

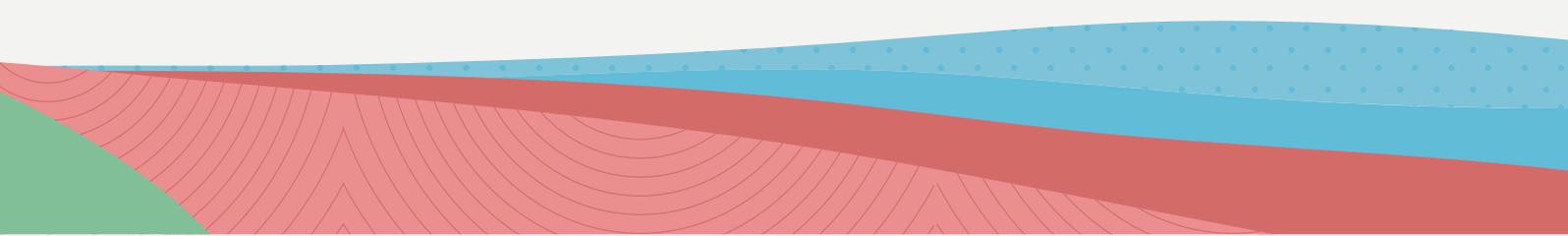
∞drive

Le cadre juridique de la signature électronique



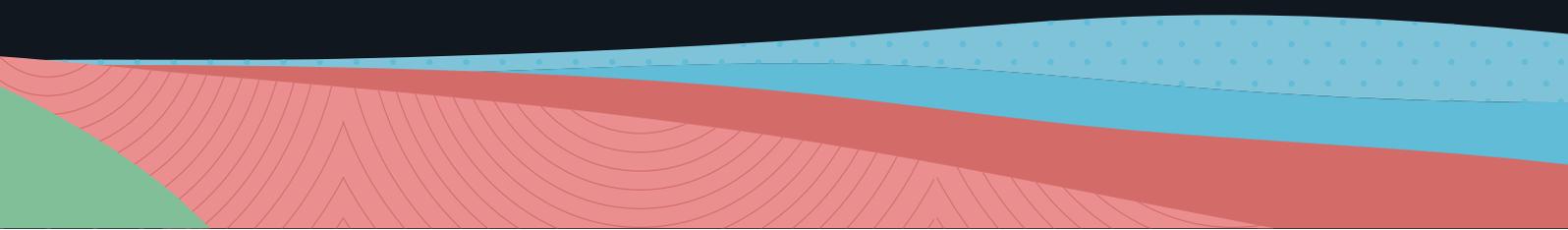
Sommaire

La définition légale de la signature électronique	3
Les textes juridiques qui régissent le cadre légal de la signature électronique	5
Vision de la signature électronique dans le monde	8
Les conditions de validité de la signature électronique	10
Les quatre types de signature électronique	12
L'identification du signataire	16
La certification de la signature électronique	18
L'archivage légal de vos documents	20
Le mode « offline »	22
La mention manuscrite	24
Que dit le juge ?	26
Conclusion	28



01

La définition légale de la signature électronique



L'article 1316-4 du code civil créé par la loi n°2000-230 du 13 mars 2000 - art. 4 JORF 14 mars 2000, devenu l'article 1367 suite à l'ordonnance 2016-131, définit la signature et pose l'équivalence entre la signature manuscrite et la signature électronique sous certaines conditions :

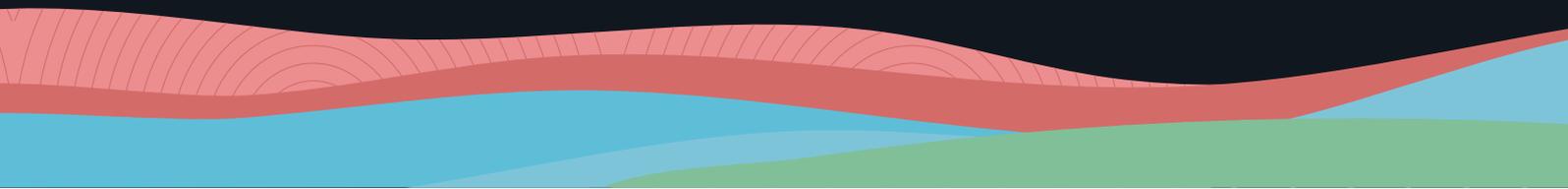
Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

En droit français, la signature est donc définie par référence au procédé technique utilisé pour signer.



02

Les textes juridiques qui encadrent
la signature électronique



Afin d'entamer la partie juridique de ce livre blanc, il est nécessaire de vous lister les textes des règlements, des lois et des décrets européens et français, concernant la construction juridique de la notion de signature électronique :

Les textes français

Aux termes de l'Art. 1367 Al1 du Code civil la signature, qu'elle soit électronique ou manuscrite, **« identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte »**.

Le droit français donne de la signature électronique une **définition fonctionnelle générale**: *« lorsque [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache »* (Art. 1367 Al. 2 Code civil).



Le texte européen : le règlement eIDAS

Le règlement européen eIDAS, directement applicable en France, définit la signature comme un « service de confiance » qui peut avoir trois niveaux (simple/ avancé/qualifié). Il s'accompagne d'une **« législation secondaire »** qui renvoie à des normes techniques ETSI à l'aune desquelles peut se mesurer la qualité d'un service de signature, même lorsque la signature n'atteint pas le niveau « qualifié » le plus élevé.

Les trois niveaux de signature prévus par le Règlement eIDAS sont les suivants :

La signature simple

Donnée sous forme électronique, qui est jointe ou associée logiquement à d'autres données sous formes électroniques et que le signataire utilise pour signer.

La signature avancée

Signature électronique qui satisfait aux exigences énoncées à l'article 26, à savoir :

- a) être liée au signataire de manière univoque
- b) permettre d'identifier le signataire
- c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et...
- d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure de ces données soit détectable

La signature qualifiée

Signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique

La signature présumée fiable du droit français

Aux termes du Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, la signature qualifiée est présumée fiable au sens du droit français :

La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.

Ce n'est pas parce qu'une signature n'est pas qualifiée qu'elle est privée d'effet juridique (Article 25.1 Règlement eIDAS): il faudra démontrer sa fiabilité en cas de litige, puisqu'elle ne bénéficie pas de présomption d'équivalence avec la signature manuscrite.

Le rôle du prestataire de service de confiance

Les services de signature ou de cachet électronique sont délivrés par des prestataires de service de confiance (PSC) qui sont tenus d'un certain nombre d'obligations légales et qui sont garants de la fiabilité du dispositif.

Les responsabilités et les modalités de contrôle des prestataires de services de confiance sont définies par le Règlement eIDAS (Art. 19).



03

Vision de la signature
électronique dans le monde



Il existe **4 cas de validité** de la signature électronique dans le monde :

Cas n°1

Ella a la **même valeur légale que la signature manuscrite** : Etats-Unis, Canada, Australie etc.

Cas n°2

Elle est valable juridiquement mais elle **n'a la même valeur que la signature manuscrite que sous certaines conditions** : Union européenne, Chine, Japon.

Cas n°3

La signature électronique est **valable uniquement si le signataire dispose d'un certificat numérique** : Argentine, Brésil, etc.

Cas n°4

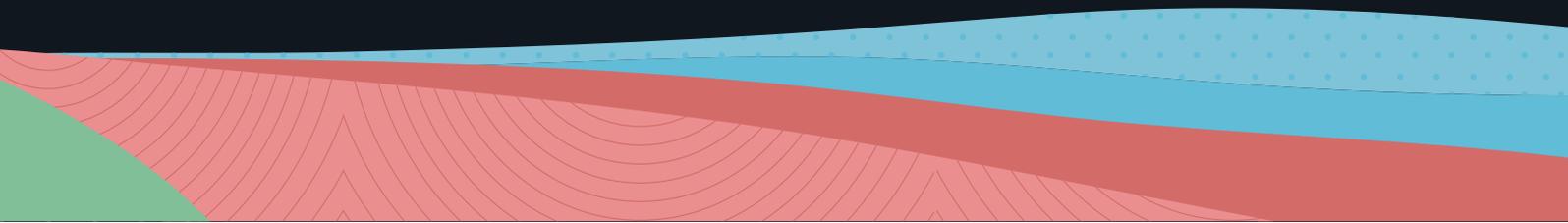
Il n'existe pas de législation. La signature manuscrite est la seule preuve évidente d'un acte signé : Ukraine, Thaïlande, Venezuela, presque toute l'Afrique etc.

Pour les cas 2 et 3, il faudra donc prouver que la signature électronique a une valeur juridique et qu'elle identifie légalement un signataire. D'où l'importance de recourir à une solution sécurisée octroyant ces garanties légales.

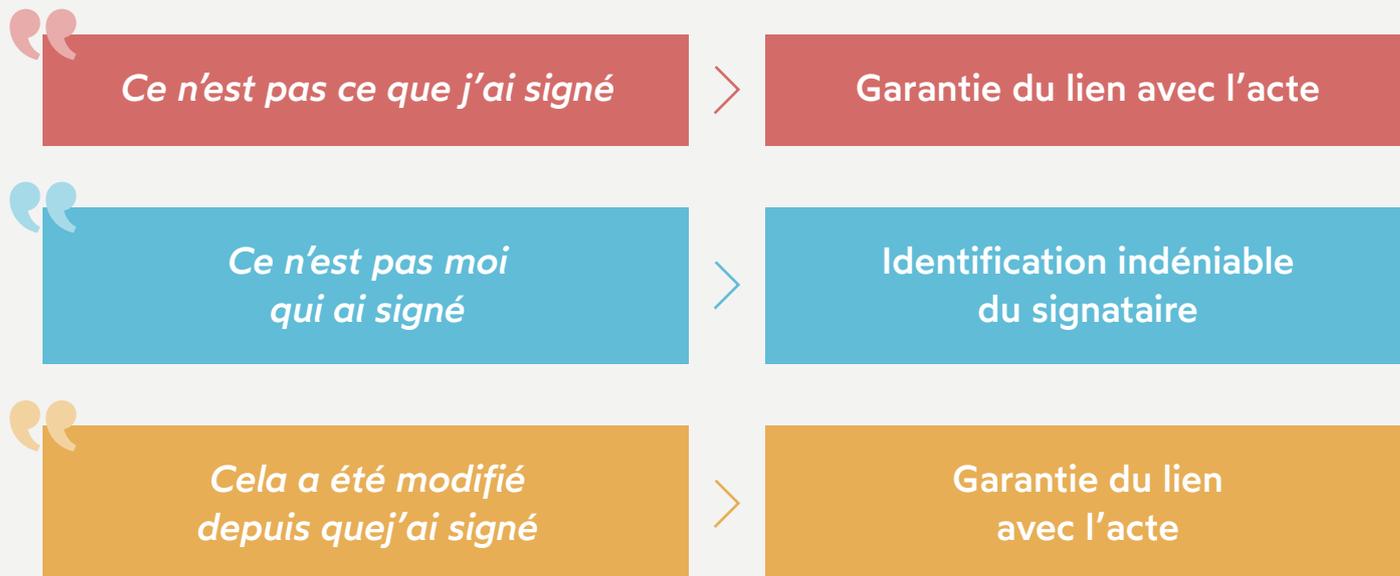


04

Les conditions de validité de la signature électronique

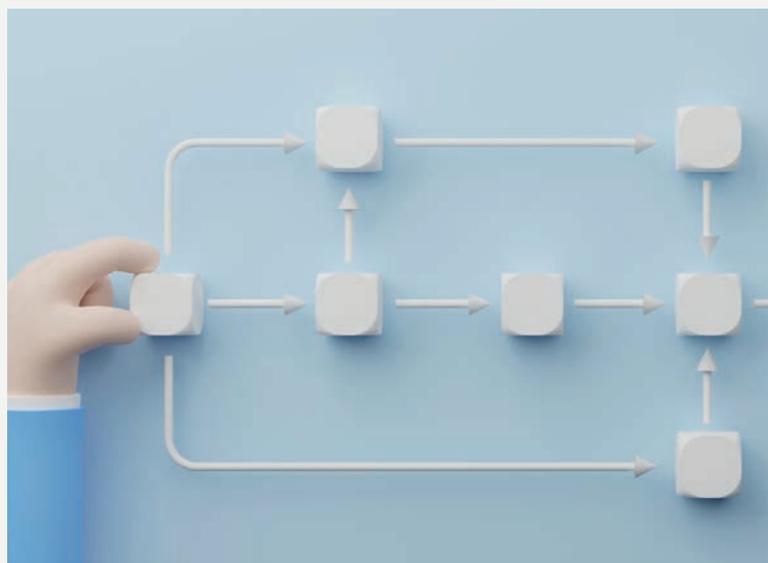


Compte tenu de la définition donnée précédemment, toutes les signatures électroniques sont recevables en justice à partir du moment où elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et la garantie de l'acte signé, tel que cela est résumé dans le schéma suivant :



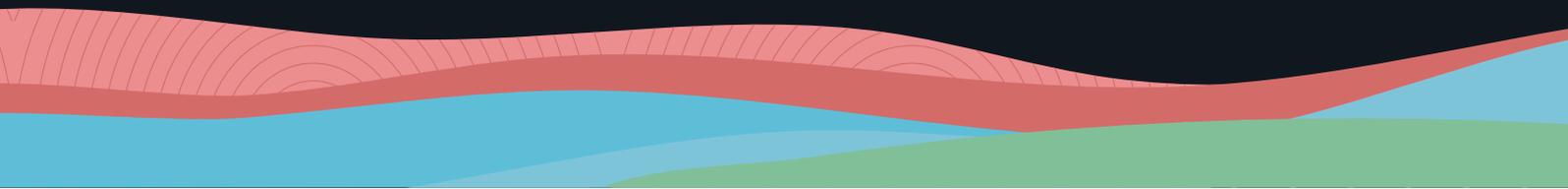
- Elle permet l'identification indéniable du signataire, aussi appelée « non répudiation »
- Elle garantit l'intégrité de l'acte
- Elle assure le lien avec l'acte

Comme pour la signature manuscrite, la signature électronique peut être contestée lors d'un litige. Mais dans la mesure où l'identification indéniable du signataire et l'intégrité de l'acte sont assurées, la remise en cause d'une signature électronique est donc plus difficile que celle de son homologue manuscrit.



05

**Les quatre types de
signature électronique**



L'article 25 du règlement eIDAS stipule :

- L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.
- L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.
- Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres.
- L'eIDAS précise donc que toute signature électronique est juridiquement valable. Toutefois, il encadre plus précisément deux types de signatures: la signature avancée et la signature qualifiée. Les autres ne sont pas encadrés et sont appelés «simples».

1. La signature simple

Dite à bas niveau de reconnaissance juridique: elle n'est pas présumée fiable mais l'écrit signé ainsi sous forme électronique ne pourra être refusé en justice à titre de preuve dès lors que le procédé permet d'identifier le signataire et de garantir le lien avec l'acte signé.

En cas de contestation, il est donc nécessaire de prouver la fiabilité du procédé de signature électronique utilisé.

A titre d'exemple, ce qui ne constitue pas une signature électronique, même simple :

La signature numérisée

La Cour de cassation a pu considérer que l'adjonction à un document électronique de l'image de la signature manuscrite ne constituait pas une signature électronique fiable: il s'agit d'une simple signature manuscrite numérisée, qui peut être jointe par toute personne détenant l'image du graphe du prétendu signataire.

Ainsi, une lettre de licenciement revêtue d'une signature numérisée est donc, sur ce point, irrégulière. (Cass. Soc. 17 mai 2006, n° 04-46.706)

La signature par mail

La Cour de cassation a annulé la décision de la cour d'appel lors d'un litige entre un bailleur et une locataire. Cette dernière accusait son bailleur d'être revenu sur sa décision énoncée par mail concernant le préavis de la location. En première instance, la cour d'appel avait donné raison à la locataire.

Cependant, la cour de cassation a réfuté cette décision car il n'y avait aucune preuve qui reliait l'auteur du mail au bailleur. Ainsi, une confirmation ou une signature par mail ne peut être considérée comme une preuve car l'identité du signataire ne peut être reconnue. (Cour de cassation du 30/09/2010)

2. La signature avancée

Une signature électronique avancée satisfait aux exigences suivantes :

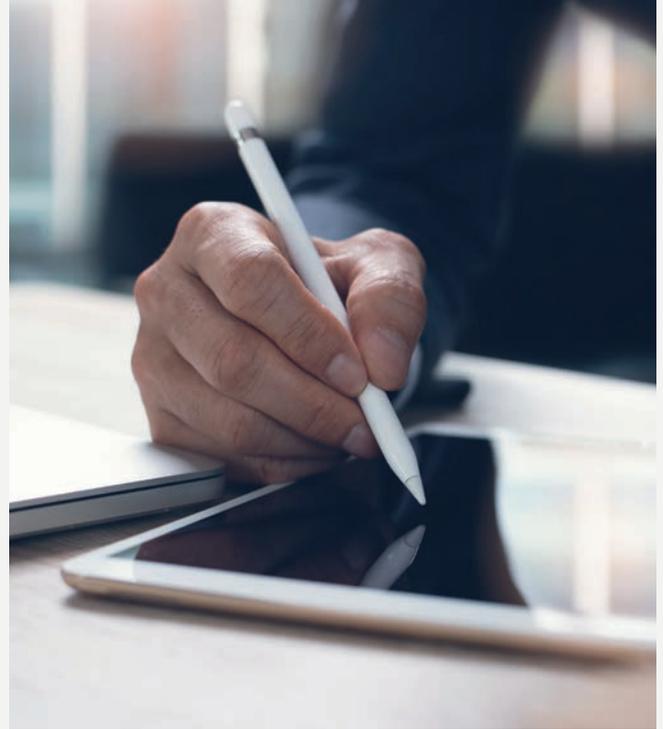
- Être liée au signataire de manière univoque ;
- Permettre d'identifier le signataire ;
- Avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;
- Être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

On le voit, dans les deux cas de la signature avancée et de la signature qualifiée, l'eIDAS exige qu'un certificat électronique nominatif soit établi au nom du signataire après vérification de son identité par une autorité de certification agréée. Les autres sont par défaut désignées comme des signatures dites simples.

3. La signature qualifiée

Celle-ci est présumée fiable jusqu'à preuve du contraire.

Lorsque la signature électronique est créée, l'identité du signataire est vérifiée en face à face par une autorité agréée et l'intégrité de l'acte garantie dans les conditions fixées par l'eIDAS. De plus, tous les services utilisés dans l'opération de signature (certificat, service de signature, horodatage) doivent être qualifiés pour que la signature soit qualifiée.



4. La signature certifiée

Dans la pratique, il est souvent nécessaire de pouvoir faire signer électroniquement une personne sans assumer les délais et les coûts d'une vérification de son identité par une autorité agréée.

Les usages ont donc fait émerger un autre type de signature, qui est devenu le plus répandu et que nous appellerons **signature certifiée**.

Avec la **signature certifiée**, des certificats qualifiés au sens eIDAS établis au nom d'un tiers de confiance sont utilisés pour signer les documents, auxquels sont adjointes un ensemble de preuves électroniques également signées qui permettront de retracer précisément dans quelles conditions les signataires ont été identifiés et ont donné leur consentement.

Tableau récapitulatif des niveaux de signature électronique

1. Signature simple		2. Signature avancée*		3. Signature certifiée*		4. Signature qualifiée*	
Normes ETSI Aucune		Normes ETSI EN 319 411		Normes ETSI EN 319 411 QCP		Normes ETSI EN 319 411 QCP QCSD EN 319 421	
Identité du signataire Aucun contrôle		Identité du signataire Contrôle par une autorité agréée		Identité du signataire Confirmé par mobile ou déclarée sur justificatifs Dossier de preuve technique certifié par le tiers de confiance		Identité du signataire Contrôle en face à face par une autorité agréée	
Délai	Instantané	Délai	24 heures	Délai	Instantané	Délai	1 semaine
Niveau de certificat Pas d'exigence		Niveau de certificat Certificat signature qualifié LCP ou QCP au nom du signataire		Niveau de certificat Certificat cachet qualifié QCP au nom du tiers de confiance		Niveau de certificat Certificat signature qualifié QCP au nom du signataire Support physique	
Niveau d'horodatage Pas d'exigence		Niveau d'horodatage Simple		Niveau d'horodatage Simple		Niveau d'horodatage Qualifié	
Valeur juridique Faible		Valeur juridique Forte		Valeur juridique Forte		Valeur juridique Très forte	
Jurisprudence Négative		Jurisprudence Aucune		Jurisprudence Positive		Jurisprudence Positive	
Quand l'utiliser ? Jamais		Quand l'utiliser ? Quand l'enjeu et le risque de fraude à l'identité sont élevés		Quand l'utiliser ? Quand il faut combiner fiabilité et rapidité		Quand l'utiliser ? Quand la législation l'exige	
		Exemples de contrats Assurance décès Ordre financier PV de décision		Exemples de contrats Contrat de vente Contrat d'abonnement Contrat de travail		Exemples de contrats Acte notarié Appel d'offres Services publics	
						Autre exigence Dispositif de signature qualifié QCSD	

*Signatures Avancée et Qualifiée : selon définition eIDAS

06

L'identification du signataire





Cette identification est une des exigences de l'article 1367 du Code Civil et pour les cas de la signature Avancée ou Qualifiée, l'identification du signataire est également encadrée par la norme ETSI EN 419 411. Ces différentes identifications, dont celle-ci, ont pour but d'accorder la même valeur probante à l'écrit électronique que l'écrit sous forme papier. Puisqu'en effet, la signature électronique permet de signer à distance sans intervention physique des parties prenantes, il est donc nécessaire de collecter des preuves juridiquement valables pour valider ce processus et les documents qui y transitent. Ces éléments de preuves peuvent être :

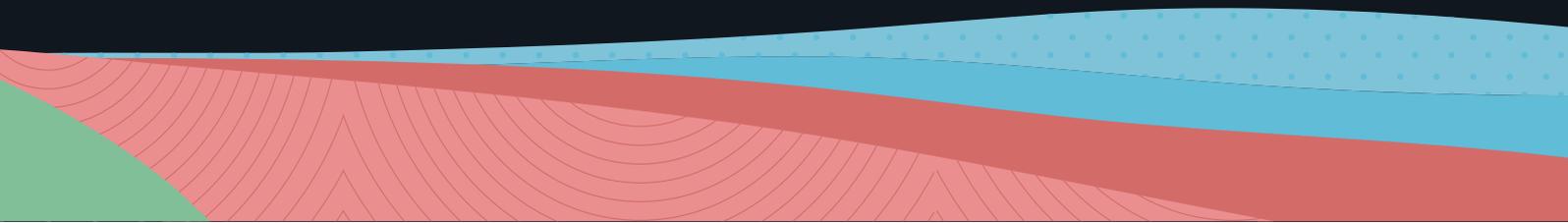
- La pièce d'identité du signataire numérisée et jointe à l'acte signé électroniquement
- L'archivage légal, qui est un moyen de garantir la mise à disposition des preuves par un tiers de confiance

- La photo du signataire prise au moment de la signature
- Ou tout autre type de document garantissant la présence du signataire au moment de l'acte de signature du contrat

Poussée à l'extrême, l'identification du signataire peut se faire directement à l'aide d'un certificat numérique à son nom, ce qui peut permettre de renverser la charge de la preuve en entrant dans le champ de la signature électronique qualifiée. Mais du fait de sa complexité et de son coût, cette solution est réservée à certains actes bien particuliers, tels que les actes notariés par exemple.

07

La certification de la signature électronique





L'eIDAS permet à chaque pays de désigner les organismes d'accréditation chargés de labelliser les prestataires de services qualifiés. La liste des organismes d'accréditation est disponible en ligne.

Comme nous l'avons vu précédemment, l'utilisation d'un certificat électronique qualifié est obligatoire pour qu'elle soit juridiquement considérée comme fiable.

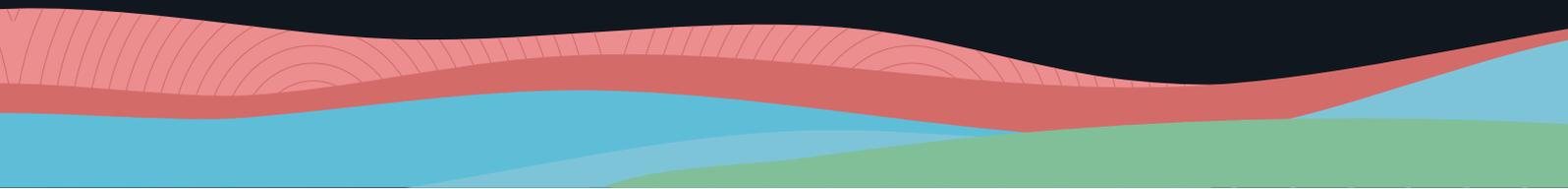
Selon le décret n°2017-1416 du 28/09/2017, une signature électronique qualifiée est une signature électronique avancée, conforme à l'article 26 du règlement susvisé et réalisée à l'aide d'un dispositif de création de signature électronique qualifié. Ce dispositif doit lui-même répondre aux exigences de l'article 29 du dit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce même règlement.

Pour la France, l'organisme d'accréditation désignée par l'**ANSSI** – Agence Nationale de la Sécurité des Systèmes d'Information – est la société **LSTI**. Les fournisseurs de signature électronique se voient délivrer un certificat de conformité lorsque leur dispositif répond à toutes ces exigences.



08

L'archivage légal
de vos documents



Enfin, le dernier aspect de la valeur juridique de la signature électronique est l'archivage des documents signés.

En effet, la conservation de la signature électronique sur le long terme est un des enjeux relatifs à la probité de la valeur de la signature électronique. L'archivage légal chez un tiers archiver est facultatif du moment que vous avez via votre solution de signature électronique un espace dans lequel retrouver vos annexes et différents documents.

Sur Oodrive Sign, tous les documents signés sont archivés de manière fiable sur la plateforme de la solution, et ce pendant toute la durée de votre abonnement. Le recours à un tiers archiver n'est donc pas obligatoire.



oodrive sign

De façon plus générale, plus vous aurez recours à une solution sécurisée, plus l'intégrité de vos documents signés est renforcée, et ce sans nécessiter de recours à l'archivage légal.

Les normes NF Z42-013 et ISO 14641-1 énoncent un ensemble de spécifications de l'AFNOR concernant les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'en assurer la conservation, l'intégrité et la pérennité.

09

La valeur juridique de la
signature en mode offline



Comme nous venons de le voir au travers de plusieurs chapitres, il est nécessaire de pouvoir constater que le signataire a signé tel document comportant tels termes, et qu'on peut faire le lien entre tous ces éléments sans revenir sur le contenu. Pour être valable, le mode OFFLINE doit respecter ces éléments afin de garantir l'intégrité de l'acte.

Chaque fois qu'un agent fera signer un document en mode offline sur sa tablette ou son smartphone, un dossier de preuve local sera constitué et signé électroniquement avec un certificat correspondant à l'utilisateur de la tablette.

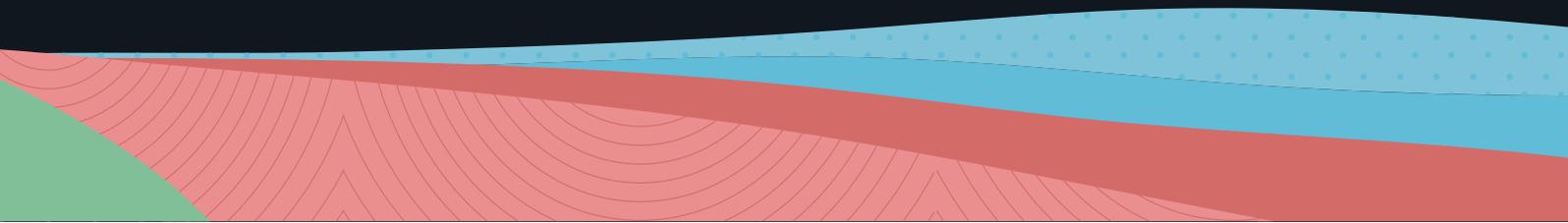
Ce dossier de preuves contiendra tous les éléments techniques disponibles permettant d'établir les conditions et l'heure de signature du contrat. Par exemple, il contiendra les coordonnées GPS du lieu de la signature. L'heure de la signature telle qu'indiquée par la tablette sera conservée, ainsi que l'horodatage serveur de la dernière synchronisation. Au moment de la synchronisation du contrat, il sera à nouveau scellé, signé et horodaté.

Ce procédé et ce triple horodatage permettent de renforcer la valeur juridique de la signature électronique en mode OFFLINE car ils permettent de sceller le document en donnant des indications précises sur les conditions et la présence du signataire au moment de l'acte de signature dudit document.



10

Qu'en est-il de la
mention manuscrite?





De nombreuses dispositions légales spéciales imposent que certaines mentions (montant d'un engagement, clause, date ou signature) soient apposées de la main de celui qui s'oblige, comme en matière de cautionnement par exemple.

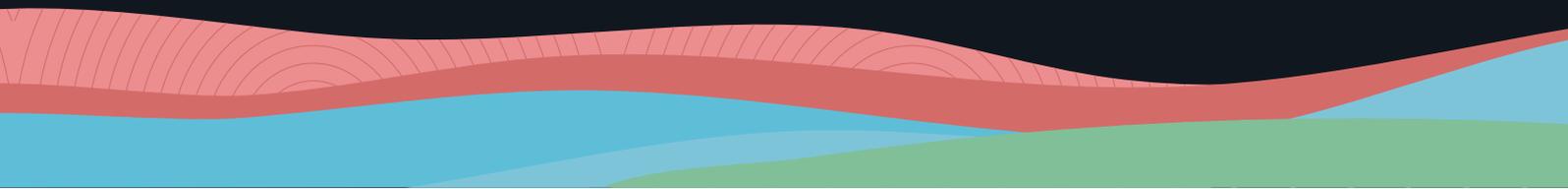
Il résulte de l'article 1326, de la loi du 13 mars 2000, que si la mention de la somme ou de la quantité en toutes lettres et en chiffres, écrite par la partie même qui s'engage, n'est pas nécessairement manuscrite, elle doit alors résulter, selon la nature du support, d'un des procédés d'identification conforme aux règles qui gouvernent la signature électronique ou de tout autre procédé permettant de s'assurer que le signataire est le scripteur de ladite mention.

Désormais, les mentions manuscrites exigées à des fins de validité pourront être apposées sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par celui qui s'oblige (article 1108-1 alinéa 2 du Code civil).

En clair, la mention manuscrite, lorsqu'elle est exigée pour la validité d'un acte juridique, peut être apposée sous forme électronique dans les mêmes conditions techniques que celles de la signature électronique.

11

Que dit le juge ?



Selon l'article 1368 du code civil, à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. Autrement dit, en cas de litige avec un signataire (sauf s'il s'agit d'actes authentiques qui font foi jusqu'à inscription de faux), le juge dispose d'un pouvoir souverain d'appréciation des preuves qu'il a en sa possession.



Ainsi, la Cour de Cassation considère que lorsque le présumé auteur d'une signature électronique nie être l'auteur de cette dernière, les juges sont tenus de vérifier si les conditions établies par l'article 1367 du Code civil à la validité de l'écrit ou de la signature électronique sont remplies (Cass. Civ. 1ère, 30 septembre 2010 n° 09-68555).

Plus récemment, la Cour de cassation, a dans sa décision du 6 avril 2016 validé la signature électronique certifiée en rejetant un recours portant sur un contrat d'assurance que l'assuré niait avoir signé en ligne, en arguant que la signature électronique avait été « établie et conservée dans des conditions de nature à garantir son intégrité, que la signature a été identifiée par un procédé fiable garantissant le lien de la signature électronique avec l'acte auquel elle s'attache, et que la demande d'adhésion produite à l'audience porte mention de la délivrance de ce document par la plateforme de contractualisation en ligne »

Encore plus récemment, en septembre 2019, une décision de la cour d'Appel d'Aix-en-Provence renforce

le processus d'identification du signataire en invalidant une signature électronique reposant sur l'envoi d'une photo de la carte d'identité du signataire. En effet, le juge a rappelé les dispositions de l'article 1367 du Code civil qui imposent que « lorsque la signature électronique n'est pas sécurisée dans les conditions fixées par le décret n°2001-272 du 30/03/01, il faut démontrer le recours à un procédé fiable d'identification garantissant le lien de la signature identifiant le signataire avec l'acte ». Or, l'envoi d'une photo d'une carte d'identité ne contient aucun élément de vérification de l'identité réelle du signataire.

En pratique, il faut donc se préparer à pouvoir apporter au juge des preuves de l'existence et des conditions dans lesquelles s'est conclue une transaction qui s'est faite en ligne.

Voilà pourquoi, il est essentiel, si vous êtes directeur général ou directeur commercial, d'apporter aux transactions qui s'effectuent en ligne une sécurité juridique en vous munissant d'une solution de signature électronique et d'archivage légal certifiée, offrant ainsi aux juges la garantie de la teneur et de l'existence des échanges en ligne.

Conclusion

L'innovation en matière de solutions de dématérialisation est pour le moins dynamique. Cependant, cette digitalisation des processus d'entreprise doit s'opérer en tenant compte des nouvelles menaces qui touchent ces actifs stratégiques du tissu économique actuel que sont les données d'entreprises. Ainsi, le recours à des solutions sécurisées est un des critères clés, si ce n'est le plus important, à considérer.

La valeur juridique des signatures électroniques ne peut être assurée que via des solutions certifiées par les normes les plus exigeantes et par des processus d'identification plus complets et engageants que le simple envoi d'une photo.

Oodrive Sign est une solution complète de signature électronique intelligente. Elle comprend la digitalisation des contrats, leur mise en conformité, la collecte de données ainsi que la possibilité de faire signer des documents à distance, en face à face ou en ligne. Et ce au sein d'une interface sécurisée, certifiée et souveraine.

oodrive.com



∞drive

26, rue du Faubourg Poissonnière 75010 Paris - France

oodrive.com