



De la signature manuscrite à la
signature électronique

5 pratiques courantes à éviter

LUXTRUST

Sommaire

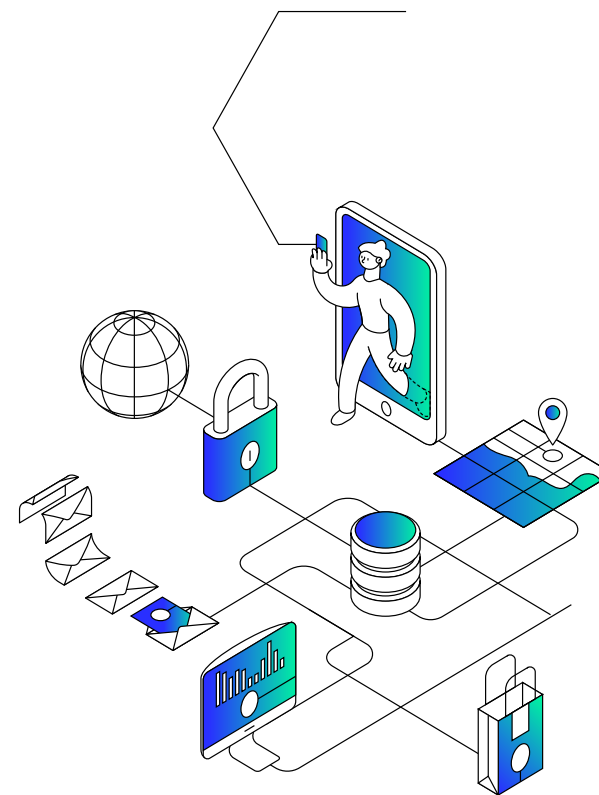
3	Introduction
4	#1 Est-il vraiment nécessaire d'ajouter ses initiales (paraphes) sur les documents signés électroniquement ?
7	#2 Apposer plusieurs signatures électroniques du même signataire sur un seul document numérique est-il vraiment utile ?
9	#3 La signature électronique doit-elle ressembler à une signature manuscrite ?
12	#4 Une signature électronique imprimée est-elle toujours valide ?
15	#5 Peut-on mélanger des signatures manuscrites avec des signatures électroniques sur un document numérique ?
18	Bonnes pratiques à adopter lors du passage du papier au numérique
20	À propos de LuxTrust

Introduction

Les êtres humains sont perclus d'habitudes. Nous développons des routines et des rituels dans tous les domaines de notre vie, de la préparation du petit-déjeuner le matin jusqu'au coucher le soir. Nos habitudes sont réconfortantes et rassurantes ; elles nous confèrent un sentiment de contrôle et nous aident à prédire ce qui va se passer, ce qui nous donne l'impression d'être également en mesure d'y faire face. Si certaines d'entre elles constituent un avantage et valent la peine d'être conservées tout au long de la vie, d'autres doivent évoluer ou changer.

Certaines habitudes affectant la façon dont nous travaillons et exécutons nos activités, dans ce livre blanc, nous allons examiner attentivement **cinq pratiques (pour ne pas dire erreurs) parmi les plus courantes*** que nous avons observées lors du passage de la signature physique à la signature électronique de documents PDF. Elles proviennent de pratiques physiques si profondément ancrées dans nos activités quotidiennes que nous pensons qu'elles fonctionneront également dans le monde numérique. Il est d'ailleurs logique de les voir mises en œuvre lors de la signature de documents numériques ; sinon, nous estimons qu'il y a un problème. Cependant, la signature électronique a ses propres règles et mécanismes qui rendent ces pratiques obsolètes. Par conséquent, les éliminer garantira une transition plus fluide et plus sûre des processus papier aux processus numériques.

* Pour être précis, nous faisons référence aux pratiques les plus courantes liées aux signatures reposant sur des certificats en format PAdES.



#1

Est-il vraiment nécessaire
d'ajouter **ses initiales (paraphes)**
sur les documents signés
électroniquement ?

Réponse : **NON**



Parapher des documents papier – pour quelle(s) raison(s) ?

Parapher chaque page d'un document papier est une pratique courante rencontrée lors de la signature de contrats ou de documents juridiques représentant un fort enjeu. Bien que fastidieuse et chronophage (imaginez le fait de parapher un contrat de 50 pages !), cette pratique a été développée pour lutter contre la fraude lors de la signature de documents papier. Elle sert deux objectifs principaux :

1. Confirmer que le signataire a examiné et validé chaque page du document ;
2. S'assurer que l'une des parties signataires ne modifie pas le contenu des pages individuelles ou n'ajoute pas de nouvelle page après la signature du document, modifiant ainsi son contenu.

Le paraphe sert de mesure de précaution destinée à protéger l'intégrité du document signé. Il est intéressant de noter que **l'ajout d'initiales sur chaque page d'un contrat n'est pas une exigence légale pour qu'une partie exprime son consentement** ; une signature est suffisante pour créer un contrat valide (en vertu du droit luxembourgeois, français [selon la décision du 27 janvier 1993, 91-12.115 de la Cour de Cassation] et belge [consulter l'article 8.1.4 du Code Civil 2019]). Même si l'accord n'est pas paraphé ou si les initiales sur une seule page sont manquantes, la signature est toujours valide et les signataires sont liés par les conditions générales définies dans le document. Dans certaines juridictions, les initiales peuvent être considérées comme un élément supplémentaire pour étayer un accord contraignant en cas de litige ; c'est pourquoi nous vous conseillons de vérifier chaque législation locale avant d'agir.

Néanmoins, cette pratique est devenue si familière et fréquente qu'elle a également été transposée dans le monde numérique. Étant conscients du sentiment d'assurance que cela confère et jouant sur celui-ci, certains fournisseurs de signature électronique la proposent aux clients comme une fonctionnalité supplémentaire, suggérant qu'il s'agit d'une couche de sécurité supplémentaire. En tant qu'êtres perclus d'habitudes, les individus peuvent facilement l'accepter sans le remettre en question.

Parapher des documents numériques – c’est juste du marketing !

L’ajout d’initiales sur des documents numériques est inutile, car les mécanismes inhérents à la signature électronique traitent les deux principales raisons existentielles du paraphe. La signature électronique a, entre autres, pour rôle de protéger l’authenticité et l’intégrité de l’ensemble du document (pas uniquement celles de la page où l’image de la signature électronique est visible). Sa principale caractéristique, « ce que vous voyez est ce que vous signez » (*What You See Is What You Sign, WYSIWYS*), garantit que les propriétés du document ne peuvent pas être modifiées par accident ou intentionnellement après sa signature. Tenter d’autoriser des pages individuelles n’est plus en adéquation avec les moyens de protection technique et ne peut même pas être respecté pour un document signé par voie électronique, car cela modifierait le contenu du document et romprait ainsi les mécanismes de signature électronique.

En outre, **la manière dont les fournisseurs de signature électronique proposent d’appliquer les initiales numériques est généralement problématique**, car il s’agit d’images apposées sur le document. Ainsi, si le document a déjà été signé, l’ajout de tell^{es} images constitue des modifications du document, ce qui à son tour rompt les mécanismes cryptographiques, rendant la signature électronique non valide. Si la pratique du paraphe est correctement mise en œuvre pour les documents numériques, malgré leur caractère inutile, chaque initiale doit être apposée à l’aide d’un moyen électronique, tel qu’un horodatage (qui peut inclure des images). Chaque page du document devant être horodatée individuellement par chaque signataire, l’intégralité des processus devient inutilement coûteuse.

Si les parties signataires veulent s’assurer que, pendant le processus de signature, chaque signataire a examiné chaque page du document, la solution de signature électronique peut alors être configurée pour obliger le signataire à lire chaque page et lui permettre de signer uniquement après avoir parcouru (fait défiler) toutes les pages. Des fonctionnalités similaires existent déjà dans l’ensemble, par exemple lors de l’examen et de l’acceptation de la mise à jour de Conditions générales, etc.

« Un paraphe est un acte inutile et superflu dans le cadre d’une signature digitale. Il rendrait même absurde les mécanismes d’une signature digitale. Donc, la signature digitale fournit des moyens beaucoup plus efficaces et user-friendly afin d’éviter l’anachronisme du monde papier. »



Thomas Kopp
Chief Scientist
LuxTrust

#2

Apposer **plusieurs signatures électroniques du même signataire** sur un seul document numérique est-il vraiment utile ?

Réponse : **NON**

Apposer plusieurs fois sa signature électronique sur le même document : lorsque le plus est l'ennemi du mieux

Lors de la signature d'un contrat papier, il n'est pas rare d'ajouter deux à trois signatures manuscrites (sur différentes pages ou dans différentes sections, bien sûr). Cela s'applique également à l'autre ou aux autres parties signataires. Un argument/motif juridique justifie-t-il cette pratique ? En fait, lorsqu'il s'agit de documents papier, il est nécessaire de demander un consentement spécifique ou un engagement ferme du signataire sur plusieurs sections du document. Cette pratique est également destinée à éviter la substitution de pages, protégeant ainsi la structure et le contenu de l'acte.

Cette pratique papier courante a été transposée comme telle dans le monde numérique. Les documents papier ne sont plus imprimés, ils sont enregistrés sous forme de documents PDF, puis envoyés pour être signés. Ils comprennent souvent plusieurs champs de signature, ce qui incite le signataire à penser qu'ils doivent être remplis. **Pour aggraver les choses, certains fournisseurs de signature électronique permettent même plusieurs signatures du même signataire sur un même document PDF.** D'autres permettent aux clients d'apposer une deuxième signature, mais dès qu'elle est exécutée, la première est invalidée ou disparaît. Cela entraîne plus de confusions, de temps perdu et cela peut même inciter les signataires à développer des « solutions de contournement » (comme copier-coller l'image de la signature électronique) pour que le document soit signé.

Tout comme dans le cas du paraphe numérique, **les mécanismes de signature électronique prennent en charge les problèmes liés au consentement ou à la falsification de contenu.** Une seule signature électronique suffit à donner un consentement pour l'intégralité du contenu du document. En outre, la signature électronique « verrouille » le document à une heure, une identité de signataire, un certificat, etc. spécifiques pour empêcher toute modification ultérieure. Cela s'applique uniquement lorsque la signature couvre l'intégralité du document (par exemple, dans le cas de l'utilisation du format PAdES). Cependant, il existe également d'autres formats de signature électronique, par exemple XAdES, qui permettent de signer des parties individuelles d'un document et, dans ces contextes, il peut être judicieux de signer des engagements sur différents aspects/parties d'un document.

Grâce à la signature électronique, plusieurs signatures sur le même document PDF ne sont plus nécessaires pour conclure des transactions ou accepter les conditions spécifiques de certaines sections du document. Cela simplifie le document et notre activité. Pour passer au numérique, la structure des accords doit être révisée et adaptée. Une façon simple serait de supprimer les champs de signature inutiles afin d'assurer au signataire qu'une seule signature électronique suffit.

#3

La signature électronique doit-elle **ressembler** à une signature manuscrite ?

Réponse : **NON**

A quoi doit ressembler une signature électronique ?

Nous sommes tellement habitués aux signatures manuscrites et à signer à l'encre qu'il est devenu presque inconcevable de ne pas voir les signatures au bas d'une page. Les signatures électroniques sont l'équivalent numérique de nos signatures sur papier, nous pourrions donc avoir tendance à croire qu'il est tout aussi important de voir la marque d'une signature électronique sur le document. Est-ce approprié ou est-ce juste un mythe ?

La valeur juridique du filigrane d'une signature électronique

La plupart des outils en ligne de signature électronique vous donnent la possibilité de créer et de concevoir votre signature électronique afin de voir à quoi elle ressemblera sur un document numérique. L'image de la signature et ses éléments sont entièrement personnalisables. Le résultat inclut généralement le nom complet du signataire, la date et l'heure auxquelles la signature a été apposée, le nom de la société et le lieu. Les signataires peuvent choisir de télécharger et de compléter l'image avec un logo, une image ou même l'image numérisée de leur signature manuscrite pour la rendre plus personnelle. Au final, la signature électronique peut ressembler à la signature que nous avons l'habitude de voir sur les papiers. C'est une fonctionnalité agréable, mais quelle est sa valeur juridique ?

D'un point de vue juridique, **il n'existe pas de règles ou d'indications sur ce à quoi doit ressembler un filigrane de signature électronique.** L'affichage d'une image d'une signature sur un document numérique n'apporte pas automatiquement de garantie quant à l'identité ou au consentement du signataire. En cas de litige juridique, des preuves supplémentaires doivent être présentées pour prouver qui a signé ce document et quand il a été signé. Par ailleurs, si vous ne voyez pas le filigrane de signature électronique sur un document, cela ne signifie pas que ce document n'est pas signé correctement.



Une signature électronique est différente d'une signature manuscrite

Lorsque vous signez un document par voie électronique, le système génère un code unique (aussi appelé « hash ») qui est lié au document. Le code sous forme hachée est une série de caractères agissant comme un identifiant du document. Il contient également des données concernant le certificat du signataire (son identité, sa validité, son émission, etc.). Si quelque chose dans le document, même un espace, est modifié après la signature électronique, le code sous forme hachée ne correspond plus aux documents originaux signés, de sorte que la signature électronique devient invalide. Le processus est plutôt technique et automatique ; il n'est pas visible à l'œil nu. C'est également la raison pour laquelle le fait de **voir le filigrane de signature électronique n'est pas obligatoire**. Le document peut être signé avec succès même si la représentation visuelle de la signature électronique est absente. Un moyen de vérifier cela consiste à consulter le volet de signature dans les outils publics disponibles comme Adobe Reader. Cependant, la présence de la coche verte ne signifie pas toujours que la signature est valide. Selon la façon dont ces outils sont configurés, le résultat peut être un faux positif ou un faux négatif. **L'application Digital Signature Service (DSS) Demonstration WebApp** est un autre outil disponible pour vérifier la validité des signatures électroniques, mais il s'agit d'un processus plutôt manuel, ce qui signifie que vous pouvez uniquement vérifier la validité d'un document à la fois selon certains paramètres prédéfinis. Ce service nécessite également la soumission des documents à valider sur la plateforme, il est donc conseillé d'éviter de partager du contenu classé secret ou confidentiel.

Comment s'assurer que les signatures électroniques sont valides ?

Au fil du temps, **les certificats de signature électronique peuvent expirer ou être révoqués et leurs composants peuvent s'affaiblir** (algorithmes, clés cryptographiques, données signées incluses dans la signature...). Ainsi, afin de pouvoir vérifier la validité de la signature électronique au moment de son exécution, le Règlement eIDAS a introduit le service de validation des signatures électroniques au niveau qualifié. Ce service procède à la vérification des signatures et cachets électroniques sur les documents signés, à condition que les signatures et cachets en question à valider soient conformes au Règlement eIDAS et aux normes applicables. Ce service permet aux entreprises de vérifier automatiquement la validité des documents volumineux et fournit un rapport détaillé des éléments de validité avec une valeur probante. Cela est très utile dans le cas de signatures reposant sur un certificat (comme les signatures avancées et qualifiées), mais cela peut également être configuré pour vérifier la validité des signatures électroniques en fonction de critères prédéfinis selon les besoins internes de la société.

#4

Une **signature électronique imprimée** est-elle toujours valide ?

Réponse : **NON**

Peut-on imprimer un document signé électroniquement ?

Les technologies émergentes ont commencé à brouiller les frontières entre les mondes papier et numériques. Si le processus de signature était auparavant simple : signer, organiser, puis archiver les documents papier dans un dossier, maintenant les documents papier et numériques sont facilement mélangés pour des raisons d'efficacité et d'expédition. Nous sommes sûrs qu'il vous est déjà arrivé d'accepter un contrat ou une offre reçus par e-mail, de l'imprimer, de le signer, puis de le scanner et de le renvoyer par e-mail. C'est beaucoup plus rapide. Cependant, les risques juridiques que cette pratique pourrait entraîner sont moins connus.

Signature manuscrite scannée – quelle est sa valeur juridique ?

La valeur juridique d'une signature manuscrite scannée (et stockée au format numérique) peut facilement être contestée devant un tribunal, car elle n'est pas reconnue comme une signature électronique par certaines jurisprudences. Donc, en cas de litige, la version scannée du contrat devra être documentée par d'autres preuves supplémentaires. De plus, dans le monde papier, l'original du document revêt beaucoup d'importance. Par exemple, l'article 1325 du Code civil luxembourgeois indique que les actes sous seing privé doivent être rédigés en autant d'originaux qu'il y a de parties, mais prévoit une exception en ce qui concerne les actes privés signés par voie électronique. En France (article 1325) et en Belgique (article 8.20) les actes sous seing privé qui contiennent des conventions synallagmatiques, ne sont valables qu'autant qu'ils ont été faits en autant d'originaux qu'il y a de parties ayant un intérêt distinct. L'exigence d'une pluralité d'originaux est réputée satisfaite pour les contrats sous forme électronique lorsque l'écrit est établi conformément aux articles 1316-1 et 1316-4 et l'article 8.1, 1° et que le procédé permet à chaque partie de disposer d'un exemplaire écrit ou d'y avoir accès.

« Si aucun original portant des signatures physiques n'est échangé et compilé par la suite, les parties n'ont en leur possession que des copies PDF des documents portant une copie d'une signature manuscrite. En cas de litige, ces documents ne constituent qu'un commencement de preuve par écrit, ce qui n'est pas toujours conseillé compte tenu des montants en jeu. » – **Anne Reuland, Directrice des affaires juridiques et réglementaires (Chief Legal & Regulatory Officer), LuxTrust.**

Signature électronique imprimée – quelle est sa valeur juridique ?

À l'instar d'une signature manuscrite qui perd sa valeur juridique lorsqu'elle est scannée, une signature électronique perd sa valeur lorsqu'elle est imprimée. Comme nous le verrons dans le chapitre suivant, **la signature électronique n'est pas le signe/l'image que nous voyons sur le fichier PDF**. C'est l'algorithme

« L'impression du document signé par voie électronique peut être utile pour vos dossiers personnels, mais le document imprimé ne bénéficie pas des mécanismes électroniques qui permettent de protéger l'intégrité du document, ni des moyens de vérifier la validité des différentes signatures électroniques qu'il contient. »



Anne Reuland
Chief Legal &
Regulatory Officer
LuxTrust

cryptographique qui « gèle » le document. En l'imprimant, le mécanisme est perdu. Il ne peut plus être vérifiable et la signature ne peut pas être validée. Ce qui reste visible, c'est le filigrane de signature électronique qui n'a pas de valeur juridique et peut être facilement falsifié. En outre, il n'existe aucune confirmation et preuve concernant l'identité du signataire. Après avoir entièrement signé le document numérique, les signataires doivent savoir que la version électronique du document signé par voie électronique correspond à « l'original » du document.

Le cycle de vie de la signature électronique : archivage électronique et conservation à long terme

La plupart des entreprises ont déjà mis en place un système d'archivage de documents papier, mais cela n'est pas compatible avec les signatures et les documents numériques. Alors que les documents de faible importance peuvent être stockés sur des serveurs pendant une courte période, il peut être très important de protéger et d'archiver les documents pendant des périodes plus longues, de sorte qu'un stockage et un archivage appropriés sont nécessaires.

Des services tels que **la conservation à long terme de la signature électronique** et **l'archivage électronique avec une valeur probante** ont été développés pour répondre à ce besoin. La deuxième option, bien qu'il ne s'agisse pas encore d'un service conforme au Règlement eIDAS (à inclure dans la version révisée du Règlement eIDAS2.), garantit qu'un document est stocké de manière à garantir son intégrité et sa disponibilité en cas de litige juridique. Elle fournit des preuves concernant l'intégrité des documents au moment de leur importation dans l'archive et pendant la période d'archivage. La première option est un service reconnu et conforme au Règlement eIDAS, qui cible le mécanisme de signature électronique et fait référence à la maintenance des signatures et des documents signés afin de garantir leur validité pendant une période illimitée et au-delà de la période de validité des certificats des signataires.

#5

Peut-on **mélanger des signatures manuscrites avec des signatures électroniques** sur un document numérique ?

Réponse : **NON**



Faut-il mélanger les signatures électroniques et manuscrites sur le même document ?

Malgré une popularité et une acceptation croissantes, il existe encore des lacunes en termes d'utilisation des signatures électroniques, car toutes les entreprises n'ont pas le même niveau de numérisation. Cela pourrait arriver que des accords et des documents soient signés par voie électronique par certains signataires, et physiquement (signature manuscrite) par d'autres.

L'un des scénarios les plus courants que nous avons rencontrés est lorsqu'une partie signe un contrat ou un devis par voie électronique, puis l'envoie par e-mail à l'autre partie. Cette dernière imprime les documents, les signe manuellement, puis les scanne et les renvoie par e-mail à la première partie comme preuve. Au final, on se retrouve avec un document qui se présente sous forme électronique, qui contient ce à quoi ressemblent deux signatures à première vue. Cependant, cela soulève diverses inquiétudes d'un point de vue juridique.

Tout d'abord, comme indiqué dans l'une des sections ci-dessus, **l'impression d'un document signé par voie électronique rend la signature invalide**, car il est impossible de vérifier si les mécanismes cryptographiques sont valides. De plus, il est impossible de prouver si le signataire est celui qui a réellement signé le document. Deuxièmement, mélanger ces types de signatures soulève des problèmes concernant ce que l'on considère comme l'original du document. Conformément à la loi luxembourgeoise, française et belge, lorsque l'on signe à l'encre, le document doit être signé en autant d'originaux que le nombre de parties signataires et chacun d'entre eux est considéré comme l'original. Néanmoins, en raison du mélange des types de signatures, l'exception ne s'applique plus. Sur la base de cet argument, en cas de litige, l'accord ou le contrat n'est pas valablement conclu et son intégrité n'est pas garantie.

Que faire si une partie refuse de signer un document par voie électronique ? En effet, un signataire peut refuser de signer par voie électronique, que ce soit parce qu'il n'est pas correctement équipé pour le faire ou pour toute autre raison. Dans ce cas, l'alternative consiste à utiliser la signature manuscrite et à suivre le protocole approprié pour signer physiquement (ce qui inclut d'éviter de scanner le document et de l'envoyer par e-mail).

Pour terminer sur une note plus positive... Si l'association d'une signature manuscrite et d'une signature électronique est fortement découragée, un mélange de différents niveaux de signature électronique peut se produire et est autorisé. Par exemple, il peut également arriver qu'au cours du processus de signature, l'une des parties signe à l'aide d'une signature électronique avancée et l'autre partie avec une signature qualifiée telle que définie dans le Règlement eIDAS. Selon **Anne Reuland, notre directrice des affaires juridiques et réglementaires (Chief Legal & Regulatory Officer)**, *« une telle combinaison de signatures électroniques ne rend pas le document invalide, mais, en cas de litige, il peut être nécessaire de fournir des preuves supplémentaires pour les signatures de niveau inférieur, ce qui ne serait pas nécessaire pour une signature électronique qualifiée ».*

Bonnes pratiques à adopter lors du passage du papier au numérique

Comme nous l'avons vu ci-dessus, la technologie de signature électronique rend obsolètes certaines pratiques papier. Le changement des pratiques peut être une tâche difficile, en particulier lorsqu'elles sont profondément ancrées (« c'est comme cela que nous faisons les choses ici »), nous avons donc compilé une série de recommandations simples pour éviter les problèmes juridiques que pourrait soulever la transposition inadéquate de pratiques papier en pratiques numériques.

1. Établir une politique de signature

Il s'agit d'un document régissant tous les aspects et modalités du processus de signature conclu entre toutes les parties signataires. Elle peut couvrir des exigences techniques et procédurales liées à l'ensemble du cycle de vie d'une signature électronique, de la création à la validation ou à la conservation à long terme, mais également divers aspects liés au niveau d'autorisation, aux informations concernant des tiers, à la divulgation de données, etc. La formalisation des règles et procédures est nécessaire pour fournir plus de transparence et créer un « terrain d'entente » pour que toutes les parties agissent. En outre, elle sert de référence en cas de litige lié au processus de signature électronique. La politique de signature est une documentation du processus avec effet juridique (en annexe au contrat de service de signature).

2. Informer et former les employés exécutant les signatures électroniques

Éliminer les mauvaises pratiques lors de l'utilisation de la signature électronique implique la mise à disposition des bonnes informations et la sensibilisation aux questions de responsabilité. Prenez le temps d'informer et de former les employés qui sont censés signer par voie électronique, de leur fournir des directives ou de bonnes pratiques.





Cela doit inclure le fait d'éviter de copier-coller l'image ou les filigranes d'une signature électronique, d'imprimer des documents signés par voie électronique ou de numériser des signatures manuscrites. Profitez de cette occasion pour renouveler les procédures et l'organisation elle-même, car l'innovation peut découler du simple fait de mettre fin à une pratique qui est préjudiciable ou inefficace.

3. S'assurer que toutes les parties sont équipées pour signer par voie électronique

Afin d'exécuter correctement les signatures électroniques, les signataires doivent être équipés pour signer par voie électronique. Cela signifie que chacun d'entre eux doit avoir une identité numérique (s'ils souhaitent signer à l'aide de signatures reposant sur des certificats, comme les signatures électroniques avancées et qualifiées), doit posséder un dispositif de signature électronique et le certificat approprié pour signer. Cela garantira que le processus de signature reste 100 % numérique et que la signature électronique apposée bénéficie d'un niveau d'assurance plus élevé en cas de litige.

4. Examiner et adapter les sections des contrats papier devant être signés par voie électronique

Grâce à la signature électronique, plusieurs signatures sur le même document ne sont plus nécessaires pour conclure des transactions ou accepter les conditions spécifiques de certaines sections du document. Cela simplifie le document et notre activité. Pour passer au numérique, la structure des accords doit être révisée et adaptée. Une façon simple serait de supprimer les champs de signature inutiles afin d'assurer au signataire qu'une seule signature électronique suffit. Cela n'est pas obligatoire, mais à long terme, cela rassurera les signataires et arrêtera de répandre de mauvaises habitudes, notamment celle consistant à apposer plusieurs signatures électroniques.

À propos de LuxTrust

Depuis plus de 17 ans, **LuxTrust**, principal fournisseur européen de services de confiance qualifié, équipe les clients et les entreprises en solutions numériques complètes et sur mesure pour numériser les processus et améliorer l'efficacité globale. Depuis sa création, LuxTrust a construit et maintenu un écosystème d'identité numérique à l'échelle nationale au coeur de l'Europe, fournissant des services d'identité numérique et de confiance à 99 % de la population luxembourgeoise et soutenant 95 % de la totalité des banques de détail opérant au Luxembourg.

LuxTrust est un **prestataire de services de confiance qualifié eIDAS** figurant sur la liste de confiance de l'UE et est **une Autorité de Certification**. Il offre toute la gamme de services de confiance qualifiés eIDAS disponibles sur le marché :

- Identification des clients ou collaborateurs (en fournissant une identité numérique)
- Services d'authentification à des applications en ligne (bancaires ou autres)
- Services de signature électronique et de cachet électronique
- Service de validation de la signature électronique
- Service d'archivage électronique à valeur probante
- Horodatage qualifié

En outre, LuxTrust propose une solution pour se conformer à la directive DSP2, aux certificats SSL et aux services de gestion des données personnelles et des consentements.

Les solutions LuxTrust bénéficient du plus haut niveau de fiabilité et de confiance sur le marché. LuxTrust est supervisé et fait régulièrement l'objet d'audits et de contrôles obligatoires menés par des organismes de réglementation indépendants qui garantissent que les solutions restent conformes aux dernières réglementations européennes et du secteur.

- ▶ Une société robuste
- ▶ Une **gamme complète** de services eIDAS qualifiés
- ▶ Plus de **17 ans d'expérience** dans les services de confiance
- ▶ Un excellent suivi des projets livrés
- ▶ Statut **PSCQo qualifié** (Prestataire de services de confiance qualifié - Qualified Trust Services Provider)
- ▶ Signatures avancées et qualifiées à distance avec application mobile

Si vous souhaitez en savoir plus sur la signature électronique et les autres services de confiance, vous pouvez nous contacter par email : sales@luxtrust.com.

LuxTrust Luxembourg

IVY Building | 13-15, Parc d'Activités
L-8308 Capellen | Luxembourg

LuxTrust France

11, avenue Delcassé
75008 Paris | France

LuxTrust Belgique

54, Av. Louise
1050 Ixelles | Belgique

LuxTrust Monaco

21, avenue de l'Hermitage
98000 | Monaco

sales@luxtrust.com

www.luxtrust.com

DISCLAIMER

Veuillez lire attentivement cette clause de non-responsabilité. Consultez des experts juridiques, techniques et financiers pour obtenir des conseils supplémentaires.

Les informations présentées dans ce livre blanc sont fournies à titre d'information uniquement et n'impliquent en aucun cas une relation contractuelle. Bien que les informations contenues dans ce livre blanc soient fournies de bonne foi et avec la meilleure interprétation de la législation actuelle, ces informations ne constituent en aucun cas un substitut à des conseils juridiques, commerciaux ou financiers et ne doivent pas être utilisées dans cet esprit. Bien que nous ayons fait tout notre possible pour nous assurer que les informations ont été obtenues à partir de sources fiables, LuxTrust ne garantit ni n'accepte la responsabilité de l'exactitude, de l'exhaustivité, de la validité, de l'actualité, de la fiabilité ou de la disponibilité de toute information. LuxTrust ne saurait être tenue responsable des résultats, dommages ou pertes que l'utilisation de ces informations pourrait entraîner.