

## **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 <sup>9</sup>
Lecture du RC par les personnes intéressées		X <sup>9</sup>
Téléchargement du DCE et mise à disposition des outils de lecture en libre disposition		X <sup>9</sup>
Identification des téléchargeurs		X <sup>9</sup>
Réception des candidatures	X <sup>10</sup> (01/01/05)	
Réception des offres	X (01/01/05)	
Gestion de l'ouverture des plis : Libération 1 <sup>ère</sup> enveloppe, Ouverture 1 <sup>ère</sup> enveloppe, Recevabilité candidature, Libération ou destruction 2 <sup>ème</sup> enveloppe, Ouverture 2 <sup>ème</sup> 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

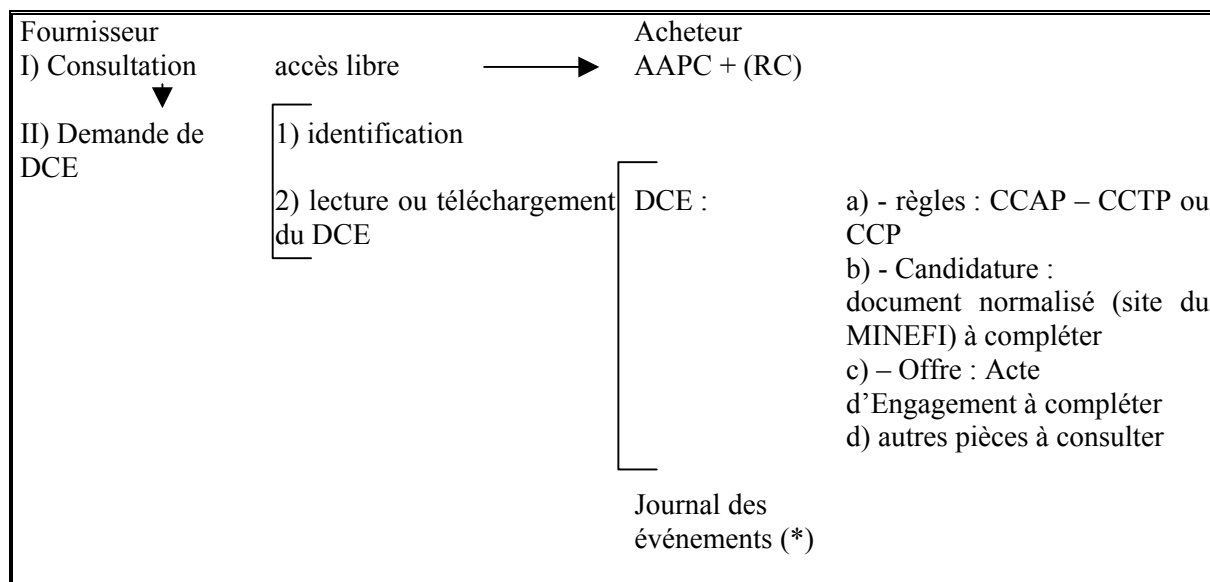
Chacune des phases principales de la procédure est décrite ci-après dans un tableau synthétique suivi d'un développement explicatif.

<sup>9</sup> 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).

<sup>10</sup> cf art. 56 du CMP, alinéa 2 : « ... Aucun avis ne pourra comporter d'interdiction à compter du 1<sup>er</sup> 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 2<sup>nd</sup> 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<sup>ème</sup> 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 :

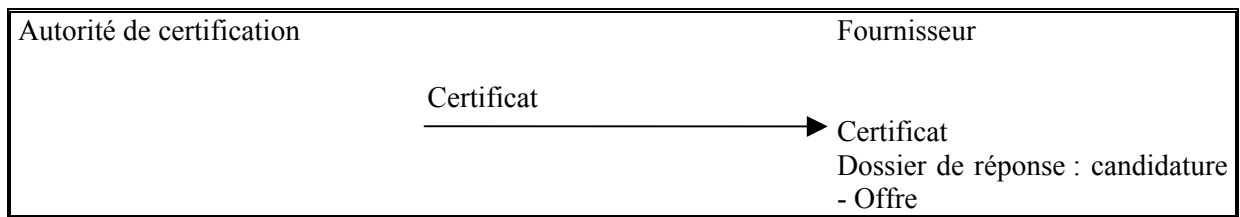
- désigner la personne habilitée à les représenter ;
- mettre en place une procédure permettant à la PRM de s'assurer que c'est bien la personne habilitée qui signe et transmet les candidatures et les offres (authentification de la signature électronique) ;
- transmettre par voie électronique, dans le 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 certification<sup>10</sup>. 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.

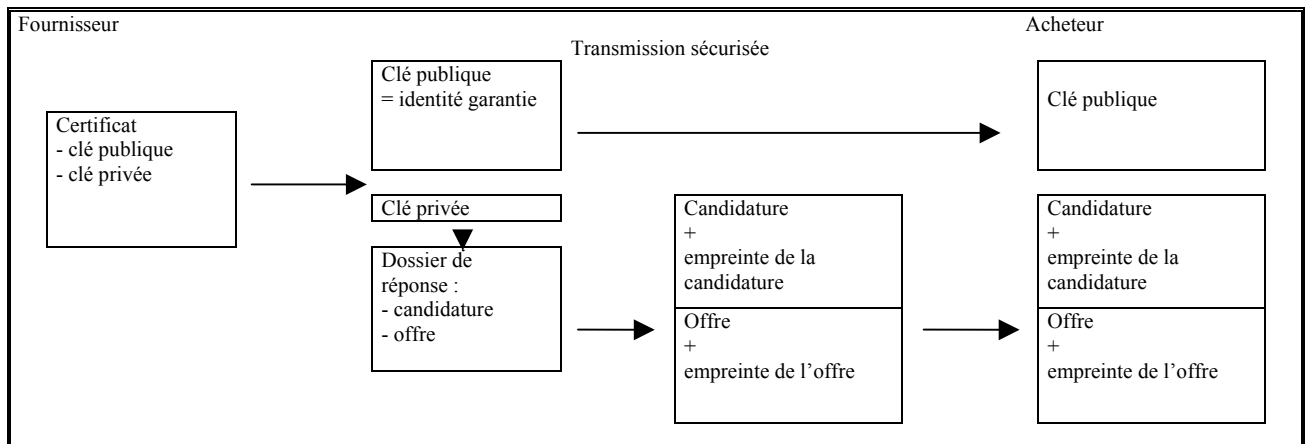
### 5.2.2 Envoi de la candidature et de l'offre

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



<sup>10</sup> 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.

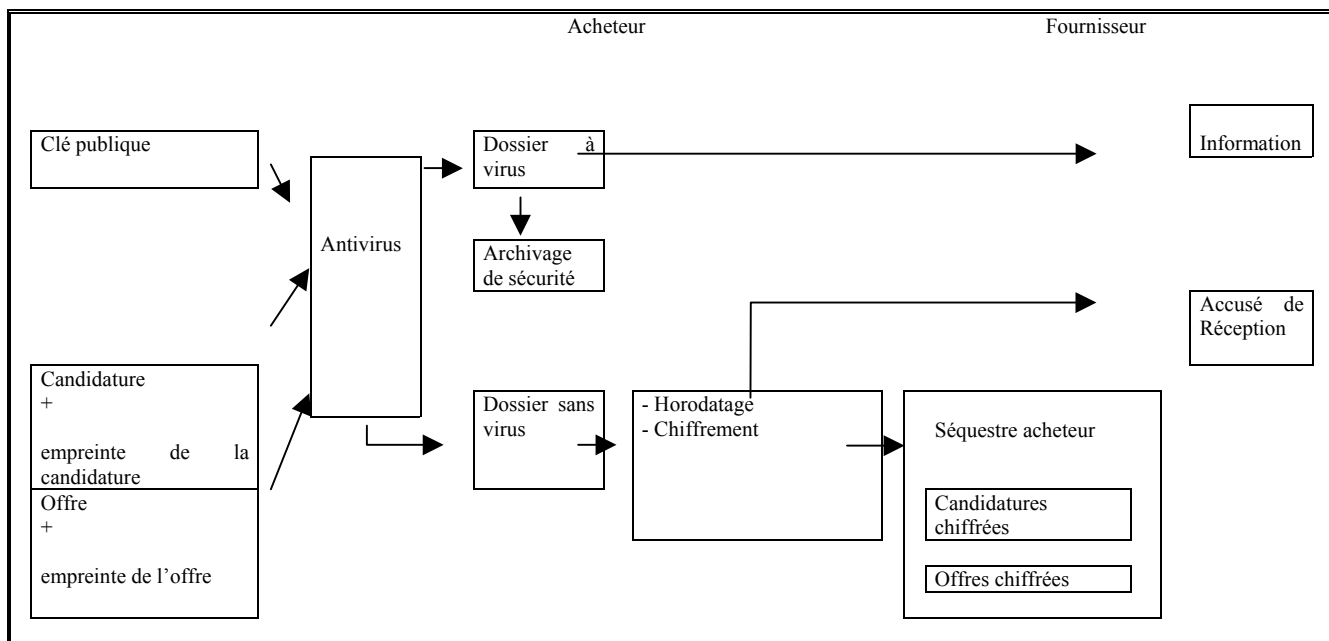
Pour sa part, la personne publique est soumise aux obligations suivantes :

- 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.

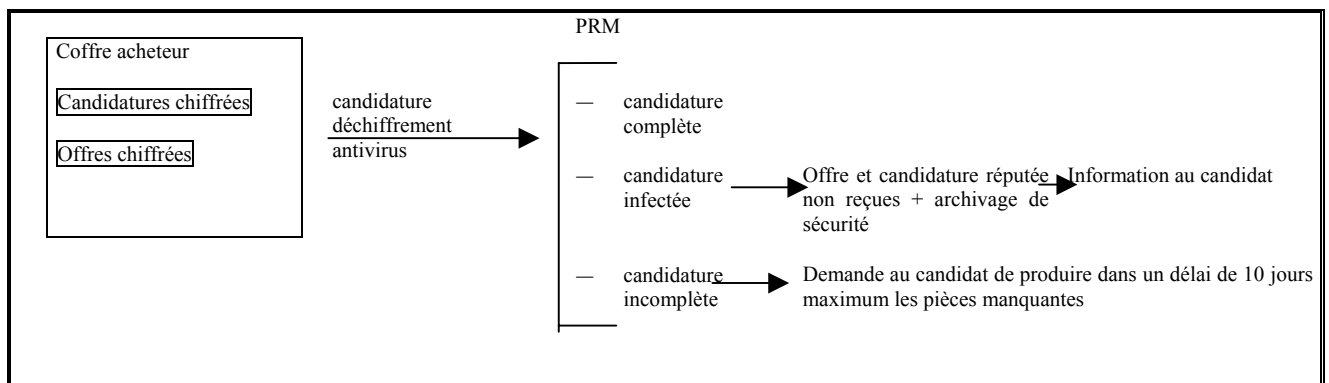
Chaque candidat à un marché public doit disposer d'un certificat d'authentification et d'une clé privée. Des empreintes sont effectuées sur les documents afin d'assurer l'authentification et la sécurité des offres (deux « fichiers-enveloppes » contenant les candidatures et les offres, chaque fichier 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<sup>er</sup> 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 ;

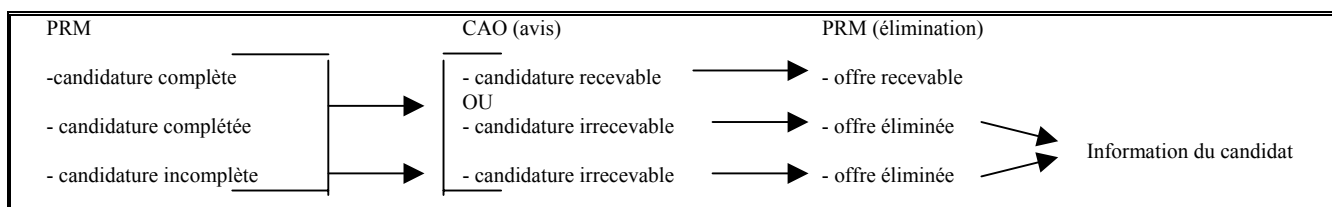
- informer les soumissionnaires en cas de détection d'un virus, entraînant un archivage de sécurité.

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

Selon le 1<sup>er</sup> 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 habilitées<sup>11</sup> 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.

<sup>11</sup> 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.