La face cachée de la signature électronique

Incluse dans le droit français par la loi du 2000-230 du 13 mars 2000, la signature électronique est actuellement régie par l'article 1367 nouveau du code civil :

> *"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.****"*

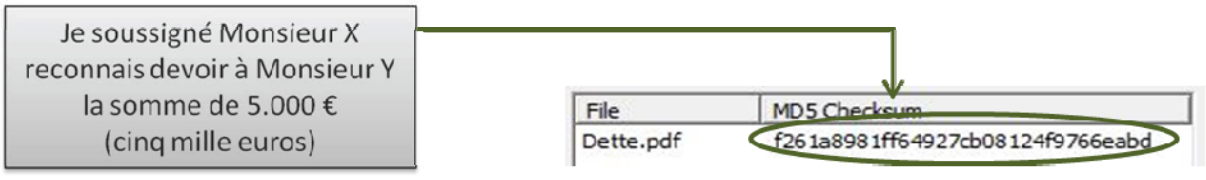
Principe

La signature électronique d'un acte dématérialisé commence par le calcul de son empreinte électronique, chaîne de caractères alphanumériques dépourvue de sens. La moindre variation de l'acte, ne serait-ce que le déplacement d'une virgule, engendre une empreinte radicalement différente. Pour vérifier qu'un document est demeuré intact, on peut donc à tout moment recalculer son empreinte et la comparer avec l'empreinte primaire. Si les deux empreintes sont identiques, c'est que le document est intègre, sinon, c'est que quelque chose a changé.

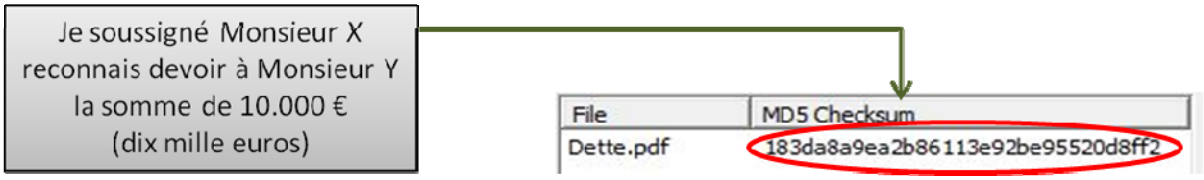
Le calcul de l'empreinte doit être *à sens unique* (on ne doit pas pouvoir reconstituer le document à partir de son empreinte), un même document ne doit produire qu'une seule empreinte, et deux documents différents ne doivent pas produire la même empreinte.

Pour assurer l'identification du signataire, l'empreinte est chiffrée avec une clé propre à une seule personne, et peut être déchiffrée avec la partie publique de cette clé.

Voici l'exemple de l'empreinte électronique[1] d'un acte symbolisé ci-dessous :



Une modification de l'acte engendre effectivement une empreinte radicalement différente :

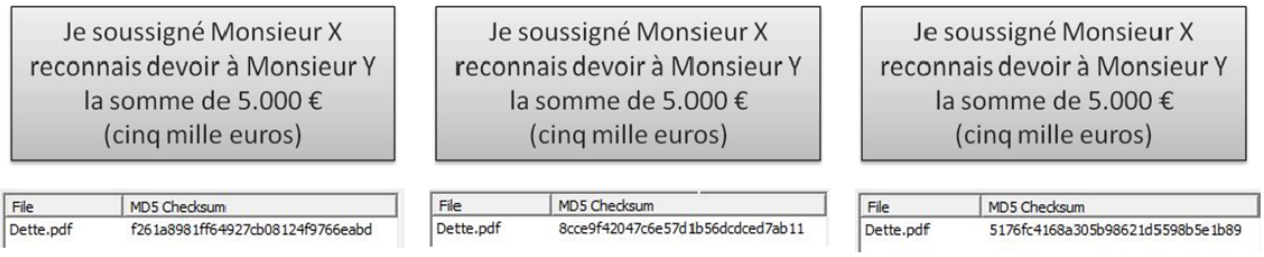


[1] Résultats réels, effectués à l'aide du gratuiciel "mst MD5"

Technique

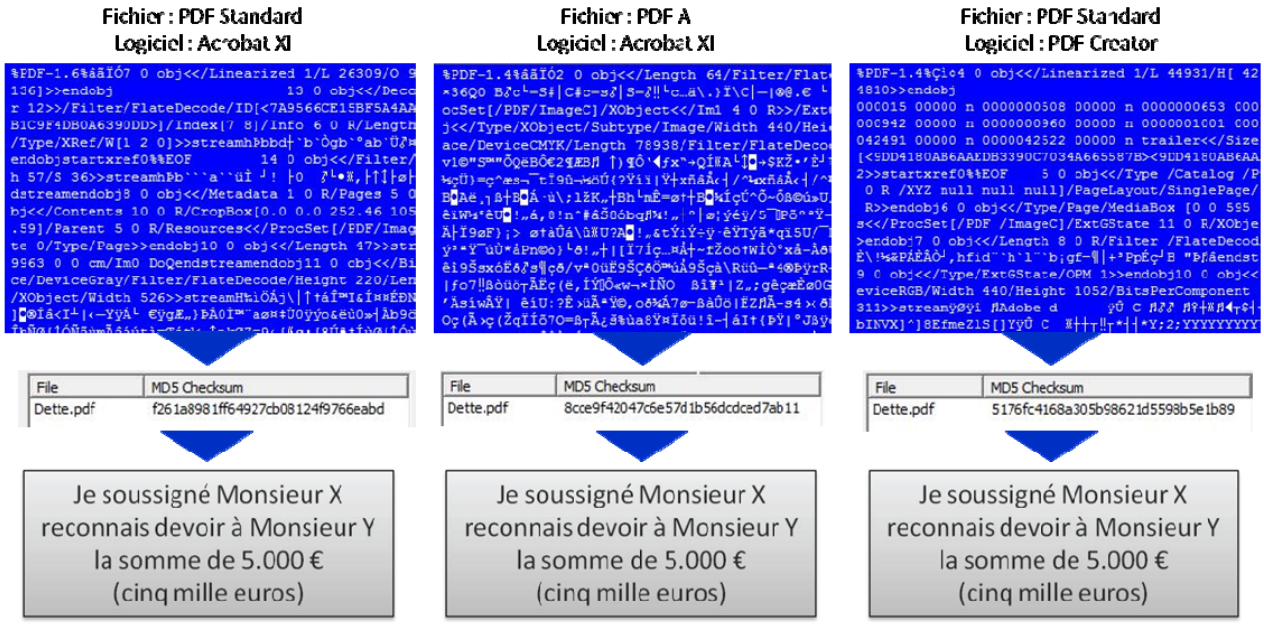
On voit que l'obligation de garantir l'intégrité de l'acte, qui pèse sur la signature électronique, se fonde sur une interaction "document-empreinte", partant du principe que, si toute modification de l'acte modifie obligatoirement son empreinte, toute variation de l'empreinte indique une modification de l'acte par réciprocité. S'agirait-il d'un simplisme?

Car que penser alors des résultats ci-dessous, qui montrent trois empreintes différentes tandis que l'acte est inchangé ?



L'explication est toute simple : l'acte est effectivement inchangé mais, dans le premier cas, c'est un ***PDF "Standard"*** réalisé avec ***Acrobat XI***, dans le second cas, c'est un ***PDF "A"*** toujours réalisé avec ***Acrobat XI***, le troisième cas est un ***PDF "Standard"*** réalisé avec ***PDF Creator***. Comme chacun sait, ces subtilités informatiques ne changent rien ni au contenu, ni à la forme du document. Mais il en résulte néanmoins trois empreintes divergentes.

Si cet imbroglio peut s'avérer problématique au plan juridique, tout est parfaitement normal au plan technique. Car il faut bien savoir que ce que voit un humain au moment de produire une signature électronique ne correspond en rien à ce que l'ordinateur "voit" au même instant. La partie en bleu[2] du schéma ci-dessous montre le fichier **dans la langue de l'ordinateur**, et il se trouve que l'empreinte électronique est une sorte de résumé numérique **du fichier** et non pas de l'acte. Or toute variation informatique modifie la structure du fichier comme on le voit ci-dessous, ce qui a pour effet inévitable de modifier l'empreinte électronique. En fait, un seul et même acte peut engendrer une foule d'empreintes différentes tout en étant intègre. C'est très sournois. Si nous montrons ici la divergence des empreintes issue de trois subtilités du PDF d'un même acte, il faut savoir qu'il en va de même avec tous les logiciels : par exemple, un même document sous Word aura deux empreintes différentes selon que certaines options seront activées ou pas.



[2] Effectués avec le gratuiciel "WnBrowse".

Mise en application

Puisque toute évolution informatique modifie l'empreinte électronique d'un acte et sème le trouble, on pourrait certes penser que le plus simple serait de conserver l'acte dématérialisé tel qu'il est, sans y toucher. Mais c'est compter sans les inconstances de l'archivage électronique, dont les précarités obligent à des migrations périodiques. Cette fatalité est juridiquement confirmée par les articles 2 à 6 du décret 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies. En effet, lorsque la copie d'un acte découle d'un processus électronique, le premier alinéa de l'article 3[3] du décret exige qu'une empreinte électronique soit générée, le second alinéa de l'article 4[4] requérant la génération d'une nouvelle empreinte en cas de migration. La nécessité d'effectuer des migrations périodiques et leurs conséquences sur l'empreinte électronique sont donc officiellement reconnues.

Mais il y a pire. Car si les articles 2 à 6 dudit décret ont vocation à suppléer les carences de l'archivage électronique, elles ouvrent du même coup une brèche insidieuse. En effet, en autorisant les migrations, le second alinéa de l'article 4 autorise *de facto* le dépositaire à revenir a posteriori sur une preuve préconstituée, de façon unilatérale, à plusieurs reprises au besoin, au motif qu'il a hé

librement décidé d'en faire une migration. Voilà qui peut constituer une belle aubaine pour une personne de mauvaise foi, qui pourra à sa guise modifier silencieusement le contenu de l'acte à son avantage avant de prétexter la nécessité d'une migration, et justifier la variation de l'empreinte électronique par ladite migration. Rappelons en effet que le processus de l'empreinte électronique est à sens unique, ce qui fait que la conservation de l'empreinte primaire ne permettra pas pour autant de rétablir l'acte initial.

Conséquences

Au plan formel, on note à titre principal que la signature électronique d'un acte juridique **ne découle pas de l'acte proprement dit** mais d'un fichier occulte, et qu'il n'y a pas d'interdépendance absolue entre l'acte et son fichier, qui peut varier sans affecter l'acte.

C'est juridiquement ennuyeux, puisqu'on en déduit *stricto sensu* que, une personne signant ainsi un acte dématérialisé ne **sait pas** ce qu'elle signe, ne **voit pas** ce qu'elle signe, et ne **comprendrait pas** ce qu'elle signe si même on lui montrait le fichier[5]. On pourrait de la sorte lui faire signer n'importe quoi d'autre que ce qu'elle croit signer.

On s'interroge encore en constatant que le second alinéa de l'art. 1367 exige que la signature électronique *"…consiste en l'usage d'un procédé fiable d'identification **garantissant son lien avec l'acte** auquel elle s'attache"*. Or il est avéré que ce n'est pas le cas puisque la signature électronique ne peut pas être en lien avec l'acte lui-même − c'est techniquement impossible −, mais qu'elle est en lien avec un fichier non-apparent, non-intelligible, et versatile.

Vingt ans plus tard…

Presque vingt ans après son intronisation, la signature électronique reste une disposition équivoque. Car s'il est exact que sa variation signale que quelque chose a changé, on ne peut savoir ce qui a précisément changé, et on ne peut donc pas savoir si cela résulte d'un faux, d'une modification sans effets sur l'acte, voire d'une inadvertance.

---

[3] *"L'intégrité de la copie résultant d'un procédé de reproduction par voie électronique est attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable."*

[4] *"Les opérations requises pour assurer la lisibilité de la copie électronique dans le temps ne constituent pas une altération de son contenu ou de sa forme dès lors qu'elles sont tracées et donnent lieu à la génération d'une nouvelle empreinte électronique de la copie."*

[5] Ce qui interroge alors sur le caractère "écrit" du moyen de preuve, dans la mesure où l'article 1365 du code civil conditionne la preuve par écrit à son caractère intelligible.

De plus, face au temps long dont la justice a besoin, ce système ne peut conduire qu'à un galimatias de métadonnées et d'empreintes électroniques diverses et variées, qui ne fera que complexifier les choses.

On voit au bilan que la signature électronique est un dispositif qui ne permet pas de distinguer le vrai du faux alors que c'en est une fonction essentielle, que ce processus manque de fiabilité juridique en créant plus de doutes que de certitudes, et que les failles qu'il contient peuvent être exploitées pour falsifier les actes juridiques sous couvert de règles établies par décret.

En tout état de cause, il y a maldonne sur les enjeux : Il est clair que ce qui est voulu par l'article 1367 du code civil, c'est que la signature électronique permette d'établir l'intégrité de l'acte, pas de s'encombrer des subtilités de l'informatique. Ce qu'une variation de l'empreinte électronique doit trahir, c'est une modification de l'acte susceptible d'être une falsification, pas une modification des outils.