# TRANSMISSION PAR VOIE ELECTRONIQUE

Les offres sont transmises en une seule fois. Si plusieurs offres sont adressées ou transmises successivement par un même candidat, seule la dernière reçue dans le délai fixé pour la remise des offres sera ouverte.

## 1 - Définition de la dématérialisation

La dématérialisation des marchés publics se traduit par l'utilisation de la voie électronique pour les échanges qui interviennent dans le processus d'achat public et qui entrent dans le champ d'application de l'article L2132-2 du Code de la commande Publique.

En vertu de l'article R2132-7 du Code de la commande publique, un candidat peut transmettre son offre par voie électronique, c'est à dire via le réseau Internet, qui peut être signée électroniquement par une personne habilitée. Il convient de ne pas confondre la transmission par voie électronique avec la transmission d'un support électronique (CD-Rom...) par voie postale, cette dernière étant assimilée à une transmission sur support papier.

Pour signer électroniquement, sont nécessaires un **certificat de signature électronique et un logiciel de signature.** Toutefois, un opérateur économique n'a pas besoin de disposer d'un logiciel de signature s'il utilise un portail (profil acheteur du pouvoir adjudicateur, plate-forme de dématérialisation) offrant cette fonctionnalité.

**Depuis le 1er octobre 2012**, les opérateurs économiques souhaitant signer leurs documents par voie électronique sont autorisés à utiliser le certificat et l'outil technique de leur choix, sous certaines conditions.

## 2 - Modalités d'envoi des candidatures et des offres électroniques

***« Le pli déposé par un candidat, sur la plateforme Maximilien, ne pourra excéder 4 Go. La taille maximale d'un fichier ne pourra excéder, quant à elle, 1Go. Au-delà, l'offre du candidat sera refusée par la plateforme Maximilien.***

La transmission des documents par voie électronique est effectuée sur le profil d'acheteur du pouvoir adjudicateur, à l'adresse URL suivante : http://www.valdemarne.fr

Le choix du mode de transmission est global et irréversible. Les candidats doivent appliquer le même mode de transmission à l'ensemble des documents transmis au pouvoir adjudicateur.

Chaque transmission fera l'objet d'une date certaine de réception et d'un accusé de réception électronique. A ce titre, le fuseau horaire de référence est celui de (GMT+01:00) Paris, Bruxelles, Copenhague, Madrid. Le pli sera considéré « hors délai » si le téléchargement se termine après la date et l'heure limites de réception des offres.

*« En application de l'article R 2151-6 du code de la commande publique**, si un nouveau pli est envoyé par voie électronique par le même candidat, celui-ci annule et remplace le pli précédent.** Aussi, si un candidat souhaite apporter un complément au sein de son pli électronique, il devra remettre un nouveau pli contenant l'ensemble des pièces, et ce, avant la date limite de remise des offres ».*

Cette plateforme de dématérialisation qui constitue le profil acheteur du Conseil départemental du Val-de-Marne, permet de :

- Rechercher et consulter les avis et consultations du Conseil départemental
- Télécharger les Dossiers de Consultation des Entreprises (DCE)
- Remettre sous forme électronique vos réponses aux marchés

**Afin de pouvoir signer vos documents le cas le cas échéant, veillez à vérifier si vous disposez bien d'un certificat électronique**

*a) Contenu de la réponse*

Voir le Règlement de consultation.

*b) Format acceptés et règles de nommage :*

Les documents doivent être réunis en un fichier unique au format « compressé » contenant les éléments mentionnés au tableau plus avant du présent document. Ces éléments seront des fichiers dans l'un des formats suivants :

- compatible Word 2010 ou inférieur (*.docx)
- compatible Excel 2010 ou inférieur (*.xlsx)
- compatible Acrobat Reader 9
- Autocad version 2010.

Par inférieur, on entend version 97.

Les fichiers seront nommés significativement, par exemple : DC2.doc ou AE.doc.

Le candidat veillera, au moment du dépôt de son offre, à ce que chaque document ait un intitulé court et surtout UNIQUE, afin qu'aucun document ne soit considéré comme un doublon d'un autre document

*c) Virus*

Avant transmission de sa réponse, le soumissionnaire devra procéder à un contrôle anti-virus de tous les fichiers constitutifs des enveloppes électroniques.

Après dépouillement de chaque enveloppe, le Conseil départemental du Val-de-Marne procédera à une analyse anti-virus de son contenu avec Norton Antivirus. Les plis contenant des virus feront l'objet d'un archivage de sécurité. Ces plis seront donc réputés n'avoir jamais été déposés et les candidats en seront informés dans les plus brefs délais.

Lorsqu'elles sont accompagnées d'une copie de sauvegarde, les offres transmises par voie électronique et dans lesquelles un programme informatique malveillant est détecté par le pouvoir adjudicateur donnent lieu à l'ouverture de la copie de sauvegarde.

*d) Se préparer à l'avance*

**Nécessité de certificat numérique – Configuration à l'avance du poste de travail - Recommandation de se préparer avec la consultation de test**

Dans l'éventualité où vous souhaiteriez signer électroniquement, vous devrez avoir au préalable fait l'acquisition d'un certificat électronique. Obtenir un certificat électronique prend plusieurs jours, voire plusieurs semaines. Si le soumissionnaire ne possède pas de certificat électronique valable dans le cadre de la réponse à un marché dématérialisé, il est impératif qu'il en fasse la demande à l'avance.

Il est également fortement recommandé au soumissionnaire de prendre ses dispositions de manière à ce que sa réponse électronique soit déposée dans les délais impartis. Un test de configuration du poste de travail ainsi que des consultations de test sont mis à sa disposition sur la plateforme (cf. Guide Utilisateur). Ces vérifications sont indispensables s'il s'agit de votre première réponse électronique mais également si vous disposez d'un nouveau poste informatique.

**Avertissement et recommandation aux Entreprises**

En disposant d'une bande passante effective de 128 kbps, une minute est nécessaire pour télécharger un fichier de 1 Mo. L'attention des entreprises est donc attirée sur la durée d'acheminement des plis électroniques volumineux : c'est la date et l'heure de fin d'acheminement qui font foi lors de la remise d'une réponse dématérialisée. Les entreprises sont donc invitées à intégrer des marges de manœuvre dans leur processus de réponse, pour tenir compte de ces délais d'acheminement.

**Un service de support téléphonique est mis en place pour les entreprises souhaitant soumissionner aux marchés publics.**
**Le service de support est ouvert de 9h00 à 19h00 les jours ouvrés.**
**Le n° d'accès est 01 76 64 74 08 (prix d'un appel local).**

*e) Transmission d'une copie de sauvegarde*

Voir Règlement de consultation.

## 3 - Si vous utilisez la possibilité de signer les documents

*a) Le cadre règlementaire*

**L'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics** et publié au Journal officiel du 3 juillet 2012, autorise les signataires par voie électronique à utiliser le certificat et la signature de leur choix, sous réserve de sa conformité aux normes du référentiel général d'interopérabilité et au référentiel général de sécurité.

Le **Référentiel Général d'Interopérabilité** (**RGI**) est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

Le **Référentiel Général de Sécurité** (**RGS**) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information (ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre autorités administratives)

*b) Choix du certificat de signature ET choix de l'outil de signature utilisés*

Les documents du soumissionnaire qui seraient signés électroniquement, le sont selon les modalités détaillées ci-dessous.

Par application de l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics en vigueur à partir du 1er octobre 2012, le candidat doit respecter les conditions relatives :

- Au certificat de signature du signataire
- À l'outil de signature utilisé (logiciel, service en ligne), devant produire des signatures électroniques conformes aux formats réglementaires

Ces conditions sont décrites ci-après. Il est impératif que le soumissionnaire en prenne connaissance avec attention. En effet, selon les choix du soumissionnaire concernant le certificat utilisé (Cas C1 ou C2) d'une part et l'outil de signature utilisé (Cas OS1 ou OS2) d'autre part, il lui faut produire différents types de justificatifs, tels que précisés dans les articles qui suivent.

| | Certificat reconnu (cas C1) | Certificat non référencé (cas C2) |
|---|---|---|
| **Outil de signature de la plate-forme (cas OS1)** | Aucun justificatif à fournir | Justificatifs "Autorité de certification" à fournir |
| **Outil de signature de soumissionnaire (cas OS2)** | Justificatifs "Outil de signature" à fournir | Justificatifs "Autorité de certification" à fournir<br>Justificatifs "Outil de signature" à fournir |

*c) Exigences relatives au certificat de signature du signataire*

Le certificat de signature du signataire doit être conforme au RGS (Référentiel général de sécurité) ou équivalent et respecter le niveau de sécurité exigé. Pour le Conseil départemental du Val-de-Marne, ce niveau de sécurité est de Niveau II (équivalent classe 3).

**Cas C1 : Certificat émis par une Autorité de certification "reconnue" - Aucun justificatif à fournir**

Des certificats de signature qualifiés RGS sont commercialisés par des prestataires de service de confiance qualifiés.

**Dans ce cas, le soumissionnaire n'a aucun justificatif à fournir sur le certificat de signature utilisé pour signer sa réponse.**

Il n'existe pas de liste officielle des produits RGS commercialisés et utilisables pour les marchés publics, mais la société LSTI (La Sécurité des Technologies de l'Information), organisme accrédité par le COFRAC (Comité Français d'Accréditation), est au 15 avril 2013 la seule habilitée à qualifier des prestataires de service de confiance qualifiés.

La page d'accueil du site de LSTI (consultable depuis son adresse : http://www.lsti-certification.fr/) propose un onglet « Prestataires qualifiés RGS » qui permet d'accéder à un tableau dénommé « Liste des prestataires de certification électronique qualifiés ». Ce tableau fournit les noms des prestataires et donne la liste, pour chacun d'eux, des produits ou services qu'il a développé et parmi lesquels, pour certains prestataires, figurent des certificats qui permettent la signature des candidatures et des offres.

L'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés prévoit que le certificat de signature utilisé puisse appartenir à l'une des catégories de certificats délivrées par une autorité de certification figurant sur la liste de confiance d'un Etat-membre, telle qu'établie, transmise et mise à disposition du public par voie électronique par la Commission européenne. Ces listes de confiance sont consultables sur l'outil EU Trust Service statuts List (TSL) Analysis Tool à l'adresse suivante : http://eutsl.3xasecurity.com

La plateforme Maximilien tient également à jour la liste des autorités délivrant des certificats conformes RGS en France:
https://marches.maximilien.fr/index.php?page=commun.ListeAcRGS&calledFrom=entreprise

**Cas C2 : Le certificat de signature électronique n'est pas référencé sur une liste de confiance - Différents justificatifs à fournir**

La plateforme de dématérialisation accepte tous les certificats de signature électronique présentant des conditions de sécurité équivalentes à celles du Référentiel général de sécurité (RGS).

Le candidat s'assure par lui-même que le certificat qu'il utilise est au moins conforme au niveau de sécurité défini par le Référentiel général de sécurité (RGS), et en fournit les justificatifs dans sa réponse électronique.

Le candidat fournit également tous les éléments techniques permettant à l'acheteur de s'assurer de la bonne validité technique du certificat utilisé. Ainsi, le signataire doit transmettre avec sa réponse électronique les éléments suivants :

1) tout élément permettant la vérification de la qualité et du niveau de sécurité du certificat de signature utilisé :
    a. preuve de la qualification de l'Autorité de certification ou compte-rendu d'audit,
    b. politique de certification,
    c. adresse du site internet du référencement de l'Autorité de certification par le pays d'établissement,
    d. etc.
2) les outils techniques de vérification du certificat :
    a. chaîne de certification complète jusqu'à l'Autorité de Certification racine,
    b. adresse de téléchargement de la dernière mise à jour de la liste de révocation des certificats (CRL)

Il est précisé que tous ces éléments doivent être d'accès et d'utilisation gratuits pour l'acheteur, et être accompagnés le cas échéant de notices d'utilisation claires, en français.

*d) Outil de signature utilisé pour signer les fichiers*

La réglementation autorise le soumissionnaire à utiliser l'outil de signature de son choix.

**Cas OS1 : Le soumissionnaire utilise l'outil de signature de la plate-forme - Aucun justificatif à fournir**

La plate-forme intègre un outil de signature électronique, qui réalise des Jetons de signature au format réglementaire XAdES.

**Dans ce cas, le soumissionnaire n'a aucun justificatif à fournir sur les signatures électroniques transmises et l'outil de signature utilisé.**

**Cas OS2 : le soumissionnaire utilise un autre outil de signature que celui intégré à la plate-forme - Différents justificatifs à fournir**

Lorsque le candidat utilise un autre outil de signature que celui de la plate-forme, il doit respecter les deux obligations suivantes :

1) produire des formats de signature XAdES, CAdES ou PAdES.
2) permettre la vérification en transmettant en parallèle les éléments nécessaires pour procéder à la vérification de la validité de la signature et de l'intégrité du document, et ce, gratuitement.

Ainsi, le signataire doit transmettre avec sa réponse électronique les éléments suivants :

1) indication du format de signature utilisé :
    a. format technique (XAdES, CAdES ou PAdES),
    b. mode d'accès à la signature ("signature enveloppée" ou "signature détachée", cf. Définition en Annexe),
    c. extension du fichier informatique du jeton de signature en cas de signature détachée (ex: extension "*.xml")

2) indication de l'outil de signature utilisé :
    a. nom de l'outil,
    b. éditeur,
    c. description succincte (ex : site Internet de présentation)

3) indication de l'outil de vérification de signature correspondant, devant être accessible par l'acheteur public :
    a. lien internet de récupération de l'outil ou fourniture de l'outil lui-même
    b. notice d'utilisation en langue française
    c. présentation des d'installation : type d'exécutable, systèmes d'exploitation supportés, etc.
    d. procédure de vérification alternative en cas d'installation ou de vérification impossible pour l'acheteur : contact à joindre, support distant, support sur site, etc.

Il est précisé que tous ces éléments doivent être d'accès et d'utilisation gratuits pour l'acheteur, et être accompagnés le cas échéant de notices d'utilisation claires, en français.

*e) Dossier format compressé et signature scannée*

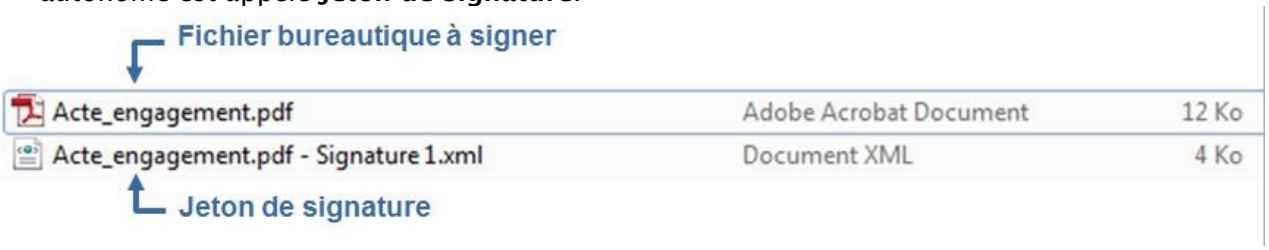
Rappels généraux :

- Tous les documents dématérialisés qui seraient signés électroniquement auraient la même valeur que les documents papier qui seraient signés de manière manuscrite.
- Chaque fichier qui serait signé doit être signé individuellement, de telle sorte que chaque signature puisse être vérifiée indépendamment des autres.
- Un dossier format compressé signé n'est pas accepté comme équivalent à la signature de chaque document qui constitue le dossier compressé.
- Une signature manuscrite scannée n'a pas d'autre valeur que celle d'une copie et ne peut pas remplacer la signature électronique.

*f) Signature enveloppée, Signature détachée, Jeton de signature*

La signature électronique d'un fichier peut être "enveloppée" ou "détachée".

On parle de "signature enveloppée" lorsque le fichier signé intègre en lui-même la signature. On parle de "signature détachée" lorsque la signature électronique se présente sous la forme d'un fichier informatique autonome, distinct du fichier d'origine. Ce fichier autonome est appelé **Jeton de signature**.




## 4 - Notification des marchés dématérialisés

Les documents transmis par voie électronique seront susceptibles d'être re- matérialisés après l'ouverture des plis. Les candidats sont informés que l'attribution du marché pourra alors donner lieu à la signature manuscrite d'un marché papier.