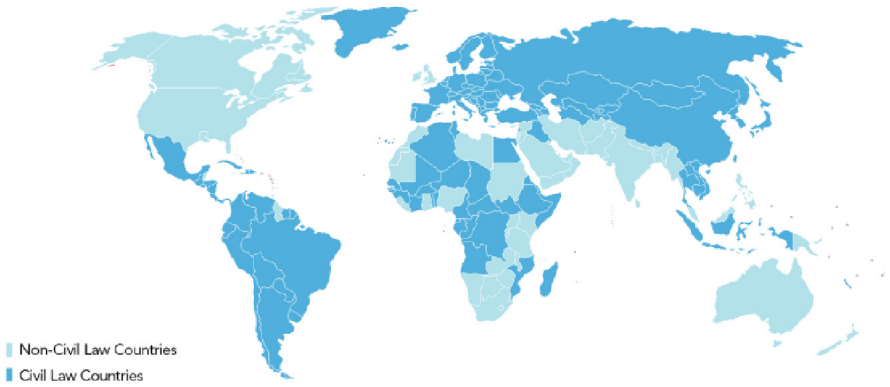
LIVRE BLANC

Démystification de l'usage de la signature numérique dans la sphère commerciale mondiale

En bref

La signature électronique est utilisée dans de nombreux cas, qu'il s'agisse d'un simple « Cliquez sur J'accepte » destiné aux clients ou de transactions contractuelles impliquant plusieurs entreprises, y compris ces solutions adaptées à certaines exigences industrielles dans les sphères pharmaceutiques, bancaires ou gouvernementales. De plus, l'utilisation de la signature électronique, ses obligations légales et son acceptation culturelle sont différentes selon les pays. Cette complexité a généré un manque de clarté, en particulier auprès des sociétés multinationales qui effectuent des transactions électroniques au niveau international. Sur le plan juridique, les différences qui entourent la signature électronique se divisent principalement entre les pays de droit civil et les pays de droit commun. Des sociétés qui opèrent sur des marchés de droit civil tels que l'Europe et l'Asie sont particulièrement intéressées par la manière dont les différences légales influent sur l'utilisation de la signature électronique pour leurs activités. Faisons un tour d'horizon de la signature électronique, clarifions les différences qui existent entre la signature électronique et la signature numérique, et découvrons pourquoi DocuSign est la seule solution dont vous aurez besoin dans les deux cas.



La signature électronique : présentation et légalité

Au cours de ces dix dernières années, la signature électronique a transformé les transactions commerciales. En effet, la signature manuscrite classique est devenue une information électronique rapidement exécutable et juridiquement contraignante qui exploite la technologie de chiffrement, afin de proposer des options telles que le contrôle de version, des documents infalsifiables, des signatures authentifiées et une consultation et une modification du document soumises à autorisation.

Le terme de signature électronique, ou eSignature, désigne la catégorie principale qui regroupe tous les types de signatures électroniques. Dans cette catégorie, vous pouvez retrouver les signatures numériques et la mise en œuvre d'une technologie de signature spécifique appliquée à la signature électronique. Les signatures numériques, tout comme les autres solutions de signature électronique, permettent de signer un document et d'authentifier l'auteur de la signature. Toutefois, des différences subsistent au niveau de leur finalité, des technologies sous-jacentes, de l'utilisation géographique et, tel que nous l'avons vu précédemment, de l'acceptation juridique et culturelle. L'utilisation de la signature électronique et de la signature numérique est notamment très variable en fonction de la législation appliquée dans le pays (pays de droit commun ou de droit civil).

La signature électronique dans les pays de droit commun

La signature électronique est très largement acceptée et utilisée dans les pays de droit commun tels que les États-Unis, le Canada, l'Australie et le Royaume-Uni. D'un point de vue juridique, l'accent est mis sur les faits et circonstances propres à l'acte de signature plutôt que sur une approche technologique particulière. Par conséquent, la définition juridique d'une signature électronique inclut des exigences telles que l'adoption du symbole de la signature par le signataire, apposant sa signature sur le document, et son intention de signer.[1]

Droit commun et droit civil

Dans les pays de droit commun (c.-à-d. les États-Unis, le Canada et le Royaume-Uni) les lois sont dérivées de coutumes ou de la jurisprudence. Les lois sont rédigées puis interprétées par le peuple. Les tribunaux déterminent ensuite si une interprétation d'une loi en particulier, telle que celles relatives à la signature électronique est juste. Les solutions de signature électronique dans les pays de droit commun ont évolué depuis cette compréhension juridique.

Droit commun et droit civil Dans les pays de droit commun (c.-à-d. les États-Unis, le Canada et le Royaume-Uni) les lois sont dérivées de coutumes ou de la jurisprudence. Les lois sont rédigées puis interprétées par le peuple. Les tribunaux déterminent ensuite si une interprétation d'une loi en particulier, telle que celles relatives à la signature électronique est juste. Les solutions de signature électronique dans les pays de droit commun ont évolué depuis cette compréhension juridique.

Par exemple, la signature électronique, telle que définie par la loi américaine ESIGN Act2 est globalement décrite comme un « son, un symbole ou un processus électronique, joint ou logiquement associé à un contrat ou à tout autre document et réalisé ou adopté par une personne dont l'intention est de signer le document ». L'ensemble des 50 États disposent de législations qui définissent les signatures électroniques de la même manière.

De plus, la loi ESIGN exige que la signature soit attribuée à l'individu. En revanche, ce sont les parties au contrat qui définissent les détails relatifs à l'authentification et l'identification du signataire et à la vérification. Toutefois, plus la forme d'authentification est fiable, plus les risques de répudiation sont faibles. Certaines dispositions stipulent qu'une version électronique de la transaction ou une « piste d'audit » doit également être conservée.

Enfin, certaines lois exigent aussi que le document soit infalsifiable, qu'il soit en transit ou stocké, afin de garantir son intégrité à la fois avant et après la signature. Bien que des lois sur la signature électronique différentes de l'ESIGN existent au Canada, au Royaume-Uni et en Australie, ces pays, ainsi que d'autres pays de droit commun, disposent d'une acceptation et de procédures légales similaires en ce qui concerne les signatures électroniques. Dans presque tous les pays, y compris ceux de droit civil, même une signature électronique basique est recevable en tant que preuve devant les tribunaux.

La signature électronique : les principaux termes juridiques

- Sphère de sécurité : une disposition légale qui fournit une protection contre toute poursuite dans la mesure où les conditions spécifiées sont respectées.
- Authentification : le processus de vérification de l'identité du signataire.
- Admissibilité : cas dans lequel la signature électronique est acceptée en tant que preuve par les tribunaux.
- Présomption d'authenticité : les documents signés sont présumés authentiques devant les tribunaux et le signataire doit réfuter l'hypothèse selon laquelle il a signé.
- Répudiation : la répudiation se produit généralement lorsqu'un individu nie toute implication dans une transaction. Le terme « non-répudiation » fait référence à la protection contre un individu qui nie à tort une implication dans une transaction.

La signature électronique dans les pays de droit civil

Dans les pays de droit civil, la procédure régissant les documents manuscrits a, d'un point de vue juridique et historique, toujours inclus les processus de vérification des signatures et documents importants, tels que les actes notariés. Par extension, dans ces pays, les dispositions relatives à la signature électronique décrivent souvent une méthode d'authentification des signatures électroniques spécifique. La signature numérique est ainsi utilisée pour satisfaire à ces dispositions principalement dans les pays de droit civil, tel que ceux d'Europe, d'Asie et d'Amérique latine.

La signature numérique est un type particulier de technologie de signature électronique qui utilise une méthode de chiffrement définie par la norme X.509 pour les infrastructures à clés publiques (PKI), ainsi qu'un processus d'authentification spécifique, le certificat numérique.

Dans les pays de l'Union européenne, la signature électronique est un système à deux niveaux.

Au sein de l'Union européenne (UE), c'est la directive 1999/93/EC portant sur un cadre communautaire pour les signatures électroniques qui régit la signature électronique. La directive européenne a adopté une approche « à deux niveaux » des signatures électroniques.

Dans ce modèle, les signatures électroniques de base, qui proposent des méthodes d'authentification, constituent le premier niveau et ne peuvent pas être considérées comme une preuve non recevable devant les tribunaux. La directive définit le second niveau, la « signature électronique avancée », par des exigences d'authentification particulières considérées comme nécessaires à la sphère de sécurité, qui équivaut à la signature manuscrite. Bien que la technologie de signature numérique régie par la norme X.509 ne soit pas mentionnée de manière explicite par la plupart des textes de loi, l'utilisation fréquente du terme certificat qualifié implique que la SEA (signature électronique avancée) utilise des formes de technologie de signature numérique sous-jacente.

La signature numérique dans l'UE : SEA et SEQ

La directive définit la signature électronique avancée (SEA) et une signature avancée connexe, à savoir la signature électronique avancée obtenue grâce à un certificat qualifié numérique, ci-après dénommée signature qualifiée électronique (SEQ). La directive européenne définit la SEA comme une signature électronique répondant aux exigences suivantes[3]

1. Être uniquement liée au signataire
2. Permettre d'identifier le signataire
3. Être créée via une méthode sous le contrôle exclusif du signataire
4. Être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable

Bien que la directive ne mentionne jamais de manière explicite les signatures numériques régies par la norme X.509, ces exigences ont été rédigées en les prenant en compte. Par conséquent, il existe une forte préférence culturelle pour les signatures numériques régies par la norme X.509 dans les pays de l'UE, malgré le fait que la technologie de signature électronique ait évolué et qu'elle inclut désormais d'autres solutions qui répondent également à ces exigences.

La SEQ, une signature connexe à la SEA. Cette signature implique un processus très strict dans lequel une autorité de certification approuvée par le gouvernement délivre le certificat servant à créer la SEA au moyen d'un « dispositif sécurisé de création de signature »4 (SSCD). Les instances européennes et autres organes de normalisation ont établi qu'un SSCD devait prendre la forme soit d'une carte d'identité physique dotée d'une puce intelligente, soit d'un jeton matériel que le signataire porterait sur lui.

Dans quelles circonstances une signature qualifiée électronique est-elle nécessaire (SEQ) ?

Lors de transactions pour lesquelles une signature manuscrite est exigée, afin de conférer au document un plein effet juridique, une SEQ constitue le seul moyen de répondre aux exigences de manière électronique. Dans la plupart des pays de l'UE, très peu de transactions font partie de cette catégorie. On recense habituellement les opérations suivantes :

- cessions de brevets et licences ;
- cessions de marques ;
- transactions immobilières exigeant la présence d'un notaire ;
- contrats d'assurance ;
- statuts (règlements intérieurs) ;
- ventes de navires ;
- lettres de change.

Système de chiffrement PKI

Dans ce système, deux clés liées sont fournies à chaque utilisateur, une clé privée pour le chiffrement de la signature et une clé publique pour la vérification. La clé privée est conservée en lieu sûr par le signataire, tandis que la clé publique est distribuée et permet de vérifier la signature sans révéler la clé privée.

Certificat numérique

Un certificat numérique est un document électronique qui propose un formulaire d'authentification. Il est obtenu grâce à une source de confiance, l'autorité de certification.

Autorité de certification (AC)

Une autorité de certification (AC) délivre un certificat numérique basé sur les exigences d'identification du signataire et garantit l'authenticité du signataire.

Pour ce qui est des transactions n'exigeant pas de signature manuscrite de manière explicite, les faits sont très différents. L'avantage d'une SEQ est qu'elle dispose du même effet juridique qu'une signature manuscrite, garantissant l'identité d'un signataire et l'authenticité du document électronique au plus haut niveau. C'est pour cette raison que le système européen de signature électronique est souvent défini comme une règle à deux niveaux. Elle reconnaît la validité et la recevabilité de nombreux types de signatures électroniques et méthodes d'authentification, tout en rehaussant le statut juridique des signatures qualifiées.

Conformément aux principes de droit commun, une telle distinction n'a guère de sens, étant donné que toute signature, manuscrite ou électronique, est considérée comme une preuve et doit être justifiée dans tous les cas. Toutefois, dans la plupart des pays de droit civil, la distinction a son importance, car une signature manuscrite (et par extension, une SEQ) est présumée authentique et impose au signataire de justifier que la signature n'est pas la sienne. Cette disparité juridique constitue la principale raison pour laquelle les praticiens du droit européen conseillent à leurs clients d'utiliser uniquement la solution SEQ.

Dans la pratique, du fait du coût et des inconvénients liés au respect de normes strictes, l'usage des SEQ est largement limité au secteur de l'administration électronique.5 Bien que sa méthode d'authentification rigoureuse fournisse une sphère de sécurité pour répondre à la définition législative d'une SEA, selon la nature et le niveau de risque de la transaction, cette catégorie de signature électronique est tout à fait inutile. De plus, permettre à chaque pays de déterminer ses propres fournisseurs de certificat qualifié numérique dignes de confiance a conduit à une fragmentation qui a atrophié le développement de solutions SEQ viables à travers plus d'un pays membre de l'UE.[6]

Les SEQ sont uniquement requises dans une minorité de cas et sont généralement peu pratiques.

Enfin, l'utilisation de la signature électronique dépend de la nature de la transaction, ainsi que des risques et des coûts associés. Par exemple, les exigences relatives à la signature avancée satisfaites par la signature numérique ne sont pas requises pour tous les types de transaction. La disposition sur la non-discrimination de la directive sur les signatures électroniques, appliquée à tous les États membres de l'UE, stipule que l'efficacité et la recevabilité juridiques d'une signature électronique ne peuvent pas être refusées au seul motif que cette dernière se trouve sous la forme électronique, ne repose pas sur un certificat qualifié ou n'est pas générée par un dispositif sécurisé de création de signature.[7]

En Europe, la confusion qui règne au sujet des types de transactions commerciales pouvant être signées de manière électronique, des cas dans lesquels une SEQ est exigée et de la combinaison de matériel et de logiciel nécessaire a conduit à une utilisation des signatures électroniques nettement inférieure à celle faite en Amérique du Nord.

Certificat qualifié

Un certificat numérique délivré par une autorité de certification (AC) approuvée par le gouvernement et qui a satisfait aux exigences strictes sur la fiabilité et le stockage du certificat, la détection de fraude et la révocation en plus des contrôles financiers et de sécurité.

L'avenir de la SEQ en Europe

En 2012, la Commission européenne, reconnaissant les limites de sa directive initiale sur les signatures électroniques, a proposé de nouvelles dispositions sur la signature électronique8. Cette proposition a été spécialement mise en œuvre pour favoriser le développement de solutions SEQ utilisables et paneuropéennes destinées à un usage commercial. Parmi les nombreuses modifications recensées, cette proposition contient des éléments spécifiques qui pourraient accroître l'adoption des SEQ :

- L'introduction de services de confiance et d'identification électronique en tant que concepts singuliers et distincts de la signature électronique.
- La capacité pour les signataires de confier des dispositifs de création de signatures électroniques qualifiées à un tiers, à condition que le signataire exerce un contrôle exclusif sur ce dispositif.
- Exigences

Tant que cette proposition ou d'autres ne seront pas entrées en vigueur, et tant que de nouvelles normes ne seront pas mises en place en conséquence, l'adoption des SEQ restera limitée en UE, et les solutions spécifiques à chaque pays et non interopérables demeureront la norme.

Signature électronique en dehors de l'UE

D'autres pays peuvent également décrire une structure à deux niveaux similaire et définir une « signature électronique simple » comme une signature électronique de base et faire référence au terme de « signature électronique sécurisée » avec les mêmes caractéristiques que celles de la signature numérique. Parmi les pays qui utilisent également le modèle à deux niveaux figurent le Japon, Singapour, la Chine, Hong Kong, l'Inde, la Nouvelle-Zélande et l'Afrique du Sud. Enfin, il existe quelques pays de droit civil tels que la Biélorussie, la Bulgarie, la Corée du Sud, la Colombie et le Costa Rica dans lesquels les experts juridiques conseillent à leurs clients d'accepter uniquement la signature numérique avec un certificat qualifié.

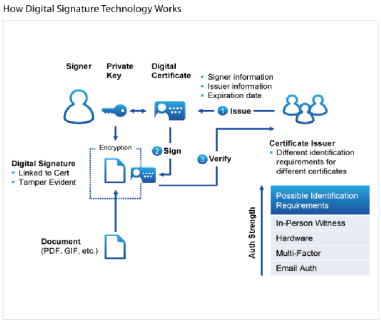
La signature numérique est utilisée dans certains secteurs

Plusieurs secteurs d'activités tels que la pharmaceutique, les banques, l'aviation, l'administration publique et l'éducation sont également contraints d'utiliser les signatures numériques. Dans la plupart des cas, ces secteurs nécessitent des certificats numériques spécifiques pour authentifier le signataire, tels que les certificats SAFEBioPharma requis pour les transactions au sein des secteurs de la pharmaceutique et des sciences de la vie et pour les transactions avec ou régies par la Food and Drug Administration (Agence américaine des produits alimentaires et médicamenteux).

Choix d'un type de signature électronique : prendre en compte la transaction, les risques et la culture

Les entreprises doivent adopter un type de signature électronique qui, non seulement répond aux exigences légales régionales, mais reflète également l'acceptation culturelle, la nature et le niveau de risque de la transaction, ainsi que les coûts associés. Dans la plupart des cas, une SEQ n'est pas nécessaire à moins qu'une loi spécifique existe et exige une signature manuscrite pour un type particulier de transaction. De plus, outre ces cas particuliers, une SEA est toujours légalement applicable en cas d'utilisation commerciale et doit être recevable en tant que preuve devant les tribunaux.

Comment fonctionne la technologie de signature numérique



La solution de gestion des transactions qui utilisent la signature électronique de DocuSign

Contrairement aux autres technologies de signature électronique, la solution de gestion des transactions qui utilisent la signature électronique de DocuSign constitue l'unique solution proposant un procédé commercial complet, sécurisé et basé sur le Cloud permettant de préparer, d'exécuter et de gérer vos transactions, que vous ayez besoin d'une simple signature électronique ou d'une signature électronique avancée avec une technologie de certificat numérique régie par la norme X.509.

PRÉPARER La solution de DocuSign permet une préparation simple de vos documents grâce à des formulaires électroniques accessibles par glisser/déplacer et un accès aux informations nécessaires depuis le Cloud ou toute autre application commerciale. La gestion électronique de processus et la capacité à attribuer des rôles et accorder des autorisations proposent une gestion et un contrôle rigoureux.

EXÉCUTER DocuSign permet d'exécuter de manière efficace et juridiquement contraignante les transactions qui peuvent être intégrées à des services tels que le traitement des paiements. DocuSign fournit une solution de signature numérique tout à fait conforme et répondant aux exigences de la SEA. De nombreuses méthodes d'identification sont également disponibles afin d'authentifier une signature électronique de base.

GÉRER La plateforme fournit également un tableau de suivi qui vous permet de contrôler la progression et le statut à chaque étape du déroulement du travail. Les documents signés, ainsi que la piste d'audit complète sont disponibles dans le système de stockage des preuves matérielles de DocuSign.

La signature électronique DocuSign.

La solution de signature électronique classique de DocuSign propose des options telles que l'authentification multiple, la détection de fraude et la saisie et le retrait du consentement du client qui excèdent les exigences réglementaires, afin de fournir la solution de signature électronique de base la plus complète, sécurisée et fiable. Parmi nos certifications et audits figurent ISO 270001, SSAE 16, TRUSTe, PCI DSS 2.0 et la certification relative au respect des principes de la sphère de sécurité du ministère du commerce des États-Unis

Prise en charge de DocuSign pour les signatures numériques

Les clients qui préfèrent ou nécessitent une solution de signature numérique peuvent désormais employer la solution complète de gestion des transactions qui utilisent la signature

Déterminer si une signature qualifiée électronique doit être utilisée ou non :

- Légalité : Une signature manuscrite est-elle explicitement exigée par la loi pour ce type particulier de transaction ?
- Facilité d'utilisation : Le signataire dispose-t-il déjà d'un certificat qualifié numérique correspondant à la juridiction qui régit la transaction ?
- Exigences relatives à l'« authentification présumée » : L'« authentification présumée » est-elle nécessaire ou le caractère admissible et exécutoire au niveau juridique est-il suffisant ?

La technologie de signature numérique fonctionne comme suit :

1. Émission : Un émetteur de certificat ou une AC authentifie ou valide l'identité du signataire et émet un certificat numérique qui inclut les informations relatives au signataire, ainsi que sa clé publique.
2. Signature : Le contenu du document est chiffré, ce qui permet de détecter toute modification apportée au contenu ou toute tentative de falsification. La signature numérique unique est créée grâce à une méthode de chiffrement du document utilisant la clé privée du signataire. L'empreinte numérique chiffrée unique ainsi obtenue est liée au document et au certificat numérique.
3. Vérification : La personne qui reçoit le document peut déchiffrer l'empreinte numérique grâce à la clé publique figurant sur le certificat numérique et ainsi vérifier l'identité du signataire et confirmer l'intégrité du contenu du document. L'intégrité du certificat numérique du signataire peut être vérifiée, car il a été signé de manière numérique par l'émetteur du certificat.

électronique de DocuSign grâce à la signature numérique Express de DocuSign pour une solution commerciale complète et sécurisée. La solution de signature numérique DocuSign utilise la norme de chiffrement PKI et de détection de fraude reconnue dans l'industrie. En outre, DocuSign simplifie l'utilisation de la signature numérique et permet un déploiement rapide grâce à notre solution de signature numérique basée sur le Cloud et entièrement intégrée.

Une solution de gestion des transactions complète

D'autres fournisseurs de solution de signatures numériques proposent uniquement un service de signature et vous contraignent à obtenir et à incorporer un système d'authentification par vos propres moyens. La solution de signature numérique de DocuSign répond parfaitement à la définition privilégiée de la signature électronique avancée par les juridictions européennes et est fournie dans une solution commerciale complète dotée de nombreuses fonctions qui vous permettent de préparer, d'exécuter et de gérer vos transactions.

Une solution basée sur le Cloud diminue les coûts, optimise la maniabilité et la commodité

La plupart des solutions de signature numérique sont matérielles et par conséquent, sont coûteuses et difficiles à déployer et à gérer. Les jetons matériels, porte-clés et cartes à puce onéreux que les utilisateurs portent sur eux afin de fournir des preuves authentifiant leur signature peuvent représenter un investissement important. La solution de signature numérique de DocuSign basée sur le Cloud ne requiert aucun matériel et est disponible, rapidement déployée et prête à l'emploi à travers le monde, à tout moment.

Une solution de signature numérique intégrée

Jusqu'à présent, déployer une solution de signature numérique et tenter d'intégrer des certificats numériques était un processus complexe et coûteux. Des efforts ont été déployés et du temps dépensé pour tenter d'obtenir un certificat intégré à un fournisseur de signature numérique ou la mise en place d'une solution de certificat sur site onéreuse. DocuSign a simplifié le déploiement du certificat et de la signature numérique en devenant une Autorité de certification et en délivrant directement des certificats dans le cadre de notre solution de signature numérique DocuSign Express.

La signature numérique DocuSign Express est totalement conforme aux normes PKI X.509 et prend en charge toutes les méthodes d'authentification de DocuSign préférées par l'industrie, afin de permettre aux utilisateurs de signer des documents rapidement et facilement. La signature numérique DocuSign Express génère automatiquement un certificat numérique, qui correspond au degré d'authentification de la transaction, au moment de la signature. Cela vous permet d'exiger des signatures électroniques avancées de tout signataire sans pour autant les contraindre à posséder un certificat numérique.

Prise en charge de la signature numérique des tierces parties

DocuSign continue à prendre en charge les signatures numériques des tierces parties grâce au certificat numérique SAFE-BioPharma destiné aux industries pharmaceutiques et des sciences de la vie.

Exemples de cas d'utilisation SÉCURISÉE de BioPharma :

1. Signature de demandes d'autorisation, de documents relatifs aux essais cliniques, de carnets de laboratoires et de contrats pour les sociétés pharmaceutiques.

2. Signature de prescriptions électroniques pour la Drug Enforcement Administration, (DEA, service chargé de la mise en application de la loi sur les stupéfiants).

3. Transactions réglementées avec la Food and Drug Administration (FDA, Administration des aliments et drogues) et l'Association médicale européenne (EMA).

Pour obtenir de plus amples informations sur les signatures numériques DocuSign Express, veuillez contacter votre représentant des ventes DocuSign ou envoyer un e-mail à l'adresse suivante : sales@docusign.com.

La référence mondiale en matière de gestion des transactions numériques (Digital Transaction Management™)

Suivez-nous

À propos de DocuSign

DocuSign® est la référence mondiale en matière de gestion des transactions numériques (Digital Transaction Management™). DocuSign est utilisé pour accélérer les délais de transaction afin d'obtenir des résultats plus rapidement, de réduire les coûts et de satisfaire les clients à travers le réseau mondial le plus simple, le plus rapide et le plus fiable du Cloud pour l'envoi, la signature, le suivi et le stockage de documents.

Pour toute demande sur le territoire américain : numéro gratuit **866 219 4318** | **docusign.com**

Pour toute demande sur le territoire EMEA : téléphone **+44 203 714 4800** | e-mail **emea@docusign.com** | **docusign.co.uk**