Service Informatique

ASSURMER

2023

Concepts et Principes de Cybersécurité.

Date	Rédacteur	Validateur
21 janvier 2023	LE DOHER Loïc ZAMBON Ronan POISSONNIER Mattéo KENNEDY John-Killian	

Table des matières

Texte communautaire de référence en termes de preuve électronique

La multiplication des échanges et des contrats par le biais de l'informatique impose que de nouvelles règles juridiques mettent en place la preuve électronique Les nouvelles technologies doivent être prises en compte pour rendre fiable ce type de preuve.

Définition de la preuve informatique

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 ». La définition, extrêmement large, vise surtout n'importe quel mode de transmission.

Et le législateur de préciser que « l'écrit sous forme électronique est admis en preuve au même titre 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 ».

Le principe est donc clair : la preuve électronique est au même rang que le document écrit. Mais il est nécessaire que l'identité de l'auteur soit certaine et que le document ne puisse faire l'objet de modification.

Texte communautaire

Le régime de la preuve diffère selon les domaines. En droit pénal, commercial ou administratif, la preuve se fait par tous moyens. En droit civil, le nouvel article 1358 (issu de la réforme du droit des contrats du 10 février 2016) dispose que « hors les cas où la loi en dispose autrement, la preuve peut être apportée par tous moyens ».

Ce que la **réforme du 13 mars 2000** a introduit en droit français est la recevabilité devant les tribunaux civils de l'écrit électronique comme preuve d'un acte juridique

Valeur juridique d'une preuve informatique

Force probante de la preuve informatique

L'article 1366 du Code civil dispose « l'écrit sur support électronique a la même force probante que l'écrit sur support papier » : les preuves informatiques ne souffrent pas de leur caractère immatériel en termes de force probante. Toutefois, la force probante peut être mise à mal par les doutes relatifs à l'intégrité de la preuve informatique.

Conditions à la recevabilité de preuve informatique

Deux conditions sont nécessaires à la recevabilité de l'écrit électronique (article 1366 du Code civil) :

- La personne dont elle émane doit pouvoir être dûment identifiée.
- Il doit être établi et conservé dans des conditions de nature à en garantir l'intégrité.
- Apporter la preuve du consentement de la personne.

Signature électronique

Notion de signature électronique

La signature électronique est un procédé permettant à une personne d'apposer son accord sur un document électronique. Elle correspond techniquement aux données électroniques jointes ou associées à un document que le signataire utilise pour signer. La signature électronique ne doit pas être confondue avec la signature numérisée (ex : signature manuscrite scannée) !

Types de signatures électroniques

La signature électronique simple (SES)

Le terme de signature électronique « simple » n'est pas concrètement utilisé dans la règlementation eI.DAS mais utilisé par la grande majorité des fournisseurs. Derrière cette appellation, on retrouve l'ensemble des systèmes de signatures électroniques n'ayant pas un niveau avancé ou qualifié.

La signature simple est la plus utilisée sur le marché car c'est la plus rapide et fluide.

Il n'y a pas de listes d'exigences liées à ce type de signatures. Une signature scannée ou numérique sur une borne par exemple peut être une signature dite simple. Néanmoins, ce sont des signatures qui n'ont aucune valeur juridique.

Regardons alors comment réaliser une signature électronique simple qui soit tout de même reconnue par la justice en cas de litiges, car c'est bien ce qui nous intéresse : être légalement protégé.

Tout d'abord voilà ce que nous dit la règlement eI.DAS concernant les signatures électroniques : ce sont « *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".*

Afin que la signature électronique soit légalement acceptée il faut donc pouvoir prouver que le signataire à bien accepter de signer lesdits documents. Pour cela, le tier de confiance qui propose ses services de signatures électroniques constitue un dossier de preuve dans lequel on retrouve plusieurs éléments essentiels :

- La carte d'identité électronique aussi appelé certificat à usage unique qui permet d'identifier le signataire
- L'horodatage de la signature
- Les éléments d'identification du signataire (adresse électronique, numéro de téléphone, adresse IP de l'ordinateur utilisé pour signer le document, …)

Ce chemin ou dossier de preuve doit ensuite être stocké dans un coffre-fort numérique afin d'assurer la pérennité de l'intégrité du document.

Ces signatures électroniques peuvent être utilisées pour des actes courants ou comportant des risques juridiques ou financiers limités tel que :

- Contrats (adhésion, fournisseurs, baux, travail, etc.)
- Devis
- Etat des lieux d'un logement
- Facture
- Mandat de prélèvement SEPA
- Etc.

La signature électronique avancée (AES)

La signature électronique avancée doit répondre à des critères de vérifications d'identité plus poussés, elle permet ainsi de disposer de niveaux de sécurité supérieurs. Elle doit être liée de manière univoque au signataire et permettre de l'identifier très précisément. La signature électronique avancée doit donc :

- Être lié a son signataire de manière unique et claire
- Permettre d'identifier formellement le signataire
- Être créée par des moyens sous contrôle exclusif du signataire (téléphone ou ordinateur personnel par exemple)
- Garantir que le document ne pourra pas être modifié ultérieurement

On peut ainsi, avec ce type de signatures, être amené à télécharger une pièce d'identité avant de pouvoir signer le document qui sera ensuite ajouté au dossier de preuve. Une case à cocher, ou un texte

à recopier peuvent venir accompagner le document afin de renforcer la preuve de consentement du signataire.

La signature électronique avancée est conseillée dans des transactions financières conséquentes ou dans des documents présentant des enjeux juridiques importants tels que :

- Compromis de vente immobiliers
- Contrats de crédits
- Contrats de certains produits bancaires et d'assurances (épargne, assurance-vie, prévoyance dit « loi Madelin »)

Une solution intermédiaire entre la signature avancée et la signature qualifiée consiste à ajouter une étape de vérification en face-à-face (physique ou distant) de l'identité du signataire permettant d'obtenir un certificat qualifié. Ce type de solution peut être utilisé pour des appels d'offres pour les marchés publics par exemple.

La signature électronique qualifiée (QES)

D'un point de vue légal, la différence entre les signatures simples ou avancées et la signature qualifiée est importante. Ce niveau de signature est contraignant en matière de vérification de l'identité du signataire et de protection de la clé de signature. Elle permet toutefois d'avoir une valeur juridique équivalente à la signature manuscrite alors que les autres niveaux de signatures électroniques ont quant à eux une valeur probatoire.

La signature qualifiée reprend les mêmes critères de sécurité que la signature avancée avec néanmoins quelques subtilités :

- L'identité du signataire doit être validée en amont de la signature
- La clé de signature se trouve dans un dispositif qualifié de création de signature électronique aussi appelé QSCD

La signature électronique qualifiée est le niveau le plus poussé en sécurité. Elle n'est utilisée que dans des cas bien précis, car elle se révèle bien souvent très contraignante :

- Actes d'avocat (conventions de concubinages, PACS, statuts de sociétés, contrats de cessions de fonds de commerce, de parts sociales ou d'actions, etc.)
- Actes produisant des effets hors France, mais dans l'Union européenne (souscriptions de produits financiers européens, opérations bancaires intra-UE)
- Actes auprès d'organismes publics nécessitant de hauts niveaux de sécurité (passation de marchés publics, factures transmises sous format électronique, etc.)

Le choix du mode de signature électronique doit donc être un bon compromis entre l'expérience utilisateur et la sécurité. La signature électronique qualifiée possède des cas d'usage très précis. Lorsque l'on en sort, il faut donc se positionner entre la signature avancée ou simple, les axes de réflexion doivent alors se faire autour du contexte juridique de notre utilisation de la signature électronique, mais également l'analyse des risques et opportunités (enjeux financier, impact sur la productivité, expérience utilisateurs, etc.).

	Simple	Avancée	Qualifiée
Juridiquement contraignante	✓	✓	✓
Rapide et fluide	✓	✓	✗
Création d'un dossier de preuve	✓	✓	✓
Horodatage de la signature	✓	✓	✓
Identification du signataire	✓	✓	✓
Demande de preuve d'identité	✗	✓	✓
Peuvre de consentement	✗	✓	✓
Clef de signature sur un dispositif externe	✗	✗	✓
Cas d'utilisation	Contrat, devis, facture, ...	Contrat bancaire, compromis de vente, ...	Actes d'avocats ou nécessitant de haut niveau de sécurité...

Définition de cryptologie asymétrique

La **cryptographie asymétrique**, ou **cryptographie à clef publique** est un domaine relativement récent de la cryptographie. Elle permet d'assurer la confidentialité d'une communication, ou d'authentifier les participants, sans que cela repose sur une donnée secrète partagée entre ceux-ci, contrairement à la cryptographie symétrique qui nécessite ce secret partagé préalable.

La cryptographie asymétrique peut être illustrée avec l'exemple du *chiffrement à clef publique et privée*, dont le but, comme tout chiffrement, est de garantir la confidentialité d'une donnée lors d'une transmission de celle-ci. Le terme asymétrique s'explique par le fait qu'il utilise deux clefs différentes, l'une, la **clef publique**, pour chiffrer, l'autre, la **clef privée**, pour déchiffrer.
L'utilisateur qui souhaite recevoir des messages engendre un tel couple de clefs. Il ne transmet à personne la clef privée alors que la clef publique est transmissible sans restriction[2].

Quiconque souhaite lui envoyer un message confidentiel utilise la clef publique pour chiffrer celui-ci. Le message chiffré obtenu ne peut être déchiffré que connaissant la clef privée. Il peut donc être communiqué publiquement : la confidentialité du message original est garantie. Le destinataire, qui n'a communiqué à personne sa clef privée, est le seul à pouvoir, à l'aide de celle-ci, déchiffrer le message transmis pour reconstituer le message original.

Acteur d'une solution de signature électronique

Autorité de certification

En cryptographie, une **Autorité de Certification** (AC ou CA pour Certificate Authority en anglais) est un tiers de confiance permettant d'authentifier l'identité des correspondants. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fournis.

Prestataire de confiance

Un prestataire de services de confiance est "une **personne physique ou morale** qui fournit un ou plusieurs **services de confiance**, en tant que prestataire de services de confiance qualifié ou non qualifié". Un prestataire technologique de services de confiance est considéré comme qualifié dès lors qu'il apparaît sur la liste de confiance numérique de l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Certificat de cachet électronique

Le cachet électronique est un **mécanisme cryptographique** permettant d'attester que le créateur de celui-ci est bien à l'origine du document sur lequel il est apposé et d'en garantir l'intégrité et l'intégrité du document sur lequel il est apposé. Il repose notamment sur l'usage d'un procédé fiable d'identification garantissant le lien entre le créateur du cachet électronique et le document électronique auquel il se rattache. Le cachet électronique concerne les personnes morales.