborateur d'une organisation, vous pouvez acquérir un certificat utilisable pendant une durée déterminée (généralement 3 ans) via un logiciel de signature. Vous devez généralement installer une application mobile pour confirmer de façon sécurisée les signatures avec ce certificat.

Ces trois méthodes satisfont pleinement aux exigences d'une signature électronique qualifiée selon eIDAS et ont donc la même valeur juridique qu'une signature classique, dans tous les États membres de l'UE. Attention toutefois à la remarque concernant les « anciennes » eID belges.

9. Les certificats de signature d'un (Q)PSC

Les **certificats de signature** — tant les certificats personnels que les cachets électroniques d'organisation (*eseals*) — peuvent satisfaire au règlement eIDAS s'ils répondent à certaines exigences techniques et organisationnelles.

Pour une **signature électronique avancée**, le certificat doit être lié de façon unique au signataire, rester sous son contrôle exclusif et permettre de détecter toute modification du document signé. Ces certificats sont en principe émis par un PSC (Prestataire de Services de Confiance) ou un QPSC (PSC Qualifié).

> ***ESEAL*** **: Un eseal (cachet électronique) est associé à une organisation (ou à une partie de celle-ci) plutôt qu'à une personne physique.**

Une **signature électronique qualifiée** requiert en outre l'utilisation d'un **certificat qualifié**, émis par un prestataire de services de confiance qualifié (QPSC), et doit être créée avec un dispositif qualifié de création de signature électronique (QSCD: *Qualified Signature Creation Device*).

Des entreprises comme Digicert, SK ID Solutions ou GlobalSign sont des QPSC disposant de systèmes servant de QSCD. Leurs certificats et systèmes sont donc reconnus comme **juridiquement équivalents** à une signature manuscrite.

Leurs systèmes utilisent souvent des HSM *(Hardware Security Modules*) — des serveurs et logiciels dédiés qui stockent et utilisent les clés numériques de façon extrêmement sécurisée pour signer des documents. Le HSM garantit que la clé de signature ne quitte jamais le module, empêchant ainsi tout abus ou falsification.

Des plateformes de signature comme **eSignFlow** peuvent faire appel aux services de QPSC pour permettre à leurs utilisateurs de signer des documents de façon avancée ou qualifiée (avec certificat personnel) ou de les « certifier » (avec *eseal*).

10. L’horodatage qualifié

Un **horodatage qualifié** associé à une signature électronique est une preuve électronique qui enregistre le moment précis où une signature électronique a été créée, avec un très haut niveau de fiabilité. Cet horodatage est également émis par un prestataire de services de confiance qualifié (QPSC) et satisfait aux exigences du **règlement eIDAS**.

L’horodatage garantit :

1. **La preuve du moment** : il confirme l’instant précis où la signature électronique a été apposée.
2. **L’intégrité** : l’horodatage est cryptographiquement lié au document et indique clairement si celui-ci a été modifié depuis ce moment.
3. **La validité à long terme** : en combinaison avec les normes d’archivage, un horodatage qualifié permet à la signature d’être encore reconnue comme juridiquement valide des années plus tard, même si le certificat sous-jacent a entretemps expiré ou été révoqué.
4. **La sécurité juridique** : dans les procédures judiciaires, un horodatage qualifié apporte une garantie supplémentaire sur l’authenticité et le moment de la signature.

Les plateformes de signature fiables (comme eSignFlow) génèrent systématiquement un horodatage qualifié via un QPSC à chaque signature, quel que soit le moyen de signature utilisé.

Conclusion

- Les signatures électroniques sont un outil puissant pour prouver qui a signé un document, **à quel moment** et que celui-ci n'a pas été modifié depuis (sauf exceptions expressément autorisées).
- Il est donc primordial d'utiliser des logiciels **fiables** et **des procédures claires** pour garantir la validité juridique des signatures dans vos documents.
- Grâce au **règlement eIDAS** de l'Union européenne et aux moyens de signature qualifiés tels que la carte d'identité électronique belge, Itsme ou les certificats HSM d'un (Q)PSC, vous pouvez signer numériquement avec une pleine valeur juridique — à condition d'éviter toute modification non autorisée du document après signature.

eIDAS 2.0 : Régulation (UE) 2022/858 en ligne

Si vous modifiez un document signé, les signatures précédentes sont invalidées. Pour éviter cela, ne touchez plus au document après sa signature complète. Tout écart à cette règle impose de conserver chaque exemplaire signé.

Soyez particulièrement vigilant lorsque des signatures sont apposées via différents systèmes, ou lorsque des signatures manuscrites et électroniques sont combinées.

Découvrez eSignFlow, la plateforme de signature sur mesure pour les administrations locales

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 et à l'envoi électronique sécurisé et juridiquement valable, n'hésitez pas à nous contacter à l'adresse **bienvenue@esignflow.be**.

eSignFlow

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

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 : https://www.esignflow.be/fr-be