LA SIGNATURE ÉLECTRONIQUE

Définitions et cas d'usage

CR2PA Club des Responsables de Politiques et Projets d'Archivage

fntc

QUI SOMMES-NOUS ?

CR2PA

Le CR2PA, club de l'archivage managérial, est une association regroupant une quarantaine de membres issus d'organismes publics et du monde de l'entreprise.

Indépendant des acteurs du marché, le CR2PA est un lieu d'échange et de partage entre pairs du métier de l'archivage.

FnTC

Créée en 2001, la **Fédération des Tiers de Confiance du Numérique** opère avec pertinence la fusion de la technologie avec le droit et le « chiffre », et ses membres offrent au **marché du Numérique** un inestimable gisement de compétences dans les domaines historiques de la **digitalisation** : signature électronique, archivage électronique, identité numérique, facture électronique, vote électroniques, e-finance, e-santé, ... mais également dans ses domaines montants : Blockchain, KYC, Cachet électronique visible (CEV), ...

Nous contacter

CR2PA

75 rue de Lourmel
75015 PARIS
contact@cr2pa.fr

FNTC

Délégation Générale
43 rue de Douai
75009 PARIS
infos@fntc-numerique.com

INTRODUCTION

Au milieu des années 90, la Commission des Nations Unies pour le Droit Commercial International s'est vivement préoccupée d'envisager l'adaptation des conventions internationales régissant les transactions commerciales, aux moyens électroniques de communication en voie de mutation radicale avec l'essor d'Internet.

Sa Loi-type de 1996 sur le commerce électronique, s'applique à toute information, de quelque nature qu'elle soit, prenant la forme d'un message de données utilisé dans le contexte d'activités commerciales.

La réponse aux enjeux de la « *société de l'information* » va dès lors consister en la fixation de règles facilitant le développement de l'utilisation d'un procédé de « *signature électronique* », et permettant sa reconnaissance juridique.

Cette signature électronique, s'appuyant sur la technologie ancienne de cryptographie asymétrique, est produite par un dispositif créant un résumé du message de données (hachage) – résumé qui sera ensuite chiffré par la clé privée du signataire (« *codage* » du hachage).

Sous-tendu par la mécanique cryptographique, le processus permet de remplir des fonctions essentielles (garantie de l'intégrité des données durant leur transfert dans l'espace et durant leur conservation dans le temps/ et identification de la personne qui a signé) pour offrir une assise sécuritaire « *juridico-technologique* » aux utilisateurs.

Mais la règlementation du sujet initiée il y a vingt et un ans, en se complexifiant, a ralenti sa mise en œuvre au sein de l'entreprise, et enrayé la généralisation de son appropriation par les petites entreprises et la population déjà converties à la dématérialisation, mais souvent bloquées par des freins culturels et des habitudes séculaires.

Les réfractaires estimant que le dispositif et l'organisation qui le sous-tend constituent une « *usine à gaz* » dont la complexité n'est interprétable que par des experts, et que les bénéfices à retirer de son usage ne couvriraient pas le prix de l'effort à déployer pour le maîtriser.

Il importe de dissiper leurs appréhensions pour stimuler leur confiance, et emporter leur adhésion.

Ce n'est qu'au prix d'un travail pédagogique de conviction, reposant sur des arguments clairs et concis, et portant notamment sur la « *transparence* » pour l'utilisateur de l'emploi de ce nouveau mode de signature de ses documents, que cet outil sera mentalement intégré, puis agréé et adopté à grande échelle (comme l'est désormais la carte bancaire).

A cette fin, des experts de la FnTC et du CR2PA se sont réunis dans un groupe de travail afin de rédiger graduellement plusieurs supports destinés à favoriser une approche accessible et éclairante du sujet, en proposant une lecture sobre, et aisée à appréhender, de la problématique de la signature électronique tant dans son utilisation que dans la gestion de son cycle de vie et dans sa conservation.

Alain BOBANT,
Président FnTC

SOMMAIRE

LEXIQUE

Autorité de Certification (AC)

Entité responsable de l'émission, de la délivrance et de la gestion des certificats électroniques.

L'Autorité de Certification est responsable des certificats émis en son nom.

Dispositif de création de cachet électronique

Dispositif logiciel ou matériel configuré, utilisé pour créer un cachet électronique.

Dispositif de création de signature électronique

Dispositif logiciel ou matériel configuré, servant à créer une signature électronique.

Horodatage électronique

Données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant.

Prestataire de services de confiance (PSCO)

Personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié.

Prestataire de services de confiance qualifié (PSCQ)

Prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié.

One Time Password (OTP)

Mot de passe à usage unique et à durée de vie limitée pour valider un accès à un système d'information.

Ce procédé « *dynamique* » est d'un niveau de sécurité supérieur par rapport au mot de passe « *statique* »).

Ce lexique est une aide précieuse pour vous accompagner dans la lecture de ce livret.

QU'EST CE QUE LA SIGNATURE ÉLECTRONIQUE ?

La signature électronique est un procédé technique permettant de lier des signataires identifiés à un document et à son approbation tel, qu'en principe, la signature manuscrite.

Ce procédé permet de garantir l'intégrité des documents signés (documents à valeur juridique, fichiers, données, etc.).

La signature manuscrite scannée doit donc répondre à certaines exigences d'intégrité et d'identification pour être considérée comme une signature électronique au sens juridique du terme

1.1 Définition technologique de la signature

Le procédé technique de la signature électronique se base sur un certificat électronique délivré par une Autorité de Certification. Celle-ci est responsable du processus de délivrance des certificats, une fois la vérification d'identité effectuée par une autre entité (autorité d'enregistrement par exemple).

Elle est également responsable de tenir et publier la liste de révocation des certificats qu'elle a émis.

Une fois délivré, le certificat contient les clés permettant d'assurer l'authenticité du document signé ainsi que son intégrité. Ses clés sont connues comme clés de chiffrement (clé privée) et de déchiffrement (clé publique).

1.2 Autorité de Certification

Qui va délivrer le certificat ?

C'est l'Autorité de Certification qui peut être une entreprise ou une organisation. Elle délivre un certificat électronique permettant de valider l'identité de personnes morales ou physiques.

L'Autorité de Certification agit pour son compte soit :

- **En interne** : en utilisant le certificat existant pour la création de badges d'accès, de cartes de décryptage ou de signatures électroniques pour les membres de son organisation.
- **En externe** : en délivrant des certificats permettant l'utilisation de la signature électronique avec ses interlocuteurs commerciaux au moyen d'une convention de preuve préétablie et pré-validée.

Mais elle peut aussi agir pour le compte de tiers en tant que Tiers de Confiance reconnu :

- **Au niveau national** (En France reconnue par l'ANSSI) : elle devient un PSCO qui répond au référentiel national (RGS-Référentiel Général de Sécurité).
- **Au niveau européen** (avec respect des exigences du Règlement eIDAS) : elle est une PSCQ qui répond au référentiel européen (via l'ANSSI qui en est l'organe de contrôle en France). Attention les référentiels européen et national ne sont pas les mêmes.
- **Au niveau international** : il n'existe pas d'exigences reconnues au niveau international. La démarche serait de déterminer si il y a des accords de reconnaissance croisée entre les prestataires nationaux ou européens et le pays étranger en question.

  Il s'agit alors d'une initiative purement privée et la démarche devra être reconduite en fonction de l'évolution de la règlementation d'un côté ou de l'autre.

1.3 Certificats de signature et de cachet

Les certificats électroniques sont délivrés pour des personnes physiques ou morales.

Selon le type de personnes il s'agira de certificats visant à créer une signature électronique ou un cachet électronique.

Le certificat de signature électronique identifie une personne physique. Il lui permet d'apporter son consentement au document qu'elle signe.

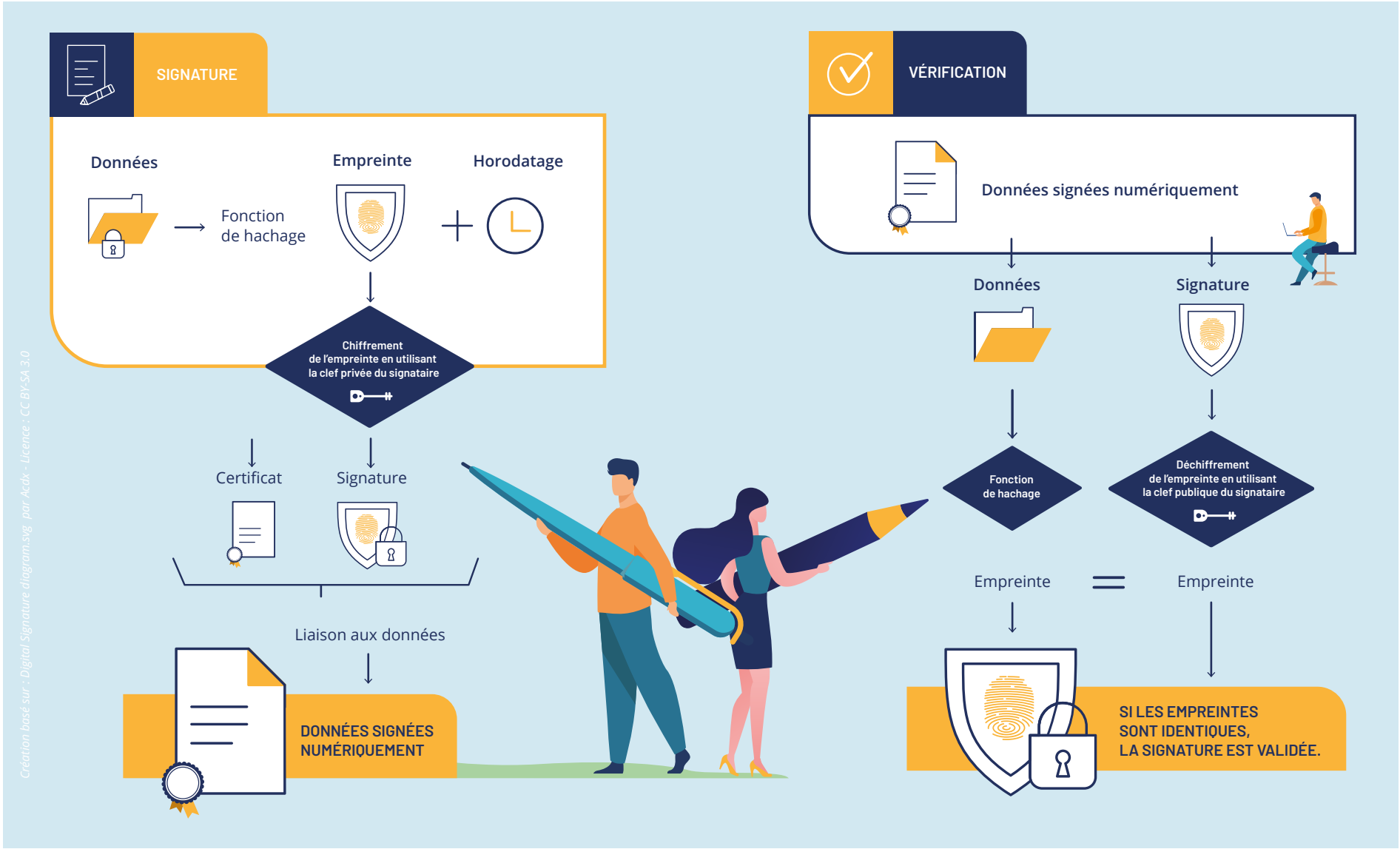
Le certificat de cachet électronique identifie une personne morale. Il permet à l'entité de s'authentifier mais il ne traduit pas un consentement. D'ailleurs ce cachet peut être installé directement sur un serveur dans le but de « *signer* » en masse et de manière automatisée. Il s'apparente alors au tampon de l'entreprise.

La signature électronique et le cachet électronique utilisent le même procédé cryptographique.

Dans la pratique, on dit « *signer un document* » qu'il s'agisse d'un certificat de signature ou d'un certificat de cachet. Dans le cas précis du cachet, on peut également rencontrer le terme « *sceller* ».

Il arrive de rencontrer le terme « ***mettre un coup de cachet (ou tampon)*** » pour évoquer l'utilisation du cachet serveur.

LE PROCÉDÉ CRYPTOGRAPHIQUE DE LA SIGNATURE ET DU CACHET ÉLECTRONIQUE



On ne peut pas rejouer une signature (avec la même empreinte et le même horodatage).

LE CADRE RÈGLEMENTAIRE DE LA SIGNATURE ÉLECTRONIQUE

2

A l'échelle européenne, le Règlement eIDAS (Identification et services de confiance) du 23 juillet 2014 constitue le texte de référence (le socle) auxquelles doivent se référer en principe toutes les législations nationales en matière de signature électronique. Les législations nationales ne peuvent créer des obligations supplémentaires pour les signatures électroniques qualifiées.

En France, l'article 1367 al.2 du Code civil définit de manière fonctionnelle la signature électronique.

Le décret d'application du 28 décembre 2017 vient préciser les modalités de fiabilité de la signature électronique avec un renvoi express au Règlement eIDAS.

De nombreux arrêtés ou décrets dans des domaines divers du droit (Commande publique, droit des sociétés, etc.) y font référence.

2.1 Code civil Art. 1367

« *La signature nécessaire à la perfection d'un acte juridique* ***identifie*** *son auteur. Elle manifeste son* ***consentement*** *aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*

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. ***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'État* »

En bref...

- La définition du Code civil est donc bien en accord avec les caractéristiques communes et technologiques de la signature électronique : identification, consentement et intégrité.

2.2 Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique

« *La fiabilité d'un procédé de signature électronique est présumée,* ***jusqu'à preuve du contraire****, lorsque ce procédé met en œuvre une signature électronique qualifiée.*

Est une signature électronique ***qualifiée*** *une signature électronique* ***avancée****, conforme à l'article 26 du* ***règlement susvisé eIDAS*** *et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement* »

En bref...

- **Jusqu'à preuve du contraire**
  Renversement de la charge de la preuve selon que la signature est ou non qualifiée.
- **Avancée**
  Le décret met en avant différentes signatures (qualifiée et avancée). Toutes les signatures n'apportent pas le renversement de la charge de la preuve.
- **Charge de la preuve**
  C'est à celui qui se prévaut d'une signature électronique simple ou avancée de rapporter la preuve de la fiabilité de celle-ci, tandis que pour une signature électronique qualifiée, c'est à celui qui la conteste de rapporter la preuve de l'absence de fiabilité.

Récapitulatif du décret et de ses références au Règlement eIDAS

Article 25	Effets juridiques des signatures électroniques
Article 26	Exigences relatives à une signature électronique avancée
Article 28	Certificats qualifiés de signature électronique
Article 29	Exigences applicables aux dispositifs de création de signature électronique qualifiés

2

2.3 Règlement européen 910/2014 eIDAS

Article 25 :

*« 1. 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.*

*2. **L'effet juridique** d'une signature électronique qualifiée est équivalent à celui d'une **signature manuscrite**.*

*3. 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** »*

En bref...

- **Preuve en justice**
  Un juge ne devrait pas refuser une signature au seul motif qu'elle n'est pas qualifiée.
- **Dans tous les États membres**
  La signature électronique qualifiée est reconnue juridiquement et interopérable.

Récapitulatif du niveau de signature et charge de la preuve

	Demandeur	Défendeur
Signature simple		√
Signature avancée		√
Signature qualifiée	√	

Article 26 :

« Une signature électronique avancée satisfait aux exigences suivantes:

a) être liée au signataire de manière univoque (authentification) ;

b) permettre d'identifier le signataire (identification) ;

*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 des données soit détectable** (intégrité) ».*

En bref...

- **Contrôle exclusif**
  Le contrôle exclusif définit le procédé de signature à la seule maîtrise du signataire.
  Comme, par exemple :
  - *carte bancaire (outil) + code (secret),*
  - *clé USB (outil) + mot de passe (secret),*
  - *smartphone (outil) + élément biométrique ou Code PIN (secret)*

Article 29 :

*«Les dispositifs de création de signature électronique qualifiés **respectent les exigences** fixées à l'annexe II.*

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux dispositifs de création de signature électronique qualifiés. Un dispositif de création de signature électronique qualifié est présumé satisfaire aux exigences fixées à l'annexe II lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2. »

En bref...

- **Respect d'exigences**
  Ces dispositifs sont donc contrôlés pour la signature qualifiée. Ils sont garantis par une certification.

2

2.4 Le Prestataire de Service de Confiance Qualifié

Pour chacun des services de confiance le statut « qualifié » est accordé par l'organe de contrôle (ANSSI pour la France) après un audit à la charge du prestataire pour vérifier le respect des exigences imposées par le Règlement.

Les services de confiance que peut délivrer un PSCQ :

- Certificats qualifiés de signature électronique et de cachet électronique ;
- Validation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés ;
- Conservation qualifiée des signatures électroniques et des cachets électroniques ;
- Horodatages électroniques qualifiés ;
- Services d'envoi recommandé électronique qualifiés;
- Certificats qualifiés d'authentification de site internet.

Entre autres, le PSCQ doit satisfaire aux exigences suivantes (article 24) :

- A en charge de vérifier l'identité des personnes physique ou morale auxquelles il délivre un certificat qualifié ;
- Utilise des systèmes fiables protégés contre les modifications et assure la sécurité technique et la fiabilité de ses processus ;
- Utilise des systèmes fiables pour stocker les données qui lui sont confiées ;
- Prend les mesures nécessaires pour se protéger contre la falsification et le vol de données;
- Conserve et maintient accessibles pour une durée appropriée, y compris après que les activités du PSCQ ont cessé, les données permettant d'apporter des preuves en justice ;
- A un plan de continuité d'arrêt d'activité afin d'assurer la continuité de service ;
- Est conforme aux règles de traitement des données à caractère personnel;
- Tient à jour une base de données des certificats qualifiés qu'il délivre et de leur statut (valide ou révoqué) ;
- Doit pouvoir fournir à son utilisateur l'historique du statut d'un certificat qualifié même après sa révocation ;
- Maintient des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée.

2

2.5 Le processus de qualification du prestataire

Afin de répondre aux exigences du règlement eIDAS, le prestataire passe un audit auprès d'un organisme d'évaluation de la conformité. Le résultat de cet audit est ensuite envoyé à l'organe de contrôle national pour sa qualification.

- Les États membres désignent un organe de contrôle établi sur leur territoire chargé des tâches de contrôle (Article 17, organe de contrôle).

- Rôle de l'organe de contrôle : contrôler les PSCQ afin de s'assurer, par des activités de contrôle a priori et a posteriori, que ces PSCQ et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences fixées dans le présent règlement.

- Les PSCO et PSCQ prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent (article 19 : exigences de sécurité applicables aux prestataires de services de confiance).

- Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque.

2.6 Le processus de contrôle des PSCQ

Les PSCQ font l'objet, au moins tous les **vingt-quatre mois**, d'un audit effectué à leurs frais par un **organisme d'évaluation de la conformité**.

Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité à l'organe de contrôle dans un délai de trois jours ouvrables qui suivent sa réception.

Des contrôles inopinés par l'organe de contrôle peuvent avoir lieu (Article 20).

« *Chaque État membre établit, tient à jour et publie des* ***listes de confiance****, y compris des informations relatives aux PSCQ dont il est responsable, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent* » (Article 22).

- Liste de confiance nationale
- Liste de confiance européenne

Les PSCQ peuvent utiliser le label de confiance de l'Union européenne (Article 23).

eIDAS-compliant

En bref...

- Un cadre très rigoureux pour le niveau qualifié avec une certification donnée par l'organe de contrôle indépendant.
- Ces certifications récurrentes et coûteuses (audit, hardware, etc.) expliquent que la signature qualifiée est aujourd'hui, dans le marché, un service peu utilisé et souvent plus onéreux qu'une signature d'un autre niveau.

fntc 2

LES NIVEAUX DE SIGNATURE

3

Les cadres règlementaires (national et européen) font état de différents niveaux de signature.

Il convient de rappeler que toutes les signatures électroniques sont recevables d'un point de vue juridique. En cas de litige ou de contentieux, le juge et/ou la partie adverse peut demander la présentation des preuves d'authenticité et d'intégrité.

Il existe donc différents niveaux de signature et de cachets pouvant être utilisés.

3.1 Signature qualifiée

Pour une signature qualifiée, la présentation des preuves revient à la partie qui la conteste (**renversement de la charge de la preuve**) sauf si le juge exige le contraire (cf. Article 288-1 du CPC).

Si la signature qualifiée a le même effet juridique que la signature manuscrite elle en possède aussi les mêmes limites et peut donc être contestée.

Une signature électronique qualifiée ne peut être construite et délivrée que par un Prestataire de Service de Confiance Qualifié (PSCQ).

Elle est également appelée SEA pour Signature Electronique Avancée.

Pour un cachet serveur qualifié, celui-ci sera protégé sur un HSM (serveur reconnu par le règlement eIDAS comme dispositif de création de signature qualifié).

3.2 Signature avancée

La signature avancée, par sa définition et son procédé technique, garantit l'authenticité et l'intégrité.

La présentation des preuves n'entraîne pas de difficultés particulières à condition que :

- elles soient disponibles ;
- elles soient lisibles ;
- elles soient connues par l'utilisateur de la signature.

La signature avancée peut être construite et délivrée par une Autorité de Certification ou un PSCQ (au sens eIDAS).

3

3.3 Signature simple

Une signature dite « *simple* » est une signature ne répondant pas aux prérequis d'une signature avancée ou qualifiée. Dès lors, il s'agit, selon le règlement eIDAS d'une « ***signature électronique*** » : des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ;

La signature manuscrite scannée doit donc répondre à certaines exigences d'intégrité et d'identification pour être considérée comme une signature électronique au sens juridique du terme.

L'usage d'une signature électronique dite « *simple* » est donc **reconnu** et **largement utilisé**, mais sa fiabilité et par là, son opposabilité, dépendront des preuves qui lui sont associées.

A contrario des signatures avancées et qualifiées, le procédé technique de la signature « *simple* » n'est pas détaillé dans le cadre règlementaire.

De ce fait, seule l'association de preuves au procédé de signature apportera les éléments nécessaires pour démontrer les garanties d'authenticité, d'identification et d'intégrité.

Cette signature peut être construite et délivrée par une Autorité de Certification.

Elle peut être appelée SE pour Signature Electronique.

Niveau de signature	Description eIDAS
Électronique simple	C'est un ensemble de « *données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer.* »
Électronique avancée	**C'est une signature électronique qui doit :** • 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.
Électronique qualifiée	C'est une « *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.* »

Tableau récapitulatif

AC	Signature qualifiée	Signature avancée	Signature simple
PSCO (eidas)	√	√	√
PSCO (ANSSI)		√	√
AC interne		√	√
AC non reconnues		√	√

3 questions pour mieux comprendre les signatures.

- **Quelle est la différence entre la signature qualifiée et la signature avancée ?**
  La signature qualifiée repose sur une procédure règlementée à l'inverse de la signature avancée.
- **Quelle est la différence entre la signature électronique avancée d'un PSCO et celle d'une AC interne ou non reconnue ?**
  - Le PSCO a fait certifier ses modalités de délivrance de signature RGS** équivalente à la signature avancée.
  - La certification augmente la confiance et facilite la convention de preuve.
- **Quelles sont les différences entre la signature avancée et la signature simple ?**
  La signature avancée dispose d'une documentation de meilleure qualité, qui facilite ainsi la présentation des preuves.

3

3.4 Convention de preuve

Accord express par lequel les parties modifient les règles normales de la preuve judiciaire soit par la charge de la preuve quant à la détermination des faits approuvés soit quant à l'emploi des procédés de preuves.

Il s'agit d'un accord passé entre des partenaires contractuels. Cette convention fixe les conditions de preuve recevables entre ceux-ci, notamment en termes de signature (en termes techniques, juridiques).

La convention peut se retrouver intégrée dans le contrat de service ou le contrat commercial.

Elle figure en général à la première étape, au début des processus de contractualisation en ligne, que ce soit pour un ou plusieurs documents.

La convention de preuve n'est pas obligatoire et ne supplante pas les exigences réglementaires. Toutefois, elle est fortement recommandée dans tous les cas où la règlementation ne statue pas sur le recours à une signature électronique qualifiée.

3

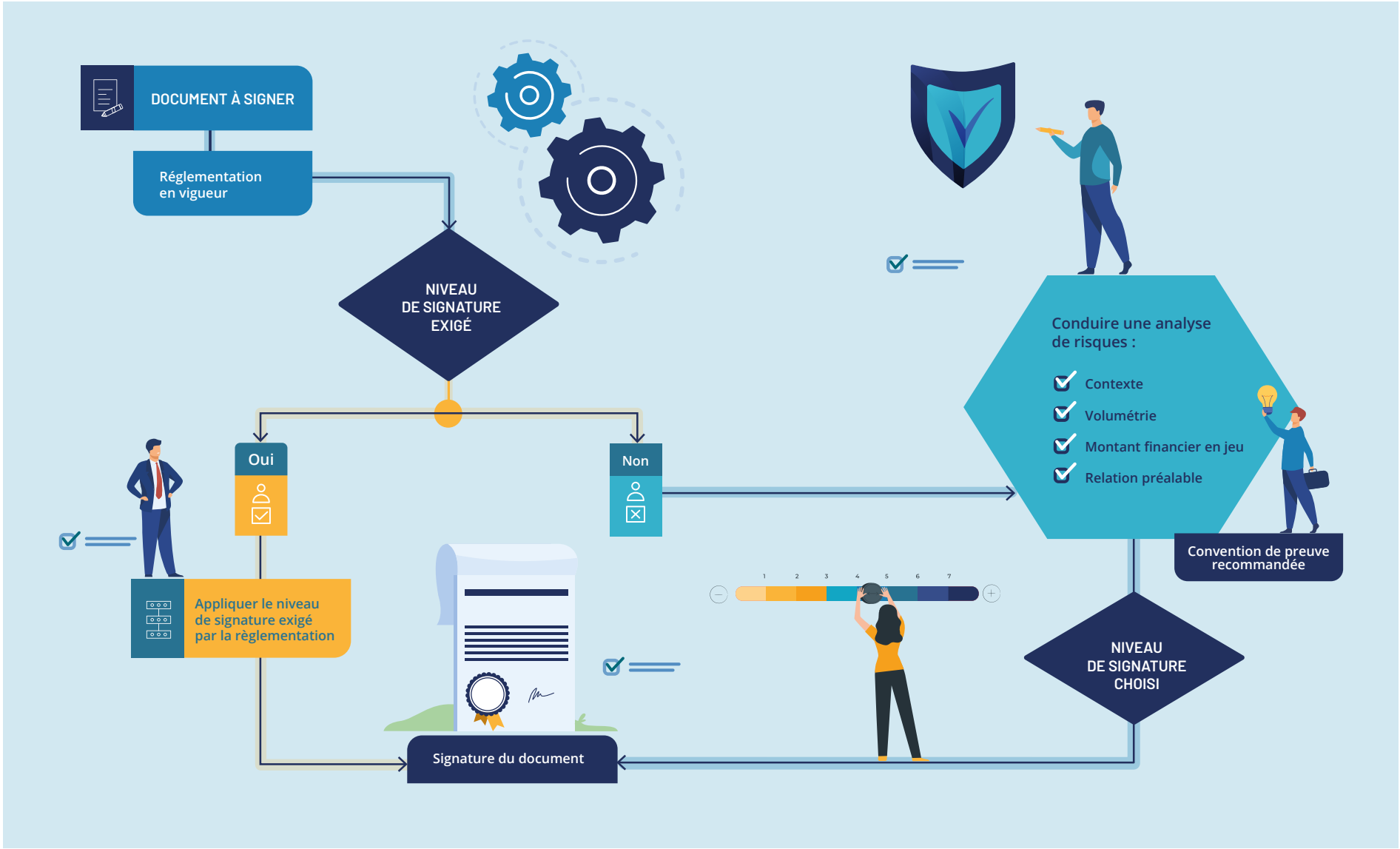
COMMENT SAVOIR QUELLE SIGNATURE UTILISER ? CAS D'USAGE

Maintenant, passons à la pratique...

4

COMMENT SAVOIR QUELLE SIGNATURE UTILISER ? CAS D'USAGES

4



Dans l'analyse de risque, l'étude du contexte jurisprudentiel constitue un indice fort quant au choix du niveau de signature.

CAS D'USAGES

4

Les cas d'usages ci-dessous visent à illustrer l'utilisation des différents niveaux de signatures en fonction des documents à signer. L'objectif étant de proposer une méthodologie pour étudier quelle signature appliquer.

Les cas d'usages proposés ici, le sont donc à titre indicatif et non-exhaustif. Dans tous les cas, il convient de se rapprocher de son expert juridique pour valider le choix de son niveau de signature.

Documents à signer

Descriptif du document.

Contexte

Description de la situation de l'entreprise.

Pourquoi signer ?

Quel est l'objectif de la signature ?

Intégrité : le fait de démontrer (cachet, horodatage), authenticité, validation, acceptation.

Les intervenants

Qui intervient dans l'acte de la signature ?

Format du document

Le format du document.

Règlementation

En fonction du cas d'usage, quelle réglementation s'applique ?

Dicte-t-elle un niveau de signature obligatoire ?

NB : Certains cas d'usage sont très précis et demanderaient une étude particulière par l'expert juridique de votre choix. Il est possible que d'autres réglementations aient à être prises en compte.

Risques

Les risques liés à l'entreprise pour ce type de document en cas de litige (juridique, financier, métier, etc.), risque de contestation et conséquences.

Niveau de signature

Simple, Avancée, Qualifiée ou aucune.

Pour aller plus loin...

Jurisprudence, exemples de litiges.

Ce lexique est une aide précieuse pour vous accompagner dans la lecture des cas d'usage.

CAS D'USAGE N°1

Documents à signer	▪ Baux ▪ Courriers avec les bailleurs
Contexte	▪ Signature d'un contrat de bail pour une surface utilisée par la société A. Cette surface sera utilisée pour une activité commerciale avec 30 salariés en son sein (commerciaux, administratifs). Le loyer de la surface a été négocié avec une avance sur 1 an. La surface a été totalement équipé par la société A. ▪ Le contrat est signé entre la société A (locataire) et le bailleur et les engage sur une durée de 5 ans.
Pourquoi signer ?	▪ Faire valoir ses droits dans le cadre d'une relation locataire/bailleur : • droit du propriétaire • droits du locataire ▪ Le contrat de bail est un justificatif de domiciliation et peut donc être présenté lors d'une procédure administrative, bancaire etc.
Les intervenants	▪ Le locataire et le bailleur (2 parties distinctes ne se connaissant pas forcément).
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Article 1366 du Code civil ▪ Article 1367 du Code civil
Risques	▪ Risques pour la société A en cas de litiges ou de contestation de la signature par le propriétaire : • Perte de la surface • Relocalisation des équipes • Déménagement des équipements et remise en état de la surface • Perte de l'investissement initial (caution, avance sur loyer, aménagement).
Niveau de signature	▪ Dans le cadre de ce contrat, le risque financier en cas de contestation de la signature est fort : il est donc recommandé d'utiliser une signature, a minima, avancée.
Jurisprudence	▪ Cour d'appel de Toulouse du 4 septembre 2020.

4

CAS D'USAGE N°2

4

Documents à signer	▪ Documents produits en interne pour un usage interne : • Note interne, note de service • Comptes rendus • Documentation projet • Documents applicables • Documents validant une décision • Documents relatifs aux audits internes
Contexte	▪ L'entreprise B émet des documents d'engagement de dépenses internes (étude non financée par les clients). Ces engagements doivent être validés et signés car la société B a mis en place un workflow de validation permettant de modifier la proposition d'engagement de dépense interne puis de le signer dans sa version finale comme acceptation des parties internes prenantes.
Pourquoi signer ?	▪ Ce document n'engage pas la société B vis-à-vis d'un tiers mais le circuit de validation et de signature permet de faire valoir le respect des procédures obligatoires pour engager des dépenses internes, notamment en termes de comptabilité.
Les intervenants	▪ Intervenants internes métiers inscrits dans la procédure de validation et de signature du document.
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Article 1366 du Code civil ▪ Article 1367 du Code civil ▪ Article 1368 du Code civil (convention de preuve)
Risques	▪ Le risque serait de ne pas pouvoir justifier de la dépense en interne, ou de se retrouver avec un document validé mais non signé et donc non intègre.
Niveau de signature	▪ Signature simple sans procédure de vérification de type SMS pendant les étapes du *workflow* de validation. ▪ Signature simple avec vérification OTP ou cachet serveur pour l'accord final. Il est préférable de prévoir pour cette dernière signature une convention de preuve interne comme description de la procédure
Jurisprudence	▪ Pas de jurisprudence *a priori*.

CAS D'USAGE N°3

Documents à signer	▪ Documents de financement, caution et garanties
Contexte	▪ Signature de documents de nature financière entre une institution bancaire et une société dans le cadre d'opérations de financement et de trésorerie.
Pourquoi signer ?	▪ Pour faciliter les échanges entre l'établissement bancaire et la société. ▪ Pour gagner du temps par rapport à la volumétrie concernée.
Les intervenants	▪ Interlocuteur banquier et directeur financier ou directeur des opérations de financement
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Article 1366 du Code civil ▪ Article 1367 du Code civil ▪ Article 1368 du Code civil (convention de preuve)
Risques	▪ Risques d'authentification, de non-dépôt conventionnel de documents auprès des établissements bancaires ▪ Vigilance concernant le risque de qualifier en sûreté personnelle.
Niveau de signature	▪ Une convention de preuve préalable aux opérations est établie entre les parties. Elle définit le niveau de signature utilisé. Ici, il s'agit d'un niveau avancé à minima.
Jurisprudence	▪ Pas de jurisprudence *a priori* sur les sûretés dématérialisées.

CAS D'USAGE N°4

4

Documents à signer	▪ Document de délégation de pouvoirs.
Contexte	▪ Signature d'un document déléguant des pouvoirs.
Pourquoi signer ?	▪ Document permettant à la direction générale de déléguer des pouvoirs spécifiques à un directeur de BU.
Les intervenants	▪ Membres du Comité exécutif et la Direction Générale.
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Article 1366 du Code civil ▪ Article 1367 du Code civil ▪ Article 1368 du Code civil
Risques	▪ Contestation du contenu de la délégation et de son acceptation. ▪ Contestation d'usage des pouvoirs délégués au-delà de la période ou contexte défini dans la délégation.
Niveau de signature	▪ Pouvoir disposer d'un mode de signature simple (sans vérification OTP) permettant de produire un certificat de réalisation en cas de contrôles d'une autorité extérieure.
Jurisprudence	▪ Cour d'appel d'Aix en Provence, 8e chambre A, 26 juin 2014.

CAS D'USAGE N°5

Documents à signer	▪ Accords ou engagements de confidentialité.
Contexte	▪ Dans le cadre d'un projet faisant intervenir un sous-traitant ou un fournisseur. La signature d'un engagement sur la non-divulgation d'informations confidentielles.
Pourquoi signer ?	▪ Nécessité de protection du savoir-faire et de la propriété intellectuelle du projet.
Les intervenants	▪ Directeurs projets de l'entreprise principale intervenante et directeurs des sous-traitants ou fournisseurs.
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Article 1366 du Code civil ▪ Article 1367 du Code civil ▪ Article 1368 du Code civil
Risques	▪ L'impossibilité de protéger le savoir-faire et le partage d'informations dans le cadre du projet. ▪ L'impossibilité de pouvoir engager la responsabilité des intervenants extérieurs en cas de divulgation d'informations.
Niveau de signature	▪ Choix de la signature avancée en vue de disposer d'un dossier de preuves complet permettant d'authentifier l'engagement du représentant ou de la personne morale sous-traitant ou fournisseur.
Jurisprudence	▪ Pas de jurisprudence *a priori*.

CAS D'USAGE N°6

4

Documents à signer	▪ Documents relatifs à des contrats B2B non stratégiques et à enjeu financier faible ou modéré : • Contrats • Avenants • Courriers relatifs à l'exécution du contrat
Contexte	▪ L'entreprise C, petite PME régionale dédiée à la conserverie artisanale employant 20 personnes, contractualise une offre de téléphonie pour ses bureaux dans lesquels travaillent 5 personnes. Le fournisseur de téléphonie lui propose de signer son contrat électroniquement.
Pourquoi signer ?	▪ Faire valoir ses droits dans le cadre d'une relation client/fournisseur.
Les intervenants	▪ Le fournisseur de service et le client.
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Article 1366 du Code civil ▪ Article 1367 du Code civil ▪ Article 1368 du Code civil
Risques	▪ Le risque pour le client comme pour le fournisseur serait une contestation ou répudiation du contenu du contrat et de son acceptation par les parties et ne pas pouvoir prouver le consentement lié au processus de signature.
Niveau de signature	▪ S'agissant d'un contrat pour un service ne représentant pas une somme financière conséquente. Le fournisseur de téléphonie propose ici une signature simple avec vérification SMS pour accentuer le consentement du client et renforcer les preuves associées à la procédure de signature.
Jurisprudence	▪ Pas de jurisprudence *a priori*.

CAS D'USAGE N°7

Documents à signer	▪ Documents relatifs à des contrats B2B stratégiques et/ou à enjeu financier élevé : • Contrats • Avenants • Courriers relatifs à l'exécution du contrat
Contexte	▪ Grande entreprise de construction employant plus de 1 500 personnes et travaillant partout en Europe. Cette entreprise travaille pour le privé ainsi que pour le public.
Pourquoi signer ?	▪ Faire valoir ses droits dans le cadre d'une relation client/fournisseur.
Les intervenants	▪ Le fournisseur et le client.
Format du document	▪ Document textuel donc format lisible et pérenne de type PDF.
Règlementation	▪ Secteur public : Arrêté du 22 Mars 2019 relatif à la signature électronique dans la commande publique. ▪ Secteur privé : Article 1366 du Code civil • Article 1367 du Code civil • Article 1368 du Code civil
Risques	▪ Concernant le secteur public : l'utilisation de la signature avancée est obligatoire (soit eIDAS soit RGS**). ▪ Dans le secteur privé le risque financier en cas de litiges est trop important pour l'entreprise. Les chantiers s'élevant souvent à plusieurs millions d'euros.
Niveau de signature	▪ Le choix a donc été porté sur l'usage d'une signature avancée (selon le règlement eIDAS) car devant être mise en place pour le secteur public. Mais aussi pour sa fiabilité avérée et pour sa reconnaissance européenne, tant dans le secteur public que privé.
Jurisprudence	▪ Pour les marchés publics : *CE, 26 juin 2015, Ministre de la Défense c/ Société Olympe services.*

4

CAS D'USAGE N°8

4

Documents à signer	▪ Documents relatifs à l'usage et aux conditions d'usage du matériel/équipement.
Contexte	▪ Preuve de remise d'un Équipement de Protection Individuelle (EPI) à un salarié.
Pourquoi signer ?	▪ Prouver la remise physique de l'objet au salarié
Les intervenants	▪ L'entreprise dotatrice et le salarié
Format du document	▪ Un texte n'est pas forcément nécessaire, on peut imaginer une sorte de log de validation.
Règlementation	Dans le cadre du Droit social, la preuve est libre. ▪ Article 1366 du Code civil ▪ Article 1367 du Code civil ▪ Article 1368 du Code civil
Risques	▪ A l'attention de l'entreprise utilisatrice : • Se protéger contre le vol • Se protéger des accidents et de leurs conséquences
Niveau de signature	▪ L'objectif serait ici de créer le faisceau d'indices le plus détaillé possible pour ainsi répondre en tout état de cause au droit social. L'ensemble du processus amenant à la délivrance de l'EPI doit être documenté. La signature simple est préconisée, elle sera ici un élément de preuve supplémentaire.
Jurisprudence	▪ Pas de jurisprudence *a priori*.

CAS D'USAGE N°9

Documents à signer	▪ Documents constitutifs de la conduite du projet (plannings, comptes rendus, etc.) ▪ Documents constitutifs des livrables attendus ▪ Procès-verbaux de réception
Contexte	▪ Mise en place de la signature de documents constitutifs de la conduite d'un projet dans un lieu hors réseau, déconnecté et donc en mode *off-line*.
Pourquoi signer ?	▪ Faire valoir ses droits dans le cadre d'une relation client/fournisseur.
Les intervenants	▪ Le fournisseur et le client.
Format du document	▪ Formulaire web responsive design puis PDF
Règlementation	• Article 1366 du Code civil • Article 1367 du Code civil • Article 1368 du Code civil
Risques	▪ Contestation de l'intervention et non-paiement.
Niveau de signature	▪ En mode *off-line*, la signature du formulaire est réalisée via une signature sur tablette. Puis, dès le retour sur des zones connectées, le formulaire est converti en PDF accompagné d'un cachet serveur et d'un horodatage avant d'être remis au client. Les preuves de la signature sur tablette accompagnent le fichier PDF. ▪ Cette procédure est préalablement établie et acceptée par les parties prenantes grâce à une convention de preuve.
Jurisprudence	▪ Pas de jurisprudence *a priori*.

CAS D'USAGE N°10

4

Documents à signer	▪ Dossier de lot dans le secteur pharmaceutique
Contexte	▪ Quand un lot de médicaments est produit, le pharmacien responsable du site de production doit « *libérer* » le lot, c'est-à-dire s'engager au nom du labo pharma, que le lot produit a suivi toutes les étapes de bonne fabrication (*Good Manufacturing Practices* (GMP)).
Pourquoi signer ?	▪ La signature rend valide la libération du dossier de lot.
Les intervenants	▪ Le pharmacien responsable.
Format du document	▪ Document PDF.
Règlementation	▪ *Good Manufacturing Practices* (GMP).
Risques	• Pas de libération, pas de médicament. • Pas de preuve d'authenticité du dossier de lot, risque de rappel de lot
Niveau de signature	▪ Signature qualifiée dans le cadre de la réglementation GMP
Jurisprudence	▪ Pas de jurisprudence *a priori*.

NOTES

Cet espace vous est dédié pour prendre des notes.

4

CONCLUSION

Le Code civil nous rappelle dans son article 1100 que « les obligations naissent d'actes juridiques [...] ».

Nous espérons que la lecture de nos travaux vous permettra de mieux préserver la mémoire de ces obligations.

En appréhendant les différents niveaux de signature électronique vous adapterez vos exigences en fonction des risques encourus. Vous gérerez en conscience l'usage de la signature électronique simple qui se répand largement et se développe grâce à sa facilité d'utilisation et à son coût attractif. La jurisprudence autorise cette utilisation à condition de savoir archiver les preuves de signature pour pouvoir les présenter au juge dans les règles de l'art : les preuves devront demeurer intègres durant toute leur période de conservation.

Il est donc primordial que la généralisation de la signature électronique des contrats s'accompagne d'une gestion des preuves de signature au même titre que celle des actes numériques. Notre travail tend à démontrer que la bonne transmission à toutes les parties des preuves de signature électronique concomitamment à la transmission du contrat s'avère nécessaire pour que chacun puisse archiver et garantir l'intégrité de cet ensemble indissociable.

Notre prochain fascicule traitera donc du contenu du dossier de preuve, de sa transmission et de son archivage.

Alain Borghesi,
Vice président de la FnTC et rapporteur du Gt archivage

REMERCIEMENTS

Comité de rédaction :

Agosti Pascal, Caprioli & Associés, Société d'Avocats
Bobant Alain, président de la FnTC
Bonnefous Jean-Mathieu, Orano
Borghesi Alain, Vice-président FNTC et PDG Cecurity.com
Delion François, Bouygues Telecom
Doussot Jean-Pierre, Esopica
Frezier Amélie, Cecurity.com
Pichat Estelle, Systra
Vincent Florent, Thales Group

Agence PENCIL-PARK : www.pencilpark.com - Conception : Graphik Projects - Crédits : ktsdesign/AdobeStock (couverture), illustration Freepik