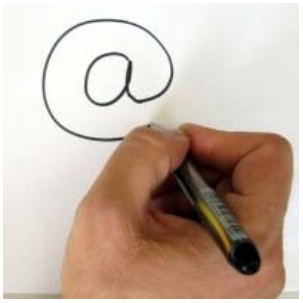
Signature électronique : plus de vérifications à l'horizon

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. Semant la panique chez les acheteurs, le nouveau texte met à leur charge plusieurs opérations de vérification quant à la conformité du certificat de signature utilisé par le candidat. Décryptage…



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* ».

l'arrêté ne révolutionne pas la pratique de la signature électronique

La directrice avoue tout de même que l'arrêté « *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.

Accompagner les acheteurs

« *Les acheteurs ne sont pas oubliés, puisque le texte permet d'accompagner en douceur la mise en conformité des plateformes avec le référentiel général de sécurité. […] Les échanges électroniques sont ainsi facilités avec, d'une part, la transmission, par le signataire, du mode d'emploi permettant la vérification de la signature, et d'autre part un encouragement à l'automatisation de ces vérifications* », écrit Catherine Bergeal dans son édito. 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… ».

Une responsabilité qui pèse au final sur l'acheteur

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 ». Pour l'avocat parisien, même si les vérifications sont à la charge de la plateforme, c'est in fine la responsabilité de l'acheteur qui est engagée. « *Si j'étais acheteur, je ne serais par serein. On leur demande plus que par la voie papier. Ils doivent vérifier que le certificat de signature est conforme, que le niveau de sécurité est adapté et enfin s'assurer que le signataire est habilité*, considère Maître Jouanneau. *Les deux premiers éléments sont certes à la charge du profil d'acheteur, mais au final c'est la responsabilité de l'acheteur public qui est engagée.*

L'arrêté ne rassure pas les acheteurs

On fait porter sur la personne publique des vérifications qui sont lourdes.Ces vérifications supplémentaires sont potentiellement sources de risque tant sur le plan juridique que contentieux. Par exemple un acheteur rejette une candidature alors qu'elle pouvait être considérée comme valable ou au contraire il admet un candidat dont la signature est en fin de compte erronée. L'arrêté ne rassure pas les acheteurs. Il ne vient rien simplifier. Selon moi, il ajoute des obligations dont l'acheteur n'a pas à s'occuper, insiste François Jouanneau. *On ne peut que recommander aux acheteurs publics la plus grande vigilance en cas de rejet d'une candidature pour défaut de conformité du certificat de signature électronique. En effet, la fiche mode d'emploi précise bien que l'examen automatique de la signature électronique n'exonère par l'acheteur de sa responsabilité dans le cas où la candidature ou l'offre serait rejetée à tort pour des raisons techniques. En définitive, en cas d'erreur ou de dysfonctionnement, le dispositif est conçu pour retenir la responsabilité résiduelle de l'acheteur, ce qui justifie la plus grande vigilance de la part de ces derniers* », ajoute-t-il. L'expert en sécurité reconnaît que c'est un peu la panique chez les acheteurs. « *Ce n'est pas clair pour eux. Ils doivent s'assurer que les outils sont compatibles avec les normes RGS*, précise-t-il. *Pour les profils d'acheteurs c'est aussi compliqué car ils doivent reconnaître les certificats d'une liste qui n'est pas fermée et qui peut être amenée à évoluer. Ils vont devoir régulièrement vérifier que les nouvelles autorités de certifications répondent aux exigences du RGS et qu'elles sont conformes au niveau de sécurité attendu* », observe l'expert. Au final, pour ne pas se retrouver le bec dans l'eau, l'avocat conseille aux acheteurs de se rapprocher de leur gestionnaire de plateforme afin de vérifier qu'ils prennent bien en compte ce type de vérification ou en amont sur les certificats délivrés.