Signature électronique : l'entreprise est libre d'utiliser le certificat de son choix

A propos de l'auteur

Mlle Emmanuelle Maupin

Voir les articles de cet auteur

La signature électronique est un procédé indispensable aux marchés publics dématérialisés. Afin de faciliter son usage, un arrêté, accompagné de deux documents explicatifs, a été publié début juillet. Les impacts sont importants pour les opérateurs économiques. En effet, ils sont désormais libres d'utiliser le certificat de leur choix à la condition qu'ils soient conformes au RGS ou garantissant un niveau de sécurité équivalent. Explications…

Dans moins de deux semaines, l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics entrera en vigueur. Pour préparer le terrain, la direction des affaires juridiques (DAJ) du MINEFE a publié deux fiches : un mode d'emploi de l'arrêté et un mémo destiné à anticiper l'échéance. Dans son édito de lettre de l'observatoire économique de l'achat public (OEAP), Catherine Bergeal, la DAJ, a affiché clairement les ambitions du texte : « *faciliter et sécuriser, tant techniquement que juridiquement, l'usage d'un procédé identifié comme l'un des principaux freins au développement de la dématérialisation, mais pourtant indispensable aux marchés publics dématérialisés : la signature électronique* ».

Tout est fait pour faciliter la vie des entreprises

La directrice avoue tout de même que « *ce texte ne révolutionne pas la pratique de la signature électronique. Il permet, en revanche d'en banaliser l'usage* ». Pour autant, le texte ne fait pas l'unanimité. Maître François Jouanneau, avocat, directeur du département commande publique du Cabinet Alain Bensoussan, estime qu'à la lecture des documents, tout est fait pour faciliter la vie des entreprises mais qu'en est-il des acheteurs publics ? « *Nous sommes assez déçus. Outre que d'être relativement succinct, l'arrêté n'aide pas à rassurer les acheteurs publics. En effet, il fait peser plus de responsabilités sur leurs épaules* », juge l'avocat. Mais à quoi les acheteurs et les opérateurs économiques doivent-ils s'attendre ?

Le RGS, kesako ?

Dans la fiche mode d'emploi, la DAJ indique tout d'abord que les profils d'acheteurs doivent se mettre en conformité par rapport au référenciel général de sécurité (RGS) et ce au plus tard au 19 mai 2013. Attention toutefois, comme le précise le document « cette obligation n'est pas propre aux marchés publics, puisqu'elle s'applique à tous les systèmes d'information entrant dans le champ de l'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives. Mais le RGS, kesako ? « *Ce document définit un certain nombre de règles de sécurité à mettre en œuvre par rapport à des cibles à atteindre. Il prévoit des critères de sécurité, des recommandations technologiques et des politiques de certification*, explique un expert en sécurité informatique. *Le RGS prévoit différents niveaux de sécurité : *, ** ou *** ainsi que les critères nécessaire pour atteindre le niveau de sécurité requis. Dès lors que le profil d'acheteur annonce un niveau de sécurité, l'ensemble de sa solution doit être au minimum au niveau annoncé. Par exemple, chaque composant d'une plateforme de dématérialisation (la signature, le chiffrement, l'horodatage) peuvent être qualifiés à un niveau de sécurité différent. Le niveau global de la plateforme correspondra au plus petit niveau de qualification. S'il est requis un niveau **, la plateforme devra accepter les produits de niveau ** et *** mais pas * »*, observe-t-il.

Des certificats de signatures conformes au RGS

Afin de banaliser l'usage de la signature électronique, plusieurs mesures ont été prises. Jusqu'à présent, les entreprises devaient acquérir des certificats PRIS V1, c'est-à-dire auprès d'une quinzaine d'autorités référencées par l'Etat. Désormais, tous les certificats, nationaux ou européens, à la condition qu'ils soient conformes au RGS ou garantissant un niveau de sécurité équivalent, pourront être utilisés. L'opérateur économique est libre d'utiliser le certificat de son choix, à condition toutefois qu'il soit conforme au niveau minimum de sécurité préconisé par le profil d'acheteur. « *L'ouverture vers d'autres autorités de certification peut avoir un effet positif d'un point de vue économique. Plus de concurrents, on peut donc espérer une réduction des coûts des certificats. Cela peut également réconcilier différent besoin de signature électronique chez le même fournisseur, c'est-à-dire une possible mutualisation des certificats au sein de la société* », explique l'expert en sécurité. Toutefois, il avoue que cette multiplication peut avoir un effet pervers. « *L'entreprise peut se trouver perdue.*

Il faut privilégier les autorités certifiées et en cas de doute demander la preuve de la compatibilité au RGS et à quel niveau

Elle devra se renseigner pour savoir qui peut lui fournir un certificat. Il lui sera en outre nécessaire de s'assurer qu'elle a pris un certificat compatible RGS», précise-t-il. L'expert recommande toutefois aux opérateurs économiques de se tourner vers des autorités de certification qui auront fait un effort d'homologation au RGS ce qui permettra de faciliter le traitement de la signature et de réduire les risques de refus. « *Il faut privilégier les autorités certifiées (voir les listes de confiances nationales et européennes) et en cas de doute demander la preuve de la compatibilité au RGS et à quel niveau* », conseille-t-il. Le

signataire pourra désormais utiliser l'outil de signature de son choix, sans être contraint par celui de la plateforme. Cependant, il devra transmettre les éléments permettant la vérification de la signature et l'intégrité du document. Peut-on par exemple utiliser l'outil de signature d'Adobe, comme cela se fait parfois ? « *Adobe n'est pas une autorité de certification, mais propose un outil de parapheur électronique, sous la forme d'un service intégré à ses lecteurs de fichiers PDF. En soi, ce service déroge aux préconisations du RGS, qui stipulent que le ou les fichiers signés doivent rester inchangés au terme de l'opération de signature. De plus, les autorités de certification validées par les outils Adobe s'appuient sur des listes qui dépassent le cadre fixé par le RGS. Une signature valide au sens Adobe n'est pas nécessairement acceptable dans le cadre des marchés publics français. Il faut cependant reconnaître que l'outil proposé par Adobe est particulièrement attractif pour les utilisateurs, de par sa simplicité d'utilisation et sa capacité à valider une signature sans avoir à appréhender de nouveaux outils* », remarque l'expert. Concernant le format de signature, l'article 3 de l'arrêté impose au pouvoir adjudicateur d'accepter les formats de signature XAdES, PAdES et CAdES. Mais rien ne l'empêche d'en accepter d'autres, à condition que cette possibilité soit mentionnée dans les documents de la consultation et que le profil acheteur soit à même de gérer ces formats.

Validité du certificat de signature, quels éléments fournir ?

Dans la fiche mode d'emploi, la DAJ indique que s'agissant de la vérification de la conformité du certificat de signature au RGS, trois cas sont à distinguer. Le premier ne pose pas de problème, le certificat émane de la liste de confiance française ou d'un autre état membre. Dans le second, la conformité est présumée, les seules vérifications à opérer sont celles du niveau de sécurité et de la validité de la signature. L'entreprise fournit seulement les éléments qui permettent la vérification de la validité de la signature. Enfin, l'Autorité de Certification n'est pas référencée. Afin de procéder à la vérification, l'entreprise fournit éléments nécessaires à la qualification du niveau de sécurité de son Autorité de Certification, en plus des éléments nécessaires à la vérification de la validité de la signature elle-même. Il peut s'agir de « l'adresse du site internet de référencement dans le pays tiers, une preuve de la qualification du prestataire ou du produit, l'adresse de l'autorité de certification qui a délivré le certificat de signature, qui mentionne la politique de certification... ». Qui opère les vérifications ? L'acheteur ou le profil d'acheteur ? Pour le MINEFE, « la vérification des certificats de signature électronique et de la validité de la signature elle-même font partie actuellement des fonctionnalités d'un profil d'acheteur, sans que l'acheteur ait dû se doter des compétences techniques pour les examiner ». En revanche, « la vérification de l'identité du signataire, et de sa capacité à engager l'entreprise, reste, comme pour les marchés non dématérialisés, effectuée par l'acheteur ».