(Marchés publics) Doctrine

Le juge administratif français et le principe européen de non discrimination des signatures électroniques et manuscrites.

n° Lexbase :N6016BSM

par Colette de Marguerye, avocat au barreau de Paris et médiateur,
société d'avocat Marguerye

A propos de l'Ordonnance du Tribunal Administratif de TOULOUSE du 9 mars 2011, n° 1 100 792 *(N° Lexbase : A7114HP8).*

Dans une Ordonnance rendue l 9 mars 2011, le tribunal administratif de Toulouse a dit pour droit que la signature de fichiers « *zip* », qui permettent l'archivage et la compression des données, ne peut être assimilée aux documents en nombre variable que ces fichiers peuvent contenir. Cette signature ne peut donc pallier l'absence de signature électronique des documents figurant dans ces fichiers. Le fait que les documents aient été signés sur le support papier, et scannés avant leur transmission électronique, est sans incidence sur le bien fondé de la constatation par le pouvoir adjudicateur de leur absence de signature sous forme électronique.
Parmi les points techniques et juridiques pôsés par l'affaire, la présente étude s'attache plus particulièrement à l' « *irrégularité* » retenue par le juge tenant aux règles de la signature, notamment du dossier de candidature par voie électronique, en l'occurence par fichiers « *zip* » lors de la passation d'un contrat par voie électronique.

I - Les faits de l'espèce

Le CNRS, Etablissement Public Administratif à caractère Scientifique et Technologique lance le 20 octobre 2010 une procédure d'Appel d'Offres Ouvert pour « *assistance à gestion de projets* ». Une société de conseils en « Organisation et en Systèmes d'Information » spécialisée en pilotages de projets répond dans les délais par voie électronique, soit avant le 2 décembre 2010.

- Par courrier du 9 décembre, le CNRS, après ouverture des plis, rejette l'offre comme ***« irrégulière »*** pour « *défaut de signature de chacune des pièces de la candidature et de l'offre pour lesquelles cela était requis »*, se fondant sur l'article 4-2-3 du Règlement de consultation[1] ainsi que sur l'article 1316-4 du Code Civil[2].(N° Lexbase : L0630ANN)

- Le 14 décembre, le candidat conteste la décision du CNRS, « *les documents papiers ont été signées et scannés et les enveloppes zippées pour optimiser les volumes d'envoi, ont été signés par clé numérique ».*

1

2

-Le 22 décembre, le CNRS maintient sa position. Il s'appuie sur l'article 56-II du Code des Marchés Publics autorisant le pouvoir adjudicateur à imposer la **transmission** des documents du candidat par voie électronique, et rendant celle-ci obligatoire pour les achats de services informatiques d'un montant supérieur à 90.000 Euros HT. Le CNRS, citant un « *chat* » de la Direction des Affaires Juridiques du minitère de l'Economie, compare : « *signer le fichier .zip est comme sceller une enveloppe papier* : *cela peut être utile pour en garantir l'intégrité, mais le cachet sur l'enveloppe ne remplace pas la signature des documents qu'elle contient ... scanner des signatures manuscrites ne donne pas valeur d'original au document scanné.* »

-Le CNRS s'appuie aussi sur l'Arrêté du 28 Août 2006,(N° Lexbase : L6698HKB) arrêté d'application de l'article 48-1 du Code des Marchés Publics (N° Lexbase : L2698ICW) disposant que, lors des procédures de passation dématérialisée des marchés publics, les candidatures et actes d'engagement sont signés par signature électronique qui garantit **notamment** l'identification du candidat.

II--<u>La décision du Tribunal Administratif-</u>

Par Ordonnance du 9 mars 2011, le Tribunal Administratif de TOULOUSE, après avoir rappelé les pouvoirs du Juge des référés, s'appuie sur un raisonnement rigoureux pour rejeter la requête de la société.

<u>1) -</u>
Après avoir rappelé ses pouvoirs lorsqu'il est saisi durant la période pré-contractuelle de passation de contrats de marchés publics, le juge toulousain, visant l'article L 551-4 du Code de Justice Administrative (N° Lexbase : L 1601IEZ) relatif aux obligations du pouvoir adjudicateur de surseoir à la signature finale du contrat jusqu'à ce que le juge ait statué, en déduit que la demande de la société est irrecevable. Ainsi, la question de la garantie de l'égalité de traitement des entreprises répondant à Appel d'Offres selon une procédure de passation de contrat dématérialisée ne reçoit pas de réponse dans cette espèce.

Cette question mérite, cependant, d'être examinée par les magistrats de l'ordre administratif,
-qu'il s'agisse des moments des échanges signés et transmis qui précédent l'accord final éventuel, ou de l'examen des différents fonctions de la signature, et des objectifs de développement des échanges fixés par la Directive (CE) 1999/93 du 13 Décembre 1999, sur un cadre communautaire pour les signatures électroniques ' N° Lexbase : L0093AWD).

Enfin, l'on peut penser que les magistrats auront à se prononcer sur leur devoir d'appréciation et d'évaluation des irrégularités lors de la **passation des contrats** de marchés publics par signature électronique sécurisée, à l'instar des magistrats de l'ordre judiciaire qui examineront les conditions de passation des contrats commerciaux de même nature dans le secteur privé.

Malheureusement, le lecteur reste sur sa faim : certes, le juge rappelle les articles L 551-1 (N° Lexbase : L1591IEN) à L 551-4 du Code de Justice Administrative aux termes desquels *« il incombe au juge des référés précontractuels de rechercher si, eu égard à leur portée et au stade de la procédure auxquels ils se rapportent, les manquements allégués aux obligations de publicité et de mise en concurrence sont susceptibles de léser la société requérante ou risquent, fût-ce de manière indirecte, de la léser en favorisant une autre entreprise* ».

Toutefois, ce rôle, comme le rappelle la jurisprudence, a une finalité et une fonction:

-le juge a un **devoir d'appréciation** du manquement par le pouvoir adjudicateur à ses obligations de mise en concurrence « *eu égard à la portée desdites obligations et au stade de la procédure auquel il se rapporte* », étant précisé qu'il s'agit d'un *« **contrôle de pleine juridiction*** », le juge n'ayant pas à *« rechercher si les irrégularités ont, en fait, porté préjudice à la société demanderesse* ».

-le **juge évalue aussi l'irrégularité** conformément à sa mission de contrôle de pleine juridiction, notamment en matière de signature, comme dans cette affaire où «*le défaut de signature antérieure à la soumission au marché constitue **une irrégularité substantielle** dès lors qu'il n'a pas été remédié avant la date limite du dépôt des offres par le gérant ou par un mandataire dûment habilité*[3]*»*

Il y a fort à parier que le juge administratif, statuant sur les conditions de passation de procédure dématérialisée, se devra d'apprécier les manquements et d'évaluer le caractère des irrégularités substantielles ou « bénignes».

Apparemment, le juge a entendu, malgré son pouvoir de contrôle de pleine juridiction, examiner les circonstances du rejet de l'offre invoquées comme motif par le CNRS, en ayant davantage pour objectif d'apprécier la sécurité des échanges dématérialisés, qu'en se fixant sur la question de savoir si l'irrégularité était substantielle plus particulièrement au stade de la procédure où il entendait la relever.

2)
-Le juge a donc examiné l'irrégularité due aux circonstances de la procédure dématérialisée relevant :
-une absence de signature électronique de chacune des pièces de la candidature
-une absence de signature électronique de l'offre

Le raisonnement du juge est d'une logique implacable :
a) depuis le 1 janvier 2010, les documents du candidat répondant à un Appel d'Offres d'un montant supérieur à 90.000 € HT sont transmis par voie électronique

b) Les candidatures et actes d'engagement transmis par voie électronique sont revêtus d'une signature sécurisée par certificat électronique

3

c) La transmission électronique implique la signature électronique de la candidature et de l'acte d'engagement

d) Ce dernier point est repris par le « *Règlement de la Consultation de l'Appel d'Offres* », ce qui n'est pas contraire à l'article 1316-4 du Code Civil, et n'interdit donc pas au CNRS d'exiger une signature de document sous forme électronique

e)la signature des fichiers de transmission **.zip** ne peut pallier l'absence de signature électronique de chaque document

f)enfin, la signature manuscrite de l'acte d'engagement sur support papier puis scannée avant transmission électronique ne saurait suffire pour répondre aux exigences de signature électronique requises

C'est ainsi que le juge, par un raccourci logique mais, à notre sens critiquable, et après appréciation essentiellement technique, conclut que le rejet de l'offre du candidat pour « *irrégularité* » par le pouvoir adjudicateur n'est pas contraire aux obligations de ce dernier en matière de publicité et mise en concurrence. On peut penser que cette décision qui ne qualifie l'irrégularité est considérée comme substantielle.

III- L'apport du droit commun de la signature électronique au développement économique

Il s'agit d' aboutir à une transmission répondant aux exigences du lien :

SE/ICS/DNA/MUDD

(Signature Electronique/ Identification et Contrôle de celle-ci par le Signataire/ Données Non Altérables/ Modification Ultérieure des Données Détectable)

1) La Directive européenne du 13 décembre 1999, afin de sécuriser les échanges sur Internet, s'est fixé pour tâche de :

-faciliter les signatures électroniques en contribuant à leur reconnaissance juridique,

-instituer des services de certification,

-définir les critères de la signature électronique,

-instituer un principe de non discrimination entre la signature électronique et manuscrite (article 5)

L'article 2 de la Directive, distinguant la « *signature électronique* » de la « *signature électronique avancée* », fait ressortir la notion de lien, notion consubstantielle au monde électronique et à ses exigence.

La **signature doit donc :**

-être liée uniquement au signataire,

-**permettre de l'identifier,**

-être sous son contrôle exclusif,

-être liée aux données auxquelles elle se rapporte de sorte que toute modification ultérieure des données soit détectable.

Ce moyen technique de signature est fondé sur des systèmes de cryptage : une signature électronique se signe au moyen d'une clé de chiffrement, dite « privée » sous contrôle de celui qui l'utilise. La « clé publique », copie restreinte de la clé privée, qui fonctionne par paire avec la clé privée, permet de déchiffrer le message de l'expéditeur, de garantir l'authentification de l'expéditeur ainsi que la non altération du message.
Le champ d'application de la Directive est très large. Il est prévu que les prestataires de services de certification (PSC) décrits dans la Directive pourront fournir aussi d'autres services : horodatage, archivage, services de publications, de consultations.. ;

Grâce à l'Europe, le législateur français qui hésitait à libéraliser l'usage de la communication électronique pour les échanges sécurisés, sensible aux applications de cryptologie, relevait le 17 mars 1999, la taille des clés de cryptage **de 40 bits à 128 bits afin de garantir la confidentialité des messages.**

2) La loi de transposition française du 13 mars 2000 relative à l'adaptation de la preuve aux Technologies de l'Information et à la signature électronique(loi n° 2000-230 N° Lexbase : L0274AIY) fût votée à l'unanimité au Sénat le 8 février 2000 et adoptée sans modification à l'Assemblée nationale le 29 février 2000.
Codifiée au sein du Code Civil, Il s'agit d'un texte fondateur destiné à assurer un cadre sécure aux transactions.

Après avoir redéfini la preuve littérale (article 1316 Code Civil), le législateur admet la force probante de l'écrit électronique et lui confère une force probante de *« même force »* que l'écrit sur support papier (articles 1316-1 et 1316-3).

Deux conditions sont exigées par le législateur pour atteindre la même force probante :
-une possibilité d'identification de celui dont émane l'acte écrit
-une conservation dans des conditions pouvant en garantir l'intégrité.
L'on peut rappeler que les 3 fonctions de la signature, à savoir l'identification, l'adhésion du signataire au contenu, et la garantie de l'intégrité du document signé doivent être respectées dans le monde numérique :

a) l'identification certaine par signature numérique repose sur un système de clés asymétrique. S'il s'agit d'une signature électronique, elle a aussi pour finalité de régir des relations sur des réseaux ouverts par l'intermédiaire desquels les parties nouent des relations contractuelles.

b) la signature électronique exprime le consentement du signataire et établit le lien entre celui-ci et le contenu du document.

c) quant au maintien de l'intégrité d'un document signé de manière manuscrite, il est assuré par l'absence de rature ou de correction sur le document signé. Le maintien de l'intégrité est assuré par la fonction dite de *« hachage irréversible »*. Cette fonction va appliquer au document une opération mathématique de manière à produire un condensé numérique du message. « **Ce résumé est codé à l'aide de la clé privée : le résultat est alors numérique. »** Cette signature est envoyée en accompagnement du fichier principal au destinataire. A la réception, la signature sera lue à l'aide de la « **clé publique »** qui lui correspond. En appliquant l'opération mathématique inverse, la fonction de hachage reconstitue le fichier condensé, qui pourra être comparé au fichier principal. Dès lors, toutes atteintes à son intégrité seront décelables.

Le mécanisme de transmission par .zip a pour fonction : l'assemblage de documents en vue d'une transmission combinant en un seul objet binaire les documents assemblés et la sécurité lors de la transmission de l'intégrité de leurs contenus ; la compression par paquets des documents à transmettre, le document principal renvoyant aux documents compactés et liés à celui ci, créant ainsi une application de compression « .zip » (il restera à lier l'expéditeur du paquet de documents compactés par une signature électronique spécifique ajoutée aux documents signés et aux pièces jointes éventuelles);l'identification de l'expéditeur de nature à permettre au destinataire de détecter les altérations éventuelles non autorisées en cours de transmission.

IV - L'enjeu économique de la position du pouvoir adjudicateur en l'espèce :

L'argument du CNRS pour rejeter l'offre après ouverture des plis est relatif à la signature du fichier de transmission **.zip** : le fichier **.zip** contenant les documents, dont l'acte d'engagement, est « *attaché à l'enveloppe et non au contenu* ». Le CNRS semble retenir un parallélisme des formes puisqu'il indique dans son argumentation que « *dans une procédure dématérialisée, vous devez signer électroniquement tous les documents qui doivent recueillir une signature manuscrite dans une procédure papier. La signature électronique doit être apposée directement sur chaque fichier constituant un document à signer* ».

Il pose une exigence technique ajoutant à celles du législateur. Selon cette exigence supplémentaire à celle de la loi, chaque document doit être signé selon la voie électronique. Ceci a des conséquences juridiques essentielles.

Le CNRS met ainsi en question la valeur de la signature manuscrite de l'acte d'engagement inclus dans l'enveloppe présentée par voie dématérialisée.
Pourtant, l'acte d'engagement a été signé et scanné. Cette signature est, selon la loi, valable en soi.
Certes, l'acte d'engagement ne comporte pas de certificat électronique dédié, mais, selon la loi, il est valablement signé.

En droit pur, reste donc à examiner les conditions dans lesquelles l'acte d'engagement, document essentiel du dossier de candidature, sera transmis. Il importe, en effet, que l'acte d'engagement reste un document intègre et ne subisse pas d'altération lors de la transmission, ceci afin que la validité de sa signature puisse être contrôlée.

Les exigences du CNRS ont, a priori, pour effet de rompre l'égalité de principe des candidats mis en concurrence, égalité voulue par le législateur, gardien des règles visant à éviter des dommages à l'économie et d'ignorer le principe de non discrimination des signatures manuscrites et électroniques voulu par le législateur européen.

Ainsi, le contrôle du juge s'impose pour plusieurs motifs : soit le pouvoir adjudicateur est privé d'une candidature, soit le candidat est privé d'une chance d'emporter le marché, soit le marché est faussé, ou encore un dommage à l'économie peut en résulter. **La société concernée, qui avait un « *intérêt manifeste* », comme le relève le juge, à conclure le marché, engageait un Référé pré-contractuel, invoquant les règles de publicité et de mise en concurrence que doivent respecter les acheteurs publics.**

D'autres développements sont nécessaires, notamment au regard du droit des contrats passés sous forme électroniques, qu'il s'agisse du secteur public ou du secteur privé,. Comme l'écrit Roland RICHER « *par leur objet, les marchés publics sont semblables aux contrats que concluent entre eux les particuliers. Il s'agit en effet de contrats par lesquels l'administration se procure des fournitures ou des services et fait réaliser des travaux moyennant un prix. Ces contrats sont identiques aux contrats de vente, de location de service du droit privé ».* Doivent aussi êtr pris en compte la volonté affirmée par le législateur européen de susciter la confiance des opérateurs économiques et des pouvoirs adjudicateurs dans le développement exponentiel de l'économie numérique(Directive européenne du 13 décembre 1999 précitée) et la mission du juge des référés pré-contractuel à travers l Ordonnance n° 2009-515 du 7 mai 2009 relative aux procédures de recours applicables aux contrats de la commande publique. - N° Lexbase : L1548IE3)

V- La question de la transmission des documents et de la candidature : la sécurité du lien signature documents transmis lors de la transmission

L'absence de signature électronique de chaque pièce et de l'offre parvenue avant l'ouverture des plis dans le cadre de la procédure dématérialisée nuit-elle à la sécurité de la signature, est-elle contraire au droit qui affirme l'égalité de force probante des signatures manuscrite et juridique ? Si oui, cette irrégularité était-elle de nature à exempter le pouvoir adjudicateur de ses obligations de mise ne concurrence à l'égard de la société candidate ou le pouvoir adjudicateur devait-il demander au candidat de remédier à l'irrégularité supposée ?

Bien que le Tribunal dans sa décision fasse référence au Code Civil, il se fonde principalement sur les textes du Code des Marchés Publics tant sur l'exigence de signature que sur les conditions de transmission des offres. L'article 11 du Code des Marchés Publics (N° Lexbase : L 7083IGG) affirme que **l'acte d'engagement**, pièce constitutive du dossier, **doit être signé par le candidat puis par le pouvoir adjudicateur.** Quant aux modalités de la transmission des offres par voie électronique, l'article 11 prévoit qu'il sera précisé par un Arrêté du ministre de l'Economie.
L'article 48 du Code des Marchés Publics (N° Lexbase : L2698ICW) précise que «*les offres sont transmises en une seule fois*». L'article 56 du même code (N° Lexbase : L2773ICP) réaffirme pour le pouvoir adjudicateur, dans les cas où la transmission électronique des offres est obligatoire, une obligation d'assurer la confidentialité et la sécurité des transactions sur un réseau informatique accessible de façon non discriminatoire, selon des modalités fixées par arrêté du ministre chargé de l'économie.
Quant aux dispositions des articles 5 à 7 de l'Arrêté du 28 Août 2006 pris en application du point I de l'article 48 CMP et de l'article 56 CMP[4], **elles ne traitent pas du mode de transmission par voie électronique** des candidatures et actes d'engagement, signés au moyen d'un certificat de signature électronique conforme au Référentiel Intersectoriel de Sécurité, **mais de la signature.**

S'agissant des « *Appels d'Offres ouverts»*, les articles 57 (N° Lexbase : L7061IEA) à 59 du Code des marchés Publics reprennent les garanties de confidentialité et de sécurité. Par ailleurs, il est indiqué que l'ouverture des plis n'est pas publique mais qu'avant de procéder à l'examen des candidatures, le pouvoir adjudicateur peut demander aux candidats de compléter leur dossier de l'enveloppe de candidature. L'article 56-4 CMP, s'il traite des garanties que le pouvoir adjudicateur doit aux candidats, ne traite pas du mode de transmission électronique des offres.

Autrement dit, si la fonction de la signature est prévue par les textes du Code des Marchés Publics, les conditions de la transmission garantissant le lien entre la signature et la sécurité de sa transmission ne sont pas traitées par les textes.

Dans un louable mais inutile souci de sécurité, le « ***Règlement de Consultation*** » du CNRS exige une signature électronique de chaque document transmis. Ce souci résulte d'une comparaison entre la sécurité de transmission d'une enveloppe contenant des documents papier et d'une enveloppe .zip. qui mérite d'être reprise :

a) dans le cas où l'on transmet une LRAR/papier contenant des documents non signés, falsifiés ou sans documents, il ne sera pas possible au destinataire de prouver que les documents supposés envoyés précisément dans cette enveloppe ne correspondent pas aux documents censés s'y trouver. Il restera avec son accusé de réception, certes, mais **le lien entre la réception et le contenu de l'envoi n'est pas sécurisé et n'est pas prouvable.**

b) si l'on transmet une enveloppe **.zip** ne contenant pas de documents ou contenant des documents différents ou non signés, la situation sera différente. La transmission .zip fonctionne paire par paire, ce qui garantit l'intégrité des données : compression et

4

décompression ne sont possibles que si les deux clés de compression et de décompression fonctionnent ensemble et sont compatibles. En l'espèce, la signature manuscrite est incorporée au document puisque le document et la signature sont « liés logiquement ». Le fichier .zip serait donc rejeté par la clé de compression au cas où les documents y inclus seraient falsifiés ou non signés.

L'on ne saurait donc exciper du caractère distinct du fichier zip et des documents qu'il contient pour en déduire que la signature peut n'être pas identifiable. Ainsi, au cas où la signature manuscrite sous l'acte d'engagement transmise par le .zip émanerait d'un tiers non autorisé à signer, ceci serait inévitablement prouvable.

Le transfert de ZIP garantit l'intégrité des données transmises. Compression et décompression ne sont possibles que si les deux clés fonctionnent ensemble et sont compatibles. Le fichier ZIP aurait été rejeté par la clé de compression au cas où la signature manuscrite incorporée au document joint n'aurait pas rempli les fonctions que le droit assigne à la signature électronique transmise dans les conditions du fonctionnement par paire. En effet, le document et la signature sont liés logiquement.

Comme le note le tribunal, ajouter à l'article 1316-4 du code civil n'est certes pas interdit.

Toutefois, ajouter aux conditions établies par le droit européen, codifiées dans le droit commun semble inutile quand bien même ce souci de sécurité 100% est de nature à rassurer le pouvoir adjudicateur et à influencer le juge de façon fort compréhensible. Oublier les circonstances dans lesquels la réforme de 2000 a été mise en application semble constituer une barrière dangereuse à un développent économique non seulement souhaité et voulu part le législateur européen. Ce dernier a clairement exprimé sa volonté d'établir la confiance dans l'établissement de contrats dans le monde numérique qu'il s'agisse du secteur public ou du secteur privé.

Ajouter au droit positif, ne serait-pas aller à l'encontre de l'objectif du législateur ?
Il serait dommage que les juges à l'avenir se penchent davantage sur les questions de sécurité, et recherchent un « 100% sécurité » lorsqu'ils examinent les conditions de passation des contrats dans le monde numérique.

Colette de Marguerye
Avocat à la Cour
médiateur
http://www.e-legal.fr

****

(1) L' article 4-2-3 du règlement de consultation « la signature électronique des candidatures et des offres se fera via l'utilisation de certificats électroniques valides… Les catégories de certificats de signature reconnues par la plateforme sont celles qui sont reconnues par le référentiel intersectoriel de sécurité et par la liste publiée à l'adresse suivante : http://.entretreprises.minefi.gouv.fr/certificats/.

L'attention des candidats est attirée sur le fait que des certificats de signature devront être utilisés à deux étapes de la procédure de dépôt :

- 1) Lors de la signature des documents : ... Ce certificat devra être utilisé pour signer numériquement chacun des documents pour lesquels cela est requis... Cette signature est l'équivalent dématérialisé de la signature manuscrite …sur des documents papier.

- 2) Lors du dépôt du dossier de candidature : le certificat, utilisé pour chiffrer le dossier sur la plateforme, devra seulement répondre aux impératifs des deux premiers alinéas du présent paragraphe… Ce chiffrement est l'équivalent dématérialisé du scellement d'une enveloppe contenant une offre physique.

Pour pouvoir faire une réponse électronique, l'opérateur doit s'assurer de répondre aux pré-requis techniques de la plateforme.

-3) La notification de l'accord-cadre se fera par voie papier. Pour ce faire, l'acte d'engagement sera rematérialisé par le CNRS et sera transmis à l'attributaire pour signature.

(2) L'article 1316-4 du Code Civil énonce que « ***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….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. »***

(3)L' Article 5 de l'Arrêté du 28 Août 2006 pris en application du point I de l'article 48 et de l'article 56 du CMP et relatif à la dématérialisation des procédures de passation des marchés publics formalisés. « les candidatures et les actes d'engagement, transmis par voie électronique ou envoyés sur support physique électronique sont signés par l'opérateur économique au moyen d'un certificat de signature électronique qui garantit notamment l'identification du candidat »….

(4) CE 3 Octobre 2008, n° 305420, publié au Recueil LEBON (N° Lexbase : A5971EAE) ; CE 2° et 7° s-s-r 20 Mai 2009, n° 318871, indédit au Recueil LEBON (N° Lexbase : A1829EH9) ; CE 28 avril 2006, n° 286 443, mentionné aux tables du Recueil LEBON (N° Lexbase : A2025DPP) -CE è°et 5° s-s-r 16 octobre 2000, n° 213953, mentionné aux tablbes du recueil LEBON (N° Lexbase : A1398B8B) ; CE 10 décembre 1993, n° 124 529, inédit au recueil LEBON (N° Lexbase : A1536AN9).

Textes de droit commun	Textes d'application , doctrine administrative
- Directive du 13/12/1999 article 1 : Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur. Article 3-5 : la commission peut attribuer, et publier au Journal Officiel des Communautés européennes des numéros de référence de normes généralement admises pour des produits de signature électronique. Lorsqu'un produit de signature électronique est conforme à ces normes, les États membres présument qu'il satisfait aux exigences visées à l'annexe II, point f) et à l'annexe III. article 5.1 : les signatures électroniques avancées, basées sur un certificat qualifié, et créées par un dispositif sécurisé de création de signature répondent aux exigences légales d'une signature à l'égard des données électroniques, de la même manière qu'une signature manuscrite répond à ces exigences à l'égard des données manuscrites ou imprimés sur papier et soient recevables en justice. **Annexe III :** Exigences pour les dispositifs sécurisés de création de signature électronique : 1. Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que: a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée; b) l'on puisse avoir l'assurance suffisante que	**- Arrêté du 28/08/2006 pris en application du I de l'article 48 et de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics formalisés.** Chapitre II : Dispositions relatives à la signature électronique des candidatures et des offres. Article 5 : Les candidatures et les actes d'engagement, transmis par voie électronique ou envoyés sur support physique électronique, sont signés par l'opérateur économique au moyen d'un certificat de signature électronique, qui garantit notamment l'identification du candidat. Article 6 : Les catégories de certificats de signature utilisées pour signer électroniquement doivent être, d'une part, conformes au référentiel intersectoriel de sécurité et, d'autre part, référencées sur une liste établie par le ministre chargé de la réforme de l'État. Le référentiel intersectoriel de sécurité et la liste des catégories de certificats de signature électronique mentionnés à l'alinéa précédent sont publiés sous forme électronique à l'adresse suivante : http://www.entreprises.minefi.gouv.fr/certificats/. Article 7 : Les prestataires de services de certification électronique peuvent demander l'inscription d'une catégorie de certificats de signature électronique sur la liste mentionnée à l'article 6. Dans ce cas, ils demandent au préalable la reconnaissance, par le ministre chargé de la réforme de l'Etat, de la conformité de cette catégorie de certificats de signature électronique au référentiel intersectoriel de sécurité.

les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles; c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres. 2. Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.	A cette fin, les prestataires de services de certification électronique produisent tous les documents utiles permettant d'attester de la conformité de la catégorie de certificats de signature électronique proposée au référentiel intersectoriel de sécurité. Les pouvoirs adjudicateurs et les entités adjudicatrices doivent accepter comme certifiant valablement leurs échanges toutes les catégories de certificats de signature électronique figurant sur la liste mentionnée à l'article 6.
- Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. La modification principale est l'insertion de l'article 1316-4 : « 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'État. » **Article 1316-1** : L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.	**- Arrêté du 28/08/2006 fixant les modèles d'avis pour la passation et l'attribution des marchés publics et des accords-cadres :** article 5 Pour les marchés publics passés selon la procédure adaptée en application des dispositions des II et III de l'article 26 et du III de l'article 144 du code des marchés publics, les demandes de publication des avis d'appel public à la concurrence, envoyées au Bulletin officiel des annonces des marchés publics, à un journal habilité à recevoir des annonces légales ou à d'autres publications sont rédigées selon le modèle d'avis d'appel public à la concurrence annexé au présent arrêté. Article 6 Sont abrogés : - l'arrêté du 30 janvier 2004 pris en application des articles 40 et 80 du code des marchés publics et fixant les modèles de formulaires pour la publication des avis relatifs à la passation et à l'attribution des marchés publics ;

Décret 30/03/2001 :

un dispositif sécurisé de création de signature électronique doit :

1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :
a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

Les prestataires de services doivent utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent.

Présomption :

Le décret a recours à deux reprises à la notion de présomption :
- article 2 : présomption de fiabilité du procédé de signature électronique …la signature créée répond à la définition de signature sécurisé au sens de l'article le 1 du décret,
le dispositif de création de signature électronique a reçu un certificat de conformité aux exigences de l'article 3-1 du décret et dans les conditions énoncées dans l'article 3.II du décret.

- le certificat électronique utilisé pour vérifier la signature comporte les champs énoncés dans l'article 6.1 du décret et a été émis par un prestataire de services de certification

- **Décret 17/12/2008** modifiant diverses dispositions régissant les marchés soumis au code des marchés publics et aux décrets pris pour l'application de l'ordonnance n° 2005-649 du 6 juin 2005 relative aux marchés passés par certaines personnes publiques ou privées non soumises au code des marchés publics.

Ce décret a modifié l'article 48 du code des marchés publics : les offres sont présentées sous la forme de l'acte d'engagement défini à l'article 11… la signature de l'acte d'engagement est présentée selon les modalités prévues par un arrêté du ministre chargé de l'économie…les offres sont transmises en une seule fois.

- Article 56 du CMP :

II. - A compter du 1er janvier 2010, le pouvoir adjudicateur peut imposer la transmission par voie électronique des documents mentionnés au premier alinéa du I.

III. - A compter du 1er janvier 2012, seul les travaux d'un montant supérieur à 90 000 euros HT sont transmis par voie électronique.

VI.- le pouvoir adjudicateur peut exiger la transmission des candidatures et des offres par voie électronique.

L'arrêté du ministère de l'économie mentionné à l'article 48 et 56 du CMP n'existe pas au 30/05/2011

- **Arrêté du 14/12/2009 relatif à la**

respectant les exigences de l'article 6.II du décret. - article 7 : présomption de conformité des certificats électroniques aux exigences de l'article 6 : un certificat électronique est considéré remplir l'ensemble des exigences de l'article 6 du décret s'il a été émis par un prestataires de service de certification qualifié. Dans ces deux cas, il s'agit d'une présomption simple qui peut être renversé en apportant la preuve contraire. **- Ordonnance du 8/12/2005 relative aux échanges électroniques**	**dématérialisation des procédures de passation des marchés publics.** **Article 4 : Les supports physiques électroniques et les fichiers électroniques utilisés pour la transmission dématérialisée sont choisis par le pouvoir adjudicateur ou l'entité adjudicatrice, dans un format largement disponible.** **- Politique de Référencement Intersectoriel de Sécurité approuvé par l'arrêté du 6/05/2010 disponible sur le site l'ANASSPI)** Le Référencement intersectoriel de sécurité semble distinguer les autorités administratives et les utilisateurs privé. « Les autorités administratives … identifier, pour chaque nouveau téléservice, son besoin de sécurité, en fonction notamment de la sensibilité des données traitées et des risques existants Les usagers ont la possibilité de choisir librement leurs produits de sécurité et leur prestataire de service de confiance… Le certificat électronique d'un usager ou le produit de sécurité qu'il utilise pour accéder à un téléservice peut ainsi lui servir pour différents téléservices, de même niveau ou inférieur, de la sphère publique » **- Guide de bonne conduite des marchés** publics : à compter du 1er janvier 2012, le pouvoir adjudicateur ne pourra refuser, pour les marchés dont le montant atteint 90 000€ HT, de recevoir les documents des candidats par voie électronique. La transmission de documents sur papier ne peut plus être imposée par le règlement des consultations.