UniHA

L'Achat Coopératif des Hôpitaux Publics

AVRIL 2018

GUIDE PRATIQUE

Signature électronique

LA COOPÉRATIVE
DES ACHETEURS
HOSPITALIERS

Sommaire

1. Objet du document

L'échéance du 1er octobre 2018 pour la dématérialisation des procédures de passation des marchés publics approche à grands pas.

Il est important de s'y préparer dès maintenant et la signature électronique fait partie de ces préparatifs.

Ce petit guide a vocation à vous orienter dans la mise en place et l'utilisation d'une signature électronique.

2. Textes de référence

- Loi n° 2000-230 du 13/03/2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Article 1316-4 du code civil
- Décret n°2001-272 du 30 mars 2001, pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique
- Arrêté du 15 juin 2012, relatif à la signature électronique dans les marchés publics
- Arrêté du 13 juin 2014, portant approbation du Référentiel Général de Sécurité et ses incidences sur la signature électronique
- Règlement UE du 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)
- DAJ : fiche explicative de l'arrêté relatif à la signature dans les marchés publics
- Décret 2017-1416, relatif à la signature électronique
- **A noter** : à l'heure où nous écrivons ce manuel, la DAJ annonce la parution d'un arrêté sur la signature électronique

3. La signature électronique en théorie

3.1. Définition et caractéristiques

La signature électronique est au document numérique, ce que la signature manuscrite est au document papier.

Elle possède la même valeur juridique que la signature manuscrite.

La personne qui signe électroniquement doit être la même que celle qui aurait signé manuellement.

La loi 2000-230 définit la signature électronique comme « l'usage de procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

Le décret 2017-1416 ajoute que la fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée.

La signature électronique est donc un mécanisme cryptographique fiable permettant :

- de garantir l'intégrité d'un document électronique
- et d'en authentifier l'auteur de manière certaine.

Elle ne peut pas être :

- falsifiée
- modifiée
- réutilisée : elle fait partie du document et ne peut être déplacée sur un autre
- ou répudiée : la personne qui a signé ne peut le nier.

Une signature électronique comprend un certificat électronique et un logiciel de signature qui permet d'apposer la signature.

3.2. Formats

Une décision de la Commission européenne du 25 février 2011, impose d'accepter 3 formats de signature.

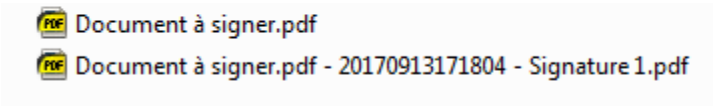
Ces 3 formats doivent donc être acceptés et vérifiables par les plateformes d'achat ; ils peuvent être utilisés indifféremment.

Ce sont les formats :

- CAdES
  - avec ce format, la signature n'est pas visible graphiquement sur le document
  - ce format génère une signature « détachée » c'est-à-dire que le document et la signature sont dans 2 fichiers séparés
  - le fichier contenant la signature est appelé « jeton » ; il porte l'extension « .p7s »

- XAdES
  - avec ce format, la signature n'est pas visible graphiquement sur le document.
  - ce format génère une signature « détachée » c'est-à-dire que le document et la signature sont dans 2 fichiers séparés
  - le fichier contenant la signature est appelé « jeton » ; il porte l'extension « .xml »

- PAdES
  - ce format est applicable aux documents PDF uniquement
  - la signature est visible graphiquement sur le document
  - ce format génère une signature « embarquée » c'est-à-dire que l'action de signer génère un nouveau document PDF comportant à la fois le texte du document et la signature
  - ce nouveau document PDF est intitulé « XXX.pdf-DateHeure-Signature1.pdf »



3.3. Certificat électronique

3.3.1. Définition

Le certificat électronique est une carte d'identité numérique qui permet d'identifier et d'authentifier le signataire d'un document.

Il garantit donc l'identité du signataire et l'intégrité des documents signés.

Il doit être attribué à une seule personne physique : la personne qui signait de manière manuscrite.

Concrètement, il s'agit d'un fichier électronique contenant un certain nombre d'informations personnelles (nom, prénom, etc.), chiffré avec une clé de chiffrement permettant de réaliser les opérations de signature.

Une signature manuscrite scannée n'a pas de valeur juridique.

La signature d'un fichier zippé ne vaut pas signature des documents qu'il contient : il convient donc de signer électroniquement chaque document qui l'aurait été manuellement.

3.3.2. Quelle catégorie de certificat utiliser ?

Dans sa fiche explicative, la DAJ rappelle que « l'utilisation de tout produit est possible à partir du moment où il présente des garanties de sécurité suffisantes ».

Ainsi, les catégories de certificats utilisables sont :

- les certificats référencés, ou figurant sur la liste de confiance d'un Etat-membre de l'Union européenne
- les certificats qui ne figurent pas sur une liste de confiance mais qui doivent présenter un niveau de sécurité suffisant. Il s'agit de certificats conformes au Référentiel Général de Sécurité mais non référencés sur une liste, ou de certificats qui présentent un niveau de sécurité équivalent.

La liste de confiance Française est accessible sur le site de l'ANSSI :
https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/

La liste de confiance Européenne est accessible sur le site de la Commission Européenne :
https://ec.europa.eu/digital-single-market/trust-services-and-eid

3.3.3. Où se procurer un certificat électronique ?

Le certificat électronique est délivré par une Autorité de Certification, dont le rôle est de vérifier l'identité du demandeur et de faire le lien entre la clé privée de signature et l'identité du signataire.

1. La liste des Autorités de Certification Françaises délivrant des certificats de signature conformes au Référentiel Général de Sécurité, est fournie sur la plateforme PLACE, en pied de page :

2. L'ANSSI propose la liste des prestataires de service de confiance : https://www.ssi.gouv.fr/administration/visa-de-securite/visas-de-securite-le-catalogue/

3. Le groupe LSTI, est un organisme de certification privé spécialisé dans le domaine de la sécurité de l'information. Il ne délivre pas de certificat mais intervient dans tous les états-membres de l'Union européenne pour la qualification des prestataires de services de confiance selon le règlement européen Eidas.
   La liste des Prestataires de Service de Confiance Electronique est accessible sur son site : http://lsti-certification.fr/index.php/fr/certification/psce

3.3.4. Comment se procurer un certificat électronique ?

La commande s'effectue en ligne : le dossier de demande de certificat doit être complété en ligne, imprimé et signé par le futur détenteur du certificat de signature.

La délivrance d'un certificat de signature nécessite un certain nombre d'opérations de vérification d'identité :

- à minima l'envoi de photocopies de pièces d'identité pour les procédures les plus souples ;
- un déplacement physique du demandeur auprès de l'autorité de certification et une vérification d'identité en face à face pour les politiques de certification les plus avancées. Lors de cette étape, le demandeur présente ses papiers d'identité contre remise du certificat.

Pensez à prévoir un délai suffisant : l'acquisition d'un certificat électronique peut prendre entre 15 jours et 1 mois.

Le certificat est activé à distance, après installation du pilote sur l'ordinateur.

Le porteur du certificat reçoit un courriel pour activer son certificat. Un guide d'installation et d'activation est téléchargeable sur le site de CERTEUROP.

3.3.5. Quel support choisir ?

Le certificat électronique peut se matérialiser sous différents supports :

- logiciel (stockage sur le disque dur d'un ordinateur)
- dispositif matériel (carte à puce, carte SIM, clé USB…)
- ou de façon dématérialisée (Cloud).

Il est recommandé d'utiliser la clé USB ou la carte à puce

3.3.6. Quel prix ?

L'obtention d'un certificat est payante.

Chaque prestataire établit le prix en fonction des services qu'il délivre.

Le renouvellement d'un certificat n'est pas automatique.

Pensez à tenir à jours la liste des certificats de votre établissement avec les dates de fin de validité.

Les certificats RGS ** vont devoir être remplacés par des certificats eIDAS (*on estime que les certificats RGS** seront sans doute utilisables jusqu'à fin 2019*).

Nous vous conseillons donc d'éviter de renouveler ou d'acheter des certificats RGS ** pour plus d'un an.

Chaque certificat étant payant, il est recommandé, avant de chercher à se munir d'une signature électronique de mener une réflexion en interne sur le nombre de certificats à acheter - notamment dans le cadre des GHT et des délégations de signature – et, de ne faire venir le prestataire qu'une seule fois pour la remise de l'ensemble des certificats.

Pensez également à anticiper les périodes de vacances et les délégations de pouvoir.

3.3.7. Quelles vérifications ?

La loi 2000-230 définit la signature électronique comme « l'usage de procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache … l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Dans sa fiche explicative, la DAJ précise que : « la vérification des certificats de signature électronique et de la validité de la signature elle-même font partie des fonctionnalités d'un profil d'acheteur, sans que l'acheteur ait dû se doter des compétences techniques pour les examiner. En revanche, la vérification de l'identité du signataire, et de sa capacité à engager l'entreprise, reste, effectuée par l'acheteur. »

La vérification de la validité d'une signature est donc gratuitement proposée par les profils d'acheteur. A ce titre, elle fait partie intégrante des fonctionnalités proposées par la plateforme PLACE.


Plate-forme des Achats de l'Etat
www.marches-publics.gouv.fr
Accédez au site
BOAMP.fr
Bulletin officiel des annonces des marchés publics
Vendredi 17 Nov. 2017 11:28
Accueil
Consultations et
Contrats
Annuaire
Administration métier
Archives
Administration PLACE
Publipostage
Outils de signature
Vérifier la signature
Aide
Outils de signature > Vérifier la signature
Afin de vérifier la validité de la signature d'un fichier, nous vous invitons à :
- Sélectionner le fichier dont la signature doit être vérifiée
- En cas de signature au format XAdES ou CAdES, sélectionner ensuite le fichier contenant la signature (appelé jeton)
- En cas de signature au format PAdES, il n'y a pas de jeton : la signature PAdES est détectée et vérifiée automatiquement
Document à vérifier :
Parcourir...
_AE DIAGNOSTICS_ANNEXE 2_CADRE MEMOIRE TECHNIQUE.pdf
Fichier de signature associé :
Parcourir...
_AE DIAGNOSTICS_ANNEXE 2_CADRE MEMOIRE TECHNIQUE.pdf - 20170925163749 - Signature 1.xml
Vérifier


Offres - Fichier(s) constituant le dossier et signature(s) électronique(s) associée(s)
Tout afficher / Tout cacher
Fichier(s) envoyé(s) par le soumissionnaire
Résultat du contrôle de signature du fichier
ATTRI1 MS GHT UNIHA-signe.pdf
Fichier signé. Signature valide
Tous les contrôles de validité de cette signature ont été passés avec succès.
Jeton de signature : ATTRI1 MS GHT UNIHA-signe.pdf
Certificat du signataire
Certificat émis à :
E : agp@govhe.com
CN :Antoine GEORGES-PICOT-MARCILLE
OU 0002 801942830
O : GOVHE
C : FR
Certificat émis par :
CN :CERTEUROPE ADVANCED CA V4
OU 0002 434202180
O : Certeurope
C : FR
Date de validité :
A partir du : 18/03/2016 15:05
Jusqu'au : 18/03/2019 15:05
Contrôles de validité du certificat
Contrôles réalisés le 11/01/2018 15:24:45
Période de validité :
Chaîne de certification :
Référentiel du certificat : Non référencé
Non révocation :
Contrôles de l'intégrité du fichier signé
Contrôles réalisés le 12/03/2018 16:37
Non répudiation

Les certificats de signature ont une durée de validité limitée.

Les plateformes ne peuvent pas vérifier la validité d'un certificat à une date antérieure.

Un rapport de vérification réalisé plusieurs semaines après la réception du document signé électroniquement risque donc d'afficher une « signature incertaine » ou « invalide » si la date d'expiration du certificat est dépassée.

Il convient, par conséquent, de veiller à toujours enregistrer le rapport de vérification de signature, dès l'ouverture des plis, pour montrer que l'acheteur a bien fait les vérifications qui s'imposent au moment voulu.

Les 2 principaux éléments à vérifier sont :

- l'intégrité du document (le document vérifié est bien celui qui a été signé)
- la validité du certificat qui a permis la signature. La date de validité du certificat est précisée dans le rapport de vérification.

Rapport de vérification de signature

Résultat de la vérification

Nom du fichier principal	Pfz ADATU2018-Lettre de consultation valant AE - MS1.pdf
Nom du fichier de signature	Pfz ADATU2018-Lettre de consultation valant AE - MS1.pdf_sig.xml

Signataire	CN : ANNE-ALIX BEAUCHATAUD E : anne-alix.beauchataud@pfizer.com OU : 0002 433623550 O : PFIZER C : ANNE-ALIX BEAUCHATAUD

Emetteur du certificat	CN : CERTEUROPE ADVANCED CA V4 OU : 0002 434202180 O : Certeurope C : FR

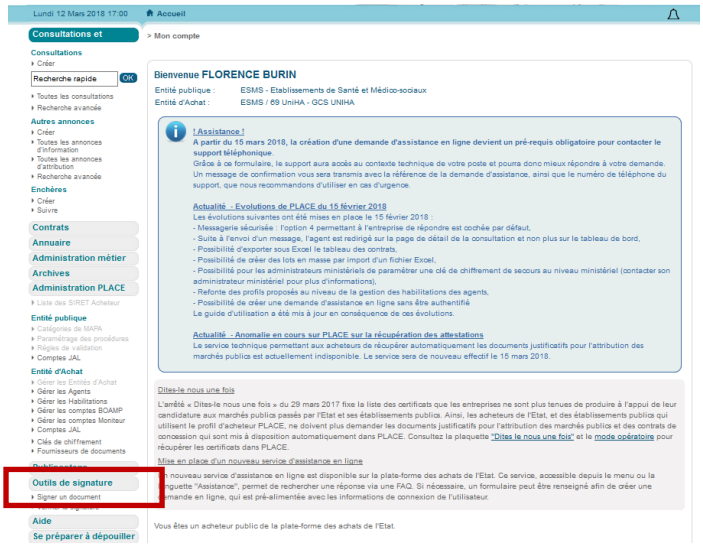
Date de validité de certificat	A partir du : 22T17:18:17+01:00/12/2014 : Jusqu'au : 22T17:18:17+01:00/12/2017 :

4. La signature électronique en pratique

4.1. Comment signer un document avec la plateforme PLACE

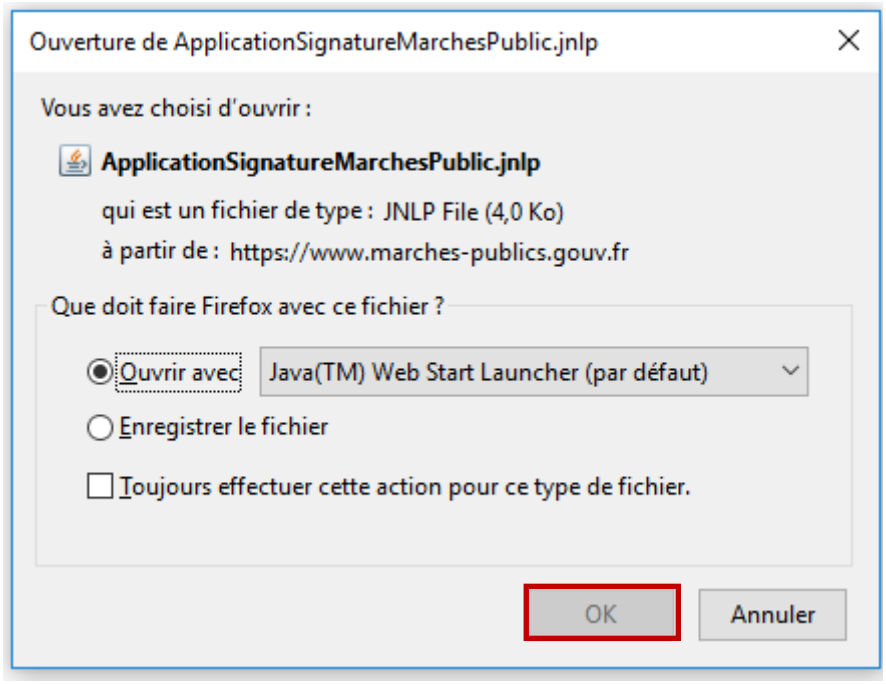
Accédez à l'outil de signature proposé par la plateforme à partir de la page d'accueil :

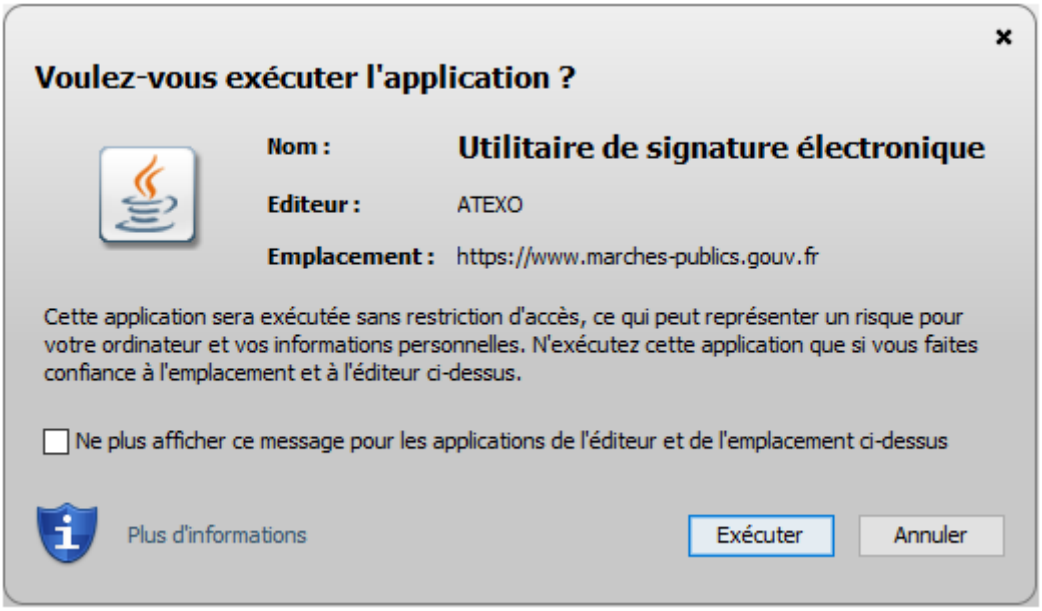
Côté acheteur



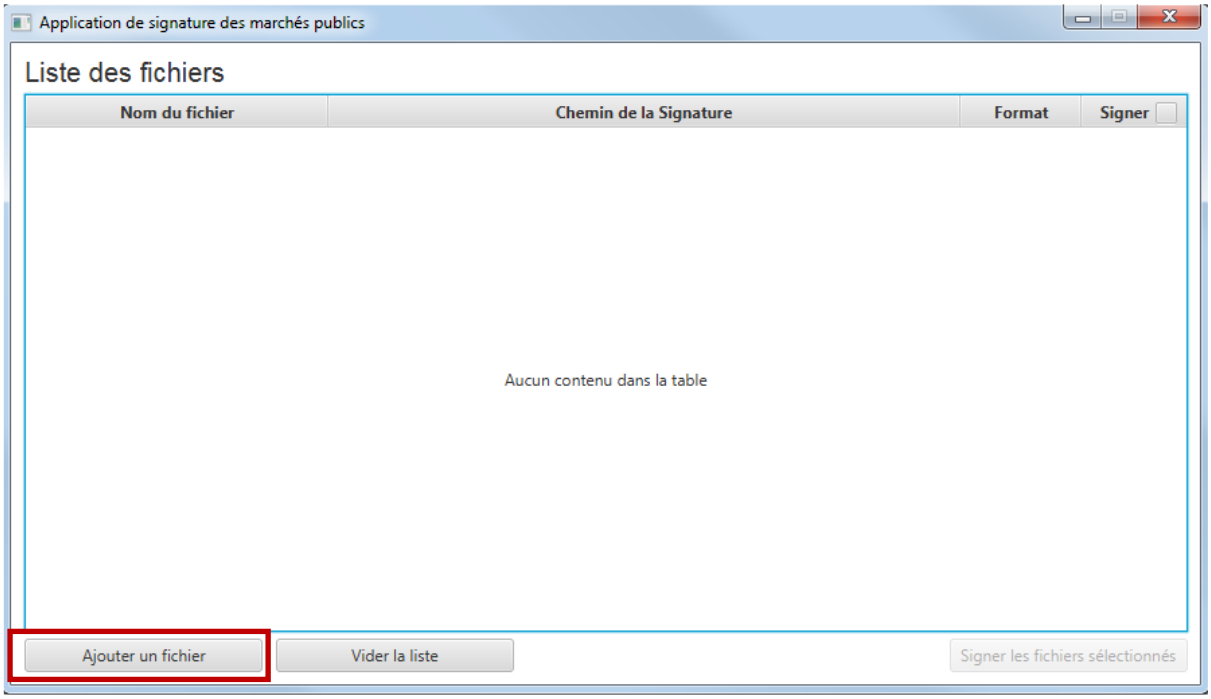
Côté fournisseur

Lancez l'outil de signature :


Ouverture de ApplicationSignatureMarchesPublic.jnlp
Vous avez choisi d'ouvrir :
ApplicationSignatureMarchesPublic.jnlp
qui est un fichier de type : JNLP File (4,0 Ko)
à partir de : https://www.marches-publics.gouv.fr
Que doit faire Firefox avec ce fichier ?
Ouvrir avec
Java(TM) Web Start Launcher (par défaut)
Enregistrer le fichier
Toujours effectuer cette action pour ce type de fichier.
OK
Annuler


Voulez-vous exécuter l'application ?
Nom :
Utilitaire de signature électronique
Editeur :
ATEXO
Emplacement :
https://www.marches-publics.gouv.fr
Cette application sera exécutée sans restriction d'accès, ce qui peut représenter un risque pour votre ordinateur et vos informations personnelles. N'exécutez cette application que si vous faites confiance à l'emplacement et à l'éditeur ci-dessus.
Ne plus afficher ce message pour les applications de l'éditeur et de l'emplacement ci-dessus
Plus d'informations
Exécuter
Annuler

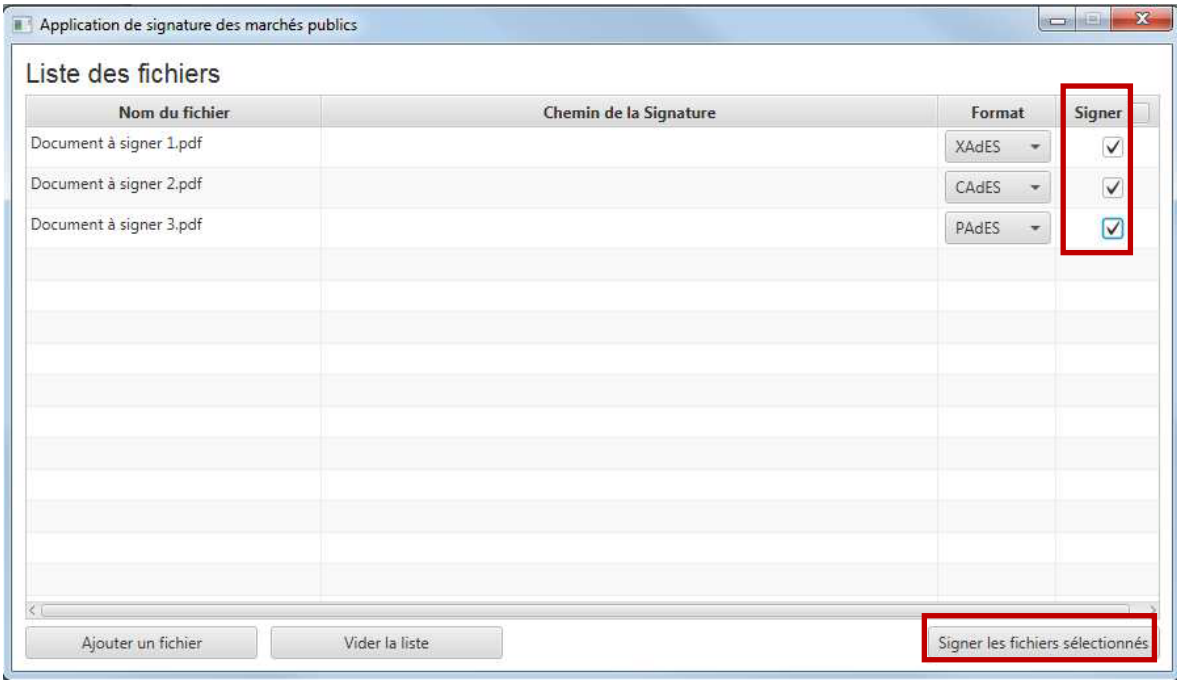
Ajoutez les fichiers à signer en allant les chercher dans les répertoires ou ils sont enregistrés :



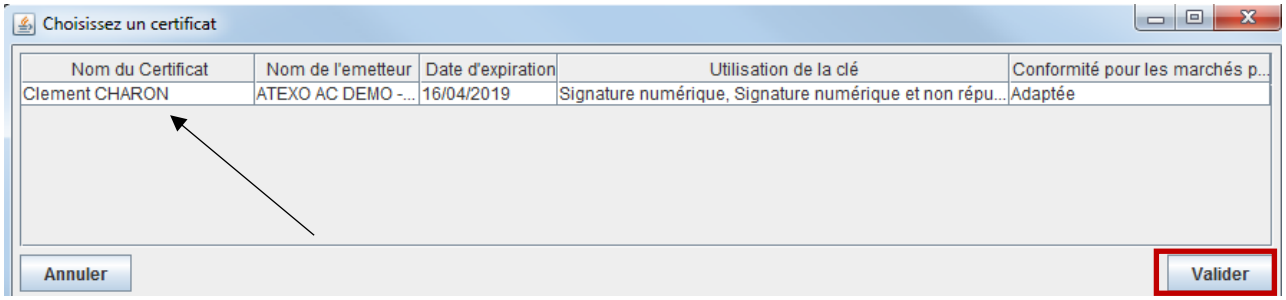
Pour chaque fichier à signer ajouté,

- choisir le format de signature souhaité
- cocher la case « signer »

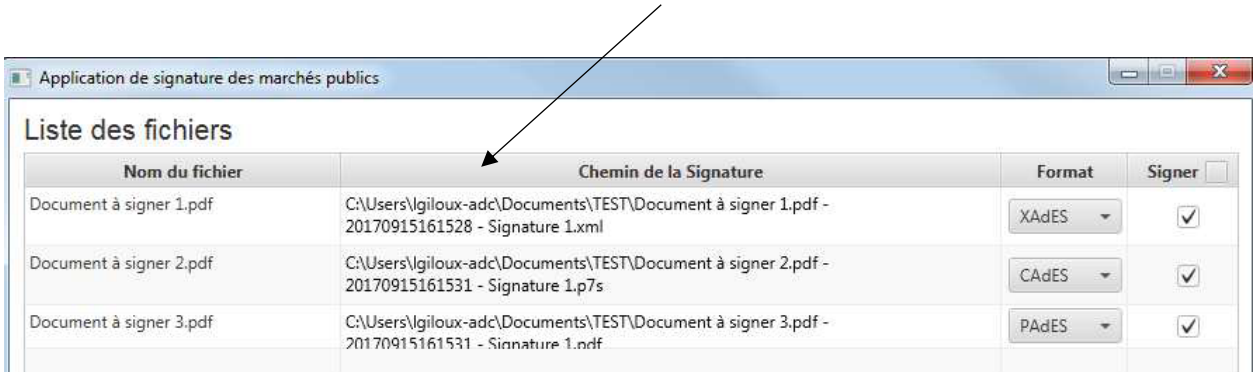
Puis, cliquez sur signer les fichiers sélectionnés.



Choisir le certificat de signature installé sur votre poste et validez.



Les fichiers sont signés et les chemins de signature s'affichent.



Pour les formats XADES et CADES, la signature se matérialise par la création d'un fichier de signature appelé jeton.

Ce jeton est généré et enregistré dans le même répertoire que le fichier signé.

Il porte le même nom que le fichier signé avec en plus, une extension différente selon le format de signature choisi :

- « .p7s » pour le format Cades
- « .xml » pour le format XAdES
- « DateHeure-Signature1.pdf » pour le format PAdES

Le fichier **et** son jeton de signature doivent être transmis au destinataire du document.

5. La jurisprudence

- Le juge confirme que la signature d'un ZIP ne suffit pas.
  TA Toulouse, 9 mars 2011 Société MC2I, n°1100792

- Le rejet des offres au motif que la signature d'un fichier ZIP ne vaut pas signature électronique des documents, ne peut être notifié au soumissionnaire qu'après ouverture du fichier ZIP afin d'y vérifier si les documents qu'il comprend, sont eux-mêmes signés.
  TGI Paris, ordonnance de référé, 19 novembre 2015

- Il n'y a pas d'irrégularité établie dans un cas où il y avait une signature mais ou l'administration ne pouvait pas le vérifier, sans démontrer en quoi le fournisseur aurait commis une irrégularité.
  CE 400791 – Ministre de la Défense c/société Tribord

Siret n°130 002 223 00027 Avril 2018. Crédits photos : Adobe Stock.

Contactez l'auteur

Florence Burin
Chargée de mission
Tel. 04 81 07 02 32
Email : florence.burin@uniha.org

GCS UniHA
9 rue Tuiliers 69003 LYON
http://fournisseurs.uniha.org
Twitter @UniHA_Hopital

UniHA
L'Achat Coopératif des Hôpitaux Publics