Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'AGRICULTURE, DE L'ALIMENTATION, DE LA PECHE ET DES AFFAIRES RURALES

EXAMEN PROFESSIONNEL D'ACCES AU GRADE DE SECRETAIRE ADMINISTRATIF D'ADMINISTRATION CENTRALE DE CLASSE EXCEPTIONNELLE

SESSION DU 09 NOVEMBRE 2004

EPREUVE ECRITE D'ADMISSIBILITE

Rédaction d'une note ou d'un rapport à l'aide des éléments d'un dossier à caractère administratif

(Durée : 3 heures – Coefficient : 1)

Vous devez vérifier que le sujet contient bien **16** pages. Si ce n'est pas le cas, signalez le immédiatement.

A l'issue de l'épreuve, vous devez rendre votre copie, même si elle est vierge, avant de signer la feuille d'émargement.

Vous devez porter sur la partie supérieure de votre copie vos nom, prénom, centre d'épreuve et votre signature.

Ne rien inscrire dans la case numéro d'ordre.

Il est rappelé au candidat qu'il ne doit pas faire apparaître son nom en quelque endroit de la copie, ni mentionner le nom du responsable hiérarchique dont il dépend effectivement, ni porter aucun signe distinctif, ni signature même fictive, sous risque de nullité de la copie.

La qualité de la rédaction, la clarté et la précision des raisonnements entrent pour une part importante dans l'appréciation du candidat.

Vous êtes rédacteur au sein de l'unité chargé des marchés publics. Votre nouveau supérieur hiérarchique doit se rendre à une réunion inter-ministérielle relative à la dématérialisation des achats publics.

Etant confronté pour la première fois à ce sujet, il vous demande de lui rédiger une note lui présentant les grandes caractéristiques de cette procédure – notamment vis-à-vis de la signature électronique - et son intérêt pour les acheteurs publics et leurs fournisseurs.

Liste des documents :

La dématérialisation de l'achat public

Article pour les Notes Bleues de Christophe Alviset, sous-directeur de l'Informatique, Direction du personnel, de la modernisation et de l'administration - ***Extraits***

La dématérialisation de l'achat public consiste à favoriser les échanges de documents par la voie électronique par rapport au support papier et, progressivement, développer l'emploi des technologies de l'information pour faciliter tous les aspects de la passation et de l'exécution des marchés publics. Cette dématérialisation est permise par le code des marchés publics : l'article 56 fait désormais obligation aux personnes publiques de pouvoir recevoir des offres électroniques pour les appels d'offres dont l'avis paraît postérieurement au 1er janvier 2005.

[...]

D'abord seront présentés quelques éléments de cadrage sur la modernisation de l'achat, puis les différents projets de dématérialisation ainsi que les repères juridiques en cette matière. Ensuite, sera rappelé le contexte de l'économie numérique dans lequel ces projets s'inscrivent et enfin, seront indiquées quelques pistes sur les enjeux pour l'avenir.

I - La modernisation de l'achat, facteur de rationalisation

Dès janvier 2003, le ministère de l'Économie, des Finances et de l'Industrie a lancé un audit des achats. Les premières conclusions sont parues début 2004 après un travail particulièrement exhaustif d'étude des dépenses de l'année 2002 pour l'ensemble du ministère. Les résultats de l'audit permettent d'identifier des gains de 18 % sur 3 ans pour 1,9 milliard d'euros d'achat par an. C'est un véritable travail d'analyse et de rationalisation par famille d'achat qui a permis d'aboutir à ces conclusions.

Quatre leviers créateurs d'économies ont été identifiés :

-la massification (le regroupement) des achats au niveau national pour 25 familles d'achat représentant 40 % de la dépense et une massification régionale pour 15 familles d'achat représentant 33 % de la dépense, par exemple les achats de PC ou de fournitures de bureau pour le niveau national et les prestations de nettoyage pour le niveau régional. Les autres achats resteront organisés comme actuellement, soit au niveau directionnel national, soit au niveau des services déconcentrés. Il s'agit là de distinguer l'achat, regroupé au niveau pertinent, de l'approvisionnement, déconcentré et respectant l'autonomie de gestion des responsables d'unité dans un cadre national permettant de faire des économies.

- la standardisation de l'achat et des consommations par la mise en place de catalogues réduits et le non recours aux achats hors catalogue ;

- la connaissance des marchés en adaptant l'expression du besoin aux capacités des entreprises ;

-la simplification des processus, en tirant tout le parti possible de la modernisation du code des marchés publics.

Ces résultats sont similaires à ceux de tout audit des achats, que ce soit dans le secteur public ou dans le secteur privé.

[...]

IV - L'économie numérique, nouvelle forme d'organisation des rapports entre les agents

Au-delà de la modernisation de l'administration et de la simplification des procédures, la dématérialisation de l'achat public sera également un facteur de modernisation des entreprises. Chaque année la Mission pour l'économie numérique, avec l'aide de la Digitip et du Sessi, produit un tableau de bord du commerce électronique dont la synthèse et le rapport complet sont accessibles sur Internet [...].

Une entreprise donnée pourra donc opter pour la dématérialisation complète de ses réponses aux appels d'offres, puisque toutes les personnes publiques devront pouvoir les accepter sous forme électronique. Par contre, du côté des acheteurs publics, il y aura une cohabitation des supports papiers et des supports électroniques pendant plusieurs années, sauf peut-être dans certains secteurs comme l'informatique ou la communication. C'est bien la capacité à entraîner petit à petit l'ensemble des entreprises vers la dématérialisation qui permettra d'obtenir le retour sur investissements attendu des plates-formes de dématérialisation.

A - Des gains notables pour les acteurs des marchés publics

Une première analyse consiste à dire que la publication des DCE (dossiers de consultation des entreprises) correspond à un transfert de charge de l'administration vers les entreprises et que la transmission des offres par les entreprises est un transfert de charge vers les administrations. En effet, les marchés publics sont très consommateurs de documents, parfois particulièrement volumineux ; par ailleurs, les documents, dossiers de consultation ou offres, sont demandés en de nombreux exemplaires. La manipulation de tous ces documents est donc coûteuse, mais les coûts directs de reproduction et d'affranchissement le sont également. Evidemment, il sera nécessaire de réimprimer les documents volumineux pour pouvoir les analyser.

Cependant, un deuxième effet est de faciliter la transmission de documents, en interne à l'administration d'une part, entre entreprises et co- et sous-traitants de l'autre, en limitant les transferts au minimum nécessaire. Dans l'ensemble de la chaîne, et non pas seulement dans les échanges administration-entreprises, on devrait donc voir apparaître des économies de papier et de manipulation.

Enfin, les transferts par voie électronique permettent de gagner en délais, de l'ordre d'un ou deux jours à chaque fois. Les délais réglementaires ne changent pas, notamment pour respecter l'égalité de traitement des entreprises, mais toutes les demandes de précision, questions et autres mises au point s'en trouveront accélérées.

Dernier sujet : la passation des marchés publics est en soi un secteur d'activité de l'économie. Journaux d'annonces légales, prestataires de services, concentrateurs d'annonces, éditeurs de logiciels, cabinets juridiques, prestataires de formation, toutes ces activités se trouveront impactées par la dématérialisation de l'achat et l'arrivée de nouveaux entrants, spécialisés dans la signature électronique, l'archivage de documents numériques et la sécurité informatique. La dématérialisation se présente donc également comme une opportunité de développement pour le secteur privé et introduira nécessairement des changements de positionnement parmi ces acteurs.

[...]

Dématérialisation des marchés publics

La dématérialisation est juridiquement possible

Les agents concernés par la dématérialisation des achats publics se posent beaucoup de questions sur la validité juridique de certaines procédures. Mais rares sont les problèmes qui ne trouvent pas de solution dans les textes actuels.

Une base de données sur les fournisseurs (entreprises, artisans...) relève-t-elle de la Cnil ? Que peut-on y mettre, sans risque juridique ? Comment traiter les signatures électroniques des membres d'un groupement de candidatures ? Que faut-il faire quand une offre électronique arrive hors délai ?

Autant de questions que les agents concernés par la dématérialisation des achats - acheteurs se posent légitimement, à moins d'un an de l'entrée en vigueur de l'obligation pour les acheteurs de recevoir des offres par voie électronique pour certains de leurs marchés.

La mise en place d'un "sous-groupe" juridique

Pour répondre à ces questions,), un "sous-groupe" juridique sur la dématérialisation des achats publics a été mis en place, au sein de l'Adae (Agence pour le développement de l'administration électronique). Il est animé par Marie-José Palasz, chef de service à la Direction des affaires juridiques du Minefi. Les participants viennent de différents ministères - Défense, Équipement, Éducation nationale, Santé, etc. - ainsi que de collectivités locales pionnières en matière de dématérialisation.

Un guide pour les acheteurs

"*L'objectif est de faire remonter les questions du terrain, de faire le tri entre ce qui est juridique, technique ou organisationnel et de produire un guide qui servira de vademecum aux acheteurs pour qu'ils retrouvent les questions les plus souvent posées, accompagnées de nos réponses étayées par les textes et par la jurisprudence*", indique Marie-José Palasz. Ce guide sera disponible pour les acheteurs dès la rentrée. Il accompagnera notamment le déploiement de la plate-forme interministérielle des achats publics de l'État.

Le cas de la signature électronique

Il n'empêche: dans une administration pétrie par la culture de l'écrit, certains aspects de la dématérialisation passent mal. C'est le cas de la signature électronique, qui a longtemps constitué un point de blocage des réflexions. Le sujet avait pourtant été abordé par l'article 3 du décret n° 2002-692 du 30 avril 2002: "*Les candidatures et les offres transmises par voie électronique doivent être envoyées dans des conditions qui permettent d'authentifier la signature du candidat.*" Restait à déterminer le niveau de sécurité de la signature. Certains souhaitaient un niveau de fiabilité tel qu'il aurait, de fait emem, empêché une mise en œuvre de la dématérialisation des échanges. L'Adae comme la Mission pour l'économie numérique (Men) travaillent sur ce sujet et envisagent que les certificats que devront utiliser les fournisseurs soient de niveau 2, c'est-à-dire de même niveau de sécurité que ceux utilisés pour Télé TVA.

La signature électronique ne peut être imprimée

Pour la Daj, des travaux de réflexions doivent encore être menés, paradoxalement, sur les problèmes liés à la rematérialisation d'un marché. En effet, pour l'instant, l'exécution des marchés notamment n'est pas dématérialisée. L'acheteur public devra donc imprimer le marché avant de l'envoyer au comptable public pour les paiements relatifs au marché. Problème: l'exemplaire ne comportera pas de signature du fournisseur, la signature électronique ne peut être imprimée.

Une solution concertée

Une des pistes examinées par le sous-groupe est que l'acheteur indique que l'exemplaire qu'il transmet est en tout point identique à celui signé électroniquement. Cette proposition va faire l'objet d'une concertation avec les services concernés (la comptabilité publique notamment).

Source : site internet de la revue Service Public n°105, ministère de la fonction publique et de la réforme de l'Etat, juin 2004

pour l'Économie Numérique

Revue de Web

La signature électronique sécurisée

Revue réalisée le 31/01/2002 (extraits)

Dans la société de l'information, l'usage de la télématique et des réseaux informatiques permet de passer des accords à distance par échange de message et sans support papier. Mais, en cas de contentieux, une preuve de nature informatique ou télématique sera-t-elle susceptible d'emporter la conviction du juge? On sait que le droit de la preuve est longtemps resté sous l'empire du document papier "*original* " et signé "*de* [la] *main* ".

Des dispositions communautaires récentes (utilisation de la signature électronique; encadrement des pratiques en matière de commerce électronique) apparaissent comme autant de tentatives d'harmonisation du positionnement des Etats membres en ce domaine ("*Les Etats veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique* ", art. 9 de la directive du 8 juin 2000).

Les nouvelle règles légales

La signature par un "*double clic*" est une réalité juridique communautaire depuis l'adoption de la directive du 13 décembre 1999. L'objectif principal de ce texte, qui introduit la notion de signature électronique "*avancée*" (= davantage de sécurité), est de "*faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique* ". En intégrant les notions d'écrit et de signature électronique, la loi du 13 mars 2000, transposition en droit français de cette directive, est une forme de révolution du *droit de la preuve*. Antérieurement à l'entrée en vigueur de cette législation, l'absence de définition légale de la signature était en effet la réalité du droit positif (*Première décision sur la signature électronique*, note JC Galloux, Jurisclasseur Communication & commerce électronique, janvier 2001).

Le principe de la signature électronique, de même nature et de même valeur qu'une signature manuelle, est désormais reconnu par le *Code civil* (nouveaux articles 1316 à 1316-4, issus de la loi précitée). En vertu de ces dispositions nouvelles, la signature électronique consiste "*en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache*".

Dans quelles conditions des signatures électroniques peuvent-elles être présumées fiables ? Le décret d'application de l'article 1316-4 du Code civil indique notamment que " *la fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée* " (art. 2).

Une qualification de " *signature électronique sécurisée* " répond nécessairement à la prise en compte d'un certain nombre d'exigences, à savoir " *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* ".

Par la suite, toute signature électronique sécurisée sera établie grâce à un dispositif, également sécurisé, de création de signature électronique. Dans quelles conditions ? Le matériel ou le logiciel utilisé garantira que les données de création de signature électronique ne peuvent être établies plus d'une fois, et assurera la confidentialité des données, mais aussi une protection contre toute falsification ou toute utilisation par des tiers. De plus, cette procédure ne devra entraîner aucune altération du contenu de l'acte à signer, ni poser aucun obstacle à la lecture de cet acte avant signature.

Enfin, la vérification de cette signature devra reposer sur l'utilisation d'un "*certificat électronique qualifié*". Répondant à des conditions particulières d'identité (du prestataire, de l'Etat d'émission, du signataire), de conformité des données (création, vérification), de validité et de sécurité (code d'identité du certificat, signature sécurisée du prestataire), ce certificat sera délivré par un " *prestataire de service de certification* "(PSC). La signature électronique présente ainsi des particularités juridiques paradoxales : "*toujours identique et pourtant jamais pareille puisqu'elle est propre à chacun des documents émis. De surcroît, il est possible de la conserver sans la garder matériellement* " (*L'Union européenne donne son feu vert à la signature électronique*, I. Pottier et A. Bensoussan, **Les Echos**, 25 janvier 2000).

[...]

J.O n° 62 du 14 mars 2000 page 3968.

Lois

LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (1)

NOR: JUSX9900020L

L'Assemblée nationale et le Sénat ont adopté,
Le Président de la République promulgue la loi dont la teneur suit :

Article 1er

I. - L'article 1316 du code civil devient l'article 1315-1.
II. - Les paragraphes 1er, 2, 3, 4 et 5 de la section 1 du chapitre VI du titre III du livre III du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.
III. - Il est inséré, avant le paragraphe 2 de la section 1 du chapitre VI du titre III du livre III du code civil, un paragraphe 1er intitulé : « Dispositions générales », comprenant les articles 1316 à 1316-2 ainsi rédigés :
« Art. 1316. - La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.
« Art. 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.
« Art. 1316-2. - Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »

Article 2

L'article 1317 du code civil est complété par un alinéa ainsi rédigé :
« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »

Article 3

Après l'article 1316-2 du code civil, il est inséré un article 1316-3 ainsi rédigé :
« Art. 1316-3. - L'écrit sur support électronique a la même force probante que l'écrit sur support papier. »

Article 4

Après l'article 1316-3 du code civil, il est inséré un article 1316-4 ainsi rédigé :
« Art. 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'Etat. »

Article 5

A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même ».

Article 6

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.
La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 13 mars 2000.

Jacques Chirac
Par le Président de la République :

Le Premier ministre,
Lionel Jospin

Le garde des sceaux, ministre de la justice,
Elisabeth Guigou

Le ministre de l'intérieur,
Jean-Pierre Chevènement

Le ministre de l'économie,
des finances et de l'industrie,
Christian Sautter

Le secrétaire d'Etat à l'outre-mer,
Jean-Jack Queyranne

Le secrétaire d'Etat à l'industrie,
Christian Pierret

(1) Loi n° 2000-230.
- Directive communautaire :
Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
- Travaux préparatoires :
Sénat :
Projet de loi no 488 (1998-1999) ;
Rapport de M. Charles Jolibois, au nom de la commission des lois, no 203 (1999-2000) ;
Discussion et adoption le 8 février 2000.
Assemblée nationale :
Projet de loi, adopté par le Sénat, no 2158 ;
Rapport de M. Christian Paul, au nom de la commission des lois, no 2197 ;
Discussion et adoption le 29 février 2000.

J.O n° 77 du 31 mars 2001 page 5070.

Textes généraux

Ministère de la justice

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

NOR: JUSC0120141D

Le Premier ministre,
Sur le rapport de la garde des sceaux, ministre de la justice,
Vu la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ;
Vu le code civil, notamment ses articles 1316 à 1316-4 ;
Vu la loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;
Le Conseil d'Etat (section de l'intérieur) entendu,
Décrète :

Art. 1er. - Au sens du présent décret, on entend par :
1. « Signature électronique » : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;
2. « Signature électronique sécurisée » : une signature électronique qui satisfait, en outre, aux exigences suivantes :
- 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 ;
3. « Signataire » : toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en oeuvre un dispositif de création de signature électronique ;
4. « Données de création de signature électronique » : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;
5. « Dispositif de création de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;
6. « Dispositif sécurisé de création de signature électronique » : un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 ;
7. « Données de vérification de signature électronique » : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;
8. « Dispositif de vérification de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;
9. « Certificat électronique » : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;
10. « Certificat électronique qualifié » : un certificat électronique répondant aux exigences définies à l'article 6 ;
11. « Prestataire de services de certification électronique » : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;

12. « Qualification des prestataires de services de certification électronique » : l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Art. 2. - La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire 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.

Chapitre Ier
Des dispositifs sécurisés de création de signature électronique

Art. 3. - Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est certifié conforme à ces exigences dans les conditions prévues au II.

I. - 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.

II. - Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I :

1o Soit par les services du Premier ministre chargés de la sécurité des systèmes d'information, après une évaluation réalisée, selon des règles définies par arrêté du Premier ministre, par des organismes agréés par ces services. La délivrance par ces services du certificat de conformité est rendue publique ;

2o Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

Art. 4. - Le contrôle de la mise en oeuvre des procédures d'évaluation et de certification prévues au 1o du II de l'article 3 est assuré par un comité directeur de la certification, institué auprès du Premier ministre.

Un arrêté du Premier ministre précise les missions attribuées à ce comité, fixe sa composition, définit les procédures de certification et d'évaluation des dispositifs de création de signature électronique mentionnées à l'alinéa précédent ainsi que les procédures d'agrément des organismes d'évaluation. Il détermine, en outre, les obligations incombant à ces organismes et fixe les conditions dans lesquelles sont présentées et instruites les demandes de certification.

Chapitre II
Des dispositifs de vérification de signature électronique

Art. 5. - Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies par l'arrêté mentionné à l'article 4, s'il répond aux exigences suivantes :

a) Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en oeuvre le dispositif et qui est dénommée « vérificateur » ;
b) Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;
c) Le vérificateur doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;
d) Les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;
e) L'identité du signataire doit sans subir d'altération être portée à la connaissance du vérificateur ;
f) Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement portée à la connaissance du vérificateur ;
g) Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.

Chapitre III
Des certificats électroniques qualifiés
et des prestataires de services de certification électronique

Art. 6. - Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II.
I. - Un certificat électronique qualifié doit comporter :
a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;
c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;
d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
f) L'indication du début et de la fin de la période de validité du certificat électronique ;
g) Le code d'identité du certificat électronique ;
h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;
i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.
II. - Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :
a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;
b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;
c) Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;
d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;
e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;

f) Appliquer des procédures de sécurité appropriées ;
g) Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;
h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;
i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;
j) Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;
k) Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.
l) Utiliser des systèmes de conservation des certificats électroniques garantissant que :
- l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;
- l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
- toute modification de nature à compromettre la sécurité du système peut être détectée ;
m) Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;
n) S'assurer au moment de la délivrance du certificat électronique :
- que les informations qu'il contient sont exactes ;
- que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;
o) Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un certificat électronique :
- des modalités et des conditions d'utilisation du certificat ;
- du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique mentionnée à l'article 7 ;
- des modalités de contestation et de règlement des litiges ;
p) Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au o) qui leur sont utiles.

Art. 7. - Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés.
Cette qualification, qui vaut présomption de conformité auxdites exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de l'industrie. Elle est précédée d'une évaluation réalisée par ces mêmes organismes selon des règles définies par arrêté du Premier ministre.
L'arrêté du ministre chargé de l'industrie prévu à l'alinéa précédent détermine la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de certification électronique.

Art. 8. - Un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat n'appartenant pas à la Communauté européenne a la même valeur juridique que celui délivré par un prestataire établi dans la Communauté, dès lors :
a) Que le prestataire satisfait aux exigences fixées au II de l'article 6 et a été accrédité, au sens de la directive du 13 décembre 1999 susvisée, dans un Etat membre ;

b) Ou que le certificat électronique délivré par le prestataire a été garanti par un prestataire établi dans la Communauté et satisfaisant aux exigences fixées au II de l'article 6 ;
c) Ou qu'un accord auquel la Communauté est partie l'a prévu.

Art. 9. - I. - Au titre de la déclaration de fourniture de prestations de cryptologie effectuée conformément aux dispositions de l'article 28 de la loi du 29 décembre 1990 susvisée, le prestataire de services de certification électronique doit, quand il entend délivrer des certificats électroniques qualifiés, l'indiquer.
II. - Le contrôle des prestataires visés au I est effectué par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information.
Ce contrôle porte sur le respect des exigences définies à l'article 6. Il peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire de services de certification électronique.
Lorsque le contrôle révèle qu'un prestataire n'a pas satisfait à ces exigences, les services du Premier ministre chargés de la sécurité des systèmes d'information assurent la publicité des résultats de ce contrôle et, dans le cas où le prestataire a été reconnu comme qualifié dans les conditions fixées à l'article 7, en informent l'organisme de qualification.
Les mesures prévues à l'alinéa précédent doivent faire l'objet, préalablement à leur adoption, d'une procédure contradictoire permettant au prestataire de présenter ses observations.

Chapitre IV
Dispositions diverses

Art. 10. - Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française, aux îles Wallis et Futuna et à Mayotte.

Art. 11. - Le ministre de l'économie, des finances et de l'industrie, la garde des sceaux, ministre de la justice, le ministre de l'intérieur, le secrétaire d'Etat à l'outre-mer et le secrétaire d'Etat à l'industrie sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 30 mars 2001.

Lionel Jospin
Par le Premier ministre :

La garde des sceaux, ministre de la justice,
Marylise Lebranchu

Le ministre de l'économie,
des finances et de l'industrie,
Laurent Fabius

Le ministre de l'intérieur,
Daniel Vaillant

Le secrétaire d'Etat à l'outre-mer,
Christian Paul

Le secrétaire d'Etat à l'industrie,
Christian Pierret

J.O n° 103 du 3 mai 2002 page 8064.

Décrets, arrêtés, circulaires

Textes généraux

Ministère de l'économie, des finances et de l'industrie

Décret n° 2002-692 du 30 avril 2002 pris en application du 1° et du 2° de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics

NOR: ECOM0210072D

Le Premier ministre,

Sur le rapport du ministre de l'économie, des finances et de l'industrie,

Vu le code civil, notamment ses articles 1316 à 1316-4 ;

Vu le code des marchés publics, notamment son article 56 ;

Vu le décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique,

Décrète :

Article 1

Dans les cas où les marchés publics passés selon les règles mentionnées au titre III du code des marchés publics donnent lieu à des échanges d'informations par voie électronique en application de l'article 56 dudit code, ces échanges s'effectuent dans les conditions prévues aux articles 2 à 10 ci-dessous.

Article 2

Conformément aux dispositions de l'article 56 (1°) du code des marchés publics, 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 dont les modalités d'accès sont précisées dans l'avis d'appel public à la concurrence.

Quelle que soit la procédure, les personnes intéressées doivent pouvoir consulter et archiver sur leur ordinateur le règlement de la consultation. Les personnes intéressées, dans le cadre d'un appel d'offres ouvert, et les candidats invités à présenter une offre, dans le cadre d'une mise en concurrence simplifiée, d'un appel d'offres restreint ou d'une procédure négociée, doivent pouvoir également consulter et archiver sur leur ordinateur le cahier des charges, les documents et renseignements complémentaires. 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.

Dans le cadre d'une mise en concurrence simplifiée, d'un appel d'offres restreint ou d'une procédure négociée, la personne responsable du marché peut également envoyer par voie électronique la lettre de consultation aux candidats invités à présenter une offre. Ceux-ci sont alors avisés qu'ils sont habilités à télécharger le dossier de la consultation. Hormis le cas des marchés négociés sans publicité préalable, mention doit avoir été faite de cette possibilité dans l'avis d'appel public à concurrence.

Les personnes intéressées et les candidats peuvent demander que les documents mentionnés au premier alinéa leur soient envoyés par voie postale, sous forme d'un support physique électronique ou sous forme d'un support papier.

Les candidats qui choisissent de prendre connaissance par voie électronique des documents mentionnés au premier alinéa conservent la possibilité, au moment du dépôt de leur candidature ou de leur offre, de choisir entre la transmission par voie électronique et la transmission sur un support papier ou, si le règlement de la consultation le permet, la transmission sur un support physique électronique.

Article 3

Conformément aux dispositions de l'article 56 (2°) du code des marchés publics, la personne publique peut accepter la transmission des candidatures et des offres par voie électronique. Cette décision ainsi que les modalités de la transmission sont mentionnées dans l'avis d'appel public à la concurrence ou, dans le cas des marchés négociés sans publicité préalable, dans la lettre de consultation.

Les candidatures et les offres transmises par voie électronique doivent être envoyées dans des conditions qui permettent d'authentifier la signature du candidat selon les exigences posées aux articles 1316 à 1316-4 du code civil.

Dans les documents ou informations fournis à l'appui de leur candidature, qui pourront être également transmis par voie électronique, les candidats doivent désigner la personne habilitée à les représenter. Ils mettent en place des procédures permettant à la personne responsable du marché de s'assurer que les candidatures et les offres sont signées et transmises par la personne habilitée.

La transmission des candidatures et des offres doit pouvoir faire l'objet d'une date certaine de réception et d'un accusé de réception électronique.

Article 4

Dans le cas où une offre est susceptible d'entraîner la transmission de documents volumineux, et pour éviter tout retard consécutif aux aléas de transmission électronique qui pourraient en résulter, la personne publique peut autoriser les candidats à envoyer leur offre 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.

Lorsque la possibilité prévue à l'alinéa ci-dessus est utilisée, la personne responsable du marché indique dans l'avis d'appel public à la concurrence ou dans la lettre de consultation le délai qui peut séparer la réception de la signature électronique sécurisée de la réception de l'offre elle-même. Ce délai ne saurait excéder vingt-quatre heures, sous peine de l'irrecevabilité de l'offre.

Article 5

Les candidats doivent choisir entre, d'une part, la transmission électronique de leurs candidatures et de leurs offres et, d'autre part, leur envoi sur un support papier ou, le cas échéant, sur un support physique électronique.

Article 6

En cas d'appel d'offres ouvert, si une candidature n'est pas admise, l'offre correspondante est éliminée des fichiers de la personne publique sans avoir été lue. Le candidat en est informé.

Article 7

La personne publique assure la sécurité des transactions sur un réseau informatique accessible à tous les candidats de façon non discriminatoire. Les frais d'accès au réseau et de recours à la signature électronique sont à la charge de chaque candidat.

Article 8

La personne publique prend les mesures propres à garantir la sécurité des informations portant sur les candidatures et les offres. Elle s'assure que ces informations demeurent confidentielles.

A cet effet, la personne responsable des marchés peut demander aux candidats d'assortir leurs fichiers d'un système de sécurité tel que les candidatures et les offres ne puissent être ouvertes qu'avec leurs concours.

Article 9

Dans le cas de candidatures groupées, le mandataire assure la sécurité et l'authenticité des informations transmises au nom des membres du groupement.

Article 10

Tout document électronique envoyé par un candidat dans lequel un virus informatique est détecté par l'acheteur public peut faire l'objet par ce dernier d'un archivage de sécurité sans lecture dudit document. Ce document est dès lors réputé n'avoir jamais été reçu et le candidat en est informé.

Article 11

Le ministre de l'économie, des finances et de l'industrie est chargé de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 30 avril 2002.

Lionel Jospin

Par le Premier ministre :

Le ministre de l'économie,
des finances et de l'industrie,
Laurent Fabius