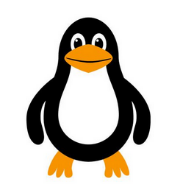
**CEJMA : le droit de la preuve électronique**



Toute entreprise ou organisation (comme le lycée) passe des contrats. Or il est parfois nécessaire d’avoir **la preuve électronique** des échanges pour faire valoir ses droits, pour défendre sa e-réputation.

La preuve est la démonstration de la réalité d’un fait ou de l’existence d’un acte juridique. Celui qui prouve gagne son procès

De nombreuses transactions informatisées ne génèrent pas d’écrit au sens traditionnel (paiement électronique..) ce qui pose la question de la preuve

A partir des ressources jointes et de vos recherches, répondez aux questions suivantes :

**Mission 1  : comprendre ce qu’est la preuve électronique**

**Document 1 : définition de la preuve par écrit**

Le législateur a **défini la preuve par écrit** comme celle résultant « d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*»*

**A la lecture de cette définition, indiquez si un document électronique est considéré comme une preuve**

Oui, pdf ou txt envoyé par mail ou autrement, il s’agit « d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible  quels que soient leur support et leurs modalités de transmission »...

**Document 2 : la force probante de l’écrit électronique**

La loi adoptée le 13 mars 2000 modifie les règles du Code Civil en matière de preuve

**Article 1366 du Code Civil** :"L'écrit électronique a la **même force probante** que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. "

1. **Indiquez ce qu’a reconnu la loi du 13 mars 2000 en matière de preuve.**

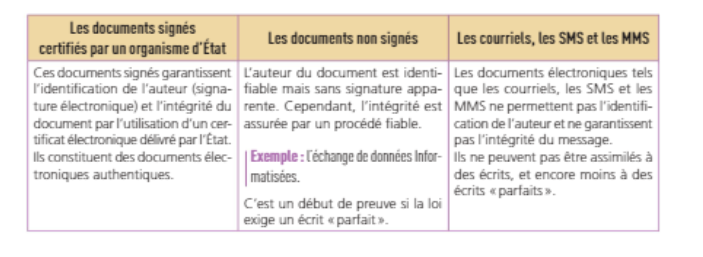
La loi du 13 mars 2000 a reconnu l’écrit électronique comme preuve, aux mêmes titre et conditions que l’écrit sur support papier.

1. **A partir de cet article : à quelles conditions l’écrit électronique à la même valeur probante (cad aussi efficace comme moyen de preuve) qu’un écrit ?**

L’écrit sur support électronique pour qu’il soit recevable il doit

* Être identifiable
* Être conservé de sorte à garantir son intégrité (empêcher son altération)

**Document 3 : les documents électroniques recevables comme preuves électroniques**

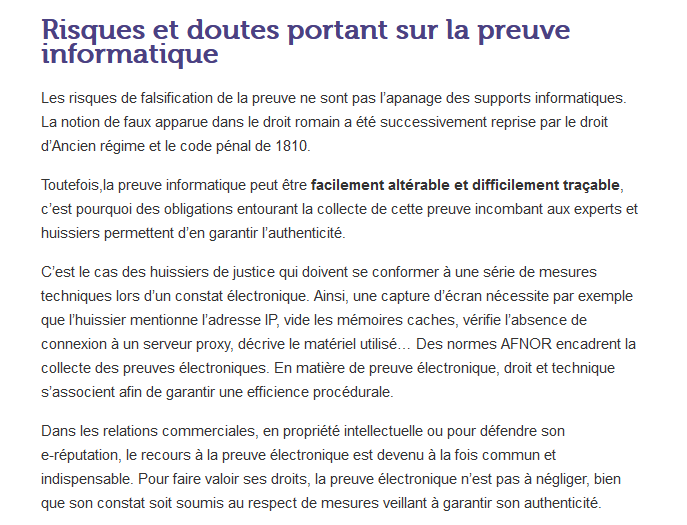


**Pensez vous qu’un simple mail puisse servir de preuve pour établir la réalité d’un fait, d’un accord ?**

Non, car il ne permet pas l’identification de l’auteur et l’intégrité du message n’est pas garantie. Or l’écrit électronique doit être identifiable et intact.

Un mail a une valeur juridique s’il est certifié par une signature électronique réalisée par un organisme agréé et sécurisé. Le mail est un commencement de preuve.

**Document 4 : les risques et doutent portant sur la preuve informatique**



<https://justice.ooreka.fr/astuce/voir/311105/preuve-informatique>

**Soulignez dans le texte, ce qui doit être fait quand il s’agit de collecter des preuves électroniques**

Les risques de falsification de la preuve ne sont pas l’apanage des supports informatiques. La notion de faux apparue dans le droit romain a été successivement reprise par le droit d’Ancien régime et le code pénal de 1810.

Toutefois, la preuve informatique peut être facilement altérable et difficilement traçable, c’est pourquoi des obligations entourant la collecte de cette preuve incombant aux experts et huissiers permettent d’en garantir l’authenticité.

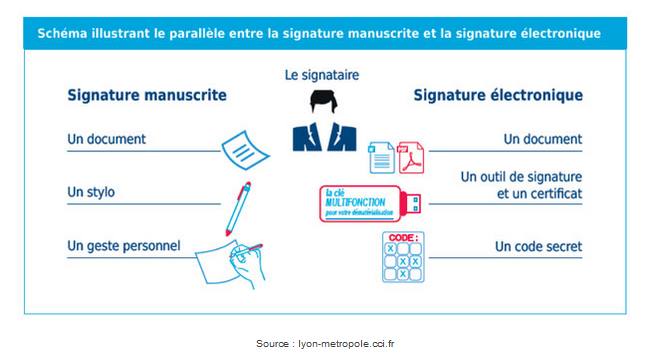
C’est le cas des huissiers de justice qui doivent se conformer à une série de mesures techniques lors d’un constat électronique. Ainsi, une capture d’écran nécessite par exemple que l’huissier mentionne l’adresse IP, vide les mémoires caches, vérifie l’absence de connexion à un serveur proxy, décrive le matériel utilisé… Des normes AFNOR encadrent la collecte des preuves électroniques. En matière de preuve électronique, droit et technique s’associent afin de garantir une efficience procédurale.

Dans les relations commerciales, en propriété intellectuelle ou pour défendre son e-réputation, le recours à la preuve électronique est devenu à la fois commun et indispensable. Pour faire valoir ses droits, la preuve électronique n’est pas à négliger, bien que son constat soit soumis au respect de mesures veillant à garantir son authenticité.

**Mission 2: comprendre la signature électronique**

**Vidéo 1 : la signature électronique : comment ça marche ?**

[**https://www.leolagrange.tv/video/la-signature-electronique-comment-ca-marche/**](https://www.leolagrange.tv/video/la-signature-electronique-comment-ca-marche/)



**à partir de cette vidéo et de l’image, répondez aux questions suivantes :**

1. **Qu’est ce que la signature électronique**

Un code dans le document, unique à son expéditeur. C’est l’usage d’un procédé fiable de l’identification de l’auteur, par la cryptologie.

1. **Que garantit cette signature**

Cette signature permet de distinguer un vrai d’un faux, de vérifier l’authenticité d’un document électronique. Elle garantit l’identité du signataire et l’intégrité du document.

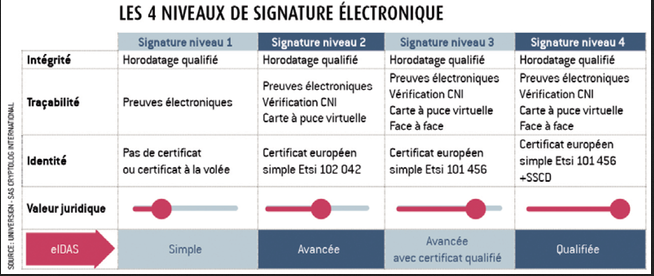
1. **Cherchez ce qu’est la non répudiation en informatique**

L’impossibilité de nier avoir reçu ou envoyé un message. La garantie que deux personnes qui ont participé à une communication ne pourra pas nier y avoir participé.

1. **Quels sont les outils utilisés pour rendre fiable la signature électronique**

Hashage, chiffrement. Dans la majorité des cas, il s’agit d’un certificat numérique porté sur différent supports qui permet d’identifier l’auteur et de garantir l’intégrité du document.

**Document 5 : les 4 types de signatures électroniques**



Nb : Les signatures « simples et avancées » seront acceptées en justice comme des commencements de preuve

**Mission 3 : comprendre la cryptologie car il faut un procédé fiable**

* A **partir de ce site, et de vos recherches répondez aux questions**

<https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>

1. **Définir la cryptologie. Quels sont ses objectifs** ?

Science du secret, du chiffrement. Garantir l’intégrité, l’authenticité, et la confidentialité d’un document électronique.

1. **Quels sont ses applications actuelles ? (les domaines)**

Paiement électronique, authentification des personnes, Assurance (contrat).

1. **Qu’est ce qu’un tiers de confiance**

Prestataire de service dans le domaine des documents dématérialisés qui garantit la sécurisation et la confidentialité et l’intégrité des données transmises.

**Document 6 : comment fonctionne l’authentification ?**

**Vidéo 2 sur les clés publiques et privées**

<https://www.futura-sciences.com/tech/videos/kezako-crypte-t-on-donnees-internet-2001/>

**Définissez les moyens de cryptage**.

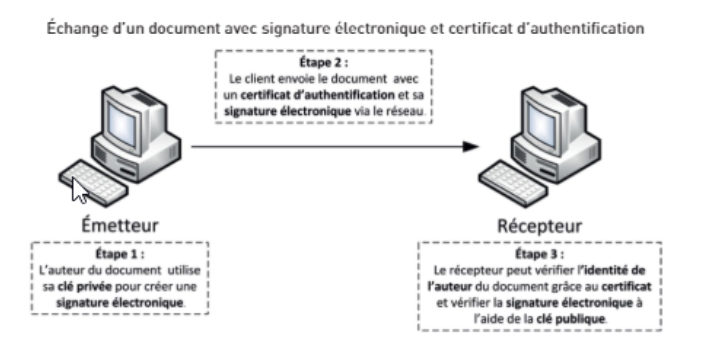
Le cryptage peut se faire par deux méthodes : symétrique et asymétrique. Symétrique : les deux parties qui se partagent le document crypté se partagent aussi une clé de décryptage. Asymétrique : Les deux parties se partagent une clé d’encryptage « publique » pour encrypter le document, et le décryptent de leurs côtés avec leurs clés de décryptages privées.

La signature est réalisée à partir de la cryptographie asymétrique. Elle repose sur un couple de clés, l’une privée, connue par son seul propriétaire, l’autre publique connue de tous. La clé publique a pour fonction de crypter le message et la clé privée, de le décrypter.

La problématique est de pouvoir vérifier l’identité de l’auteur de la signature. L’utilisation d’un certificat électronique, délivré par une autorité de certification de confiance (les tiers de confiance) permet de répondre à ce besoin.

Un certificat doit contenir :

* Les informations d’identification (par exemple, le nom, la localisation..)
* Une clé publique
* Une signature construite à partir de la clé publique



En pratique, on évite de crypter tout le message. On crypte une forme abrégée du message. Cette forme est obtenue à l'aide d'une fonction mathématique complexe appelée fonction de hachage à sens unique.

**Mission 4: réaliser une synthèse**

A l’aide de vos réponses et des ressources

Réaliser **un résumé** :

**La preuve électronique en droit**

Pour réaliser ce travail, **vous répondrez aux questions posées dans un fichier qui** est sur Moodle