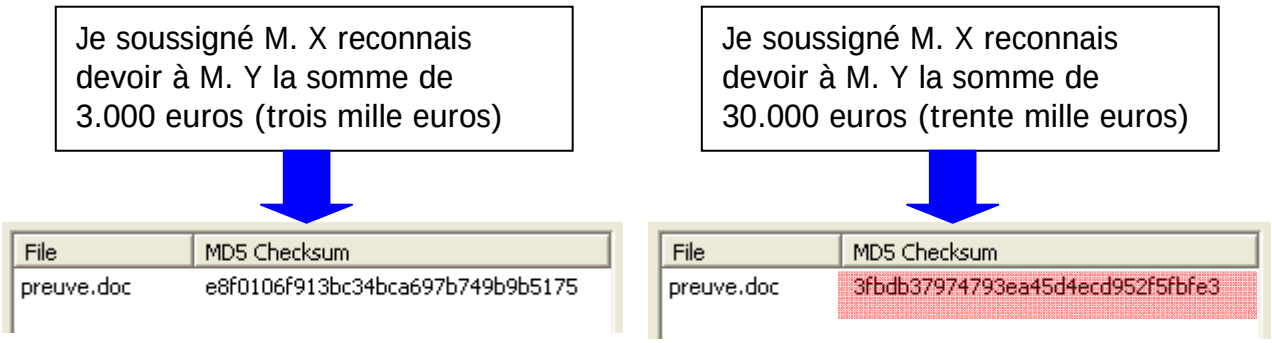
La face cachée de la signature électronique

Analyse effectuée par Lucien PAULIAC
Président de l'Association Preuve & Archivage

La signature électronique[1] fut intégrée dans le droit français le 13 mars 2000, par l'article 1316-4 du code civil. Les descriptions qui en sont faites par ailleurs semblent lui conférer une portée juridique considérable, un document ainsi signé étant réputé être :

- imputable;
- intègre;
- infalsifiable;
- irrévocable.

Dix ans plus tard, on a la nette impression que les mécanismes de cette signature restent largement méconnus, d'où l'intérêt d'en observer le fonctionnement, et de mesurer la réalité de ses conséquences techniques et juridiques dans les usages actuels. Morceaux choisis :

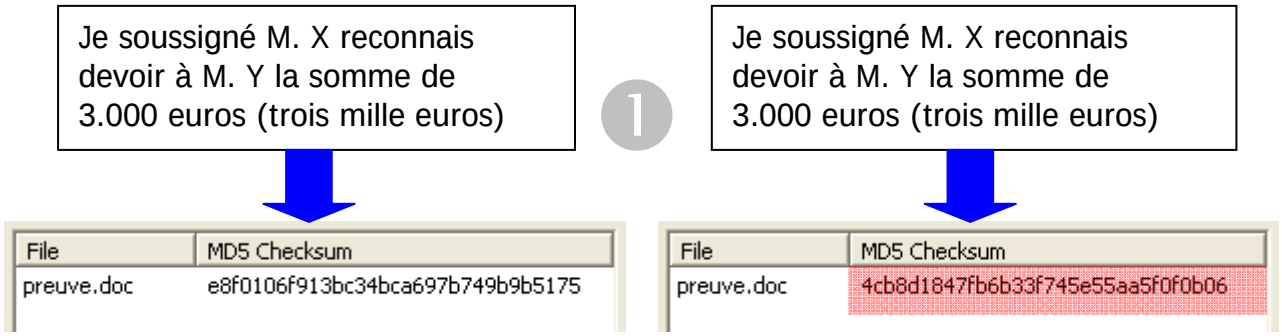


L'exemple ci-dessus montre une application efficace de la signature électronique. Nous sommes dans une hypothèse d'école dans laquelle M. Y, détenteur d'une reconnaissance de dette que M. X lui a délivrée sous forme électronique, a modifié le montant de la somme à son

[1] Rappelons sommairement que la signature électronique fonctionne sur un principe de cryptographie, par le calcul d'une empreinte numérique (parfois appelée "condensat") propre au document concerné. Ladite empreinte est le résumé numérique d'un fichier, effectué à partir d'un algorithme de "hachage" (les plus connus sont le MD5 et le SHA1), résumé aboutissant à une chaîne de caractères échappant à l'entendement. 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 pouvoir produire qu'une seule empreinte, et deux documents différents ne doivent pas pouvoir aboutir à la même empreinte (le fait de déplacer ne serait-ce qu'une virgule engendre une empreinte numérique radicalement différente). Pour ces raisons, on considère qu'un document produisant une empreinte dissemblable de ce qu'elle était à l'origine a été altéré. Dans le processus complet, l'empreinte est elle-même cryptée avec une clé de chiffrement propre à une personne, puis déchiffrée avec la partie publique de ladite clé, ceci étant destiné à identifier le signataire.

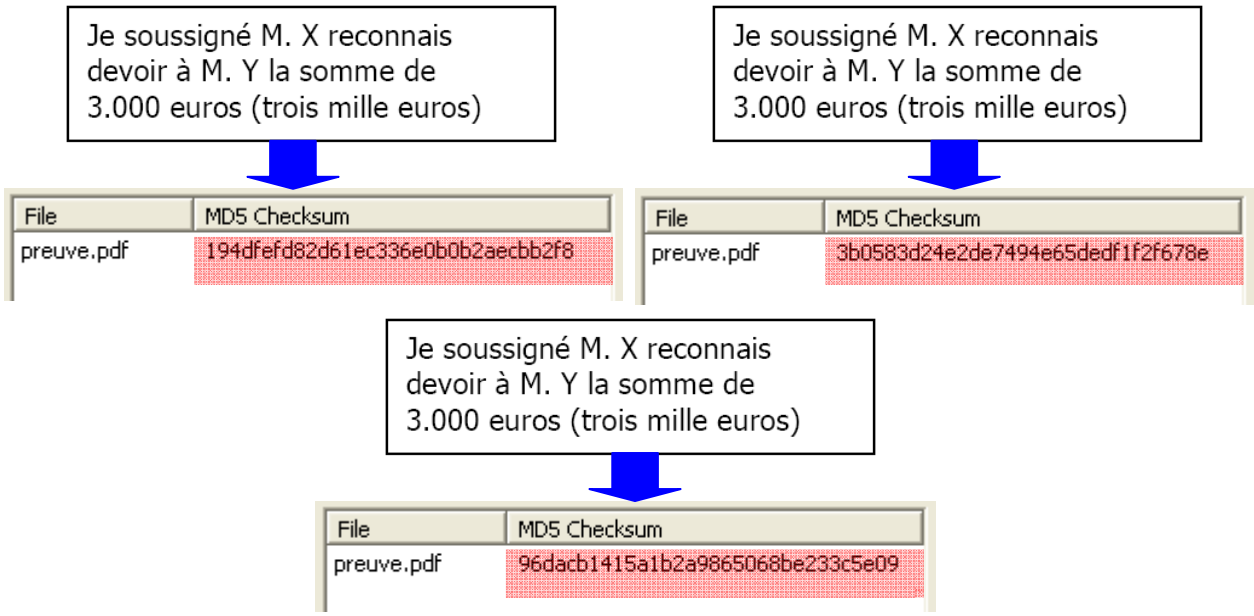
avantage. Cette malversation est signalée par une différence flagrante de l'empreinte numérique (MD5 Checksum[2]) et, fort heureusement, l'indélicat M. Y ne pourra se prévaloir en justice de cet acte, dénoncé comme faux par la signature électronique. La malhonnêteté est donc mise en échec, et tout va bien.

Mais supposons maintenant que M. Y soit honnête homme et n'ait rien modifié. On ne peut alors que s'interroger sur ce qui suit :



Ici, la vérification numérique indique que le message qui se trouve sur la droite a été altéré, puisque son empreinte numérique est différente de celle de gauche. Le problème, c'est que le message est parfaitement intact, mais qu'il est néanmoins déclaré "faux" par la signature électronique.

C'est fort ennuyeux puisqu'un document considéré comme faux devient inopposable, alors qu'en l'espèce il n'a été falsifié en aucune manière. Cela pose un problème de droit aussi grave que si la signature électronique avait été "cassée". Et il ne s'agit pas là d'un cas fortuit, ainsi qu'on le constate ci-après :



Comme on le voit, trois versions PDF strictement identiques du même document engendrent, elles aussi, des empreintes numériques dissonantes, et toutes seront donc suspectées d'être des faux.

Que se passe-t-il? Y a-t-il dysfonctionnement? Y aurait-il une faille?

[2] Démonstrations effectuées à l'aide du gratuiciel "mst MD5"

Explication

En fait, tout ceci est parfaitement normal d'un point de vue technique.
Dans l'exemple ❶, le fichier "preuve.doc" situé à gauche a été établi à partir du logiciel "Word" version 1997, tandis que le "preuve.doc" situé à droite a été converti avec "Word" version 2003. Quant aux trois PDF :

- le premier est un PDF "standard" effectué avec le logiciel *Acrobat 8*;
- le second est lui aussi un PDF "standard", mais effectué avec le logiciel *PDFCreator*;
- le troisième est un PDF-A, effectué avec le logiciel *Acrobat 8*.

Et on voit que toutes les empreintes numériques divergent, et il ne peut pas en être autrement.

Car l'algorithme de hachage ne prend pas en compte la représentation matérielle ou le contenu sémantique du document. Il provient de ses données numériques. Et il se trouve que toute conversion de format d'un fichier en modifie les données. C'est ainsi par exemple que la conversion d'un fichier, de Word 97 vers Word 2003, n'entraîne aucune adultération du document lui-même, mais n'en modifie pas moins la structure du fichier[3]. Les données ayant varié, leur empreinte numérique change avec elles; c'est inévitable.

Autrement dit, toute conversion de format informatique (ou "migration" comme on dit désormais), si anodine qu'elle paraisse (comme le passage d'un PDF standard à un PDF-A), modifie l'empreinte numérique et dénonce un faux.

Le problème, c'est que si l'on veut conserver des documents sous forme numérique, ces conversions sont obligatoires. Il n'est qu'à lire la norme Afnor NF Z 42-013 (2009) pour s'en convaincre, celle-ci expliquant que la survie de l'archivage électronique oblige à faire des conversions périodiques pour de multiples raisons[4].

Ça n'est pas une découverte

Le pire, c'est qu'il ne s'agit pas là d'une découverte. Cette faille structurelle de la signature électronique a officiellement été rendue publique le 1er décembre 2005 dans la Recommandation rendue par le Forum des droits sur Internet, laquelle contenait notamment ces lignes :

> *Ainsi, un même texte représenté sous deux formats différents, par exemple en « .doc » et en « .pdf », aura deux signatures cryptographiques complètement différentes, même si ces deux documents numériques correspondent exactement à la même information et produisent des documents papier strictement identiques.*
> *…/…*
> *La signature [électronique] perd entièrement sa validité dès que l'on change le format de codage du document (ou la version d'un même format). La conservation de la signature cryptographique interdit donc toute migration de format de codage, opération généralement nécessaire pour assurer la lisibilité du document sur le long terme.*

Autrement dit, le dysfonctionnement a été décrit, et on est un peu étonné qu'il n'ait pas davantage porté à conséquences et que la plupart des descriptions de la signature électronique continuent d'être aussi lénifiantes.

---

[3] Voir à cet égard *L'intégrité en question* http://www.megapreuve.org/cariboost_files/integrite_en_question.pdf

[4] On observera en passant que cette même norme prescrit de garantir les données par une fonction de hachage et par la signature électronique, en même temps qu'elle conseille leur conversion régulière, sans le moindre état d'âme pour les conséquences juridiques résultant de l'incompatibilité des deux procédures.

Au plan juridique, on semble être dans l'impasse. Car une personne détenant la preuve de ses droits établie sous forme électronique aura le choix entre :

- le risque de tout perdre par un inexorable phénomène d'obsolescence;
- la certitude de voir ladite preuve être dénoncée "fausse" par son empreinte numérique si le fichier fait l'objet de la moindre évolution nécessaire à sa conservation.

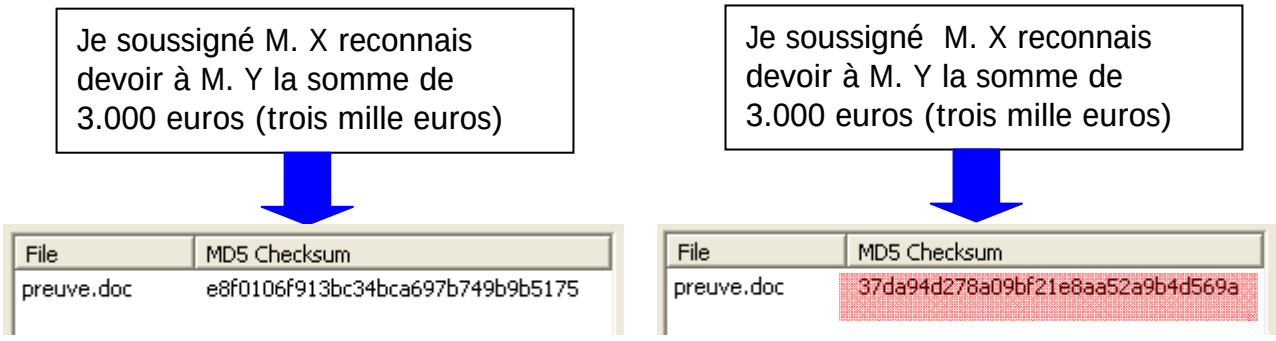
C'est critique, car le rôle essentiel d'une preuve préconstituée est de véhiculer dans le futur les droits ou les obligations qui y ont été consignés. Et le terme *futur* n'est pas un vain mot. Rappelons que les textes relatifs à la prescription extinctive conduisent à une durée minimale de 20 ans[5] pour l'archivage des documents probatoires, sans préjudice de règles exigeant des durées supérieures, comme ce qui concerne la propriété immobilière ou certains types d'archives dans le monde de la santé notamment. Sur de telles durées, plusieurs migrations de format informatique s'avèreront nécessaires.

Face à ces réalités, on s'aperçoit tout bonnement que la signature électronique n'est pas archivable en tant que telle, puisqu'elle ne supporte pas les conversions alors que celles-ci sont impératives si l'on veut conserver des documents sous forme numérique.

La boîte de Pandore

La situation paraît inextricable. Admettre qu'une distorsion de l'empreinte d'un document numérique puisse n'être due qu'à une variation de format informatique ouvrirait la boîte de Pandore. Une telle brèche serait naturellement exploitée. Pour reprendre notre petit exemple schématique, il deviendrait possible à M. Y d'être malhonnête pour pas cher, en modifiant le contenu significatif de l'acte avant d'effectuer une simple migration de format pour lui servir d'alibi.

Au summum, il faut encore savoir que le risque d'erreur d'appréciation lié à l'empreinte numérique d'un document peut tout aussi bien concerner une modification casuelle de son contenu. Ainsi ce nouvel exemple :



Ici, quelque chose s'est bien trouvé modifié : une espace a été ajoutée entre "Je soussigné" et "M. X". Naturellement, l'empreinte numérique signale une altération. Mais il n'y a aucun *faux* pour autant. Aux termes de l'article 441-1 du code pénal[6], le faux est une *"…altération*

---

[5] Voir notamment *La preuve numérique face à la réalité*
http://www.megapreuve.org/cariboost_files/Prescription_20extinctive.pdf

6 Code pénal, article 441-1 : *Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.*
Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende.

frauduleuse de la vérité, de nature à causer un préjudice…". En l'espèce, la vérité n'est pas altérée, et l'ajout d'un blanc à cet endroit ne peut causer de préjudice à personne. Pourtant, le document n'en sera pas moins réputé faux par une variation de son hachage. On constate dans ce cas que le passage au rouge de l'empreinte numérique ne fait que brouiller la vue, et va finalement à l'encontre de la recherche de la vérité.

Le droit à la preuve

Il apparaît au bilan que la signature électronique n'apporte pas aux données la sécurité juridique dont on la crédite. On voit aussi que ce modèle de signature est potentiellement porteur de plus de trouble que de certitude, en faisant passer pour "faux" ce qui est "vrai" à la suite d'actions inévitables et apparemment anodines, et en ne permettant pas de faire la différence entre ce qui est conséquent et ce qui est insignifiant.

Mais le pire sans doute est la perniciosité du contexte actuel. Car en ce moment même, appliquant peut-être une norme française homologuée, des personnes de bonne foi effectuent des conversions de format de leurs documents probatoires dans l'unique but de mettre leurs fichiers à niveau, et sans se douter qu'elles agissent à leur détriment si les documents étaient bordés par une empreinte numérique.

Le principe de la signature électronique nécessite que son processus échappe à l'entendement, et ne peut donc fonctionner que si on lui voue une confiance aveugle par une sorte de concession au mystère. Il apparaît désormais que la confiance requise est sujette à caution.

L'administration de la preuve est le pivot des décisions de justice et, ainsi que cela a déjà été écrit[7], *la ruine pratique ou la perte de crédibilité des moyens de preuve sont les signes avant-coureurs d'un désastre social et économique, puisque ce sont les modes de régulation des conflits qui perdent en conséquence toute efficacité*.

Paris, 27 septembre 2010

[7] In *Archivage des documents numériques à vocation probatoire*, Groupe PragmArchive http://www.pragmarchive.org/PA_002.PDF