SUPPLÉER L'OPACITÉ DE LA SIGNATURE ÉLECTRONIQUE

Ayant la certitude qu'un acte signé électroniquement a été modifié a posteriori(1), une partie le conteste en justice. Mais, en application de l'article 1367 du code civil, si le juge considère que la signature électronique a été formée par un procédé présumé fiable, la partie qui conteste aura la charge de la preuve, c'est-à-dire que ce sera à elle de prouver que l'acte a été altéré, et elle se retrouvera alors face à un dispositif particulièrement opaque.

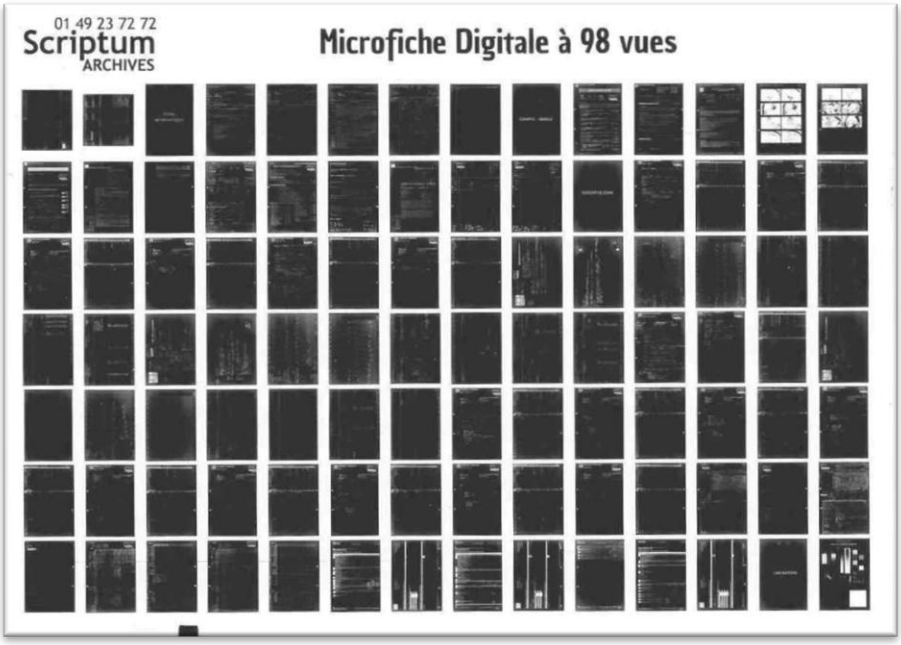
Il existe pourtant un moyen simple et transparent de garantir et de prouver l'intégrité des actes numériques envers et contre tout, et jusqu'au plus long terme. Il est en effet possible d'en établir une **COPIE FIABLE** sur un support **irréversible et durable**.

Cette opération est juridiquement pertinente puisque l'art. 1379 du code civil confère à la copie fiable la même force probante que l'original, et qu'aux termes de l'art. 1er du décret 2016-1673, la copie résultant *"d'un procédé de reproduction qui entraîne une modification irréversible du support de la copie"* bénéficie de la présomption légale de fiabilité.
Et c'est d'autant plus avisé que les moyens appropriés sont en place.

(1) Sur la faculté de modifier un acte signé numériquement, lire La face cachée de la signature électronique.

DÉMATÉRIALISATION ET IRRÉVERSIBILITÉ

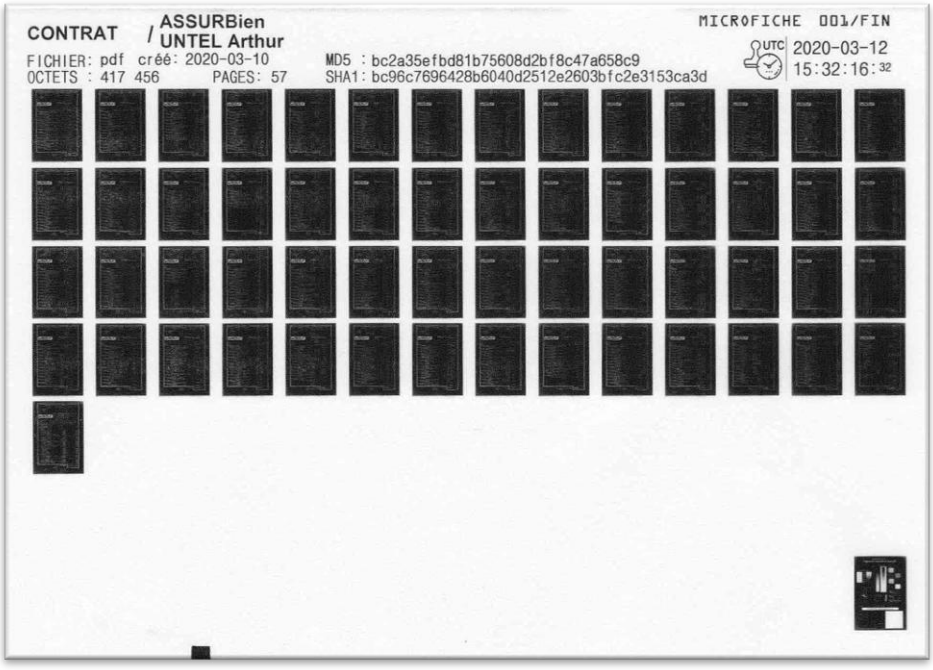
la microfiche digitale



La **microfiche digitale** est un support d'enregistrement irréversible de documents dématérialisés ou immatérialisés
- support argentique
- enregistrement "en clair"
- horodatage systématisé
- cinq siècles de durée de vie
- modification impossible
- aucune obsolescence
Dans l'économie numérique, la microfiche digitale forme donc un moyen de preuve **naturel** de la plus haute fiabilité, apte à sécuriser la force probante des actes numériques jusqu'au plus long terme.

la microfiche LegaLTech

La microfiche LegaLTech est dotée des mêmes propriétés, mais certains arguments juridiques y sont extériorisés. Ainsi, aux fins d'anticiper l'hypothèse d'une vérification d'écriture, le processus de clonage de l'acte met automatiquement en exergue des métadonnées extraites du fichier-source et les rend irréversibles. Notamment :
- le type de fichier
- sa date de création
- sa taille en octets
- le nombre de pages de l'acte
- l'agrégation des empreintes électroniques MD5 et SHA1

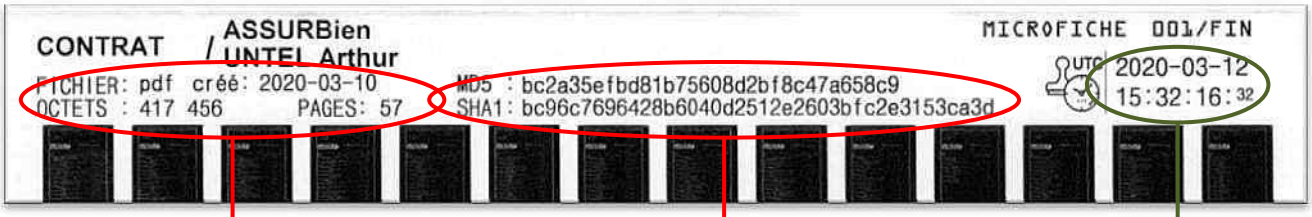


 https://www.scriptum-archives.fr

DÉMATÉRIALISATION ET IRRÉVERSIBILITÉ

qu'est-ce que ça garantit?

Faire établir la **copie fiable sur support irréversible** d'un acte passé par voie électronique peut s'avérer salutaire. Car cela ouvre la possibilité d'effectuer à tout moment une comparaison entre l'acte numérique examiné et son enregistrement homologue non-modifiable.
Face à l'éventuelle obligation d'avoir à prouver qu'un acte électronique n'est pas intègre, voici ce que son enregistrement sur microfiche LegaLTech permet :



Au vu des métadonnées figées sur la microfiche, il suffit d'ouvrir les "propriétés" de l'acte numérique contesté, ce qui permet de vérifier très vite :
- s'il s'agit du même format informatique
- s'il a été créé à la même date
- si sa taille en octets est la même
- s'il comporte le même nombre de pages

Il suffit encore de calculer les empreintes électroniques MD5 et SHA1 de l'acte contesté (opération qui se fait gratuitement, en ligne, et en quelques secondes), et de les comparer avec celles qui figurent sur la microfiche.

Finalisation de la microfiche en temps universel

L'absence de divergence sur la totalité de ces critères atteste d'une parfaite identité entre l'acte électronique et sa version irréversible.
Par contre, toute différence portant sur une ou plusieurs de ces métadonnées démontre qu'il existe une discordance dont toutes conséquences pourront être tirées. Au besoin, l'examen du contenu intégral de la microfiche sous une forme accessible à l'œil nu est toujours possible.

*Rappel : **Une empreinte électronique** est le résumé numérique d'un fichier, issu d'un calcul effectué par un algorithme de "hachage". Toute variation de l'empreinte sous le même algorithme indique que quelque chose du fichier a changé, soit dans sa structure, soit dans son contenu.*
***Si la microfiche LegaLTech se fonde sur l'agrégation des algorithmes MD5 et SHA1,** c'est à la fois par souci de continuité et de fiabilité juridiques :*
- la validité de ces algorithmes n'est pas limitée dans le temps et permet une vérification à long terme.
- l'agrégation de ces deux algorithmes résout le risque de collision(2), car les algorithmes MD5 et SHA1 fonctionnent de manière différente. Dès lors, le fait qu'une collision puisse reproduire à la fois l'empreinte du MD5 et celle du SHA1 relève de l'impossible.

(2) On désigne ainsi le fait que deux fichiers différents engendrent la même empreinte, soit de façon accidentelle, soit de façon provoquée afin de masquer une falsification par exemple.

 https://www.scriptum-archives.fr