

Les signatures Notarius sont-elles juridiquement fiables et reconnues par les tribunaux?



Chez Notarius, on nous demande souvent si nos signatures numériques et électroniques sont juridiquement fiables et reconnues par les tribunaux. Bien qu'en apparence simple, cette question requiert la compréhension de certaines notions. Clarifions d'abord quelques termes, définitions et concepts en lien avec les signatures sur support électronique.

Termes, définitions et concepts

Chez Notarius, nous considérons que l'expression « **signature électronique** » englobe toutes les signatures sur support électronique. Les signatures électroniques comprennent donc les images de signature manuscrite, les enregistrements vocaux permettant de consentir à une transaction, les signatures apposées via une plateforme de signature électronique ainsi que les signatures apposées par les titulaires d'un certificat de signature numérique.

SIGNATURE ÉLECTRONIQUE AUTODÉCLARÉE



L'expression « **signature électronique autodéclarée** » signifie que l'identité du signataire est autodéclarée et qu'elle n'a pas été autrement vérifiée ou validée par un tiers. Par exemple, le certificat numérique autosigné d'Adobe ou le bloc-signature d'un compte Gmail correspondent à cette définition.

SIGNATURE ÉLECTRONIQUE DE CONFIANCE



L'expression « **signature électronique de confiance** » signifie que l'identité du signataire a été à tout le moins vérifiée ou validée par un tiers. Les signatures apposées via la plateforme ConsignO Cloud, qui requiert que *deux facteurs d'authentification* connus du signataire (tels son adresse de courriel et son numéro de téléphone cellulaire) soient utilisés pour authentifier le signataire avant qu'il n'appose sa signature, en sont un exemple. Si les informations d'authentification sont incorporées à la signature, celle-ci peut être qualifiée de « signature électronique de confiance », puisque ces informations d'authentification proviennent d'un tiers et qu'elles sont divulguées de façon transparente aux parties concernées.

SIGNATURE NUMÉRIQUE



Chez Notarius, la « **signature numérique** » représente une signature plus fiable qu'une signature électronique puisqu'elle :



contient des informations protégées cryptographiquement



est émise par une autorité de certification de confiance via une infrastructure à clé publique robuste



2 pièces d'identité



Vérification de l'identité en face à face avec un agent

requiert que le signataire soit titulaire d'un certificat de signature numérique



exige des méthodes d'authentification fortes

En se basant sur cette terminologie, on peut affirmer que les différentes signatures CertifiO de Notarius sont des *signatures numériques* et que la solution ConsignO Cloud permet à la fois d'apposer des *signatures électroniques de confiance* (le signataire n'a pas de certificat de signature numérique) et des *signatures numériques* (le signataire possède un certificat de signature numérique délivré par Notarius).

Fiabilité de la signature

Afin de savoir si une signature est valide en droit et reconnue par les tribunaux, il est également nécessaire de parler de la fiabilité de la signature. Chez Notarius, la fiabilité d'une signature repose sur quatre éléments fondamentaux :



L'identité : Dans quelle mesure les parties concernées peuvent-elles être assurées que l'identité du signataire est véridique ?



L'authenticité : Tous les renseignements permettant d'attester de l'identité des signataires et de l'intégrité du document sont-ils intégrés au document ?



L'intégrité : Dans quelle mesure les parties concernées peuvent-elles être assurées que le document n'a pas été modifié ?



La pérennité : Dans quelle mesure les parties concernées peuvent-elles être assurées que le document pourra être ouvert, lu et authentifié sur plusieurs décennies ?

En fonction des technologies actuelles, la meilleure façon d'assurer un niveau de fiabilité élevé en matière d'*identité*, d'*intégrité* et d'*authenticité* consiste à apposer une signature numérique en utilisant un certificat de signature numérique, lequel est délivré au signataire par une autorité de certification de confiance via une infrastructure à clé publique robuste. Comme mentionné ci-dessus, les *signatures électroniques de confiance* offrent également un niveau de fiabilité élevé.

En fonction des technologies actuelles, la meilleure façon d'assurer la pérennité d'un document est de le rendre conforme à la norme PDF/A (ISO 19005) et d'utiliser une signature numérique conforme à la norme PAdES, qui assure la validité à long terme des signatures.

Notarius est l'une des très rares autorités de certification au monde, sinon la seule, à combiner une expertise approfondie des opérations effectuées par l'entremise d'une infrastructure à clé publique et les différentes normes PDF et PDF/A. À titre d'exemple, Notarius est la seule autorité de certification [membre de l'Association PDF](#). Grâce à cette expertise combinée, les clients de Notarius peuvent véritablement créer, vérifier et conserver des documents électroniques hautement fiables.

Validité en droit

La validité en droit de tout type de signature électronique requiert l'analyse des points suivants - il n'y a malheureusement **PAS** de raccourcis :



Sur quel type de document la signature sera-t-elle apposée ? Quel processus sera utilisé ? Et quelles seront les modalités ? À titre d'exemple, les modalités pourraient comprendre une clause de *forum conveniens* selon laquelle les parties conviennent de la juridiction régissant leur contrat. (Une « juridiction » peut être un État, une province, un pays ou même l'Europe dans son ensemble.)



En fonction du type de document utilisé et de la juridiction applicable, **quelles lois régissent les signatures électroniques ?**



En fonction de la juridiction applicable, **existe-t-il des dispositions législatives ou réglementaires particulières** exigeant l'utilisation d'un certain type de signature ou de document qui pourraient avoir une incidence directe sur la validité en droit des signatures électroniques ? (Au Québec, par exemple, seulement trois formes de testaments sont prescrites, et aucune d'entre elles n'est un document électronique signé uniquement par le testateur.)



En fonction de la juridiction applicable et à l'exception de toute disposition législative ou réglementaire régissant un certain type de signature ou de document, **quel est le cadre juridique applicable** par défaut pour les signatures électroniques ?

Il incombe à chaque organisation qui envisage d'utiliser des signatures électroniques d'effectuer l'analyse en quatre étapes décrite ci-dessus, et ce, pour chaque type de document qu'elle souhaite utiliser. En guise de point de départ dans cette analyse, voici quelques généralités concernant la validité en droit des signatures électroniques.

Au Canada, aux États-Unis et en Europe, le cadre général régissant la validité des signatures électroniques découle du travail de la Commission des Nations Unies pour le droit commercial international (CNUDCI) à la fin des années 1990. Au terme de ce travail, des lois modèles ont été proposées, puis finalement adoptées partout au Canada, aux États-Unis et en Europe. Le principe général que l'on retrouve dans toutes ces juridictions est le même :

On ne peut priver un document électronique de ses effets juridiques uniquement parce qu'il s'agit d'un document électronique.

De plus, une lecture attentive des lois sur les signatures électroniques permet de constater qu'il existe deux types de signature électronique au sens de la loi :

- La **signature électronique authentique**, laquelle est acceptée par les tribunaux comme une preuve ne requérant pas de preuves corroborantes. Il incombe habituellement à la partie qui prétend que la signature électronique n'est pas valide de prouver qu'elle ne l'est pas;
- La **signature électronique non authentique**, laquelle est acceptée par les tribunaux comme un commencement de preuve requérant des preuves corroborantes. Il incombe généralement à la partie qui prétend que la signature électronique est valide de prouver qu'elle l'est.

Il est également possible de dégager les grandes lignes suivantes en ce qui concerne la validité des signatures électroniques au Canada, aux États-Unis et en Europe :



Au Canada, la validité de la plupart des signatures électroniques est régie par les lois provinciales. Toutes les provinces ont adopté, dans une certaine mesure, la même [loi type sur le commerce électronique de la Conférence pour l'harmonisation des lois au Canada \(CHLC\)](#) au début des années 2000. Les signatures numériques et les signatures électroniques de confiance de Notarius dépassent les exigences de validité juridique des lois provinciales et fédérales canadiennes sur le commerce électronique.



Aux États-Unis, l'utilisation des signatures électroniques est une pratique acceptée depuis que le Congrès a adopté la *Electronic Signatures in Global and National Commerce Act (ESIGN Act)* en 2000. Cette loi est fondée sur une loi antérieure, la *Uniform Electronic Transactions Act (UETA)*. Quarante-sept États ont ratifié l'UETA, tandis que les États de New York, de Washington et de l'Illinois ont adopté des lois semblables. Les signatures numériques et les signatures électroniques de confiance de Notarius répondent aux exigences juridiques des États-Unis et peuvent garantir l'identité des signataires ainsi que l'intégrité, l'authenticité et la pérennité des documents signés électroniquement.



Le règlement de l'Union européenne sur l'identification électronique et les services fiduciaires pour les transactions électroniques du marché intérieur (eIDAS) est la loi régissant les signatures électroniques en Europe. Cette loi partage des similitudes avec la législation nord-américaine. Notarius répond aux exigences du règlement européen eIDAS en matière d'émission de signatures électroniques qualifiées grâce à sa conformité aux normes ETSI EN 319 401; ETSI EN 319 411-1; et ETSI EN 319 411-2. Le certificat eIDAS de Notarius (n° CEIDAS-122017-OCU00210) couvre l'ensemble des activités de Notarius, tant techniques qu'administratives, pour le développement, l'exploitation et le service de soutien de ses produits de signature numérique, à titre de tiers de confiance.

En résumé, les *signatures numériques* et les *signatures électroniques de confiance* de Notarius offrent un niveau de fiabilité très élevé, et les documents signés à l'aide de ces signatures seront considérés comme valides en droit, sous réserve de rares dispositions législatives et réglementaires excluant l'utilisation de toute signature électronique ou numérique.

Validité devant les tribunaux

Au regard de l'analyse en quatre étapes suggérée ci-dessus, il est impossible d'affirmer avec certitude qu'une quelconque forme de signature sera universellement acceptée dans toutes les juridictions et pour tous les types de document. Notarius soutient néanmoins que toutes ses signatures, *si elles sont utilisées dans un contexte où aucune disposition législative ou réglementaire particulière n'interdit leur utilisation ou ne prescrit un type bien précis de signature électronique, seraient jugées valides par les tribunaux au Canada, aux États-Unis et en Europe.*

À ce jour, bien que Notarius soit en affaires depuis plus de 20 ans et que des millions de documents aient été signés à l'aide de ses produits dans le monde entier, jamais une signature de Notarius n'a été jugée invalide par un tribunal, [ce qui ne peut être affirmé par le principal fournisseur de signatures électroniques.](#)

Certifications

- Première autorité de certification en Amérique du Nord à être certifiée **ISO 27001**;
- Seule entreprise canadienne à émettre des signatures de confiance reconnues par **Adobe** (Adobe Approved Trust List – AATL) et **eIDAS** (electronic IDentification Authentication and trust Services);
- Notarius est également conforme à la norme de gestion de la qualité **ISO 9001**.



Pour plus d'information

notarius.com | 1 888 588-0011 | info@notarius.com



notarius

Transformation numérique.
Documents juridiquement fiables.