

RC ANNEXE 1 – SIGNATURE ÉLECTRONIQUE DE L'OFFRE

La signature électronique est l'équivalent de la signature manuscrite (en référence au Code civil) pour un document dématérialisé qui peut adopter différents formats : fichier texte, tableur, .pdf, .jpg, .xml

Les documents dont la signature est exigée doivent être signés par la société dans des conditions permettant d'authentifier leur signature au moyen d'un certificat de signature électronique, conformément à l'article 1316-4 du Code civil. Le signataire doit pouvoir produire les éléments permettant d'établir que la signature électronique utilisée a été délivrée à une personne qui pouvait valablement engager l'entreprise.

Dans le cas d'une candidature groupée conformément aux articles R. 2142-19 et R. 2142-20 du code de la commande publique, le mandataire du groupement assure la sécurité et l'authenticité des informations transmises au nom des membres du groupement. Si le mandataire du groupement n'est pas habilité à représenter l'ensemble des opérateurs économiques groupés, toutes les pièces doivent être signées par l'ensemble des membres du groupement. Un parapheur électronique peut alors être utilisé, permettant la signature d'un même document par plusieurs signataires.

Les frais de recours à la signature électronique sont à la charge de l'opérateur économique.

Il doit disposer d'une signature électronique au minimum avancée reposant sur un certificat qualifié, conforme au règlement n° 910/2014 dit « eIDAS » (règlement du 23 juillet 2014 sur l'identification électronique et les services de confiance et les services de confiance pour les transactions électroniques au sein du marché intérieur).

Dans la commande publique (en Europe comme en France) qui concentre des enjeux économiques et juridiques importants sont autorisés :

- Soit la signature électronique avancée avec certificat qualifié (niveau 3)
- Soit la signature électronique qualifiée (niveau 4)

Les prestataires de services de confiance qualifiés sont référencés dans une liste consultable via le lien <https://www.ssi.gouv.fr/entreprise/visa-de-securite/visas-de-securite-le-catalogue/>

Les candidats européens trouveront également la liste complète des prestataires sur la liste de confiance tenue par la Commission européenne.

NB : Les certificats de signature électronique de type RGS, conformes à l'arrêté du 15 juin 2012 qui est abrogé par l'arrêté du 12 avril 2018 depuis le 1^{er} octobre 2018, peuvent être utilisés au-delà de cette date, le temps de leur validité.

Les fichiers peuvent être signés avec la fonctionnalité de signature de documents accessible au niveau de la procédure concernée sur la plate-forme <https://www.marches-publics.gouv.fr>.

L'opération de signature de document est décrite dans le guide d'utilisation accessible dans la rubrique « Aide » de la plate-forme <https://www.marches-publics.gouv.fr>.

Le candidat peut choisir d'utiliser un autre outil de signature que celui proposé par le profil d'acheteur <https://www.marches-publics.gouv.fr>, s'il transmet, avec les documents signés, l'outil et le processus permettant de procéder gratuitement à la vérification technique et juridique de la signature. Il est précisé que la vérification technique de la signature électronique porte sur l'appartenance du certificat du signataire, le respect du format de signature, le caractère non échu et non révoqué du certificat, l'intégrité des données transmises, la signature électronique apposée sur le fichier et l'identifiant de la politique de signature.

La signature électronique n'est pas nécessairement visible (empreinte apparente) dans le document ou sur le document. Cela dépend notamment du format de signature (XAdES, CAdES et PAdES) et du format du document signé (xml, tableur, Pdf...).

Par exemple, avec le format XAdES, les informations sur la signature (identité, date...) sont dans le fichier .xml qui est généré. Avec le format PAdES, la signature peut être identifiable dans le fichier sous forme d'empreinte visible.

Cela signifie que dans certains cas, la signature est intégrée au document et qu'un seul fichier existe pour le document et la signature, alors que, dans d'autres cas, il y a un fichier pour la signature et un fichier pour le document. Les deux fichiers sont alors transmis simultanément.

Dans tous les cas, l'identité du signataire est affichée lors de la création de la signature, puis demeure avec ou dans le fichier.

Le pouvoir adjudicateur rappelle que :

- **une signature manuscrite scannée n'a pas de valeur juridique et ne peut remplacer la signature électronique.**
- **un fichier compressé (zippé avec un logiciel zip) est un contenant. Sa signature ne vaut pas signature des fichiers qu'il contient (un zip signé est, en effet, assimilable à une enveloppe papier signée au lieu des documents contenus). Un fichier doit donc être signé électroniquement individuellement.**
- **Dès lors que la signature électronique a été générée, toute modification du fichier invalide la signature. Par conséquent, l'opération de signature du document modifié est à renouveler.**