



Annexe n°2 au règlement de la consultation : note explicative sur la signature électronique

SOMMAIRE

1.	EXIGENCES RELATIVES AUX CERTIFICATS DE SIGNATURE DU SIGNATAIRE.....	3
1.1.	1er cas : Certificat émis par une Autorité de certification "reconnue"	3
1.2.	2ème cas : Le certificat de signature électronique n'est pas référencé sur une liste de confiance	3
2.	OUTIL DE SIGNATURE UTILISE POUR SIGNER LES FICHIERS	4
2.1.	Cas 1 : Utilisation de l'outil de signature de la plateforme des achats de l'État PLACE..	4
2.2.	Cas 2 : Utilisation d'un autre outil de signature que celui proposé sur PLACE,	4

Les candidatures et les offres transmises par voie électronique peuvent être signées par l'opérateur économique au moyen d'un certificat de signature électronique selon les modalités détaillées ci-dessous.

A défaut, **la signature électronique est requise au moment de l'attribution du marché.**

Le candidat doit respecter les conditions relatives :

- au certificat de signature du signataire,
- à l'outil de signature utilisé (logiciel, service en ligne, parapheur le cas échéant), devant produire des jetons de signature¹ conformes aux formats réglementaires dans l'un des trois formats acceptés.

¹ Le jeton d'horodatage peut être enveloppé dans le fichier d'origine ou bien apparaître sous la forme d'un fichier autonome (non enveloppé)

1. EXIGENCES RELATIVES AUX CERTIFICATS DE SIGNATURE DU SIGNATAIRE

Le certificat de signature du signataire respecte au moins le niveau de sécurité préconisé.

1.1. 1er cas : Certificat émis par une Autorité de certification "reconnue"

Le certificat de signature est émis par une Autorité de certification mentionnée dans l'une des listes de confiance suivantes :

- <https://references.modernisation.gouv.fr/> ;
- http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm;
- <http://www.industrie.gouv.fr/tic/certificats>.

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

1.2. 2ème cas : Le certificat de signature électronique n'est pas référencé sur une liste de confiance

La plateforme de dématérialisation « PLACE » accepte tous certificats de signature électronique présentant des conditions de sécurité équivalentes à celles du référentiel général de sécurité (RGS).

Le candidat s'assure que le certificat qu'il utilise est au moins conforme au niveau de sécurité préconisé sur le profil d'acheteur, et donne tous les éléments nécessaires à la vérification de cette conformité par l'acheteur.

Dans ce cas, le signataire transmet les justificatifs de conformité suivants :

- la procédure permettant la vérification de la qualité et du niveau de sécurité du certificat de signature utilisé : preuve de la qualification de l'Autorité de certification, la politique de certification...
- le candidat fournit notamment les outils techniques de vérification du certificat : chaîne de certification complète jusqu'à l'AC racine, adresse de téléchargement de la dernière mise à jour de la liste de révocation ;
- l'adresse du site internet du référencement du prestataire par le pays d'établissement ou, à défaut, les données publiques relatives au certificat du signataire, qui comportent, au moins, la liste de révocation et le certificat du prestataire de services de certification électronique émetteur.

2. OUTIL DE SIGNATURE UTILISE POUR SIGNER LES FICHIERS

Le candidat utilise l'outil de signature de son choix.

2.1. Cas 1 : Utilisation de l'outil de signature de la plateforme des achats de l'État PLACE

Dans ce cas, le soumissionnaire est dispensé de fournir tout mode d'emploi ou information.

2.2. Cas 2 : Utilisation d'un autre outil de signature que celui proposé sur PLACE,

Dans ce cas, le soumissionnaire doit respecter les deux obligations suivantes :

- produire des formats de signature XAdES, CAdES ou PAdES.
- 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.

Dans ce cas, le signataire indique la procédure permettant la vérification de la validité de la signature en fournissant notamment :

- le lien sur lequel l'outil de vérification de signature peut être récupéré, avec une notice d'explication et les pré-requis d'installation (type d'exécutable, systèmes d'exploitation supportés, etc.). La fourniture d'une notice en français est souhaitée ;
- le mode de vérification alternatif en cas d'installation impossible pour l'acheteur (contact à joindre, support distant, support sur site etc.).

Le certificat électronique utilisé pour ces signatures doit être reconnu par la procédure électronique et détenu par une personne ayant la capacité pour engager le soumissionnaire dans le cadre de la présente consultation. A cette fin, le signataire doit figurer au Kbis de la société ou à défaut disposer des pouvoirs nécessaires.

La signature électronique n'est pas considérée valide et le document correspondant réputé non signé lorsque :

- la signature est absente,
- le certificat a été révoqué avant la date de signature du document,
- le certificat expire avant la date de signature du document,
- le certificat est établi au nom d'une personne physique qui n'a pas la capacité à engager la société.

La signature électronique a la même valeur juridique qu'une signature manuscrite.

Rappel général :

Un zip signé ne vaut pas signature des documents qu'il contient. En cas de fichier zippé, chaque document pour lequel une signature est requise doit être signé séparément.

Une signature manuscrite scannée n'a pas d'autre valeur que celle d'une copie et ne peut pas remplacer la signature électronique.

L'absence de signature électronique valide sur l'acte d'engagement n'entraînera pas le rejet de l'offre.