

La signature électronique dans les marchés publics

La dématérialisation des procédures de passation des marchés publics a été introduite le 7 mars 2001 dans le code des marchés publics. L'article 56 dudit code dans sa rédaction actuelle suite au décret du 7 janvier 2004 impose la transmission par voie électronique des offres et des candidatures.

Au 1^{er} janvier 2005 les acheteurs publics doivent être en mesure et ne peuvent plus s'opposer au fait de recevoir la réponse d'un soumissionnaire d'un appel d'offre par voie électronique. Le décret du 30 avril 2002 pris en application du 1^o et du 2^o de l'article 56 du code des marchés publics vient préciser les modalités d'application de l'article.

Le décret dans son visa fait référence aux dispositions légales sur la signature électronique, à savoir les articles 1316 à 1316-4 du code civil et le décret du 30 mars 2001. On peut en déduire que la signature électronique est un élément essentiel de la dématérialisation des procédures de passation des marchés publics.

Qu'est ce qu'une signature électronique ?

Pour signer un document on utilise actuellement le système dit des clé asymétriques ICP (Infrastructure à Clés Publique) ou PKI (Public Key Infrastructure),

Concrètement il y a plusieurs étapes. On va avoir recours d'une part à la technique du hachage, on va ensuite utiliser la cryptographie asymétrique, enfin on a recours aux certificats.

Le condensé ou hachage

Faire un condensé revient à générer une version réduite du texte. Le condensé du document est généré à partir d'un algorithme, dont la mise en œuvre garantit que deux textes différents ne peuvent aboutir à un même condensé.

Donc si le document change, le condensé ici du document modifié ne peut être le même. A contrario à chaque fois que l'on générera un condensé à partir du même document on obtiendra le même condensé.

Le condensé permet de vérifier l'intégrité d'un document, puisqu'à un document est associé un condensé, si le document est modifié le condensé généré n'est pas le même.

La cryptographie asymétrique

La cryptographie asymétrique repose sur l'existence de deux clés associées, une clé privée connue du seul propriétaire des clés et une clé publique que le propriétaire porte à la connaissance de tous.

Si l'on crypte avec une clé publique, seul le propriétaire de cette clé pourra décrypter le document grâce à la clé privée associée, l'intérêt étant de garder les informations confidentielles.

Si l'on crypte un document avec sa clé privée, tout le monde ayant accès à la clé publique peut décrypter le document, l'intérêt n'est donc pas la confidentialité mais l'authentification. L'auteur étant le seul à connaître le clé privée, si le document est crypté avec cette clé c'est donc qu'il émane de l'auteur.

Le certificat

C'est un petit fichier qui accompagne la clé, il est émis par une Autorité de Certification (AC). Le but du certificat est d'identifier de manière certaine le propriétaire de la clé. Ce certificat contient toutes les informations nécessaires sur le propriétaire et sur l'AC.

Une fois ces pré requis techniques posés on peut expliquer en quoi consiste une signature électronique.

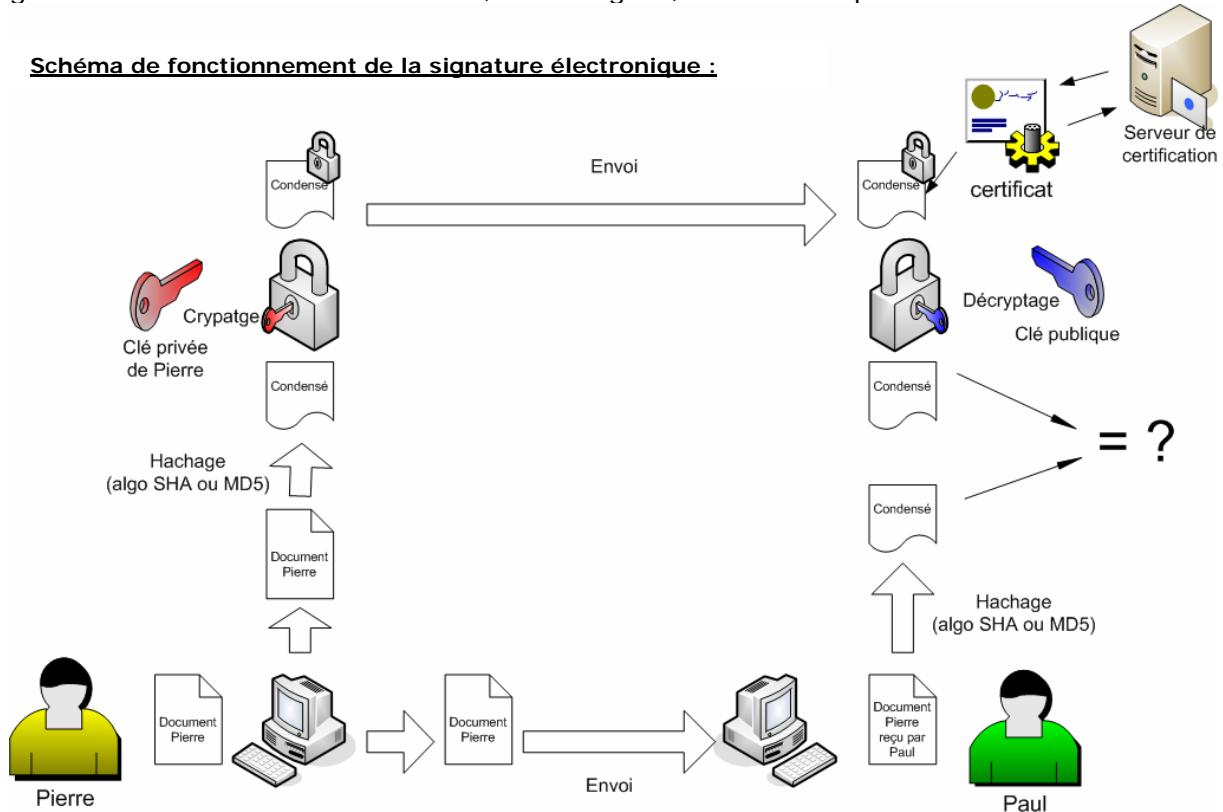
Pour signer un document on génère un condensé que l'on crypte avec la clé privée de l'auteur et on envoie le condensé en même temps que le document.

Pour décrypter le condensé, le destinataire n'a alors qu'à utiliser la clé publique de l'auteur du document, clé publique que l'AC certifie via le certificat. Ce destinataire dispose ainsi d'un condensé dont il connaît l'auteur de manière certaine.

Ensuite, il est nécessaire de générer, selon le même algorithme, le condensé du document qu'on a reçu en clair. Si les deux condensés sont identiques, on est sûr d'une part que le document n'a pas été modifié. D'autre part, si le condensé signé est identique au condensé du document reçu en clair, celui-ci provient forcément de la même personne que celle qui a signé le condensé, l'auteur étant le seul à connaître sa clé privée. Tout le processus repose en effet sur le lien unique et indissociable existant entre un document et son condensé.

Donc en cryptant le condensé d'un document avec sa propre clé privée l'auteur garantit l'authenticité du document, son intégrité, et sa non-répudiation.

Schéma de fonctionnement de la signature électronique :



Une ICP répond-t-elle aux exigences de l'art. 1316-4 ?

Article 1316-4 issu de la Loi du 13 mars 2000 :

« 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 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'Etat. »

La signature a deux fonctions :

- L'identification de la personne qui signe
- La manifestation de la volonté de celui qui signe

La loi établit, dans certains cas, une présomption de fiabilité du procédé, ce qui fait reposer la charge de la preuve sur celui qui contestera ce procédé.

Le Décret du 30 mars 2001 vient préciser les cas où un dispositif de signature électronique va bénéficier de cette présomption. Celle-ci intervient « *lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* ».

Ainsi pour bénéficier de la présomption, la signature doit répondre à trois conditions : elle doit être sécurisée, établie grâce à un dispositif sécurisé de création, utiliser un certificat électronique qualifié

Signature électronique sécurisée

Le décret définit dans l'article 1^{er} la signature électronique sécurisée par les trois exigences auxquelles elle doit satisfaire :

« - être propre au signataire ;

- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ; »

Dispositif sécurisé de création de signature électronique

L'article 3 définit ce que l'on entend par dispositif sécurisé de création de signature électronique. Deux conditions cumulatives :

- Garantir par des moyens techniques et des procédures appropriées que les données de création de signature électronique sont uniques, confidentielles, inviolables, non falsifiables, protégées contre l'action des tiers et enfin n'entraînant aucune altération du contenu de l'acte à signer et ne faisant pas obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

- Etre certifié conforme aux exigences définies précédemment, soit par le Premier ministre, dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002, soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

Certificat électronique qualifié

L'article 6 définit le certificat électronique qualifié

Un certificat électronique ne peut être regardé comme qualifié que s'il comporte certains éléments tels que des mentions spécifiques et que s'il est délivré par un prestataire de services de certification électronique (PSCE) satisfaisant aux exigences réglementaires.

En conséquence, on voit bien que les systèmes ICP sont une réponse tout à fait adéquate par rapport aux exigences légales.

Dans un processus de dématérialisation que faut-il signer ?

En l'état actuel pour déterminer quels sont les documents à signer il faut se référer au décret du 30 avril 2002.

L'article 2 dispose que « la personne publique peut mettre le règlement de la consultation, le cahier des charges, les documents et renseignements complémentaires à la disposition des personnes intéressées sur un réseau informatique [...]. Les personnes intéressées doivent pouvoir consulter et archiver sur leur ordinateur le règlement de la consultation. A cet effet, ils fournissent le nom de l'organisme, le nom de la personne

physique téléchargeant les documents et une adresse permettant de façon certaine une correspondance électronique assortie d'une procédure d'accusé de réception. »

On peut donc en déduire que le téléchargement des DCE n'induit pas la mise en œuvre de la signature électronique du candidat.

Ensuite l'article 3 relatif à la transmission des candidatures ne fait référence qu'aux « conditions qui permettent d'authentifier la signature du candidat selon les exigences posées aux articles 1316 à 1316-4 du code civil. » Les candidats n'ont besoin de recourir qu'à un dispositif de signature électronique « simple » (par opposition à « sécurisée »).

Il n'est fait référence au recours à un dispositif de signature électronique sécurisée que dans le cas où la PRM dans l'AAPC a autorisé les candidats à transmettre leur dossier « sous la forme d'un double envoi » : « En premier lieu, ils transmettent leur *signature électronique sécurisée*. La réception de cette signature vaut date certaine de réception de l'offre. En second lieu, ils transmettent l'offre elle-même. »

Evidemment le décret de 2002 ne répond qu'à quelques situations particulières, il faut attendre les futurs décrets d'application du code de 2004.

Mais cela n'empêche pas de raisonner avec bon sens en essayant de déterminer les cas où il faut signer. Par exemple l'entreprise devra signer dans les mêmes conditions que celles de la signature de son enveloppe (1316 et 1316-4) les documents qu'elle envoie à la PRM suite à une demande de complément d'information à l'ouverture des candidatures.

En revanche pour certains documents (les DCE par exemple) il n'y a pas de contraintes juridique relative à la signature, néanmoins on pourra recourir à des procédés de signature, ou d'authentification de l'auteur dans un souci d'identification et de sécurité.

Alexandre VELIKOV et Renaud PASCAL
DESS Droit et Système d'information
Service juridique FORMI SA