Les Ateliers de la démat' - Jeudi 24 novembre 2016 -Salle Charles De Gaulle,
Hôtel du Département, place de la Préfecture à Tours

La signature électronique

Conférence de Céline Guyon, archiviste expert en dématérialisation, consultante en gestion de données et archivage électronique, vice-présidente de l'Association des archivistes français (AAF).

La signature électronique est souvent présentée comme indispensable dans l'univers numérique. Mais qu'entend-on par-là exactement ? Quelle différence y a-t-il entre clé, certificat, empreinte et horodatage ? Juridiquement, quelles sont les obligations à respecter ?

L'objectif de cette intervention était d'acquérir le vocabulaire et de comprendre les enjeux et les techniques de la signature électronique.

Cette rencontre a été conçue et organisée par une équipe d'archivistes de différentes structures tourangelles : Archives départementales d'Indre-et-Loire, Université François Rabelais de Tours, CCAS de Tours, Syndicat intercommunal d'énergie d'Indre-et-Loire (SIEIL) et avec le concours d'une archiviste de Saint-Gobain Archives.

80 personnes ont participé à cet atelier, témoignant ainsi d'un réel besoin d'information et d'échanges. Ils étaient pour la plupart élus ou agents des collectivités territoriales et établissements publics locaux.

L'intervention aura permis de dédramatiser la question de la signature électronique, en trois points :

1) Le rôle de la signature électronique.
2) Comment fonctionne-t-elle ?
3) Le déploiement d'un système de signature électronique.

La signature électronique ne se forme pas comme la signature manuscrite, elle ne se voit pas : on ne peut pas identifier immédiatement un élément graphique qui suffise à reconnaître la signature électronique.

1) Le rôle de la signature électronique

Les signes de validation apposés sur un document existent depuis des millénaires (exemple : les sceaux). En France, c'est une ordonnance royale de 1554 qui a institué l'apposition de la marque autographe du nom propre sur les actes notariés.

La signature est présentée comme indispensable pour authentifier un document. Elle permet au lecteur d'identifier la personne et l'organisme qui l'a émis. Elle apporte de la confiance dans l'environnement numérique, la confiance dans le signataire et dans le contenu de l'information.

La signature électronique est un mécanisme permettant de garantir **l'intégrité** d'un document électronique et d'en **authentifier** l'auteur, par analogie avec la signature manuscrite d'un document papier.

Cependant elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle : l'identification ne repose sur aucun élément graphique.

Dans l'environnement numérique : l'écrit devient indépendant de son support.
Dans l'environnement papier, la preuve littérale ou preuve par écrit consiste en une suite de caractères, lettres, chiffres ou autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et les modalités d'écriture.

L'écrit sur support électronique est admis comme preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dument identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à garantir son intégrité.

Quelle valeur juridique ?

En France, ce sont la loi du 13 mars 2000 et son décret d'application du 30 mars 2001 qui ont adapté le droit de la preuve aux technologies de l'information et permettent le recours à la signature électronique. L'existence de la signature électronique sécurisée est reconnue selon des critères stricts.

Article 1316-4 du Code civil : définition de la signature électronique
« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité de 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'Etat

La signature électronique a donc plus de 15 ans d'existence. C'est beaucoup... et peu à la fois, au regard de plusieurs siècles de signature manuscrite ! Aussi reste-t-elle encore relativement méconnue non seulement du grand public mais aussi des professionnels.

La signature électronique est aujourd'hui le meilleur procédé informatique permettant de donner la même valeur juridique à un écrit électronique qu'à un écrit papier. Elle a pour principales caractéristiques d'identifier celui qui l'a produit et de garantir que le contenu de la pièce numérique ainsi signée n'a pas été altéré.

Dans le monde numérique, comme dans les processus traditionnels non dématérialisés, tous les documents ne nécessitent pas d'être signés. Néanmoins, dès lors que l'organisation ou l'individu à l'origine de la production d'une pièce numérique (document, son, image) souhaite pouvoir prouver qu'il en est bien l'auteur et qu'elle est représentative de sa volonté, qu'elle est bien sa création, et qu'elle n'a pas été altérée depuis sa création, il n'a guère de meilleur choix que de recourir à une signature électronique.

La signature électronique ne consiste en aucun cas dans l'apposition d'une image numérisée de la signature manuscrite sur un document numérique mais en l'usage de procédés cryptographiques permettant de faire le lien entre l'identité du signataire et le contenu du document et de préserver son intégrité.

2) Comment fonctionne la signature électronique ?

La signature électronique est un signe de validation, c'est-à-dire qu'elle authentifie un acte, elle transforme un document en instrument juridique. La loi de 2000 et le décret de 2001 déjà cités lui donnent la même valeur légale qu'une signature manuscrite. Cette question est abordée au niveau européen (règlement de juillet 2014 dit eIdas) pour permettre les échanges marchands.

Un document numérique signé électroniquement est un original. L'impression sur papier de ce document n'est qu'une copie.

Attention, l'équivalence de preuve entre le papier et le numérique est assujettie à un certain nombre d'exigences techniques en termes d'élaboration et de conservation, ce qui pose le problème de l'obsolescence technologique.

La signature électronique a trois rôles :
- identifier le signataire ;
- marquer l'adhésion du signataire au contenu de l'acte ;
- valider un acte.

Identifier le signataire :
- identité personne physique, son nom propre ;
- identité personne physique agissant dans son cadre professionnel ;
- identité personne morale ;
- identité fonction du contexte dans lequel la signature est réalisée. Une même personne peut signer alternativement en son nom propre ou au nom d'une personne morale.

Le niveau de fiabilité de l'identité :
- besoin de certifier l'identité : l'identité peut être simplement déclarative ou peut-être fiable, c'est-à-dire garantie par un système d'authentification ;
- adapter le niveau de fiabilité aux besoins, c'est-à-dire au contexte dans lequel cette identité est requise.

La **fiabilité** de l'identité est définie en trois niveaux réglementaires (3 classes = 3 niveaux de fiabilité) :
- Classe 1 : la certification de l'identité d'un signataire sans autre contrôle que la validation de son adresse mail ;
- Classe 2 : la certification de l'identité à distance : un tiers atteste l'identité sur la base de copies des papiers d'identité ;
- Classe 3 : la certification de l'identité d'un signataire par une rencontre en face à face et sur présentation des papiers d'identité originaux.

Le certificat est délivré par une **autorité de certification**. C'est une pièce d'identité électronique. La signature prend la forme d'un **certificat**.

L'enregistrement du porteur de certificat :
- le demandeur du certificat prouve son identité en respectant le processus défini par l'autorité de certification et définissant le niveau de certification qu'il souhaite acquérir ;
- l'enregistrement est réalisé par l'autorité d'enregistrement, qui peut être distincte de l'autorité de certification.

La fabrication du certificat
Le système actuel repose sur une paire de clés cryptographiques, appelées « clé privée » et « clé publique » ; la clé privée est la « marque de création » de la signature électronique.
L'identité du signataire et sa clé publique sont liées entre elles dans un fichier appelé certificat, scellé par l'autorité de certification émettrice, qui garantit son intégrité, son niveau de sécurité.

Le certificat a une durée de vie contractuelle de 2 à 3 ans, il faut donc prévoir son renouvellement. Le coût d'un certificat dépend du niveau de fiabilité (d'une à trois étoiles).

Ces niveaux sont déclinés dans le référentiel général de sécurité[1] (RGS) :
- 1 étoile correspond à la classe 2 ;
- 2 étoiles correspondent à la classe 3+ ;
- 3 étoiles correspondent à un certificat qualifié de la classe 3+[2].

Le support du certificat fourni par l'opérateur de certification peut être :
- une carte ;
- une clé USB ;
- un serveur (certificat logiciel) ;

[1] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.
[2] Le symbole « + » signifie que le certificat est hébergé sur un support physique comme une carte à puce ou une clé USB.

Analogie : le code PIN de la carte bleue
Le cycle de vie du certificat :

- la durée de vie limitée dans le temps (2 à 3 ans) ;
- la révocation du certificat (inscrite sur une liste nationale) ;

En cas de perte ou de vol d'un certificat, il faut faire opposition ainsi le certificat est révoqué, comme pour une carte bleue.
Un obstacle au développement de ce système réside dans le coût élevé du renouvellement des certificats.

La durée de vie du certificat est beaucoup plus courte que celle du document ainsi validé !

La durée de vie du certificat de 2 à 3 ans pose un problème pour la conservation des documents : le plus souvent la durée d'utilité administrative (DUA) d'un document est supérieure à la durée de validité du certificat. La signature électronique n'est pas uniquement une authentification, c'est aussi un engagement juridique.
A cause de la péremption des certificats, il est important de développer, en même temps qu'un projet de signature électronique, un système d'archivage électronique, métadonnées. Cela sécurise le document et sa signature, au-delà de la durée de vie du certificat. Cela montre en quoi un projet de système de signature électronique peut être structurant pour une collectivité.

Est-il possible de signer durablement un document sous forme électronique ?
Comme tout projet numérique c'est un problème technique certes, mais surtout un problème d'organisation, de conduite du changement et de sensibilisation.

Il faut mettre en place une chaîne de confiance, un tiers se porte garant de l'identité du signataire :

- la confiance dans l'identité du signataire découle de la confiance dans l'autorité de certification ;
- l'autorité de certification se porte garante de l'identité du signataire ;
- la confiance repose sur le contrôle de l'autorité de certification par l'Etat ;

Les autorités de certification sont auditées et agréées en application de l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de service de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

D'autres éléments de confiance
L'horodatage, qui garantit la date et l'heure de la réalisation de la signature, permet de savoir entre autres si le certificat du signataire n'est pas révoqué au moment de la signature. La seule date fournie par le serveur n'est pas fiable.

La preuve de validité du certificat au moment de la réalisation de la signature se présente sous forme d'une liste de certificats révoqués ou d'un jeton OCSP (Online Certificate Status Protocol) garantissant que le certificat n'est ni périmé, ni révoqué.

3) Le déploiement de la signature électronique.

La signature électronique côté technique

La signature électronique, fondée sur la cryptographie asymétrique, repose sur l'exploitation d'une clé publique et d'une clé privée qui sont mathématiquement liées.
L'émetteur « hache » le document à envoyer (calcul d'une « empreinte » pour garantir l'intégrité du document entre l'émetteur et le destinataire) et chiffre le « condensat » à l'aide de sa clé privée. Le document est ensuite envoyé au destinataire avec son condensat chiffré et les informations du certificat électronique du signataire.

A l'arrivée, le destinataire peut déchiffrer la signature électronique grâce à la clé publique contenue dans le certificat électronique du signataire, accessible sur l'annuaire ou sur le site web de l'autorité de certification. La comparaison du condensat reçu, déchiffré avec l'empreinte obtenue par un hachage du document reçu, permettra de vérifier la correspondance entre les empreintes et donc la non-altération du document.

En d'autres termes, la réalisation technique d'une signature électronique consiste en un calcul mathématique réalisé à partir :

- du document à signer (ce qui garantit son intégrité) ;
- de la clé privée du signataire (ce qui garantit le lien avec son identité au travers du certificat).

Le mécanisme est donc fondé sur l'usage de deux clés distinctes :
- la clé privée est utilisée par le signataire (chiffrement) ;
- la clé publique est utilisée pour la vérification de la signature (lecture, décodage)

Deux étapes :
- Calculs mathématiques d'empreinte appliqués au document
- La clé privée permet de chiffrer l'empreinte et permet de conserver le lien entre le document et le signataire.

L'empreinte est indissociable du document dont elle est extraite.

Le chiffrement de l'empreinte avec la clé privée (sécurité) : établissement du lien entre clé privée et son propriétaire.

La vérification de l'empreinte à l'arrivée avec la clé publique.

Les différents modes de réalisation d'une signature électronique
En fonction des besoins, on peut envisager différentes manières de réaliser une signature électronique.

– Autonome : le signataire a le certificat sur clé USB et sur serveur logiciel.
– La signature électronique à la volée :
  - le signataire acquiert un certificat à usage unique ;
  - le signataire s'authentifie sur une plateforme ;
  - le niveau de confiance est fonction des conditions d'authentification.

La signature électronique sur tablette :
- le client appose sa signature manuscrite sur tablette avec un stylet ;
- une signature électronique à la volée est réalisée en plus de la signature manuscrite.

Les différents formats de la signature électronique (tous types de fichiers peuvent être signés) :
- XAdES = signature électronique XML
- PAdES = signature électronique PDF
- CAdES = aussi appelé PKCS#7 ou CMS

Il faut continuer à se poser la question du rôle du document, comme dans l'environnement papier**.** Toutes les signatures électroniques ont une valeur juridique (signature simple ou sécurisée/qualifiée). La signature électronique sécurisée emporte présomption de fiabilité.

Les exigences relatives à la signature sécurisée sont contraignantes à mettre en œuvre et ne concernent dans la pratique qu'une population très réduite, principalement les professions réglementées pour la perfection des actes authentiques.

A retenir

- La signature doit : être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir entre le signataire et l'acte un lien tel que toute tentative de falsification soit détectable.

La signature électronique renvoie aux notions :

- d'authenticité (= certificat) ;
- d'intégrité (= contrôle de l'empreinte).

⇨ **Un document signé électroniquement doit faire immédiatement l'objet d'un archivage électronique. Seul un système d'archivage électronique sécurisé permettra de garantir cette signature dans le temps après la fin de la durée de validité du certificat.**

⇨ **Dans l'environnement numérique, plus encore que pour le papier, l'archivage doit être organisé dès la création du document.**

⇨ **Lors de la migration des formats on modifie l'empreinte des fichiers mais grâce au système d'archivage électronique on peut conserver la valeur probante du document.**

⇨ **Une image de signature scannée n'a aucune valeur juridique car elle ne permet ni identification ni authentification.**

⇨ **Il convient de ne pas acheter un parapheur pour chaque progiciel utilisé dans une collectivité mais d'utiliser au contraire un parapheur unique pour tous les flux.**

⇨ **Tous les aspects sont à prendre en compte dans un projet de signature électronique : outils ; organisation ; procédures ; archivage.**