

**DÉMATÉRIALISATION
DES PROCÉDURES D'ACHAT
DE FOURNITURES
DES ETABLISSEMENTS PUBLICS
DE SANTÉ**

Approuvé par la Commission technique des marchés le 11 mai 2004

Introduction	5
1. Dématérialisation des procédures d'achat de fournitures par les établissements de santé	6
1.1 Définition	6
1.2 Une nouvelle approche	6
1.2.1 Phase 1 : mise en ligne de l'Avis d'Appel Public à la Concurrence et du Dossier de Consultation des Entreprises	6
1.2.2 Phase 2 : Réponse aux consultations par voie électronique	6
1.3 Domaine couvert par le présent guide	7
1.4 Avantages de la dématérialisation	7
1.5 Cadre juridique et application technique	8
2 Description et terminologie relative à la dématérialisation des procédures	8
2.1 Problématique de la sécurisation : identifiant et mot de passe	9
2.2 Problématique de la sécurisation : certificats et signatures	10
2.2.1 Familles de Certificats	11
2.2.2 Utilisation des certificats pour la signature	11
2.2.3 Chiffrement (ou cryptage)	12
2.3 Horodatage	12
2.4 Enchères électroniques inversées	12
2.5 Echange de données informatisé (EDI)	13
2.6 Utilisation de portails	13
2.7 Archivage	13
2.7.1 Que faut-il archiver ?	13
2.7.2 Sur quel support ?	14
2.7.3 Durée d'archivage	14
2.8 Virus et anti-virus	14
2.8.1 Virus	14
2.8.2 Antivirus	15
2.8.3 Conséquences pour les échanges de documents par une plate-forme de dématérialisation	16
3 Environnement réglementaire	16
4 L'AAPC, le règlement de consultation et la lettre de consultation dans une procédure d'achat public dématérialisée	17
4.1 L'AAPC	17
4.2 Le règlement de consultation	18
4.2.1 Article « Modalités de la consultation »	18
4.2.2 Article « Présentation des offres »	19
4.2.3 Article « Conditions d'envoi ou de remise des offres »	19
4.3 La lettre de consultation	20

5	Etapes d'une procédure d'achat public dématérialisée	21
5.1	Consultation des Avis d'Appel Public à la Concurrence, demande et transmission du Dossier de Consultation des Entreprises	23
	Figure n° 1 : consultation de l'AAPC et du RC et demande du DCE.....	23
5.1.1	Consultation de l'AAPC et du RC par le fournisseur	23
5.1.2	Demande du DCE.....	24
5.2	Envoi de l'offre.....	25
5.2.1	Délivrance du certificat de signature électronique	26
	Figure n° 2 : délivrance du certificat de signature	26
5.2.2	Envoi de la candidature et de l'offre.....	26
	Figure n° 3 : envoi de la candidature et de l'offre	26
5.3	Réception des plis	28
	Figure n° 4 : réception du dossier de réponse	28
5.3.1	Réception chez l'acheteur public.....	28
5.3.2	Notion de séquestre ou « coffre fort électronique ».....	29
5.4	Examen des candidatures par la PRM (art. 52-1 ^{er} alinéa CMP)	30
	Figure n° 5 : examen des candidatures par la PRM	30
5.5	Examen des candidatures, avis de la CAO, élimination des candidatures par la PRM (Art. 58-II du CMP).....	31
	Figure n° 6 : examen des candidatures par la CAO	31
5.6	Ouverture des offres (CAO) (art 58-III)	31
5.7	Avertir les candidats non retenus.....	32
5.8	Avertir les candidats retenus et poursuite de la procédure.....	32
5.9	Archivage.....	32
	Glossaire	33
	Liste des abréviations	38
	Annexe n°1 : textes	40
	Annexe n°2 : Archivage	52
	Annexe n°3 : Eléments de cahier des clauses pour la recherche d'un prestataire de services dans le cadre de la mise en place initiale d'un système de dématérialisation des procédures d'achat de fournitures des établissements publics de santé	57
	Annexe n°4 : Comité de Rédaction	65
	Annexe n°5 : Comité de Lecture	66

Introduction

Dès l'apparition de **techniques fiables** de dématérialisation et d'automatisation, les **pharmaciens des établissements de santé** ont, grâce à leurs structures associatives professionnelles, mis en place **les applications de la dématérialisation pour leur exercice professionnel journalier** (codification CIP ou Club Inter-Pharmaceutique des médicaments, standardisation des échanges pour les appels d'offres, utilisation de portails de commandes / factures par EDI puis par Internet, Rapport Ediphast du Conseil de l'Informatique Hospitalière publié en 1995).

Fort de cette antériorité (de près de 15 ans), le groupe de travail **GPEM/SL dématérialisation** créé dès décembre 2002, a été réuni autour de pharmaciens hospitaliers expérimentés.

L'équipe constituée aujourd'hui pour la rédaction du guide est formée de **spécialistes de tous les métiers de l'hôpital public** (collectivités territoriales, armée) concernés par l'achat de **fournitures** et la **dématérialisation** : **directeurs de services économiques, pharmaciens, ingénieurs informaticiens** ; par ailleurs, participent aux travaux deux représentants d'organisations représentatives des fournisseurs de médicaments (Les Entreprises du Médicament ou LEEM) et de dispositifs médicaux (Syndicat National de l'Industrie des Technologies Médicales ou SNITEM) ainsi que des représentants du Ministère de l'Economie, des Finances et de l'Industrie ou MINEFI.

Ce guide rédigé en moins d'une année, a pour objectif de donner les solutions simples pour mettre en place dès janvier 2005 la transmission par voie électronique des échanges d'informations entre établissements et fournisseurs intervenant en application de l'article 56 du Code des Marchés Publics (dématérialisation des procédures), dans des conditions économiques et techniques accessibles à tous les établissements de santé.

Volontairement limités aux achats de fournitures, les principes déclinés dans ce guide peuvent servir de support à l'ensemble des domaines de l'achat public.

1 Dématérialisation des procédures d'achat de fournitures par les établissements de santé

1.1 Définition

La dématérialisation des données consiste à transmettre et à stocker des informations sans support papier.

Ceci est maintenant rendu possible par l'essor de la technologie informatique et du développement d'Internet. L'habitude du support papier a, le plus souvent perduré, ne serait-ce que pour un archivage sous cette forme quand cela n'est pas tout simplement dû à des obstacles techniques et à des habitudes culturelles.

Le fait nouveau est que l'on voit la notion de dématérialisation inscrite dans les textes officiels : c'est un véritable changement de culture qui s'annonce.

1.2 Une nouvelle approche...

Le lecteur trouvera ci-après une description sommaire de ces nouvelles approches dont les processus de mise en œuvre seront développés dans le corps de ce guide.

1.2.1 Phase 1 : mise en ligne de l'Avis d'Appel Public à la Concurrence et du Dossier de Consultation des Entreprises

Les Avis d'Appel Public à la Concurrence (AAPC) sont, selon l'article 40 du Code des Marchés Publics (CMP), les seuls documents obligatoirement dématérialisés pour leur envoi vers l'organe officiel de publication des annonces des marchés publics : Bulletin Officiel des Annonces des Marchés Publics (BOAMP).

Le Dossier de Consultation des Entreprises (DCE) n'étant plus obligatoirement envoyé par voie postale est rendu disponible sur un site dont l'adresse est indiquée dans l'AAPC. Le Règlement de la Consultation (RC), s'il existe en complément de l'AAPC, est en libre consultation sur ce site. Par contre, les autres documents (Cahier des Clauses Administratives Particulières ou CCAP, Cahier des Clauses Techniques Particulières ou CCTP, documents de candidatures et éventuels autres documents annexes) ne seront téléchargeables par le candidat qu'après renseignement d'une fiche mentionnant : 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. Cette étape correspond à la demande de dossier et l'adresse électronique permet de respecter l'égalité de traitement des candidats en assurant la possibilité de leur signaler par la suite l'existence éventuelle de modifications apportées au dossier.

1.2.2 Phase 2 : Réponse aux consultations par voie électronique

Pour la réception des candidatures et des offres, la dématérialisation doit apporter l'équivalent électronique de la lettre recommandée postale ou de l'adressage par porteur garantissant leur réception et la non-ouverture des offres avant la Commission d'Appel d'Offres (CAO) réunie à cet effet. Cette exigence nécessitera, dans la grande majorité des cas, le recours à un prestataire de services mettant à disposition un séquestre (ou « coffre-fort électronique »).

Le lecteur se reportera utilement au chapitre 2 pour une approche plus précise des éléments techniques et au chapitre 5 pour une connaissance détaillée des différentes phases de l'Appel d'Offres Ouvert (AOO) en procédure dématérialisée.

1.3 Domaine couvert par le présent guide

Sont concernées par la dématérialisation¹ des consultations pour l'achat de fournitures dans les établissements publics de santé (EPS), les procédures suivantes :

- la procédure d'appel d'offres ouvert (double enveloppe) ;
- la procédure d'appel d'offres restreint (peu utilisée dans le domaine des produits de santé) ;
- la procédure du marché négocié (utilisation de la lettre de consultation) avec ou sans concurrence ;
- la procédure de dialogue compétitif ;
- la procédure relative aux marchés passés selon la procédure adaptée (art. 28 du CMP) ou « Marchés Sans Formalités Préalables » (MSFP), au sens de la loi n° 2001-1168 du 11 décembre 2001 portant Mesures Urgentes de Réformes à Caractère Economique et Financier dite loi MURCEF, qui requiert cependant, en raison des montants à engager, un minimum de formalisme surtout dès lors qu'il y a concurrence potentielle entre plusieurs fournisseurs : les règles de la concurrence et du libre accès à tout marché, fut-il sans formalités, s'appliquent dès le premier euro.

Le domaine le plus exigeant en termes réglementaires est celui de l'appel d'offres : c'est celui que nous détaillerons le plus dans le présent document, en sachant que le niveau de formalités sera moindre pour toutes les autres procédures de consultation, a fortiori pour les marchés passés selon la procédure adaptée.

1.4 Avantages de la dématérialisation

La dématérialisation présente :

- des avantages économiques (diminution des coûts postaux, de reprographie, de préparation et d'envoi des dossiers de consultations, ...),
- et des avantages techniques (facilitation de l'accès à la commande publique, rapidité des échanges...).

¹ Il ne faut pas confondre « dématérialisation » et « automatisation » ! En effet, la dématérialisation consiste à mettre en place des échanges par voie électronique offrant un niveau de sécurité défini qui se faisaient jusqu'alors essentiellement par voie postale classique. L'automatisation est une étape supplémentaire autorisant des transferts de données entre logiciels adaptés : ceci suppose l'utilisation d'identifiants univoques reconnus. A ce jour, les logiciels existent sur le marché, mais la notion d'identifiants univoques ne semble possible que dans le domaine du médicament (classification Anatomical Therapeutical Chemical ou ATC pour les mises en concurrence et/ou Unité Commune de Dispensation et/ou Distribution ou UCD pour les réponses par spécialité). L'extension de l'utilisation de procédures dématérialisées va conduire les fournisseurs de logiciels à proposer de plus en plus d'outils permettant un maximum d'automatisation en plus de la seule dématérialisation. Une offre existe déjà et va encore se développer : si l'établissement hospitalier ne possède pas les outils nécessaires à la réalisation de telles procédures, la recherche d'un prestataire de service sera nécessaire par le biais d'une mise en concurrence selon un cahier des clauses dont des éléments sont fournis en annexe 3. L'outil qu'est la messagerie électronique, d'usage devenu courant, est insuffisant pour pouvoir réaliser des procédures dématérialisées en termes de marchés publics, tout au moins lorsqu'il s'agit de l'appel d'offres.

Indirectement, la dématérialisation conduit le praticien des marchés à un respect plus strict des différentes étapes du calendrier des marchés de par l'informatisation de la procédure d'appel d'offres. De ce fait, elle améliore la gestion par la Personne Responsable des Marchés (PRM) des procédures de marchés au sein de son établissement.

La dématérialisation amène à réaliser au mieux ce qui se passait en échanges classiques, respectant en cela à la lettre les prescriptions du CMP. Il y a tout lieu de penser qu'un de ses effets bénéfiques sera de modifier les procédures internes des établissements de santé pour mettre en place de nouvelles modalités organisationnelles guidées par une politique d'amélioration continue de la qualité.

La mise en œuvre de la dématérialisation ne doit cependant pas conduire à ajouter des exigences par rapport aux échanges classiques sur papier.

1.5 Cadre juridique et application technique

Les moyens techniques existent par la disponibilité des outils informatiques et l'existence et le développement d'un marché significatif de prestataires de services dans le domaine, voire d'éditeurs de modules informatiques dédiés.

Le cadre juridique recouvre les textes suivants :

- Articles 40 et 56 du Code des Marchés Publics ;
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (Journal officiel du 14 mars 2000) ;
- Décret n°2001-846 du 18 septembre 2001 pris en application du 3° de l'article 56 du CMP et relatif aux enchères électroniques (Journal officiel du 19 septembre 2001) ;
- Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique (Journal officiel du 31 mars 2001) ;
- Décret n°2002-692 du 30 avril 2002 pris en application du 1° et du 2° de l'article 56 du CMP et relatif à la dématérialisation des procédures de passation des marchés publics (Journal officiel du 3 mai 2002).

La dématérialisation, telle qu'elle est précisée par le décret du 30 avril 2002, concerne seulement la procédure de passation des marchés publics depuis la mise en ligne des DCE jusqu'à la transmission par voie électronique à la PRM des candidatures et des offres. L'exécution des marchés n'est pas traitée dans ce décret, ce qui n'exclut pas de l'envisager. Si aujourd'hui un marché reste le plus souvent un document « matérialisé » (papier) avec signature des engagements réciproques du fournisseur et de l'acheteur, il est bon de se rapporter au dernier alinéa de l'article 56 du CMP qui précise que « Les dispositions du présent code qui font référence à des écrits ne font pas obstacle au remplacement de ceux-ci par un support ou un échange électronique ».

2 Description et terminologie relative à la dématérialisation des procédures

1. La dématérialisation s'applique aux échanges d'informations tout au long des procédures de passation des marchés publics.

2. L'échange électronique se substitue à l'échange postal, au dépôt par porteur, etc.

3. Tout écrit sur un support papier peut être remplacé par un écrit sur support électronique dans les conditions posées par l'article 1316-1 du Code Civil².

4. L'édition papier d'un document écrit sur support électronique n'est pas équivalente à son original électronique.

5. La consultation ou le téléchargement du DCE n'implique pas, pour le fournisseur, le dépôt d'une candidature et d'une offre par voie électronique.

6. Le choix par le fournisseur du support (électronique ou papier) de présentation des candidatures et des offres est libre. Mais ce choix est définitif pour la consultation concernée.

7. La PRM ne peut pas interdire la réception d'offres électroniques à compter du 1er janvier 2005.

8. La PRM ne peut pas rendre obligatoire le recours à une procédure dématérialisée. Pour éviter une distorsion de concurrence, les deux supports, papier et électronique, sont autorisés pour une procédure. La PRM reste dans l'obligation de traiter la procédure de façon bi-modale (certaines candidatures et/ou offres sur support papier, d'autres sur support électronique).

2.1 Problématique de la sécurisation : identifiant et mot de passe

Il existe une gradation dans la sécurisation des systèmes informatiques en fonction des objectifs de sécurité nécessaires. La sécurité se décompose en trois volets :

- la disponibilité du système ;
- la confidentialité des données qu'il contient ;
- la capacité du système à conserver son intégrité.

Les considérations qui suivent traitent de l'intégrité et de la confidentialité.

Plusieurs systèmes existent :

Certains systèmes ne demandent pas aux utilisateurs d'identification préalable à leur accès (sites Internet tous publics).

Pour l'accès à d'autres systèmes (Extranet, certains Intranet, sites de travail interactifs), l'identification et l'authentification sont partagées : le système est accessible par un identifiant et un mot de passe partagés par un groupe d'utilisateurs. Dans ce genre de système, il n'y a en pratique ni identification ni authentification individuelle des utilisateurs, encore moins de preuve d'accès ou d'absence d'accès. En cas de perte d'intégrité du système, il n'est pas possible de remonter aux auteurs possibles de l'infraction.

Le dernier mode d'accès repose sur un couple identifiant / mot de passe spécifique d'un utilisateur. Dans ce cas, il est possible d'identifier l'utilisateur, de l'authentifier (être sûr que c'est lui), de prouver qu'il a réalisé telle ou telle transaction, etc... Attention : malgré l'utilisation d'un identifiant / mot de passe pour accéder à son système de messagerie, cela ne suffit pas à identifier l'émetteur d'un message à coup sûr. Il en est de même pour l'identification des auteurs de documents bureautiques. Dans ces 2 cas (messagerie, bureautique), la sécurisation passe par l'utilisation de certificats numériques.

² L'article 1316-1 du Code Civil est un article introduit par la loi n°2000-230 du 13 mars 2000 (voir Annexe n°1).

Par ailleurs, la délivrance d'un identifiant et d'un mot de passe pour un système suppose que l'utilisateur soit déclaré avant qu'il puisse utiliser le système en question. Sur Internet, se pose la question de pouvoir faire confiance *a priori* à un utilisateur donné avant de le connaître. Dans ce cas également, la solution passe par l'utilisation de certificats numériques.

2.2 Problématique de la sécurisation : certificats et signatures

La signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. C'est donc la combinaison d'un dispositif technique et d'un dispositif organisationnel qui permet d'assurer la validité de la signature d'un message, d'un document ou d'une transaction.

La signature électronique est un procédé ayant une double fonction :

- servir à identifier le signataire ;
- manifester la volonté d'adhésion de celui-ci à l'acte signé.

Ce dispositif doit être en place chez les candidats qui souhaitent envoyer leurs candidatures et leurs offres par voie électronique. Il peut l'être dans les services acheteurs si ceux-ci souhaitent signer électroniquement certains documents ou pour assurer la sécurité de la gestion des documents utiles à la procédure d'achat public.

La capacité à signer électroniquement repose sur l'utilisation d'un certificat et de logiciels spécifiques de l'objet informatique que l'on souhaite signer (message, fichier Word³, fichier Acrobat, plan, etc...).

Un certificat est délivré par une autorité de certification qui assure le lien entre le signataire et le certificat, par exemple par l'examen de pièces d'identité et une rencontre en face-à-face. Sa durée de validité est habituellement de deux ou trois ans.

Le chiffrement ou la cryptographie est un procédé qui permet de rendre inintelligible un message ou un document pour un tiers. Le but recherché est la garantie de confidentialité d'un message. La cryptographie peut être utilisée par différents moyens : les certificats électroniques permettent de chiffrer (ou « crypter », selon un anglicisme couramment utilisé) un document ou un courrier électronique, le protocole http/ssl permet de chiffrer un échange.

La signature électronique est plus sûre que la signature manuscrite puisqu'elle peut être vérifiée à tout moment par le destinataire du document signé.

Du point de vue juridique, on distingue deux types de signature : la signature simple et la signature sécurisée. Les dispositifs techniques peuvent être identiques. Dans le cas de la signature sécurisée, le dispositif de signature a fait l'objet d'une certification par un organisme agréé.

La signature électronique sécurisée ou qualifiée (SEQ) bénéficie d'une présomption de fiabilité en justice, ce qui signifie que la charge de la preuve revient à l'organisme qui conteste la signature tandis que, dans le cas de la signature simple, la charge de la preuve de la validité de la signature revient au signataire. Des autorités de certification françaises proposant des certificats qualifiés devraient être disponibles dès 2004.

La sauvegarde de documents signés ne pose pas de problème différent de celui de la sauvegarde de fichiers informatiques.

2.2.1 Familles de Certificats

Une famille de certificat correspond à une Politique de Certification, c'est à dire des pratiques : pratiques d'enregistrement, de validation, d'usage, responsabilités... On définit une nouvelle famille de certificats dès lors que l'on modifie un de ses éléments, ex : pratique de distribution.

L'Agence pour le Développement de l'Administration Electronique (www.adae.pm.gouv.fr) référence un certain nombre de familles de certificats (par le passage d'un audit). Ce référencement est utilisable par toute entreprise qui le souhaite.

La liste des familles de certificats⁴ référencées par le Ministère de l'Economie, des Finances et de l'Industrie, est accessible par votre navigateur :

http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm

Pour reconnaître un certificat de signature électronique, les logiciels doivent en être techniquement capables (exemples : navigateurs, applets spécifiques, clients de messagerie, Adobe, Microsoft Office...).

Un certificat⁵ est attribué à un individu (personne physique représentant une personne morale) ; il n'existe pas de certificat pour un groupe de personnes. Il faut prévoir un délai global de un à trois mois environ pour l'ensemble des démarches internes et externes permettant l'obtention d'un premier certificat.

Les certificats se présentent sur différents supports :

- soit fixe sur disque dur ;
- soit mobile sur autre support matériel (carte magnétique ou clé USB), ...

2.2.2 Utilisation des certificats pour la signature

L'autorité de certification délivre à l'utilisateur une clé privée, une clé publique et un certificat (qui contient la description de son identité, la clé publique et la même clé publique signée par l'autorité de certification).

La signature d'un document est réalisée par l'application de la clé privée au document avec l'aide d'un algorithme, qui produit une empreinte liée à la fois au document et au signataire. Le signataire envoie le document original, son empreinte et son certificat au destinataire qui peut ainsi vérifier l'authenticité du document. La signature électronique n'est donc pas détachable du document, contrairement à la signature manuelle. La clé privée ne circule jamais.

³ Les marques et produits cités dans ce guide le sont uniquement à titre illustratif et ne sont aucunement des recommandations d'utilisation, implicites ou explicites.

⁴ La liste des familles de certificat que vous reconnaissez dans Internet Explorer est accessible ainsi dans la version 6 : faire Outils / Options Internet / Contenu / Certificats / Autorités principales de confiance.

⁵ En janvier 2004, le coût moyen d'un certificat s'établit environ à 40 - 60 € pour une période de 2 à 3 ans.

Le candidat adresse son dossier signé. Le dossier contient la candidature et l'offre (dans le cas d'un appel d'offres ouvert).

Le dossier de candidature et l'offre sont signés séparément. Pour pouvoir profiter du délai d'au plus vingt quatre heures mentionné dans l'article 4 du décret n°2002-692 du 30 avril 2002, le dispositif de signature doit permettre de dissocier le dossier et son empreinte résultant de l'application de la clé privée. L'empreinte et le dossier sont envoyés séparément. La date d'arrivée de l'empreinte fait foi pour le respect du délai de réception des offres.

Dans le cas d'un envoi séparé de l'empreinte et du document signé, celui-ci ne peut en aucun cas être modifié pendant l'intervalle séparant les deux envois car l'empreinte envoyée préalablement ne serait plus valable et le dépôt serait refusé.

La clé privée peut servir à signer autant de documents que nécessaire.

2.2.3 Chiffrement (ou cryptage)

Sur un message chiffré porteur de virus, le traitement antivirus est inefficace. Pour ce motif, les auteurs du guide ne retiennent pas le chiffrement pour le dépôt des plis.

Pour assurer la confidentialité des offres, le dépôt des plis est effectué sous le protocole https (=http/ssl). Ce protocole est mis en œuvre par le site de la personne publique ; il constitue le moyen le plus fiable d'assurer la sécurité des échanges de documents (cette solution est celle retenue par le Ministère de la Défense dans le cadre de la dématérialisation de ses marchés).

2.3 Horodatage

Un horodatage est un système qui permet de dater les actions ou les événements ; le but est de tracer les accès, mouvements, créations, modifications ou destructions de documents. Un relevé horodaté ou « journal des événements » demeure indispensable afin de garantir la traçabilité tant en ce qui concerne la publication et le téléchargement des DCE que la

Le CMP n'a pas prévu d'obligation de certification de l'horodatage, ce qui ne dispense pas l'acheteur public de l'obligation de veiller à la conformité des informations du système.

Aucune obligation n'existe sur la date de signature d'un document : seul le respect de la date de réception dans les délais prévus dans l'AAPC importe (article 58 du CMP).

2.4 Enchères électroniques inversées

Pour la méthode des enchères électroniques inversées, le prix constitue le plus souvent le seul critère déterminant de l'offre (recherche des offres au prix le plus faible, indépendamment de tout autre critère) : ceci peut alors théoriquement s'appliquer aux achats de médicaments, par exemple dans le cas des génériques. Il est également possible de faire des enchères sur la base d'une combinaison du prix et de critères qualitatifs.

La notion d'enchères électroniques n'est donc pas à rejeter même si son utilisation semble a priori non généralisable à toutes les fournitures hospitalières et requiert une recherche de soumissionnaires potentiels efficiente.

2.5 Echange de données informatisé (EDI)

Cet outil de travail technique, simple et pratique pour les acheteurs publics est maintenant de plus en plus utilisé dans les établissements de santé pour la fonction « commande » de médicaments, un peu moins pour les dispositifs médicaux en raison de l'absence de codification unique.

L'envoi de factures dématérialisées est également (à la fois techniquement et réglementairement) possible : ceci n'est cependant réellement intéressant que lorsque l'intégration de ces données dans les outils informatiques hospitaliers de gestion peut se faire.

2.6 Utilisation de portails

C'est par un système de mots de passe ou de fiches d'identification renseignées que le fournisseur récupère par téléchargement le dossier de consultation des entreprises. Il en est de même pour la PRM qui a accès à la liste des fournisseurs identifiés.

A ce jour, seulement quelques entreprises spécialisées occupent ce secteur d'activité des procédures dématérialisées des marchés, offrant des niveaux de garantie variables selon le coût de la prestation.

A terme, il pourrait être envisagé l'utilisation de portails spécifiques hospitaliers, comme le portail envisagé aujourd'hui par un groupement de Centres hospitaliers universitaires pour la dématérialisation des procédures.

2.7 Archivage

Les règles générales de l'archivage des documents électroniques sont les mêmes que celles s'appliquant aux documents papier (voir en Annexe 2). Le décret n°2002-692 du 30 avril 2002 pose toutefois des règles particulières dont il convient de tirer les conséquences pour l'archivage des documents issus d'une procédure dématérialisée. Les règles principales sont les suivantes :

2.7.1 Que faut-il archiver ?

- Candidatures non retenues : celles ci sont archivées et les offres correspondantes sont éliminées ; l'établissement doit seulement garder la preuve de cette opération,
- Candidatures et offres retenues : celles ci sont archivées et sont des éléments constitutifs d'un marché conclu ; l'archivage ne semble pas poser de problème particulier par rapport à l'archivage classique connu aujourd'hui,
- Candidatures retenues / Offres non retenues : celles ci sont archivées.

2.7.2 Sur quel support ?

Un archivage sous forme d'un CEDEROM ou sur le serveur de l'établissement de toutes les données concernant une procédure (journal des évènements, ensemble des offres, conclusions, etc...) semble suffisant. Cet archivage est alors effectué à la fin de la procédure et reflète notamment le contenu exact des fichiers lors de la CAO d'ouverture des plis, sous réserve de procéder à la suppression des « enveloppes n°2 » d'offres non admises.

2.7.3 Durée d'archivage

La durée de l'archivage (cf. annexe 2) peut être relativement courte si on n'envisage que la notion de recours de candidats non retenus, ou beaucoup plus longue au regard du contrôle des marchés (délai de contrôles possibles de la Cour des Comptes, Inspection Générale des Affaires Sociales ou IGAS, Mission Interministérielle d'Enquête sur les Marchés ou MIEM, enquête rétrospective de la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes ou DGCCRF sur les offres reçues en provenance d'une entreprise donnée ou sur des fournitures particulières) ou toute autre action menée par un pouvoir judiciaire.

2.8 Virus et antivirus

Pour mettre au point l'organisation permettant de se prémunir des virus, il est important de faire appel à une compétence informatique et de former les utilisateurs.

2.8.1 Virus

Par commodité, nous désignerons par virus tout programme s'exécutant et se propageant à l'insu de l'utilisateur d'une machine. Techniquement, il existe différents types de programmes en fonction du type de fichier infecté, du mode de propagation, des effets du programme (virus, ver, troyen, etc...). En pratique, les virus combinent maintenant ces différentes caractéristiques.

Les virus sont le plus souvent transmis par des programmes ou des messages ; ils peuvent être également transmis par des documents contenant des macros.

Un virus est un programme qui a trois caractéristiques :

- ✓ Il s'exécute à l'occasion de l'exécution d'un autre programme (par exemple, quand vous ouvrez un message ou une pièce jointe)
- ✓ Il se propage en infectant (en « se collant à ») d'autres programmes ou en envoyant des messages
- ✓ Il réalise des actions spécifiques.

Un fichier contenant un virus peut être obtenu initialement par messagerie, téléchargement, lecture d'un support amovible (disquette), connexion à un poste de travail ou à un serveur infecté.

Le mode de propagation d'un virus peut être :

- ✓ par exploration de votre carnet d'adresses de messagerie ou d'un annuaire
- ✓ par création aléatoire d'adresses de messagerie sur un modèle donné (ex prénom.nom@gouv.fr)

- ✓ par utilisation d'adresses récupérées sur un site web
- ✓ par exploration de votre disque dur ou de tout support de fichiers (disquette, clé USB, ...)
- ✓ par transmission entre utilisateurs de supports contenant des virus (disquette, clé USB, ...)
- ✓ par exploration du réseau auquel vous êtes connecté (serveur bureautique par exemple).

Les actions d'un virus peuvent être :

- ✓ rien d'autre que sa propagation
- ✓ l'affichage de messages (par exemple, politiques)
- ✓ la collecte d'adresses mail afin de leur envoyer des courriers électroniques de masse (spam)
- ✓ l'exploitation de failles de sécurité d'un ou plusieurs logiciels présents sur votre ordinateur
- ✓ l'installation d'un programme permettant à un autre utilisateur de se servir de votre ordinateur (par exemple pour attaquer un site web par déni de service)
- ✓ la transmission sur internet de tout ou partie de fichiers trouvés sur un disque
- ✓ la modification de fichiers
- ✓ la destruction de fichiers
- ✓ de rendre un ordinateur inopérant.

Ces trois derniers cas sont rares.

Enfin, les effets supplémentaires d'un virus sont liés à ses effets de masse :

- ✓ privation de ressources informatiques
- ✓ engorgement de la bande passante d'un réseau, voire d'une partie de l'internet
- ✓ allongement des temps de traitement.

2.8.2 Antivirus

La principale défense contre les virus est l'installation préventive et l'utilisation permanente d'un antivirus appliqué à tous les types de fichiers.

Un antivirus est un programme qui peut :

- ✓ détecter la présence d'un virus dans un fichier
- ✓ détecter l'activité d'un virus
- ✓ réparer les fichiers infectés
- ✓ transférer les fichiers infectés sur un support donné
- ✓ détruire les fichiers infectés.

Un antivirus peut/doit être installé sur plusieurs machines : le poste de travail de l'utilisateur, le serveur pare-feu entre l'entreprise et l'internet, le serveur de messagerie pour les messages circulant entre l'entreprise et l'internet, voire pour les messages internes à l'entreprise, les serveurs web.

Comme tout programme, un antivirus est disponible en versions successives, mais repose également sur un fichier de signatures, ces signatures caractérisant les virus qu'il cherche à détecter. Pour un antivirus donné, le nombre de signatures se compte en dizaines de milliers.

Pour chaque nouveau virus, le fichier de signatures ou l'antivirus lui-même doivent être mis à jour. Un virus peut être développé pour une cible précise et ne sera donc pas connu tant que la cible ne l'aura pas détecté.

Tous les éditeurs d'antivirus ne réagissent pas dans les mêmes délais et tous les utilisateurs ne mettent pas à jour leur antivirus immédiatement.

La réparation d'un fichier infecté par un virus peut fonctionner ou non ; si elle fonctionne, on peut récupérer tout ou partie du fichier initial.

2.8.3 Conséquences pour les échanges de documents par une plate-forme de dématérialisation

Un fichier Zip® est le résultat de la compression d'un ou plusieurs autres fichiers. Il existe un certain nombre de virus qui reposent sur l'utilisation du format Zip®. Ces virus fonctionnent non pas en infectant des fichiers Zip®, mais en se cachant à l'intérieur au même titre qu'un autre fichier. Le format Zip® est ainsi utilisé pour propager le virus mais ne déclenche pas son exécution. Les antivirus sont en train de s'adapter à cette nouvelle forme de transmission.

Les épidémies de virus Word® ou Excel® datent de la fin des années 1990. Une résurgence reste possible, mais ce n'est clairement pas ce genre de virus qui défrayent ces derniers jours la chronique.

La possibilité théorique de l'infection de fichiers pdf a été démontrée en 2001. Ceci était rendu possible dans la version 5.0.5 d'Acrobat® ; cette version peut être corrigée et de toutes façons cette vulnérabilité n'existe plus dans Acrobat 6®. *A priori*, un fichier pdf ne sera donc pas infecté.

L'infection d'autres documents, aux formats moins répandus, est peu probable car ils n'ont pas le nombre critique d'utilisateurs qui rend l'opération intéressante pour les créateurs de virus, comparée à la propagation de virus par la messagerie.

3 Environnement réglementaire

L'article 56 du CMP (cf. annexe 1), relatif à la dématérialisation, précise que les candidatures et les offres peuvent être communiquées à la personne publique par voie électronique, sans que cette dernière ne puisse l'interdire à compter du 1^{er} janvier 2005⁶.

Deux décrets d'application relatifs à la dématérialisation ont été publiés au Journal officiel.

Il s'agit :

- du décret n°2001-846 du 18 septembre 2001, relatif aux conditions dans lesquelles des enchères électroniques sont organisées pour l'achat de fournitures courantes,
- du décret n°2002-692 du 30 avril 2002, précisant les modalités de mise à disposition des entreprises par voie électronique du règlement de la consultation, de la lettre de consultation, des cahiers des charges, des documents et des renseignements complémentaires, ainsi que les modalités de transmission par voie électronique à la personne publique des candidatures et des offres.

⁶ L'obligation de réception des candidatures et des offres ne s'applique pas aux procédures de passation des marchés selon la procédure adaptée de l'article 28-I du CMP.

4 L'AAPC, le règlement de consultation et la lettre de consultation dans une procédure d'achat public dématérialisée.

La mise en œuvre d'une procédure d'achat dématérialisée suppose préalablement une information des soumissionnaires potentiels. Cette information a notamment pour objet d'indiquer les modalités d'accès aux documents dématérialisés mis à disposition par la personne publique, ainsi que les modalités de transmission des candidatures et des offres dématérialisées par les soumissionnaires.

Le décret du 30 avril 2002 en indique certaines que la personne publique doit mentionner dans l'AAPC, le règlement de consultation ou la lettre de consultation.

4.1 L'AAPC

Le 1^{er} alinéa de l'article 2 du décret n° 2002-692 du 30 avril 2002 relatif à la dématérialisation indique que l'AAPC précise les modalités d'accès aux documents mentionnés ci-dessus.

Les informations suivantes doivent figurer dans l'AAPC :

- Mention de l'acceptation ou refus par la personne publique de la transmission des candidatures et des offres par voie électronique (jusqu'au 31 décembre 2004)⁷;
- Définition des modalités d'accès au réseau informatique en précisant clairement l'adresse Internet où télécharger le DCE permettant aux personnes intéressées et aux candidats de consulter et de télécharger les différents documents (RC, cahier des charges, documents et renseignements complémentaires) ;
- Définition des modalités de transmission par voie électronique des candidatures et des offres à la personne publique ;
- Mention, le cas échéant, que la lettre de consultation (AO restreint, dialogue compétitif et procédure négociée, procédure adaptée) est transmise par voie électronique ;
- Mention de l'autorisation de transmettre une offre sous la forme d'un double envoi électronique pour la transmission de documents volumineux ; cette mention précise le délai supplémentaire accordé aux candidats s'écoulant entre la réception de la signature électronique sécurisée (impérativement avant la limite fixée dans l'AAPC) et la réception de l'offre. Ce délai ne peut pas excéder vingt-quatre heures ;
- Mention de la possibilité pour un fournisseur de se faire adresser sur demande écrite les documents du DCE par voie postale, s'il ne choisit pas la voie électronique ;
- Mention de l'obligation pour le fournisseur de laisser ses coordonnées précises et complètes lors du téléchargement du dossier de consultation, celles-ci permettant en cas de besoin, d'adresser des éléments complémentaires ;
- Mention de l'obligation pour le fournisseur d'accuser réception à la personne responsable du marché (PRM), l'accusé de réception indiquant la totalité et la bonne réussite du téléchargement du dossier.

NB : si certains des items ci-dessus ne figurent pas dans l'AAPC, ils doivent obligatoirement figurer dans le RC. Le règlement de la consultation doit pouvoir être consulté et archivé par les personnes intéressées sans condition, notamment d'identification.

⁷ A compter du 1^{er} janvier 2005, la personne publique ne pourra plus interdire la transmission des candidatures et des offres par voie électronique.

La personne publique doit rendre certaine la date d'envoi de l'AAPC à la publication (BOAMP et éventuellement JOUE).

Pour le BOAMP, une saisie en ligne est possible sur <http://boamp.journal-officiel.gouv.fr/> avec confidentialité des données garanties puisque gérées dans un compte personnel protégé par mot de passe.

Pour le JOUE, l'ensemble des formulaires européens ayant trait aux marchés publics est téléchargeable à l'adresse : <http://simap.eu.int/FR/pub/src/formsOJS.htm>

Le BOAMP propose une rédaction directe dématérialisée sur son site. Ceci a pour avantage de mettre à la disposition du rédacteur un support modélisé et d'optimiser les délais de transmission puisque cette dernière est de fait immédiate.

Dans le cas où la personne publique décide de mettre le DCE à disposition des personnes intéressées sur un réseau informatique, les modalités de téléchargement de ces documents doivent être clairement indiquées dans l'AAPC.

4.2 Le règlement de consultation

Ce chapitre traite des éléments complémentaires ayant trait à la dématérialisation dans le modèle type du RC figurant dans le « Guide d'approvisionnement des médicaments, des dispositifs médicaux et autres produits du domaine pharmaceutique » GPEM/SL octobre 2002. A titre d'exemple quelques points sont suggérés ci dessous, à adapter à chaque cas :

4.2.1 Article « Modalités de la consultation »

« En application de l'article 56 du CMP et du décret n° 2002-692 du 30 avril 2002, en complément aux modalités classiques de déroulement de la consultation, les soumissionnaires auront la possibilité de télécharger le Dossier de Consultation des Entreprises (DCE) dans son intégralité et de répondre via le site dont l'adresse Internet est www..... »

Afin de pouvoir décompresser et lire les documents mis à disposition par la personne publique, les soumissionnaires devront disposer des logiciels permettant de lire les formats suivants : Adobe® Acrobat® (.pdf), et/ou Rich Text Format (.rtf), et/ou les fichiers compressés au format Zip® (.zip). La liste des formats acceptés doit être précisée.

Les soumissionnaires souhaitant répondre sous forme dématérialisée devront tenir compte des indications suivantes, afin de garantir au mieux le bon déroulement de cette procédure dématérialisée ».

Le service acheteur devra, d'une part, préciser dans le règlement de consultation la ou les familles de certificats qui doivent être employées par le soumissionnaire et, d'autre part, indiquer sur son site l'autorité de certification qu'il utilise.

Dans le choix des formats demandés pour la réponse (à préciser), il revient à la personne publique de s'assurer que ceux-ci sont suffisamment diffusés auprès du public intéressé de manière à respecter les principes de liberté d'accès à la commande publique et d'égalité de traitement des candidats, d'une part, et que ce choix ne favorise pas un éditeur particulier, d'autre part.

« *Le soumissionnaire :*

- *ne doit pas utiliser certains formats, notamment les ".exe" ou autres exécutables ;*
- *ne doit pas utiliser certains outils, notamment les "macros" ;*
- *ne doit pas chiffrer (= crypter) sa candidature et son offre ;*
- *doit faire en sorte que sa candidature et/ou son offre ne soient pas trop volumineuses [l'indication, si nécessaire, d'un volume maximum est recommandée] ;*
- *doit renseigner lors du téléchargement du DCE, le nom du soumissionnaire, une adresse électronique ainsi que le nom d'un correspondant afin qu'il puisse bénéficier, en tant que de besoin, de toutes les informations complémentaires diffusées lors du déroulement de la présente consultation, en particulier les éventuelles précisions.*

De plus, il est précisé que le retrait des documents électroniques n'oblige pas le soumissionnaire à déposer électroniquement son offre ».

NB : La personne publique doit mettre en place une organisation interne rendant impossible toute modification des documents « mis en ligne » après validation du dossier par la PRM.

NB : les auteurs du guide recommandent pour les échanges de documents, l'utilisation de formats réputés les moins sensibles aux virus.

4.2.2 Article « Présentation des offres »

« *Les candidats doivent choisir entre :*

- *soit la transmission électronique de leurs candidatures et de leurs offres ;*
- *soit leur envoi sur un support papier.*

Ils ne peuvent en aucun cas utiliser conjointement, dans le cadre d'une même consultation, ces deux modes de transmission sous peine de rejet des deux réponses⁸.

Dans le cas d'une transmission par voie électronique, le dossier constitué des deux enveloppes (candidature et offre) est substitué par l'envoi de fichiers informatisés reprenant les mêmes éléments et scindés en deux fichiers ou deux groupes de fichiers permettant d'ouvrir individuellement et de façon chronologique la partie candidature et la partie offre.

Les candidatures et les offres doivent être transmises dans des conditions qui permettent d'authentifier la signature de la personne habilitée à engager l'entreprise selon les exigences posées aux articles 1316 à 1316-4 du code civil (alinéa 2 de l'article 3 du décret du 30 avril 2002) ».

4.2.3 Article « Conditions d'envoi ou de remise des offres »

« En application de l'article 56 du CMP et du décret 2002-692 du 30 avril 2002, les candidats peuvent remettre candidature et offre de façon dématérialisée sur le site précisé à l'article n°... du présent RC.

⁸ Une transmission par voie électronique n'exclut toutefois pas la possibilité pour la personne publique d'exiger que les offres soient accompagnées d'échantillons conformément à l'article 49 du CMP. Dans ce cas, les modalités de transmission et de réception des échantillons doivent être mentionnées dans l'AAPC.

** Présentation de la procédure dématérialisée d'envoi des offres :*

Le dossier à remettre par le candidat doit être constitué de documents réalisés avec des outils bureautiques (correspondants au descriptif de l'article).

Ce dossier dématérialisé doit contenir :

- 1. un fichier CANDIDATURE contenant les justificatifs à produire quant aux qualités et capacités du candidat : cf. article...*
- 2. un fichier OFFRE contenant les documents relatifs à l'offre du candidat : cf. article*

** Modalités d'envoi des candidatures et des offres :*

La procédure de dépôt de pli est détaillée sur le site (adresse électronique).

Schématiquement, le soumissionnaire :

constitue son pli,

le date,

le signe,

le dépose sur le site dédié.

Les échanges sont sécurisés grâce à l'utilisation du protocole https.

** Avertissements :*

*Tout fichier constitutif de la candidature ou de l'offre, sera traité préalablement par le soumissionnaire par un anti-virus régulièrement mis à jour. **Conformément au décret du 30 avril 2002, tout fichier contenant un virus est réputé n'avoir jamais été reçu.***

Pour que le soumissionnaire puisse procéder à la signature de ses documents, il doit disposer ::

- d'un navigateur web internet (à préciser),

- d'un outil de signature.

Le candidat transmet ses fichiers informatisés de façon à différencier sa candidature et son offre ».

Par rapport à la date et à l'heure limite de dépôt des dossiers et afin de prendre en considération les aléas dans la transmission électronique, l'acheteur public précisera si les candidats disposent d'un délai supplémentaire entre la transmission de la signature et la fin de la transmission de l'offre sous forme électronique (art. 4 du décret n°2002-692 du 30 avril 2002).

Les auteurs du guide recommandent aux acheteurs publics de prévoir dans leur règlement de consultation l'interdiction de chiffrement (ou « cryptage ») des dossiers de réponse des soumissionnaires (cf. § 5.3.1.).

4.3 La lettre de consultation

Elle ne concerne que les procédures d'appel d'offres restreint, les procédures négociées et éventuellement les marchés passés selon une procédure adaptée.

S'agissant des marchés négociés sans publicité préalable, la lettre de consultation doit mentionner les informations minimales prévues dans le CMP.

La lettre de consultation peut être envoyée par voie électronique aux candidats sélectionnés. L'envoi de la lettre de consultation habilite les candidats sélectionnés à consulter, à télécharger et à archiver le dossier de la consultation (cahier des charges, documents et renseignements complémentaires, etc.).

5 Etapes d'une procédure d'achat public dématérialisée

La procédure d'achat dématérialisée décrite ci-après est celle d'un appel d'offres ouvert. Les autres procédures ne seront évoquées que pour leurs particularités propres.

Trois préalables sont nécessaires et indispensables avant tout commencement d'une procédure d'achat public dématérialisée :

1 – la mise en place et l'officialisation d'une organisation de la fonction achat au sein de l'établissement public de santé (EPS) pour déterminer les responsabilités et délégations de chaque intervenant. Ceci s'exprime, notamment, dans l'attribution de signature électronique (une seule ou plus si plusieurs PRM et/ou présidents de CAO, les procédures de délégation pour certains actes, ...), la gestion des certificats et leur actualisation ;

2 – l'obtention de ces mêmes certificats auprès d'un organisme certificateur, démarche pouvant nécessiter globalement un à trois mois, en incluant les démarches internes de l'administration ;

3 – la mise en place de toute l'infrastructure informatique nécessaire : en fonction des possibilités et des choix de l'EPS, celui-ci peut faire appel aux services d'un prestataire qui assurera tout ou partie des opérations techniques relatives aux procédures d'achat dématérialisées, par exemple, la gestion du séquestre (voir annexe n°3 : Aide à la recherche d'un prestataire).

Il convient de définir et mettre en œuvre un degré de sécurité nécessaire à chacune des étapes afin de garantir :

- l'authentification au moyen de la signature électronique ;
- la stricte confidentialité des informations échangées ;
- la permanence des accès aux services ;
- la sécurité et l'intégrité des informations échangées ;
- l'horodatage des accès et connexions identifiés ;
- l'archivage de tous les échanges.

L'ensemble des actions inhérentes à la procédure d'achat doit être authentifié et tracé. A ce titre, il est fait référence à la mise en place d'un journal des événements retraçant toutes les actions effectuées.

Remarque :

Comme pour toute procédure d'achat (dématérialisée ou non) une attention toute particulière doit être portée sur le calendrier de l'ensemble des étapes dans le but d'assurer une continuité d'approvisionnement.

Le tableau ci-après récapitule les étapes d'une procédure d'appel d'offres en précisant le caractère obligatoire ou facultatif de la dématérialisation :

	Obligatoire	Facultatif
Avis d'appel public à la concurrence : JOUE, BOAMP	X	
Mise en ligne de l'AAPC, du RC et du DCE		X ⁹
Lecture du RC par les personnes intéressées		X ⁹
Téléchargement du DCE et mise à disposition des outils de lecture en libre disposition		X ⁹
Identification des téléchargeurs		X ⁹
Réception des candidatures	X ¹⁰ (01/01/05)	
Réception des offres	X (01/01/05)	
Gestion de l'ouverture des plis : Libération 1 ^{ère} enveloppe, Ouverture 1 ^{ère} enveloppe, Recevabilité candidature, Libération ou destruction 2 ^{ème} enveloppe, Ouverture 2 ^{ème} enveloppe.	X	
Intégration de candidatures et offres papier		X
Analyse des offres/Interface logiciel de gestion des marchés		X
Demande des attestations ou éléments complémentaires		X
Elaboration du marché		X
Envoi contrôle de légalité		X
Notification au fournisseur		X
Information Trésorerie		X
Archivage dynamique de la « procédure », Traçabilité : « journal des événements »	X	
Production d'informations sur les marchés dématérialisés		X
Envoi au JOUE, BOAMP de l'avis d'attribution	BOAMP	JOUE

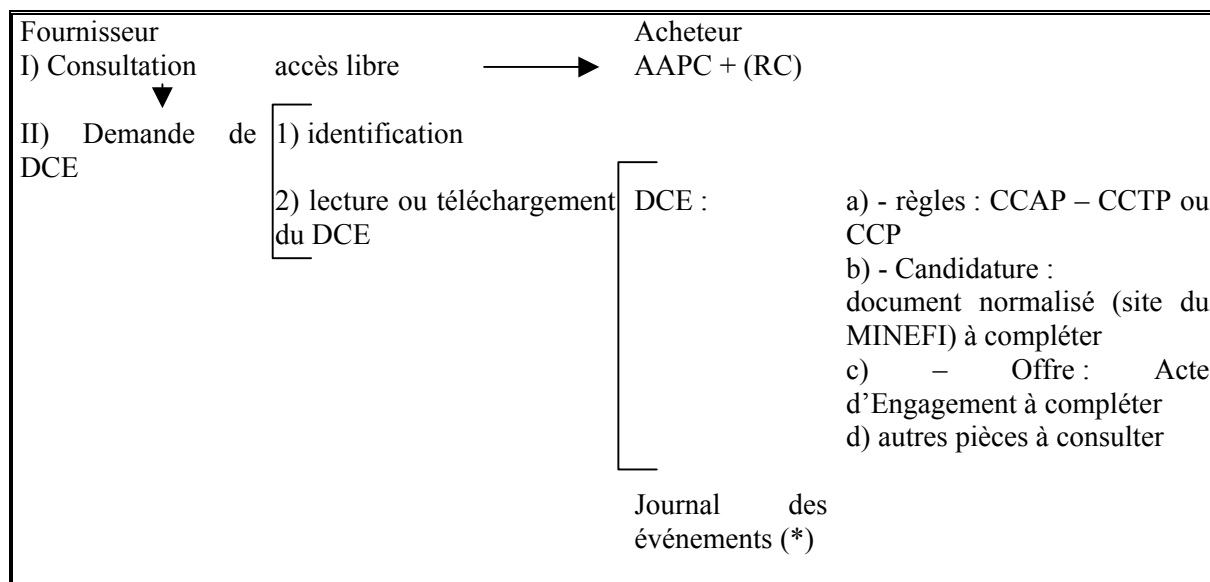
Chacune des phases principales de la procédure est décrite ci-après dans un tableau synthétique suivi d'un développement explicatif.

⁹ Dématérialisation non obligatoire (cf art. 56 du CMP, alinéa 1 : « ... **peuvent** être mis à disposition des entreprises par voie électronique... »), mais fortement recommandée par les auteurs du présent guide, d'autant plus que la réception des candidatures et des offres est obligatoirement dématérialisée (cf note suivante).

¹⁰ cf art. 56 du CMP, alinéa 2 : « ... Aucun avis ne pourra comporter d'interdiction à compter du 1^{er} janvier 2005. »

5.1 Consultation des Avis d'Appel Public à la Concurrence, demande et transmission du Dossier de Consultation des Entreprises

Figure n° 1 : consultation de l'AAPC et du RC et demande du DCE



(*) Le journal des événements comporte une fonction d'horodatage et reçoit : le nom de l'entreprise et de la personne physique qui télécharge les documents, une adresse électronique.

Cette phase correspond à la mise en œuvre des articles 40 et 56 du CMP, c'est à dire la mise à disposition des entreprises du Règlement de la Consultation (RC), de la lettre de consultation, du (ou des) cahier(s) des clauses, des documents et des renseignements complémentaires.

5.1.1 Consultation de l'AAPC et du RC par le fournisseur

La notion de téléchargement rend obligatoire la mise en ligne du DCE sur une plate-forme ou un serveur : un EPS peut avoir développé cette modalité sur son propre site Internet ou, s'il n'en dispose pas, peut négocier son hébergement sur un serveur existant d'un autre établissement ou un prestataire de service spécialisé.

En terme de sécurisation, le niveau requis préférable est celui du format *.pdf ou format équivalent, qui reste difficilement falsifiable.

5.1.2 Demande du DCE

Lorsqu'un fournisseur souhaite être candidat, deux phases préalables se succèdent :

5.1.2.1 Identification

Si le fournisseur souhaite consulter, télécharger et archiver les documents précités, il doit s'identifier auprès de l'acheteur public. Le 2nd alinéa de l'article 2 du décret du 30 avril 2002 indique en effet : « *A cet effet, ils [les personnes intéressées, ici les entreprises] 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* ». Un journal des événements répond à l'obligation de traçabilité qui incombe à l'acheteur public.

5.1.2.2 Lecture ou téléchargement du DCE

Il convient de mettre en place une modalité permettant la remise du DCE contre les renseignements précités. Cela peut être traité par le renseignement d'un formulaire de demande, complété par la personne intéressée, contre lequel est remis au demandeur, par courriel sécurisé, un mot de passe lui donnant accès au téléchargement des documents. Le formulaire de demande comporte *a minima* une adresse électronique par laquelle le demandeur pourra être, le cas échéant, avisé de toute modification ou complément utile ayant trait à la procédure concernée, afin de respecter le principe d'égalité de traitement de tous les candidats potentiels connus.

Le journal des événements comportera l'identité et l'adresse de ceux qui auront téléchargé ces documents, ainsi que les accusés de réception émis par ceux ci, avec mention des horaires correspondants. Cet accusé de réception doit comporter les mêmes éléments que celui par voie postale ; un horodatage est conseillé.

Lorsque le fournisseur s'est identifié, il peut alors télécharger le DCE qui doit contenir au minimum :

- un projet d'Acte d'Engagement (AE) ;
- un Cahier des Clauses Administratives Particulières (CCAP) ;
- un Cahier des Clauses Techniques Particulières (CCTP) ;
- ou un Cahier des Clauses Particulières (CCP), regroupant les deux précédents.

Afin de faciliter l'exploitation des fichiers informatiques, l'assemblage de ces pièces peut être envisagé de la façon suivante :

- en premier lieu, celles qui servent de cadre à l'établissement de l'offre : (CCAP + CCTP) ou CCP ;
- En second lieu, des pièces-type qui permettront de formaliser les candidatures sur un modèle issu du site du MINEFI ;
- Enfin, l'offre qui se présente sous la forme d'un AE sur un modèle issu du site du MINEFI à compléter par le fournisseur et les différentes pièces qui peuvent l'accompagner (tableaux d'offres de prix type CIP, documents techniques demandés ...).

Avant mise en ligne du DCE, un traitement antivirus est nécessaire.

Afin d'obtenir une offre complète et conforme aux attentes de la PRM, les documents administratifs nécessaires aux réponses (« fichier-enveloppe » n°1 + « fichier-enveloppe » n°2) peuvent au choix :

- être téléchargés sur le site du MINEFI (<http://www.minefi.gouv.fr/formulaires/daj:htm>).
- être fournis pré-remplis par l'établissement et téléchargeables en même temps que le DCE sur la même adresse que celle permettant l'obtention du DCE : le candidat n'aura ainsi à renseigner que les parties le concernant,
- être ceux du fournisseur, dûment complétés.

5.2 Envoi de l'offre

Les candidats doivent choisir :

soit de transmettre par voie électronique leurs candidatures et leurs offres,
soit de transmettre leur dossier sur support papier ou le cas échéant sur support physique électronique.

Ils ne peuvent en aucun cas utiliser conjointement, dans le cadre d'une même consultation, ces deux modes de transmission sous peine de rejet des deux réponses.

Dans le cas d'une transmission par voie électronique, la totalité des frais d'accès au réseau informatique et des frais pour le recours à la signature électronique est à la charge du candidat.

La transmission dématérialisée d'une offre se fonde sur le 2^{ème} alinéa de l'article 56 du CMP. Sa mise en œuvre est prévue par les articles 3 et suivants du décret n°2002-692 du 30 avril 2002. Pour mémoire, l'AAPC doit mentionner les modalités de transmission des plis dématérialisés.

Les candidats doivent se soumettre aux obligations suivantes :

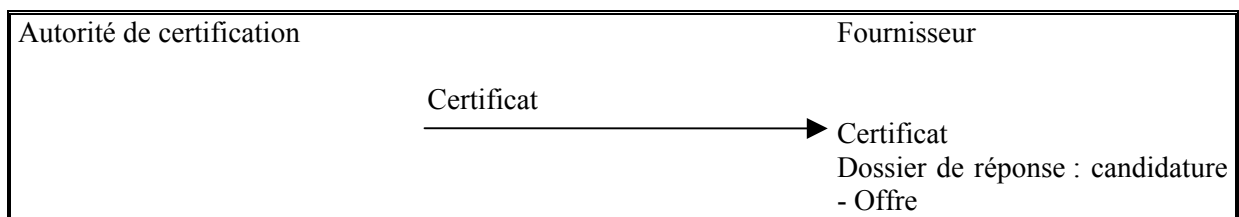
- désigner la personne habilitée à les représenter ;
- mettre en place une procédure permettant à la PRM de s'assurer que c'est bien la personne habilitée qui signe et transmet les candidatures et les offres (authentification de la signature électronique) ;
- transmettre par voie électronique, dans le cas où ils ont choisi cette solution, l'intégralité des documents demandés par la personne publique dans le DCE (dossier de candidature, dossier offre, documents ou informations techniques demandés à l'appui de la candidature, ...).

Trois étapes peuvent être identifiées :

- 1) Le candidat doit se procurer les moyens électroniques pour authentifier la signature de son offre dématérialisée,
- 2) Le candidat envoie son offre à l'acheteur public,
- 3) L'acheteur public doit réceptionner cette offre.

5.2.1 Délivrance du certificat de signature électronique

Figure n° 2 : délivrance du certificat de signature



L'authentification de la signature résulte de l'utilisation d'un certificat délivré par une autorité de certification¹⁰. Ce certificat accompagnera le dossier de réponse qui, conformément à l'art. 57-III du CMP sera composé d'une candidature et d'une offre distinctes.

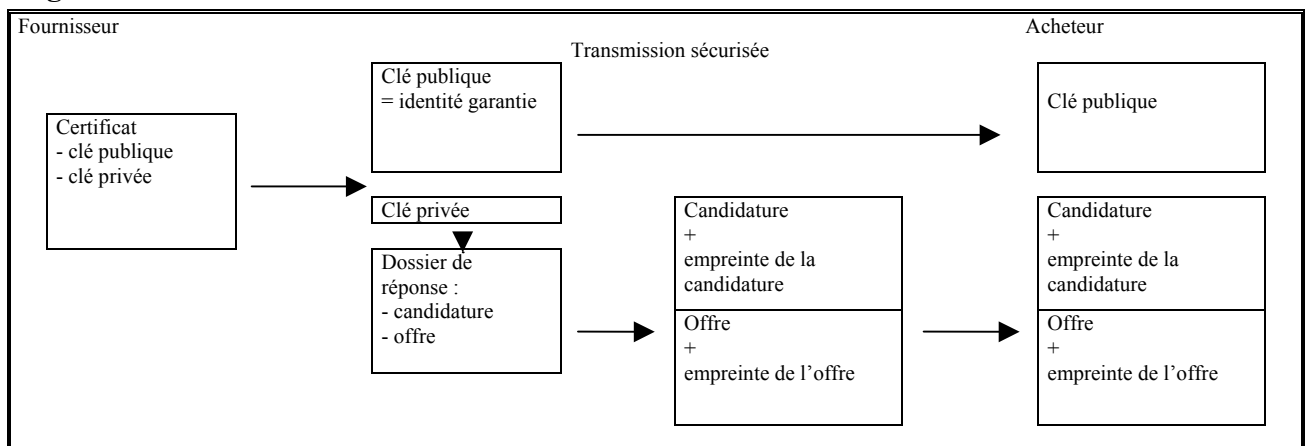
5.2.2 Envoi de la candidature et de l'offre

Le fournisseur dispose d'un certificat qui comprend la clé publique, qui correspond à sa clé privée.

La clé publique transmise à l'acheteur public dans le certificat permettra à ce dernier de vérifier l'identité du fournisseur et l'authenticité de la candidature et de l'offre. Il incombera donc à l'acheteur de vérifier que le certificat n'est pas révoqué et qu'il est valide au regard de la capacité nécessaire pour conclure le marché public en cours de passation.

La clé privée qui reste chez le fournisseur lui permet de créer une empreinte d'un document. Dans le cadre d'un AO ouvert, deux empreintes, l'une pour la candidature, l'autre pour l'offre, seront envoyées simultanément à l'acheteur public.

Figure n° 3 : envoi de la candidature et de l'offre



¹⁰ Les candidats s'assurent que le coût de la vérification est compris dans la prestation d'obtention du certificat.

Il est fortement conseillé qu'avant tout envoi par voie électronique, les fichiers constitutifs de la candidature ou de l'offre, soient traités préalablement par le soumissionnaire par un anti-virus régulièrement mis à jour. Conformément au décret n°2002-692 du 30 avril 2002, tout fichier contenant un virus est réputé n'avoir jamais été reçu.

L'offre du candidat n'est pas chiffrée (= cryptée).

La réponse du candidat comportera plusieurs items :

- le certificat, avec la clé publique (à noter que l'autorité de certification doit être reconnue par le site acheteur : la liste des autorités de certification reconnues figure dans le règlement de consultation cf. 4.2.1).
- la candidature, authentifiée par rapprochement avec la clé publique et associée à son empreinte ;
- l'offre, authentifiée par rapprochement avec la clé publique et associée à son empreinte ;
- les éventuels documents et informations techniques demandés par la personne publique.

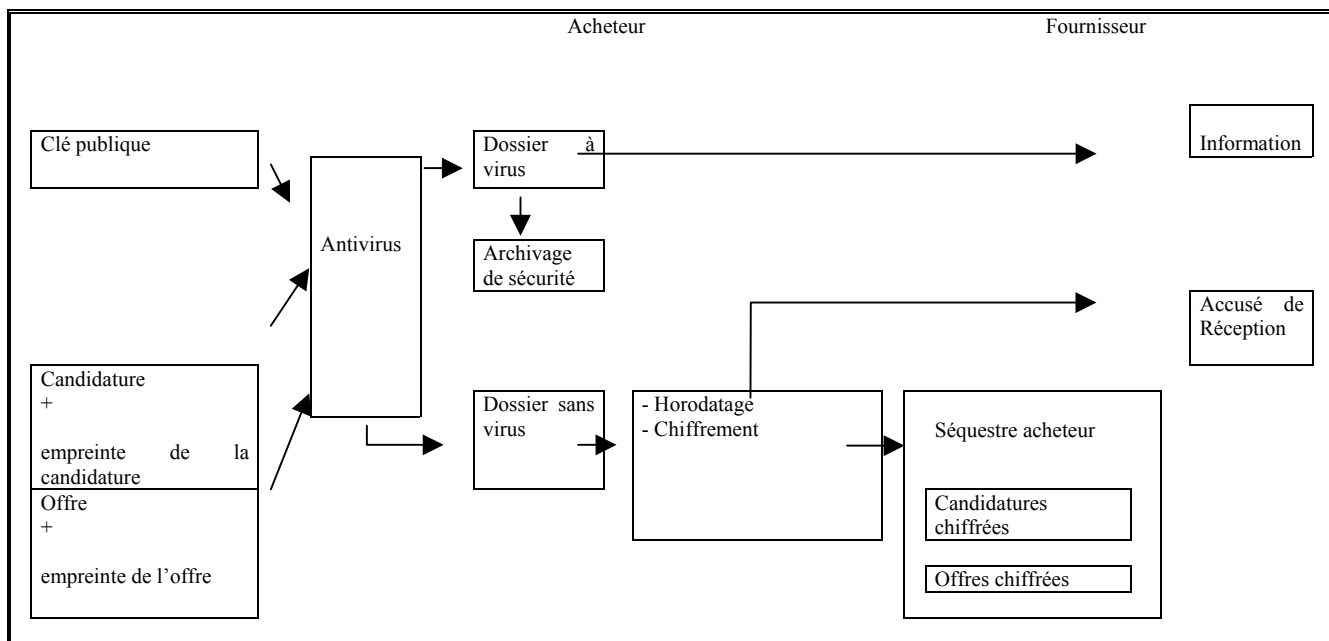
Pour sa part, la personne publique est soumise aux obligations suivantes :

- assurer la sécurité des transactions sur le réseau informatique ;
- assurer la liberté d'accès à ce réseau à tous les candidats potentiels de manière non discriminatoire ;
- assurer la confidentialité relative aux candidatures et aux offres ;
- informer la totalité des fournisseurs ayant téléchargé le DCE des éventuels modifications et éléments complémentaires ayant trait à la présente consultation ;
- fixer une date certaine de réception des candidatures et des offres avec transmission aux candidats d'un accusé de réception électronique ;
- assurer le dépôt et le maintien de l'intégrité des candidatures et des offres dans un séquestre jusqu'à la date et l'heure d'ouverture des candidatures par la PRM puis des offres par la CAO. La gestion du séquestre peut être sous-traitée à un prestataire de services dûment qualifié. Un (ou plusieurs) antivirus doivent être utilisés sur les fichiers envoyés non chiffrés par les soumissionnaires avant mise en dépôt dans le séquestre ;
- informer les soumissionnaires en cas de détection d'un virus par la PRM, entraînant un archivage de sécurité ; dans cette situation, la candidature ou l'offre est considérée comme n'étant pas parvenue à la PRM ;
- préciser, en cas de transmission de documents volumineux, le délai supplémentaire (maximum de vingt quatre heures) possible entre la réception de la signature électronique (antérieur à l'horaire limite indiqué sur l'AAPC) et la réception des empreintes du dossier de réponse.

La personne publique pourra envisager le dépôt des dossiers de réponses soit sur une partie sécurisée (https:) d'un site pouvant être propre à l'établissement, soit sur un site mutualisé (https:) type portail, soit chez un prestataire de services qualifié disposant d'un site sécurisé (https:).

5.3 Réception des plis

Figure n° 4 : réception du dossier de réponse



5.3.1 Réception chez l'acheteur public

L'acheteur public a reçu cinq éléments : la clé publique, l'empreinte de la candidature, l'empreinte de l'offre, la candidature et l'offre. L'article 10 du décret n°2002-692 du 30 avril 2002 suppose que ces éléments font l'objet d'un traitement antivirus mais ne précise pas à quel stade de la procédure celui-ci doit avoir lieu.

Un anti-virus est sans action sur un fichier chiffré.

Un fichier chiffré peut ne pas être autorisé à franchir la barrière de certains « pare-feux » ou firewalls.

Pour ces 2 raisons, les auteurs du guide recommandent aux acheteurs publics de prévoir dans leur RC l'interdiction de chiffrement (ou « cryptage ») des dossiers de réponse des soumissionnaires.

Dans le processus décrit ici, il est choisi par souci de sécurité de prévoir une détection dès réception du dossier de réponse par l'acheteur public. Dans ce cas, deux possibilités existent :

- soit le dossier de réponse comporte un virus, le dossier fait l'objet d'un archivage de sécurité, et le candidat en est informé (article 10 du décret n°2002-692 du 30 avril 2002) ;
- soit le dossier de réponse ne comporte pas de virus, l'authentification de la signature et des documents sont vérifiés. La personne publique a pour obligation de rendre certaine la date et l'heure de remise des plis : un horodatage doit donc être prévu, complété par l'envoi d'un accusé de réception électronique au candidat. Ces événements sont retracés dans l'outil « journal des événements ».

Si un virus est découvert avant la date limite de dépôt des candidatures et des offres, le candidat informé a la possibilité d'effectuer un nouvel envoi.

L'anti-virus fait l'objet de mises à jour régulières, en tant que de besoin : il peut être envisagé de repasser cet anti-virus sur toutes les offres à chaque mise à jour.

Dans le cas de transmission de documents volumineux et si cela est prévu dans l'AAPC, la personne publique doit prévoir dans son calendrier interne de procédure un délai minimum de 24 heures après la date limite de réception des dossiers pour la tenue de la séance d'ouverture des plis, afin de permettre le recueil intégral des documents.

5.3.2 Notion de séquestre ou « coffre fort électronique »

La confidentialité des candidatures et des offres dans une procédure d'AO ouvert impose jusqu'à l'ouverture des candidatures par la PRM puis des offres en CAO, leur conservation dans un séquestre.

La personne publique doit également rendre impossible l'ouverture des offres des soumissionnaires avant la CAO : paramétrage du séquestre avec nécessité du « double clic » avant ouverture qui ne sera possible que par le contrôle de la date (date d'ouverture des candidatures par la PRM, postérieure à la date limite de réception des plis, et date de la CAO d'ouverture des offres) et de la personne habilitée, détentrice de la clé publique (PRM / président de CAO). Le séquestre devra également être paramétré pour permettre, lors de la CAO, l'ouverture des offres des seuls soumissionnaires ayant été retenus par la PRM après avis de la CAO.

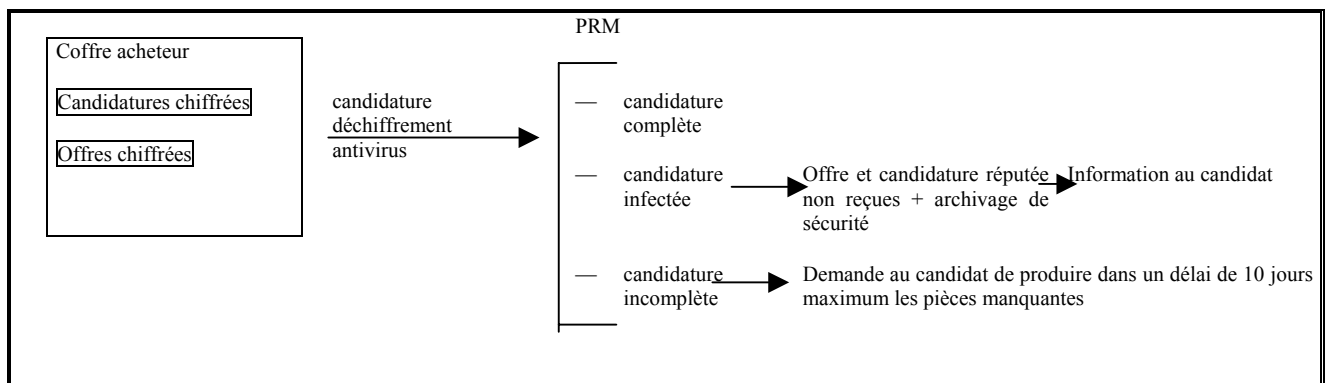
Chaque candidat à un marché public doit disposer d'un certificat d'authentification et d'une clé privée. Des empreintes sont effectuées sur les documents afin d'assurer l'authentification et la sécurité des offres (deux « fichiers-enveloppes » contenant les candidatures et les offres, chaque fichier comportant une empreinte électronique, mais il est conseillé de recourir à un envoi unique des deux fichiers).

La personne publique dispose de la clé publique du candidat pour l'identifier et authentifier les offres. Le candidat a besoin d'un certificat pour signer les plis contenant les candidatures d'une part, et les offres, d'autre part. Les réponses sont déposées ensuite dans le séquestre.

Afin d'assurer une garantie supplémentaire, il peut être envisagé un chiffrement automatique à la réception des plis (après passage de l'anti-virus), avec deux chiffrements différents pour les candidatures et pour les offres (afin de diminuer les risques d'erreur). Le déchiffrement s'effectuera alors par la PRM (pour les candidatures) et par la CAO (pour les offres).

5.4 Examen des candidatures par la PRM (art. 52-1^{er} alinéa CMP)

Figure n° 5 : examen des candidatures par la PRM



L'ouverture des candidatures dématérialisées par la PRM doit intervenir après la date limite de réception des dossiers. Ceci nécessite qu'elles soient déchiffrées et que leur soit appliqué éventuellement un nouveau traitement antivirus (il n'est en effet pas certain que le traitement pratiqué à la réception ait pu écarter tout risque). Ceci implique notamment de prévoir qu'un dossier puisse contenir un virus à l'ouverture des candidatures et d'en tirer les conséquences (cf. article 52 du CMP et article 10 du décret du 30 avril 2002).

La personne publique doit établir les procédures permettant de garantir aux soumissionnaires la sécurité des informations portant sur les candidatures et les offres.

Lors de l'ouverture des candidatures, elle a pour obligations de :

- permettre l'authentification de la signature de la personne qui « ouvre » le séquestre (PRM ou son représentant), la seule qui dispose des codes d'accès correspondants ;
- empêcher toute modification des documents transmis par les soumissionnaires ;
- vérifier que tous les documents transmis sont signés par la personne habilitée à engager la société ;

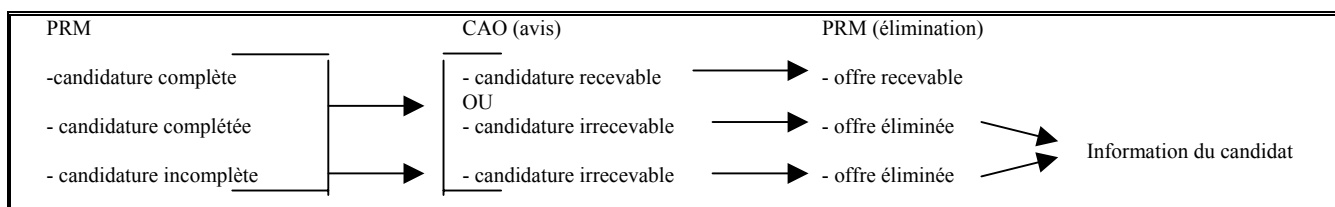
- informer les soumissionnaires en cas de détection d'un virus, entraînant un archivage de sécurité.

Dans cette situation, la candidature et l'offre sont considérées comme n'étant pas parvenues à la PRM.

Selon le 1^{er} alinéa de l'article 52 du CMP, « Avant de procéder à l'examen des candidatures, si la personne responsable du marché constate que des pièces dont la production était réclamée sont absentes ou incomplètes, elle peut décider de demander à tous les candidats concernés de produire ou de compléter ces pièces dans un délai identique pour tous les candidats et qui ne saurait être supérieur à dix jours ».

5.5 Examen des candidatures, avis de la CAO, élimination des candidatures par la PRM (Art. 58-II du CMP)

Figure n° 6 : examen des candidatures par la CAO



La PRM présente les candidatures complètes, complétées ou incomplètes à la CAO qui émet un avis sur leur conformité et leur recevabilité. La PRM procède ensuite à l'élimination des candidatures et en informe les candidats éliminés.

La personne publique doit garantir la non-ouverture des offres des candidats éliminés. Ces offres sont alors détruites et ne sont pas conservées dans les fichiers de l'établissement, ce dernier devant garder preuve de l'opération de destruction des fichiers.

Cette étape fait l'objet d'une mention dans le « journal des événements ». A ce stade, l'authentification des personnes habilitées¹¹ est indispensable.

5.6 Ouverture des offres (CAO) (art 58-III)

Une fois la liste de candidatures recevables établie, la CAO procède dans des conditions similaires à l'ouverture des offres correspondantes dont certaines risquent aussi d'être écartées au motif qu'elles contiennent un virus informatique.

¹¹ Article 20, alinéa 2 du CMP : « la personne responsable du marché peut se faire représenter dans l'exercice de ses fonctions, sauf pour le choix de l'attributaire et la signature du marché ».

Lors de l'ouverture des offres, la personne publique a pour obligations de :

- permettre l'authentification de la personne qui « ouvre » les offres ;
- empêcher toute modification des documents transmis par les candidats retenus ;
- vérifier que tous les documents transmis sont signés par la personne habilitée à engager la société ;
- informer les soumissionnaires en cas de détection d'un virus, entraînant un archivage de sécurité ; dans cette situation, l'offre est considérée comme n'étant pas parvenue à la PRM.

5.7 Avertir les candidats non retenus

La PRM doit informer les candidats non retenus du rejet de leur offre, en rendant certaine la date de l'envoi (délai de 10 jours francs à respecter strictement entre l'information des candidats non retenus et la signature par la PRM du marché avec le candidat retenu).

5.8 Avertir les candidats retenus et poursuite de la procédure

Il existe un intérêt tout particulier à poursuivre la procédure par voie dématérialisée. En effet, les systèmes d'information et les outils bureautiques donnent la possibilité à la PRM de :

- demander au(x) fournisseur(s) retenu(s) des éléments complémentaires pour conclure le marché (attestations, certificats fiscaux et sociaux, ...) en maintenant la confidentialité de la demande et en rendant certaine la date de la demande ;
- adresser les pièces du marché au contrôle de légalité ;
- notifier le marché auprès du titulaire, en rendant certaine la date d'envoi et de réception du marché ;
- faire parvenir aux soumissionnaires les informations relatives à la conclusion du ou des marchés ;
- adresser au BOAMP et si besoin au JOUE, l'avis d'attribution du marché, en rendant certaine la date d'envoi (délai de 30 jours maximum après la notification).

Les marchés peuvent être ensuite intégrés à un outil d'exécution de passation des commandes, de type e-procurement.

5.9 Archivage

A l'issue de la procédure, la personne publique archive conformément aux règles indiquées au point 2.7 :

- les offres retenues ;
- les offres non retenues ;
- le « journal des événements » de la consultation, soit au sein de l'établissement, soit auprès d'un prestataire de services qualifié.

Glossaire

Antivirus

Programme installé sur l'ordinateur et chargé de détecter et d'éliminer les virus informatiques contenus dans les fichiers. Ces programmes doivent être régulièrement actualisés afin de pouvoir reconnaître les virus récemment répertoriés.

Archivage

Le fait de mettre des fichiers, généralement sous forme compressée, dans une archive et d'assurer la conservation de documents sur une longue durée (3, 5, 10, 30, 60, voire 100 ans).

Autorité de certification (AC)

Il s'agit d'une société ou d'un service administratif chargé de créer, de délivrer et de gérer des certificats électroniques.

Autorité de certification racine

Il s'agit d'une autorité de certification qui référence d'autres autorités de certification (dites alors déléguées) dans un modèle hiérarchique.

Certificat ou certificat électronique

Il s'agit d'un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.

Certificat qualifié

Il s'agit d'un certificat électronique répondant aux exigences de l'article 6 du décret n° 2001-272 du 30 mars 2001 sur la signature électronique (ou aux annexes I et II de la directive européenne sur la signature électronique).

Certificat racine

Il s'agit du certificat électronique par lequel l'autorité de certification racine de l'IGC certifie les certificats électroniques des autorités de certification déléguées.

Chiffrement (ou anglicisme « cryptage »)

Opération consistant à transformer un fichier à l'aide d'une clé (privée ou publique, en fonction de l'utilisation du chiffrement)

Clés (publique, privée)

Chaîne de caractères permettant d'authentifier et de chiffrer (ou déchiffrer) un message.

« Coffre-fort » électronique

Espace sécurisé, non accessible pendant une période définie, permettant de conserver les offres reçues des prestataires avant la commission d'ouverture des plis (voir également « séquestre »).

Déclaration des pratiques de certification

Il s'agit de l'énoncé des procédures de certification effectivement mises en œuvre par une autorité de certification pour délivrer et gérer des certificats électroniques.

Dématérialisation

La dématérialisation des données consiste à stocker et faire circuler des données sans support matériel autre que des équipements informatiques.

Dispositif de création de signature

Il s'agit d'un matériel ou d'un logiciel destiné à mettre en application les données de création de signature électronique (par exemple une combinaison entre une carte à puce et Netscape Form Signing ou une messagerie électronique).

Dispositif sécurisé de création de signature

Il s'agit d'un dispositif de création de signature électronique conforme aux exigences de l'article 3 du décret n° 2001-272 du 30 mars 2001 sur la signature électronique (ou à l'annexe III de la directive européenne sur la signature électronique). Cette conformité est reconnue sur la base d'une certification de sécurité délivrée par la DCSSI (décret n°2002-535 du 18 avril 2002).

Données de création de signature

Ce sont les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique.

Données de vérification de signature

Ce sont les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique.

e-business

Commerce électronique sous internet. On distingue le B2C (commerce avec les particuliers), le B2B (commerce entre entreprises) et le B2G (commerce entre les entreprises et les administrations/les gouvernements). De plus, on distinguera l'e-sourcing limité au choix des fournisseurs, et l'e-procurement qui traite de la passation des commandes dans le cadre des contrats en vigueur (e-approvisionnement).

e-procurement

Le « e – procurement » ou gestion électronique des approvisionnements représente toutes les possibilités que l'entreprise peut utiliser via Internet pour effectuer ses approvisionnements. Les sociétés ont pour but de réduire les coûts administratifs liés aux approvisionnements.

Empreinte

Fichier obtenu par un algorithme appliqué à un fichier initial (offre ou candidature par exemple). L'algorithme peut utiliser une clé privée ou une clé publique.

Extranet

Intranet ouvert à quelques organismes extérieurs à l'entreprise, dûment autorisés (clients, fournisseurs, partenaires).

Format de fichier

Manière dont un fichier est agencé afin d'être directement exploité par un logiciel spécifique. Dans l'intitulé des fichiers Windows, ce format est précisé par l'extension du fichier (généralement 3 caractères précédés d'un point : .doc .xls .exe .htm .pdf .txt .wav)

IGC (PKI en anglais)

Une Infrastructure de Gestion de Clef (IGC) - ou « Public Key Infrastructure » en anglais - est un système assurant la gestion de certificats électroniques au sein d'une communauté d'utilisateurs. Une IGC est notamment composée d'au moins une autorité de certification, et peut comprendre au moins une autorité d'enregistrement chargée de vérifier les données d'identification des utilisateurs de certificat électronique, et de contrôler les droits liés à l'utilisation des certificats électroniques conformément à la politique de certification.

Internet

(International Network) Réseau mondial associant des ressources de télécommunication et des ordinateurs (serveurs et clients), destiné à l'échange de messages électroniques (courriel ou e-mail), d'informations multimédia (web) et de fichiers (FTP). Il fonctionne en utilisant le protocole commun IP (Internet Protocol) spécifié par l'Internet Society (ISOC), qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants. L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un organisme accrédité. Sa gestion est décentralisée en réseaux interconnectés.

Intranet

Réseau privé qui utilise les technologies de l'Internet ; destiné à l'usage exclusif d'un organisme il ne s'ouvre pas aux connexions publiques.

Journal des événements

Ce document énumère chronologiquement l'ensemble des opérations d'une procédure de passation. Dans une procédure papier, celui-ci prend la forme d'un registre tenu à jour par le service chargé de la procédure. Dans une procédure électronique, celui-ci consiste en un document électronique généré par le système informatique de l'acheteur. Il décrit toutes les opérations dont l'initiative revient à la personne publique comme, notamment la mention de la mise en ligne de l'AAPC, du règlement de consultation et du DCE, la liste des personnes ayant téléchargé ces documents, et la mention de tous les échanges d'informations intervenus entre ces personnes et les soumissionnaires avec l'acheteur.

LCR

Liste des certificats révoqués. La tenue d'une LCR incombe à chaque autorité de certification.

Personne publique

Personne morale soumise au Code des Marchés Publics (« pouvoir adjudicateur » au sens du droit européen).

Place de marché

Site Internet offrant notamment des services d'e-procurement. Lieu de médiation entre acheteurs et vendeurs de services ou d'expertise particulière.

Plate-forme

PC ou serveur supportant des logiciels applicatifs.

Politique de certification

Il s'agit de l'ensemble des règles, identifiées, qui définit le type d'applications auxquelles un certificat électronique est adapté ou dédié (par exemple, pour les téléprocédures du MINEFI effectuées en mode EFI, une politique de certification « type » a été énoncée ; elle est disponible à l'adresse :

http://www.minefi.gouv.fr/dematerialisation_icp/pc_type_minefi_dsi.pdf).

Portail

Page d'entrée d'un site Web offrant le maximum de liens vers les différentes parties du site ou vers d'autres sites.

Présomption de fiabilité

Le second alinéa de l'article 1316-4 du Code civil reconnaît à la signature électronique une valeur probante lorsqu'elle "consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache".

Si cette signature dite "simple" est contestée, il appartiendra au signataire, aidé par celui qui lui a délivré le procédé de signature, de rapporter par tout moyen la preuve que le procédé utilisé est fiable. Cette qualité s'apprécie notamment au regard des éléments techniques et d'organisation mis en œuvre par ce procédé. L'article du Code civil poursuit en prévoyant que la fiabilité pourra être présumée 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".

Il s'agira alors d'une signature électronique dite "sécurisée" établie conformément aux dispositions du décret n°2001-272 du 30 mars 2001. Dans ce cas, il appartiendra à celui qui conteste cette signature de rapporter la preuve que le procédé utilisé n'est pas fiable.

Prestataire de services de certification électronique

Toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique (par exemple, une Autorité de certification).

Protocole d'échange sécurisé (https: ou http/ssl)

(HyperText Transfer Protocol over SSL) Le même protocole de transport de pages, mais sécurisé (chiffrement).

Protocole d'échange simple (http:)

(HyperText Transfer Protocol) Protocole utilisé pour assurer, sur le réseau, l'accès et le transport des pages HTML (HyperText Markup Language) du Web. L'accès aux services Web se fait en donnant une adresse de type <http://nom de domaine/répertoire...>

Qualification d'un prestataire de services de certification électronique

Il s'agit d'une procédure volontaire de vérification de conformité de services de certification électronique aux exigences portant sur les certificats qualifiés et aux normes européennes développées au sein de l'European Electronic Signature Standardisation Initiative (EESSI) et qui seront publiées au JOUE (la qualification sera effectuée par un organisme indépendant accrédité par le COFRAC) (arrêté du 30/05/2002).

Référencement

Il peut s'agir de procédures de vérification de conformité de services de certification électronique à certains critères propres à une ou plusieurs télé procédures (par exemple, le référencement de certificats électroniques utilisés pour TéléTVA en mode EFI).

Séquestre

Un séquestre électronique permet d'accepter des documents (candidatures et/ou offres) signés jusqu'à expiration du délai de la procédure, de conserver ces documents jusqu'à leur(s) date(s) d'ouverture, de les ouvrir de façon sécurisée, et de tracer toutes les actions les concernant.

Signataire

Il s'agit de toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique

Signature électronique

Au sens du droit de la preuve, il s'agit d'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.

Signature électronique sécurisée

Il s'agit d'une signature électronique qui satisfait 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.

Sourcing

Recherche de fournisseurs (par Internet : e-sourcing)

Virus

Séquence d'instructions parasites destinée à nuire, cachée dans un fichier externe (disquette, pièce-jointe d'un courriel, ...) lu par l'ordinateur et susceptible d'infecter ses fichiers ou son système d'exploitation (principalement les fichiers exécutables) par réplique de cette séquence d'instructions. Il peut en résulter des dysfonctionnements divers, immédiats ou différés, dont l'effacement du disque dur.

Liste des abréviations

AAPC

Avis d'Appel Public à la Concurrence

AC

Autorité de Certification (voir Glossaire)

AE

Acte d'Engagement

AFA

Association des Fournisseurs d'Accès

AFNOR

Association Française de NORmalisation (www.afnor.fr)

AO

Appel d'Offres

ATC

Anatomical Therapeutical Chemical (classification)

BOAMP

Bulletin Officiel des Annonces des Marchés Publics

CAO

Commission d'Appel d'Offres

CCAP

Cahier des Clauses Administratives Particulières

CCP

Cahier des Clauses Particulières

CCTP

Cahier des Clauses Techniques Particulières

CIP

Club Inter-Pharmaceutique

COFRAC

COmité FRançais d'ACcréditation

CMP

Code des Marchés Publics

DCE

Dossier de Consultation des Entreprises

DCSSI

Direction Centrale de la Sécurité des Systèmes d'Information (<http://www.dcssi.gouv.fr>)

EDI

Échange de Données Informatisé

EFI

Échange de Formulaire Informatisé, effectué via Internet.

EPS

Etablissement Public de Santé

GIP-CPS

Groupement d'Intérêt Public chargé de gérer les Cartes des Professionnels de Santé.

GPEM/SL

Groupe permanent d'étude des marchés/soins et laboratoires

IGC (PKI en anglais)

Infrastructure de Gestion de Clef ou « Public Key Infrastructure » en anglais (voir glossaire)

JOUE

Journal Officiel de l'Union Européenne

LCR

Liste des Certificats Révoqués (voir glossaire)

MEN

Mission pour l'Economie Numérique (<http://www.men.minefi.gouv.fr/>)

MINEFI

MINistère de l'Economie, des Finances et de l'Industrie (www.minefi.gouv.fr)

PRM

Personne Responsable du Marché

RC

Règlement de la Consultation

UCD

Unité Commune de Dispensation et/ou de Distribution

USB

Universal Serial Bus

ANNEXE N°1 : TEXTES

Code civil extraits : ces dispositions sont issues de la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O n° 62 du 14 mars 2000 page 3968).

Article 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.

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.

Article 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 1316-3 – L'écrit sur support électronique a la même force probante que l'écrit sur support papier.

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 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 du 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.

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 (J.O n° 77 du 31 mars 2001 page 5070)

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 œuvre 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 œuvre 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 œuvre 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.

Décret no 2001-846 du 18 septembre 2001 pris en application du 3o de l'article 56 du code des marchés publics et relatif aux enchères électroniques (J.O n° 217 du 19 septembre 2001 page 14847)

Art. 1er. - Pour la mise en œuvre de la procédure d'enchères électroniques prévue au 3o de l'article 56 du code des marchés publics, sont réputées être des fournitures courantes celles pour lesquelles la personne publique n'impose pas des spécifications techniques qui lui soient propres.

Les enchères électroniques constituent le procédé par lequel les candidats à un marché public admis à présenter une offre s'engagent sur une offre de prix transmise par voie électronique dans une période de temps préalablement déterminée par l'acheteur public et portée à la connaissance de l'ensemble des candidats.

A l'intérieur de cette période, qui peut être prolongée dans des conditions prévues par le règlement de la consultation, les candidats sont tenus informés du niveau des offres de prix faites par les autres candidats, dont l'identité ne doit en aucun cas leur être communiquée. Ils ont la possibilité de faire varier leur offre de prix à la baisse.

A l'issue de la période d'enchères, les offres de prix formulées par les candidats deviennent intangibles. Elles engagent leurs auteurs pendant la durée de validité des offres.

Cette procédure n'exclut pas que la personne publique sélectionne les offres sur d'autres critères que le seul prix, conformément aux dispositions de l'article 53 du code des marchés publics. Le cas échéant, la personne publique peut décider d'appliquer la procédure d'enchères électroniques à tout ou partie de ces autres éléments de l'offre qui font l'objet d'une procédure de sélection.

Art. 2. - Les marchés pour lesquels est organisée une procédure d'enchères publiques sont passés, en fonction de leur montant, selon les procédures prévues aux articles 28, 32 et 33 du code des marchés publics ainsi que, le cas échéant, au 1o du I, 1o du II et 3o du II de l'article 35 et à l'article 72 du même code.

Art. 3. - Conformément aux dispositions du 4o de l'article 56 du code des marchés publics, l'ensemble des écrits mentionnés audit code et dont la production accompagne les différentes procédures de passation ou mesures d'exécution des marchés peut être remplacé par un support ou un échange électronique, à chacun des stades de la passation et de l'exécution d'un marché à l'occasion duquel la personne publique organise des enchères électroniques.

Art. 4. - La personne publique assure la sécurité des transactions et organise les enchères électroniques sur un réseau informatique accessible à tous les candidats de façon non discriminatoire. Les frais d'accès au réseau sont à la charge de chaque candidat.

En cas de défaillance du dispositif d'échanges électroniques, la personne publique met à la disposition des candidats des moyens de transmission susceptibles de se substituer dans les meilleures conditions de sécurité aux moyens électroniques initialement prévus.

Art. 5. - 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 jusqu'à l'expiration des délais de remise des candidatures et des offres et ne sont ensuite accessibles qu'à des personnes autorisées par la personne responsable du marché.

Art. 6. - La procédure des enchères électroniques peut être utilisée dans le cadre de marchés passés selon les procédures de coordination ou de groupement prévues aux articles 7 et 8 du code des marchés publics. Dans ce cas, le centralisateur ou le coordonnateur assument, respectivement, les obligations prévues aux articles 4 et 5 du présent décret dans l'accomplissement des fonctions qui leur sont dévolues conformément aux dispositions dudit code.

Art. 7. - Les candidatures peuvent être individuelles ou groupées. Dans ce dernier cas, le mandataire assure la sécurité et l'authenticité des informations transmises au nom des membres du groupement.

Dans les documents fournis à l'appui de leur candidature, les candidats doivent désigner la personne habilitée à présenter des offres de prix pendant la période d'enchères. Ils mettent en place des procédures permettant à la personne publique de s'assurer que les offres de prix sont transmises par la personne habilitée. Le candidat ne peut révoquer ces offres.

Art. 8. - 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 18 septembre 2001.

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 (J.O n° 103 du 3 mai 2002 page 8064)

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.

Décret ° 2004-15 du 7 janvier 2004 portant Code des Marchés Publics (J.O. n° 6 du 8 janvier 2004) : extraits

TITRE III - PASSATION DES MARCHES
Chapitre III - Règles générales de passation
Section 1 - Organisation de la publicité

Article 40

I. - En dehors des cas prévus à l'article 30 et aux II et III de l'article 35, tout marché doit être précédé d'une publicité suffisante permettant une mise en concurrence effective, dans les conditions définies ci-après.

II. - Pour les marchés d'un montant inférieur à 90 000 EUR HT, la personne publique choisit librement les modalités de publicité adaptées au montant et à la nature des travaux, des fournitures ou des services en cause.

III. - Pour les marchés de fournitures et de services d'un montant compris entre 90 000 EUR HT et 150 000 EUR HT pour l'Etat ou 230 000 EUR HT pour les collectivités territoriales, la personne publique est tenue de publier un avis d'appel public à la concurrence soit dans le Bulletin officiel des annonces des marchés publics, soit dans un journal habilité à recevoir des annonces légales. La personne publique apprécie de plus si, compte tenu de la nature ou du montant des fournitures ou des services en cause, une publication dans un journal spécialisé correspondant au secteur économique concerné est par ailleurs utile pour assurer une publicité conforme aux objectifs mentionnés à l'article 1er du présent code.

IV. - Pour les marchés de travaux d'un montant compris entre 90 000 EUR HT et 5 900 000 EUR HT, la personne publique est tenue de publier un avis d'appel public à la concurrence soit dans le Bulletin officiel des annonces des marchés publics, soit dans un journal habilité à recevoir des annonces légales. La personne publique apprécie de plus si, compte tenu de la nature ou du montant des travaux en cause, une publication dans un journal spécialisé correspondant au secteur économique concerné est par ailleurs utile pour assurer une publicité conforme aux objectifs mentionnés à l'article 1er du présent code.

V. - Pour les marchés de fournitures et de services d'un montant supérieur à 150 000 EUR HT pour l'Etat et 230 000 EUR HT pour les collectivités territoriales, et pour les marchés de travaux d'un montant supérieur à 5 900 000 EUR HT, la personne publique est tenue de publier un avis d'appel public à la concurrence dans le Bulletin officiel des annonces des marchés publics et au Journal officiel de l'Union européenne.

La publication des avis dans le Bulletin officiel des annonces des marchés publics ne peut intervenir avant l'envoi à l'Office des publications de l'Union européenne ; ces avis ne peuvent fournir d'autres renseignements que ceux qui sont adressés à l'office précité.

VI. - Les avis mentionnés aux III, IV et V sont établis conformément aux modèles fixés par arrêté du ministre chargé de l'économie. Les avis destinés au Bulletin officiel des annonces des marchés publics sont envoyés par téléprocédure.

VII. - Le Bulletin officiel des annonces des marchés publics est tenu de publier les avis d'appel public à la concurrence, conformément au texte transmis par la personne responsable du marché, dans les onze jours ou, en cas d'urgence, dans les six jours qui suivent la date de leur réception.

VIII. - En cas d'appel d'offres restreint, de concours restreint ou de marché négocié avec publicité préalable, la personne responsable du marché peut faire paraître un seul avis pour un ensemble de marchés qu'elle prévoit de lancer, pour des prestations de même nature, au cours d'une période maximale de douze mois.

Section 8 : Dématérialisation des procédures

Article 56

Le règlement de la consultation, la lettre de consultation, le cahier des charges, les documents et les renseignements complémentaires peuvent être mis à disposition des entreprises par voie électronique dans des conditions fixées par décret. Néanmoins, au cas où ces dernières le demandent, ces documents leur sont transmis par voie postale.

Sauf disposition contraire prévue dans l'avis de publicité, les candidatures et les offres peuvent également être communiquées à la personne publique par voie électronique, dans des conditions définies par décret. Aucun avis ne pourra comporter d'interdiction à compter du 1er janvier 2005.

Un décret précise les conditions dans lesquelles des enchères électroniques peuvent être organisées pour l'achat de fournitures courantes.

Les dispositions du présent code qui font référence à des écrits ne font pas obstacle au remplacement de ceux-ci par un support ou un échange électronique.

ANNEXE N°2 : ARCHIVAGE

Dématérialisation des procédures de passation des marchés publics : Archivage (source : Direction des Affaires Juridiques / MINEFI)

1/ L'archivage des dossiers "papier" relatifs aux marchés publics obéit aux règles suivantes :

Celles-ci ont fait l'objet de plusieurs articles dans Télégrammes Marchés Publics (TMP)⁶.

En application du code du patrimoine, articles L 211-1 et suivants, sur les archives, les modalités de conservation des archives publiques (durée d'utilité administrative, sort final) sont fixées d'un commun accord entre l'autorité qui les a produits ou reçus et l'administration des archives.

Pour décider de la durée d'utilité administrative (DUA) des marchés et des offres non retenues, l'administration concernée et le service des archives tiennent compte du temps pendant lequel le document conservera un intérêt juridique ou pratique (valeur primaire de l'archive).

A l'issue de cette durée, certaines archives en raison de leur intérêt patrimonial (intérêt historique, scientifique, sociologique, architectural...) acquièrent une valeur secondaire qui justifie leur conservation définitive et leur versement, à ce moment-là, dans un service public d'archives. Les autres archives dépourvues de cette valeur sont, à l'issue de la DUA, éliminées, l'élimination ne pouvant s'effectuer qu'après l'obtention d'un visa par l'Administration des archives (services des archives nationales, services départementaux des archives).

Cette collaboration entre service producteur et service d'archives donne lieu à l'élaboration d'un document appelé "tableau de tri et de gestion" qui dresse, par producteur et grand domaine d'action administrative, la liste des types de documents concernés et qui affecte à chacun une durée d'utilité administrative (DUA) et un sort final (conservation totale ou après tris –avec explicitation de ces tris, élimination).

Des articles publiés dans TMP, peuvent être déduites différentes approches justifiant des durées d'utilité administrative diverses. Ainsi, peuvent être distingués les documents qui ont trait à la passation des marchés et ceux qui sont relatifs à leur exécution, les premiers concernant l'ensemble des candidats alors que les seconds sont relatifs aux seuls candidats retenus. L'objet ou les résultats d'un marché peuvent aussi induire une durée de conservation spécifique. Enfin, le choix de la durée de conservation s'apprécie différemment selon que la pérennité de ces documents est justifiée pour l'exercice de contrôles administratifs et juridictionnels ou pour la protection des intérêts de l'administration dans un éventuel contentieux.

⁶ TMP n°159 en 1991, n°205 en 1996 et n°218 en 1999.

L'article du TMP n°218 de 1999 synthétise les différentes règles en vigueur.

En tout état de cause, afin d'éviter la destruction de pièces pouvant être nécessaires à l'action des organismes de contrôles administratifs et juridictionnels, **une durée de conservation de dix ans minimum à compter de l'admission ou de la réception des prestations objet du marché**, ne peut être que conseillée.

Pour les marchés de fournitures et de services, une durée de dix ans est estimée suffisante pour préserver les intérêts de l'administration au regard de l'article 189bis du code de commerce qui dispose « *les obligations nées à l'occasion de leur commerce entre commerçants, ou entre commerçants et non commerçants, se prescrivent par dix ans si elles ne sont pas soumises à des prescriptions spéciales plus courtes* ».

Pour les marchés de travaux, la durée de conservation proposée est de trente ans au motif que la mise en jeu de la garantie décennale fait courir un nouveau délai décennal (CE, 13 janvier 1984, OPHLM de Firminy) et qu'en cas de fraude ou de dol c'est le délai de la prescription civile qui s'applique (CE, 3 avril 1991, société SMAC Aciroid).

Lorsqu'un auteur a consenti des droits à l'administration, l'article L123-1 du code de la propriété intellectuelle (CPI) dispose « *au décès de l'auteur, ce droit [à protection] persiste au bénéfice de ses ayants droits pendant l'année civile en cours et les soixante-dix années qui suivent* », ce qui implique pour la preuve du droit de l'administration la conservation du marché pendant une durée au moins égale.

S'agissant de la conservation des dossiers relatifs aux candidatures et aux offres non retenues, une circulaire du Premier ministre du 30 décembre 1998 (JO du 31 décembre 1998) relative à la procédure de passation des marchés publics, précise que « *le délai minimal prescrit pour la conservation des dossiers de soumission présentés par les entreprises non retenues dans le cadre des procédures de passation des marchés publics est désormais fixé à cinq ans à compter de la notification du marché à l'entreprise retenue* ».

En outre, pour alléger le volume des documents à conserver, la circulaire indique que les administrations peuvent dès achèvement de la procédure de passation d'un marché, éliminer les pièces qui figurent déjà dans le dossier de définition du marché à savoir : CCAP, CCTP, cahier des clauses communes, règlement de la consultation. Elles peuvent également éliminer ou retourner aux entreprises la documentation publicitaire figurant dans les dossiers de soumission.

Enfin, est en cours de signature un projet d'instruction interministérielle (tableau de tri et de gestion) pour le traitement et la conservation des documents d'archives produits dans le cadre de la procédure des marchés publics.

2/ L'archivage des dossiers dématérialisés doit tenir compte de certaines dispositions du décret du 30 avril 2002 en s'inspirant des règles précitées.

Il convient d'abord de rappeler que les dispositions du code du patrimoine relatives aux archives s'appliquent aux documents quel que soit leur support matériel donc y compris aux documents électroniques. L'archivage de ces documents s'effectuera donc selon des règles énoncées ci-dessus. En particulier la décision d'archiver et le choix des documents reviennent en ce qui concerne les marchés publics à l'autorité publique chargée de leur passation et/ou de leur exécution.

Deux questions sont fréquemment soulevées lorsqu'on évoque l'archivage de documents électroniques : qu'en est-il de la fiabilité des documents archivés ? Quid de la pérennité du contenu de ces documents ?

La fiabilité des documents archivés quel que soit leur support réside dans la confiance accordée à la personne publique. Aujourd'hui, il est considéré que l'exemplaire papier du marché qui fait foi est celui signé manuellement et détenu par la personne publique. Dans le cas d'un marché sous la forme d'un dossier électronique, c'est la signature électronique de ce marché par la personne publique qui lui confèrera le caractère de seul exemplaire de référence. Pour les autres pièces relatives aux marchés publics destinées à être archivées, c'est la signature électronique de la personne publique qui leur confèrera fiabilité préalablement à leur archivage.

Quant à la pérennité, elle s'apprécie en terme de sécurité dans la conservation des documents, l'obsolescence rapide des matériels, logiciels et périphériques pouvant entraîner une non lisibilité des informations dans des délais relativement courts (compris entre 5 et 10 ans).

Ces différentes opérations ne remettent pas en cause à terme la valeur probante de ces documents qui doit toujours être appréciée au regard des règles juridiques contemporaines à leur formation.

2-1/ Que faut-il archiver ?

Candidatures retenues et offres retenues : celles-ci devenant les éléments constitutifs de marchés conclus doivent être conservées.

Candidatures retenues et offres ouvertes non retenues : celles-ci doivent être conservées dans la perspective des contentieux éventuels relatifs aux procédures de passation des marchés concernés et des éventuels contrôles administratifs auxquels ils peuvent donner lieu.

Candidatures non retenues : en cas d'appel d'offre ouvert, si une candidature n'est pas admise, l'offre correspondante est éliminée des fichiers sans avoir été lue et le candidat en est informé (art. 6 du décret du 30 avril 2003), il n'y a donc pas lieu de conserver le document électronique relatif à l'offre mais la personne publique devrait en revanche conserver les documents propres à la candidature et la preuve de l'opération d'élimination de l'offre.

Document électronique dans lequel est détecté un virus informatique : la personne publique peut faire un "archivage de sécurité" sans lecture dudit document. Celui-ci est réputé n'avoir jamais été reçu et le candidat en est informé (art. 10 du décret du 30 avril 2002). Un archivage spécifique peut donc être mis en œuvre par la personne publique en particulier pour conserver la preuve du virus informatique.

2-2/ Pendant combien de temps ?

Candidatures retenues et offres retenues : la durée de conservation de ces dossiers variera selon l'objet du marché. Dix ans à compter de l'admission des prestations pour les marchés de fournitures ou de services (ou de la réception de ces prestations lorsqu'il est prévu que la conclusion de l'exécution de ces marchés se traduit par une opération de réception plutôt qu'une opération d'admission) et trente ans à compter de la réception pour les marchés de travaux. Ces durées peuvent être augmentées pour un marché compte tenu de ses caractéristiques eu égard à des questions de garantie ou de propriété intellectuelle.

Candidatures retenues et offres ouvertes non retenues : la circulaire du 30 décembre 1998 prescrit une durée de conservation minimale de cinq ans.

Candidatures non retenues : pour mémoire, l'offre correspondante à une candidature non retenue doit être éliminée des fichiers mais la personne publique devrait conserver les documents propres à la candidature et la trace de l'élimination de l'offre. Ces documents concernent la phase de passation et devraient être conservés comme les candidatures retenues et les offres ouvertes non retenues soit au minimum cinq ans.

Document électronique dans lequel est détecté un virus informatique : ici c'est la preuve de la présence d'un virus informatique qu'il conviendra de conserver. Ce virus étant détecté au cours de la phase de passation du contrat, un délai de conservation de cinq ans semble pouvoir être conseillé.

2-3/ Principes qui sous-tendent un archivage pérenne ?

Un document électronique est une donnée numérique indissociable des équipements logiciels et matériels capables de l'interpréter et de la rendre intelligible. Il en découle que la préservation d'un document électronique authentique ne peut se résumer à sa préservation en tant qu'objet physique entreposé (en d'autres termes, ne peut se contenter d'assurer l'intégrité, bit pour bit, de la donnée numérique) ; il faut plutôt préserver la capacité de rendre la donnée intelligible.

La tâche consiste par conséquent à déterminer les règles qui vont permettre d'évaluer l'authenticité des documents électroniques au moment de leur versement aux archives; et, d'autre part, d'assurer l'authenticité des copies des documents dont les archivistes ont la garde en mettant en place un système d'information fiable intégrant les procédures de description des documents produits ou reçus par une institution.

Plusieurs éléments sont à cet égard centraux :

- choisir dès la production (ou du moins prévoir une conversion à un moment donné du cycle de vie du document, dans un délai rapide), des formats de données dont les spécifications soient publiques et maîtrisées, par exemple, pour les documents texte, préférer XML si la structuration des documents est assez avancée, ou du moins, le format PDF ; pour les documents image, choisir le format TIFF ou PNG ;
- déterminer des attributs du document (métadonnées) dès sa production qui soient suffisamment riches et précis pour permettre son identification aisée dans le temps, tant au moment de sa production ou de sa réception que de son transfert sur un serveur d'archivage ;
- sécuriser les transmissions afin d'assurer l'intégrité des documents transmis et identifier précisément les acteurs ;
- assurer un contrôle et documenter ces contrôles et tests concernant les supports choisis de manière à prévenir les problèmes et anticiper les migrations nécessaires sur d'autres supports ;
- assurer une veille technologique sur les formats afin d'anticiper, si nécessaire, durant le cycle de vie du document, des migrations de formats ;
- documenter tous les événements de gestion et techniques pouvant affecter le document tout au long de son cycle de vie : transfert sur une autre plate-forme, changement d'archiviste, contrôles et tests réalisés, migrations éventuelles ;

- concernant la valeur juridique de l'acte, pondérer les exigences en matière d'intégrité (outils de signature et scellement mis en œuvre lors de la réception et de la production du document et durant les transmissions) et celles en matière de lisibilité : après une période de 5 ans, les migrations de format entraîneront la suppression des signatures. De nouvelles conventions de preuves seront alors à prévoir, qui seront fondées davantage sur des procédures organisationnelles.

3/ Les acteurs de l'archivage électronique.

Pour les marchés de l'Etat et des services de l'Etat, ce sont les services qui sont chargés, sous le contrôle des services publics d'archives, de l'archivage électronique des dossiers de marchés durant le temps de la DUA, puis à l'issue de cette DUA, pour les documents destinés à être conservés définitivement, les services publics d'archives qui prennent en charge cet archivage. Cependant, durant la période de la DUA, les services qui ne pourraient pas prendre en charge cet archivage, peuvent faire appel, sous le contrôle et avec l'autorisation des services publics d'archives (modalités explicitées dans la circulaire conjointe des ministres de l'Intérieur et de la Culture AD 97-1 du 16 janvier 1997) à des sociétés privées d'archivage.

Pour les collectivités territoriales, la procédure est identique à la différence près que ce recours exceptionnel à l'externalisation, durant le temps de la DUA, n'est pas permise, l'article R. 1421-2 du code général des collectivités territoriales faisant obligation à ces dernières, de conserver leurs documents durant la DUA, dans des bâtiments publics.

ANNEXE N°3 : ELÉMENTS DE CAHIER DES CLAUSES POUR LA RECHERCHE D'UN PRESTATAIRE DE SERVICES DANS LE CADRE DE LA MISE EN PLACE INITIALE D'UN SYSTÈME DE DÉMATÉRIALISATION DES PROCÉDURES D'ACHAT DE FOURNITURES DES ÉTABLISSEMENTS PUBLICS DE SANTÉ

REGLEMENT DE LA CONSULTATION

SERVICE ACHETEUR : Centre Hospitalier de

DATE LIMITE DE RECEPTION DES OFFRES : le JJ/MM/AA à xx heures

1. OBJET DE LA CONSULTATION

Le présent marché a pour objet de traiter la dématérialisation des procédures de marchés publics du Centre Hospitalier de

Ce marché comprend deux lots : (ou un seul si enchères électroniques non souhaitées)

Lot 1 : mise à disposition d'un support de dématérialisation des procédures de marchés publics.

Volet 1 : Mise à disposition du Règlement de Consultation

Volet 2 : Mise à disposition des CCAP et CCTP (ou CCP), consultation et téléchargement

Volet 3 : Réception des candidatures et des offres avec mise à disposition d'un séquestre

Volet 4 : Remise des candidatures et des offres avant ouverture par la PRM (candidatures) ou en CAO (offres)

Volet 5 : Clôture de la prestation et traçabilité de toutes les opérations

Lot 2 : réalisation d'enchères électroniques inversées.

2. PROCEDURE DE PASSATION

Le présent marché de services est passé selon la procédure de l'appel d'offres ouvert. Il est passé en application notamment des articles 33, et 57 à 59 du Code des Marchés Publics.

Chaque lot sera attribué à un seul soumissionnaire.

Chaque société pourra présenter sa candidature soit pour un lot, soit pour les deux lots de la consultation.

Les candidatures et les offres transmises par voie électronique ne seront pas acceptées. (clause possible uniquement jusqu'au 31/12/2004)

3. CONTENU DES OFFRES

L'offre de chaque candidat devra répondre expressément à l'ensemble des prescriptions formulées au cahier des clauses techniques particulières. (ou au CCP)

L'annexe financière à l'acte d'engagement devra être dûment complétée par chaque soumissionnaire et signée par une personne habilitée à engager la société.

Les offres devront être rédigées en langue française.

4. PRESENTATION DES OFFRES

Chaque candidat devra produire, dans une enveloppe cachetée, un dossier complet comportant deux enveloppes intérieures également cachetées. Ces enveloppes porteront respectivement la mention « CANDIDATURE » et « OFFRE ».

L'enveloppe « CANDIDATURE » comportera obligatoirement les justificatifs prévus aux articles 45 et 46 du Code des marchés publics, à savoir :

- la lettre de candidature (imprimé DC 4⁷).
- l'imprimé de déclaration du candidat DC 5 (remplaçant les imprimés DC 5E, DC 5F et DC 6).
- une attestation sur l'honneur du candidat indiquant qu'il n'a pas fait l'objet, au cours des cinq dernières années, d'une condamnation inscrite au bulletin n° 2 du casier judiciaire, pour les infractions visées aux articles L324-9, L324-10, L341-6, L125-1 et L125-3 du Code du travail.
- si l'entreprise est en redressement judiciaire, la copie du (ou des) jugement(s) prononcé(s) à cet effet.
- une déclaration sur l'honneur dûment datée et signée faisant état de la non-interdiction de concourir du candidat.
- une déclaration sur l'honneur dûment datée et signée certifiant que le candidat satisfait aux obligations fiscales et sociales ainsi que mentionné à l'article 46 du Code des marchés publics. S'il le souhaite, le candidat peut fournir à la place de cette attestation l'imprimé DC 7. Pour être valable, celui-ci devra concerner les obligations fiscales et sociales de l'année (année n-1)
- un extrait de registre du commerce de moins de trois mois (Kbis). Si le signataire des documents remis dans le cadre de la présente consultation ne figure pas au Kbis, l'extrait devra être accompagné d'un pouvoir l'habilitant à engager la société.
- un dossier de présentation de la société permettant à la personne publique d'apprécier les caractéristiques générales de l'entreprise, sa surface financière, son domaine de compétence ou son domaine privilégié d'intervention, ses références professionnelles et ses références clients, ses moyens techniques et en personnel.
- tous autres documents attestant des qualités et capacités du candidat au regard des critères de sélection des candidatures énoncés dans le présent règlement de la consultation.

L'enveloppe « OFFRE » comportera obligatoirement :

- l'offre,
- un acte d'engagement conforme au modèle joint (imprimé DC 8) ainsi que l'annexe financière. Ces deux documents devront être dûment complétés, datés et signés par une personne habilitée à engager la société et revêtus du cachet de ladite société,
- un relevé d'identité bancaire ou postal.

NB : tous les documents cités ci-dessus devront être fournis et figurer dans leurs enveloppes respectives sous peine de rejet.

5. DELAI DE VALIDITE DES OFFRES

Le délai de validité des offres est de xxx jours à compter de la date limite fixée par le présent règlement pour la réception des offres.

6. CONDITIONS D'ENVOI ET DE REMISE DES OFFRES

Les offres devront être transmises à l'adresse précise indiquée ci-dessous au plus tard le **JJ/MM/AA à xx heures**

Le dossier d'offre, présenté sous pli cacheté et contenant les deux enveloppes intérieures également cachetées, pourra être envoyé sous pli postal ou par tout moyen permettant de déterminer de façon certaine la date et l'heure de leur réception.

S'il est envoyé par voie postale en pli recommandé, le candidat devra faire en sorte que son dossier parvienne à destination avant ces mêmes date et heure limites.

Les dossiers qui seront reçus après la date et l'heure limites fixées ci-dessus ou sous enveloppe non cachetée ne seront pas retenus et seront renvoyés à leurs auteurs.

Le pli extérieur portera l'adresse suivante :

Adresse précise du Centre Hospitalier et du service destinataire (à l'attention de... pièce n° xxx, etc...)

Et la mention :

Appel d'offres n° xxxxx du « Appel d'offres Dématérialisation » - NE PAS OUVRIR -

7. CRITERES DE JUGEMENT

Pour les candidatures :

- capacités financières de la société (chiffre d'affaires global et chiffre d'affaires des trois dernières années relatifs à la fourniture de prestations identiques à l'objet du présent marché).
- références récentes (moins de 2 ans) pour des prestations similaires avec les noms et coordonnées (téléphoniques et mél) d'un responsable dans chaque organisme cité.

NB : les réponses à ces critères devront figurer dans l'enveloppe « CANDIDATURE ».

Pour les offres :

Les critères pris en considération pour le choix du titulaire sont les suivants (par ordre de priorité décroissant) :

- La qualité technique et fonctionnelle de l'offre
- Le coût complet de l'offre solution sur la durée du marché

(liste non limitative, voir CMP – utilisation de coefficients si choix de pondération, sinon hiérarchiser)

NB : les réponses à ces critères devront figurer dans l'enveloppe « OFFRE ».

8. MODE DE REGLEMENT – DELAI DE PAIEMENT

La personne publique se libérera des sommes dues au titre du présent marché par virement au compte du titulaire. Le délai global de paiement sera celui prévu à l'article 96 du CMP.

9. RENSEIGNEMENTS COMPLEMENTAIRES

Toute demande de renseignements complémentaires doit être formulée par écrit et parvenir à la personne publique au moins jours avant la date limite de remise des offres.

Ces demandes devront être transmises à l'adresse suivante :

Adresse précise

- **Appel d'offres « dématérialisation »** -

CAHIER DES CLAUSES PARTICULIERES

Pour un marché de services ayant pour objet de traiter la dématérialisation des procédures de marchés publics du Centre Hospitalier de

1. CONTEXTE DE L'INTERVENTION

Dans le cadre de l'art. 56 du CMP, le Centre Hospitalier de s'emploie à mettre en œuvre les possibilités de dématérialisation de l'achat public permises pour l'ensemble de ses services achats.

1.1. Le cadre juridique

Sur le plan juridique, le projet est encadré par l'article 56 du Code des Marchés Publics complété par les décrets du 30 avril 2002 pris en application du 1° et du 2° de l'article 56 et du 18 septembre 2001 pris en application du 3° de l'article 56 (*ce dernier ne concerne que les enchères électroniques inversées*).

1.2. Identification des candidats

L'identification et l'authentification des sociétés se feront par des certificats délivrés par les autorités de certification dont les familles de certificats sont référencées par le Ministère de l'Economie, des Finances et de l'Industrie (MINEFI), voir : Les familles de certificats référencées par le MINEFI

(http://www.minefi.gouv.fr/dematérialisation_icp/dematérialisation_declar.htm)

1.3. Identification des acheteurs

Il est envisagé d'utiliser des certificats distribués par des autorités de certification pour l'identification et l'authentification des acheteurs du Centre Hospitalier de Les autorités de certification externes devront cependant avoir été référencées par le MINEFI.

1.4. Organisation

(ici sera décrite le plus précisément possible l'organisation interne du Centre Hospitalier de en terme de circuits d'approvisionnement, centralisation ou non, nombre de PRM, identification des services acheteurs, une ou plusieurs CAO, nombre d'intervenants et des renseignements précis sur la volumétrie des marchés envisagés)

2. L'OBJET DU MARCHE

La prestation porte sur la dématérialisation des procédures de marchés publics du Centre Hospitalier de

Ce marché comprend deux lots :

Lot 1 : mise à disposition d'un support de dématérialisation des procédures de marchés publics.

Lot 2 : réalisation d'enchères électroniques inversées.

LOT 1 : Mise à disposition d'un support de dématérialisation des procédures de marchés publics

Le lot est composé de cinq volets :

Volet 1 : Mise à disposition du Règlement de Consultation (RC)

Le RC, fourni par le Centre Hospitalier, doit être mis à disposition des candidats intéressés sur site Internet en accès libre sans condition d'identification.

Volet 2 : Mise à disposition des CCAP et CCTP (ou CCP), consultation et téléchargement

Les CCAP, CCTP et documents annexes, fournis par le Centre Hospitalier doivent être mis à disposition des candidats intéressés sur site Internet après identification selon les modalités ci-dessous.

Préalablement au téléchargement du DCE, les personnes intéressées devront fournir, sur le formulaire prévu à cet effet qui apparaîtra à l'écran : le nom de leur entreprise, le nom de la personne physique qui procède au téléchargement du dossier, ainsi qu'une adresse de courrier électronique permettant, de façon certaine, une correspondance électronique assortie d'une procédure d'accusé de réception. Un code d'accès leur sera alors fourni, leur permettant le téléchargement du DCE.

Une traçabilité de ces demandes est assurée par le prestataire qui, si besoin, adressera ainsi à tous les demandeurs un avis par lequel des modifications ont été apportées au dossier, à charge pour ceux-ci de venir en prendre connaissance.

Volet 3 : Réception des candidatures et des offres avec mise à disposition d'un séquestre.

Un séquestre électronique permet d'accepter des documents (candidatures et/ou offres) signées jusqu'à l'expiration du délai de la procédure, la conservation des documents jusqu'à la date d'ouverture par la PRM ou en CAO, l'ouverture sécurisée des documents et trace toutes les actions faites sur les documents.

Le Centre Hospitalier de souhaite utiliser une solution hébergée de séquestre électronique sur site sécurisé (https) pour les besoins de ses acheteurs.

La solution doit permettre le séquestre des réponses aux avis d'appel public à la concurrence pour des appels d'offres ouverts ou restreints : réception de doubles enveloppes candidature et offre, réception de candidatures, réception d'offres.

Le prestataire doit s'assurer de l'absence de virus par utilisation d'un antivirus régulièrement mis à jour, du dépôt des candidatures et des offres jusqu'à l'ouverture par la PRM ou la CAO. En cas de détection d'un virus dans le dossier reçu, le prestataire en avertira la PRM qui prendra les dispositions nécessaires.

Le prestataire mettra à disposition de la personne publique un système permettant la gestion des accusés de réception.

Le prestataire doit garantir la confidentialité et l'intégrité des données déposées par les candidats.

Pour la sécurité des échanges et l'authentification des services acheteurs et des entreprises candidates et soumissionnaires, la solution proposée devra pouvoir utiliser au moins une des familles de certificats référencées par le MINEFI.

L'achat de certificats est à la charge de l'administration pour les services acheteurs et à la charge des entreprises pour les fournisseurs.

Volet 4 : Remise des candidatures et des offres avant ouverture par la PRM (candidatures) ou en CAO (offres). (en fixer ici date et modalités)

Volet 5 : Clôture de la prestation et traçabilité de toutes les opérations (y compris réception et conservation des fichiers contenant des virus) avec livraison d'un support contenant toutes ces données en fin de prestation (archivage de sécurité).

Statistiques, « journal des événements » et éléments pour le Rapport de Présentation.

Prestations demandées pour l'ensemble des volets :

Accompagnement des utilisateurs du Centre Hospitalier de

Assistance aux entreprises candidates

L'exploitation de la solution dans l'environnement du prestataire (hébergement du séquestre).

La fourniture des traces d'utilisation du séquestre à chaque fin de procédure, aux fins de vérification qu'il n'y a pas eu d'accès illégal.

La fourniture de statistiques d'utilisation de la plate-forme. (à définir par l'utilisateur)

Réponse du candidat

La proposition du candidat comprendra les éléments suivants :

- Une description fonctionnelle générale de la solution, y compris le traitement des points suivants : virus, formats des documents, traitement des erreurs des utilisateurs, disponibilité de la plate-forme, capacités de paramétrage, capacités d'intégration dans un autre site, gestion des utilisateurs

- Des recopies d'écran montrant la cinématique et l'ergonomie de la soumission d'une offre par l'entreprise, d'une part pour un appel d'offres ouvert, d'autre part pour un appel d'offres restreint

- Des recopies d'écran montrant la cinématique et l'ergonomie de l'ouverture des plis en commission

- Des recopies d'écran montrant la cinématique et l'ergonomie du paramétrage de la solution

- La liste des familles de certificats utilisables par les entreprises et les services acheteurs

- Les caractéristiques techniques du dispositif d'horodatage

- Les informations fournies au titre des traces d'utilisation du séquestre
- Les informations fournies au titre des statistiques d'utilisation du séquestre
- Un planning des prestations à compter de la date de notification du marché
- Une offre commerciale détaillant les différents volets

LOT 2 : Réalisation d'enchères électroniques inversées

Dans le cadre des possibilités offertes par le Code des Marchés Publics, le Centre Hospitalier de souhaite recourir aux enchères électroniques inversées pour les marchés d'acquisitions de fournitures courantes, voire de certains services en dessous des seuils.

Le recours à des enchères électroniques inversées est dissocié de la dématérialisation de la procédure d'appel d'offres. Il peut aussi être réalisé dans le cas de MPSPA.

Les enchères peuvent porter sur le prix et sur d'autres caractéristiques de l'offre.

Les enchères peuvent être réalisées en vue de l'attribution d'un marché ou en vue de l'attribution d'une commande dans le cadre d'un marché multi-attributaire.

L'exploitation de la solution devra être assurée dans l'environnement (site) du prestataire.

Seront fournies à chaque fin de procédure les traces d'utilisation de la plate-forme d'enchères, aux fins de vérification qu'il n'y a pas eu d'accès illégal pendant l'enchère, ainsi qu'un historique des offres à la fin de chaque enchère.

Sur la durée du marché, la plate-forme d'enchères sera utilisée pour (fourchette de nombre) procédures d'achats.

Aucune facturation ne sera adressée aux entreprises participant à des enchères.

Le prestataire de services assiste le service acheteur tout au long de la procédure d'achat depuis l'expression du besoin jusqu'à l'attribution du marché.

Sur la base d'une première expression des besoins de l'administration, le prestataire est chargé de :

- Rédiger une fiche sur le déroulement de la procédure jusqu'à son terme, fiche qui sera intégrée au dossier de consultation téléchargé par les candidats potentiels.
- Assister l'administration dans la rédaction des documents nécessaires à la consultation (CCTP, CCAP, règlement de la consultation dans le cas d'un appel d'offres ouvert ou restreint ; les documents pertinents dans le cas d'un marché sans formalisme) pour ce qui concerne la partie « enchères électroniques », objet du présent marché,
- Analyser qualitativement et techniquement les offres,
- Proposer les paramètres de prix et de caractéristiques des offres pertinents pour l'enchère,
- Homogénéiser les offres sur la base de ces paramètres afin de les rendre comparables,
- Organiser l'enchère inversée et paramétrer la plate-forme,
- Former les entreprises à l'utilisation de la plate-forme : envoi d'un guide utilisateur, et simulation d'enchères en ligne.
- Assister les entreprises pendant l'enchère dans le respect strict de la confidentialité : aide téléphonique + procédure de dépannage en cas de problème de connexion.
- Un bilan de l'enchère.

L'administration conserve à sa charge la rédaction des documents nécessaires à la passation du marché, notamment les avis d'appels à la concurrence, les CCAP, CCTP (ou CCP) et règlement de la consultation.

Réponse du candidat

La proposition du candidat comprendra les éléments suivants :

- une description fonctionnelle générale de la solution, y compris le traitement des points suivants : traitement des erreurs des utilisateurs, capacités de paramétrage, capacités d'intégration dans un autre site, gestion des utilisateurs ;
- des recopies d'écran montrant la cinématique et l'ergonomie de l'enchère du point de vue des entreprises et du point de vue du service achat ;
- des recopies d'écran montrant la cinématique et l'ergonomie du paramétrage de la solution ;
- les informations fournies au titre des traces d'utilisation de la plate-forme d'enchères ;
- les informations fournies au titre de l'historique des offres de chaque enchère ;
- description détaillée des prestations d'accompagnement proposées et une indication des différentiels de délais à prévoir par rapport aux procédures ne recourant pas aux enchères.

ANNEXE N°4 : COMITÉ DE RÉDACTION

M. Guy LÉBOUVIER, pharmacien des hôpitaux, CHU de Caen, président du Comité A6 du Groupe Permanent d'Études des Marchés/Soins et Laboratoires (GPEM/SL).

M. Christophe ALVISET, sous-direction Informatique et Nouvelles Technologies de la DPMA du MINEFI.

Mme Brigitte CANDELON, coordinatrice du Groupe Permanent d'Études des Marchés/Soins et Laboratoires (GPEM/SL), Direction des Affaires Juridiques du MINEFI.

M. Pascal FAVARO, Pharmacien Chimiste Principal, Direction des Approvisionnements et des Établissements Centraux du Service de Santé des Armées, Chef de la Division Achats.

M. Michel FORTIER, chef du Bureau de la Prospective et des Affaires Techniques, Direction des Affaires Juridiques du MINEFI.

M. Jean-Luc GENAY, consultant, Bureau de la Prospective et des Affaires Techniques, Direction des Affaires Juridiques du MINEFI.

M. Philippe GIRAULT, pharmacien, Directeur Commercial, Laboratoires AMGEN, représentant le LEEM (Les Entreprises du Médicament).

M. Marc LAMBERT, pharmacien des hôpitaux, Assistance Publique Hôpitaux de Marseille, Service Central Pharmacie et Médicament.

M. Jacques LEBAS, pharmacien des hôpitaux honoraire, président du Groupe Permanent d'Études des Marchés/Soins et Laboratoires (GPEM/SL).

Mme Anne MOULIN, directeur, Direction des Technologies de l'Information et des Télécommunications, CHU de Montpellier.

M. Pascal PAUBEL, pharmacien des hôpitaux, Direction Hospitalisation et Organisation des Soins (DHOS), Ministère de la Santé puis Centre hospitalier Sainte-Anne (Paris).

M. Thomas PELEN, Société Becton-Dickinson SA, représentant le SNITEM (Syndicat National de l'Industrie des Technologies Médicales).

M. Gérard PLANTIER, directeur de la direction Informatique, Hospices Civils Lyon.

M. Jean-Claude PLASSE, pharmacien des hôpitaux, Pharmacie centrale des Hospices Civils de Lyon.

M. René ROUANET, informaticien, Délégation à l'Informatique Hospitalière / CHU de Toulouse.

ANNEXE N°5 : COMITÉ DE LECTURE

Lieutenant Gabriel BARTOLINI, adjoint au chef du bureau "Achat public", Sous-Direction "Affaires administratives et juridiques", Direction centrale du Service de Santé des Armées

Mme Jacqueline BERLIOZ, pharmacien des hôpitaux, Centre Hospitalier Aix-les-Bains

M. Hervé CHARBIT, directeur, CHU de Dijon

M. DUBUC, directeur commercial / HILLROM

M. Jean-Louis FERRACCI, chargé de la politique de sécurité des téléprocédures pour le MINEFI, Délégation aux Systèmes d'Information, Ministère de l'Economie, des Finances et de l'Industrie

M. Jean-Christophe GODOT, Délégation aux Systèmes d'Information, Ministère de l'Economie, Finances et de l'Industrie

Mme Martine GUEDJ, directeur adjoint, Direction des Equipements et des Approvisionnements Médicaux et Pharmaceutiques, Assistance Publique-Hôpitaux de Marseille

Mme Marie-Hélène GUIGNARD, pharmacien des hôpitaux, Centre Hospitalier de Creil

Mme Annick ICOLE, consultante, Bureau de la Prospective et des Affaires Techniques, Direction des Affaires Juridiques du MINEFI

Capitaine Alexis KOUMBACHEFF, chef du bureau "Achat public", Sous-Direction "Affaires administratives et juridiques", Direction centrale du Service de Santé des Armées

Mme Agathe LAPORTE, élève directeur DESS, Hôpital Local de Penne d'Agenais (47)

Mme Esther LANASPA, chargée de mission Dématérialisation de l'achat public, Services du Premier Ministre, Agence pour le Développement de l'Administration Electronique

M. Robert LEROYER, pharmacien des hôpitaux, CHU de Caen

M. Roland MARGUERET, chargé de l'infrastructure de gestion de clés pour l'administration centrale du MINEFI, Sous-direction de l'Informatique, Direction du Personnel, de la Modernisation et de l'Administration, Ministère de l'Economie, des Finances et de l'Industrie

M. Emmanuel MORNET, chef du projet Dématérialisation de l'achat public pour le MINEFI, Sous-direction de l'Informatique, Direction du Personnel, de la Modernisation et de l'Administration, Ministère de l'Economie, des Finances et de l'Industrie

Mme Marie-José PALASZ, chef de service à la Direction des Affaires Juridiques, Ministère de l'Economie, des Finances et de l'Industrie

M. SCHROEDER, directeur Affaires Industrielles, SNITEM

M. Olivier SELLAL, pharmacien des hôpitaux, CHU de Nantes.

Version du 27/05/04

M. SIRCOULOMB, directeur, BD Diagnostics – Preanalytical Systems

Mme Geneviève TERRIEN, directeur, Hôpital Local de Penne d'Agenais (47)

M. Fabrice THEVAUX, adjoint au chef de bureau, Bureau du conseil aux acheteurs publics, Direction des Affaires Juridiques du MINEFI

Mme Marie-Agnès URBINA, pharmacien des hôpitaux, Centre Hospitalier de Valenciennes

M. Ange VILERBU, chef du secteur Marchés, Sous-direction de l'Informatique, Direction du Personnel, de la Modernisation et de l'Administration, Ministère de l'Economie, des Finances et de l'Industrie