Signature Electronique selon la norme PAdES

La (co-)signature de documents PDF avec Adobe Acrobat Reader

Sommaire

1 PREREQUIS 3

1.1 SIGNATURE ELECTRONIQUE 3

1.1.1 GENERALITES 3

1.1.2 DANS LE CADRE D'UN GROUPEMENT, QUI DOIT SIGNER ELECTRONIQUEMENT ? 3

1.2 COMPTE AWS ENTREPRISE 3

1.3 LOGICIEL ADOBE ACROBAT READER 3

2 INSERTION D'UNE SIGNATURE DANS UN DOCUMENT PDF 4

2.1 PROCEDURE POUR LA VERSION ACROBAT READER XI 4

2.2 PROCEDURE POUR LA VERSION ACROBAT READER DC 6

3 VERIFICATION DE SIGNATURE(S) DANS UN DOCUMENT PDF 9

4 PROCEDURE DE CO-SIGNATURE ET DE DEPOT D'UN PLI DANS LE CADRE D'UN GROUPEMENT 11

4.1 PREPARATION DES DOCUMENTS A CO-SIGNER 11

4.2 SIGNATURE SEQUENTIELLE 11

4.3 PREPARATION DU PLI 11

4.4 DEPOT DU PLI 11

5 ANNEXE 1 12

5.1 CE QUE LA SIGNATURE ELECTRONIQUE N'EST PAS 12

5.2 CE QUE LA SIGNATURE ELECTRONIQUE EST 12

5.2.1 LES DIFFERENTES FORMES DE SIGNATURE ELECTRONIQUE 12

5.2.2 LES DIFFERENTS FORMATS DE SIGNATURE ELECTRONIQUE 12

1 PREREQUIS

1.1 Signature électronique

1.1.1 Généralités

En vertu de l'Arrêté du 15 juin 2012 relatif à la signature électronique, les **certificats électroniques** acceptés sur AWS-Achat pour les réponses dématérialisées doivent-être **conformes à la norme RGS** ou RGS*****.

Vous trouverez des informations complémentaires sur les certificats de signature électronique sur le site www.entreprises.gouv.fr.

Pour acquérir un certificat électronique, il vous faut choisir et contacter l'une des sociétés qui figurent dans la liste des prestataires qualifiés fournie par la société LSTI (organisme certificateur qui apporte un label de sécurité basé sur les normes françaises, européennes et internationales) :

http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf

Attention :

AWS-Achat vérifie les signatures à la source, et donc interdit le dépôt avec des certificats qui ne sont pas émis par une AC, notamment le certificat émis par l'administration fiscale spécifiquement pour TéléTVA. Ce certificat ne permet pas le contrôle d'authentification en ligne.

Les entreprises étrangères disposant d'un certificat émis par une AC européenne doivent nous contacter 72 heures avant l'expiration, avec tous les éléments techniques de leur certificat, en français, afin que l'on puisse ajouter votre AC à la liste des certificats autorisés.

Dans ce cas AWS ne pourra pas vous apporter de garantie quant à la recevabilité de votre pli car l'acheteur public doit pouvoir vérifier votre signature.

1.1.2 Dans le cadre d'un groupement, qui doit signer électroniquement ?

Tous les membres du groupement qui auraient signés manuellement les documents dans le cadre d'un dépôt par courrier doivent signer électroniquement les fichiers.

1.2 Compte AWS Entreprise

Vous (au moins un des membres du groupement) devez (doit) posséder un compte AWS Entreprise pour effectuer le dépôt du pli.

Si nécessaire, rendez-vous sur cette page pour créer un compte.

1.3 Logiciel Adobe Acrobat Reader

Ce manuel utilise le logiciel Adobe Acrobat Reader version XI et DC téléchargeable depuis le site d'Adobe.

Configuration matérielle requise :

Windows :

- Processeur de 1,5 GHz ou plus rapide
- Windows Server 2008 R2 (64 bits), 2012 (64 bits) ou 2012 R2 (64 bits) ; Windows 7 (32 bits et 64 bits), Windows 8 (32 bits et 64 bits) ou Windows 10
- 1 Go de mémoire RAM
- 380 Mo d'espace disponible sur le disque
- Résolution d'écran 1024x768
- Internet Explorer 8, 9, 10, 11 ; Firefox (ESR)

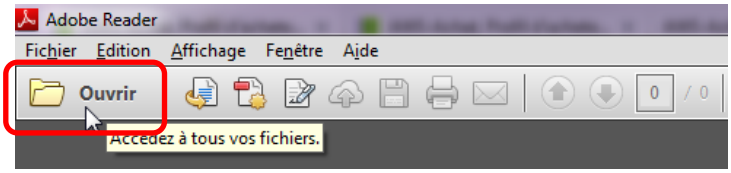
Mac OS :

- Processeur Intel
- Mac OS X v10.9, 10.10
- 1 Go de mémoire RAM
- 450 Mo d'espace disponible sur le disque
- Résolution d'écran 1024x768
- Safari 7 ou 8 (le module externe de navigation pour Safari est pris en charge sur processeur Intel 64 bits uniquement)

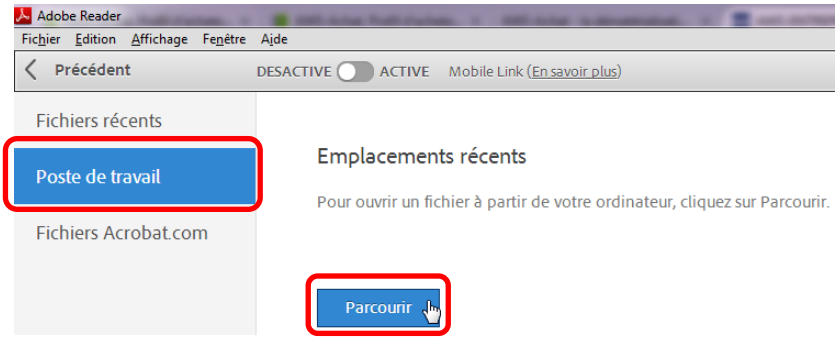
2 INSERTION D'UNE SIGNATURE DANS UN DOCUMENT Pdf

2.1 Procédure pour la version Acrobat Reader XI

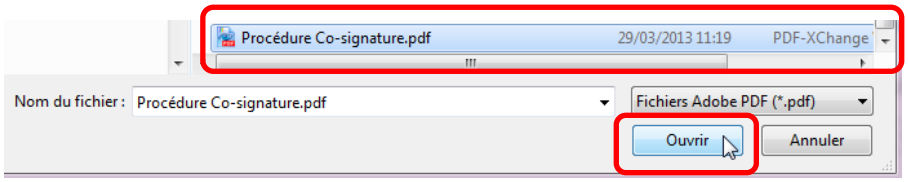
- Si votre certificat RGS** vous a été livré sur une clé cryptographique, branchez cette dernière sur un port USB
- Lancez le *programme* Adobe Acrobat Reader XI
- Dans la *barre d'outils*, cliquez sur le *bouton* **Ouvrir** :



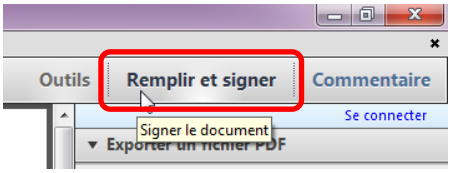
- Dans le *volet* **gauche**, cliquez sur *l'emplacement* **Poste de travail**, puis cliquez sur le *bouton* **Parcourir** :



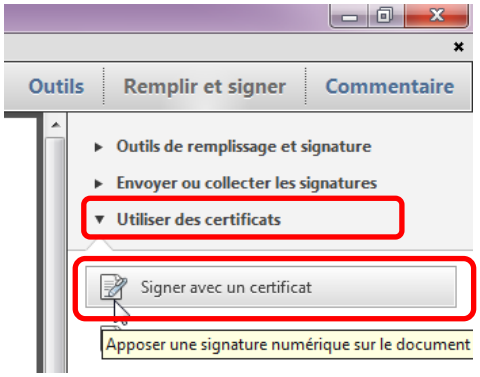
- Une **boite de dialogue** s'ouvre : sélectionnez le *document* **Pdf** que vous souhaitez signer puis cliquez sur le *bouton* **Ouvrir** :



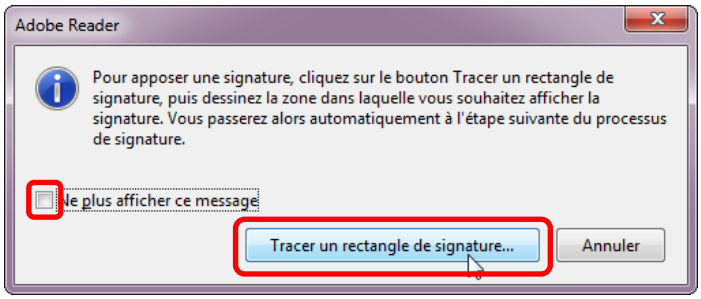
- Dans la barre d'outils, cliquez sur le *bouton* **Remplir et signer** :



- Dans le *volet* **Remplir et signer**, cliquez successivement sur **Utiliser des certificats** puis sur **Signer avec un certificat** :

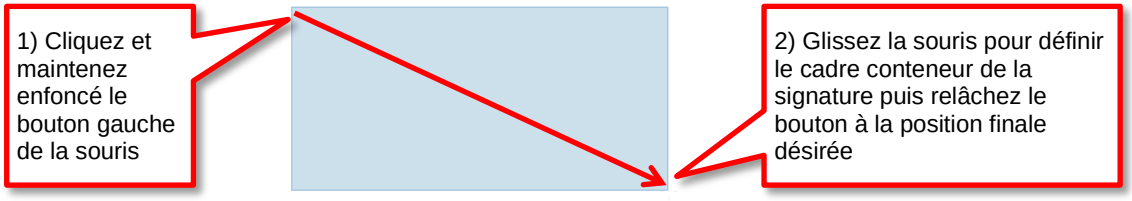


- Si la *boite de dialogue* suivante s'ouvre, vous pouvez cocher *l'option* **Ne plus afficher ce message**, puis cliquez sur le *bouton* **Tracer un rectangle de signature …** :

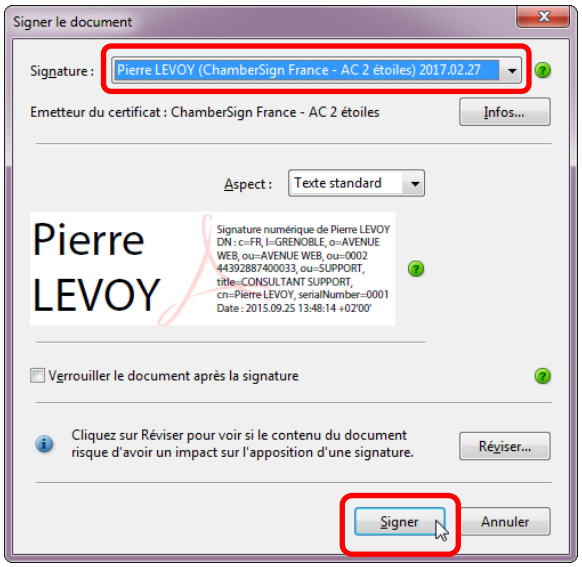


- Eventuellement, faites défiler l'écran pour visualiser la partie du document ou vous souhaitez apposer votre signature.

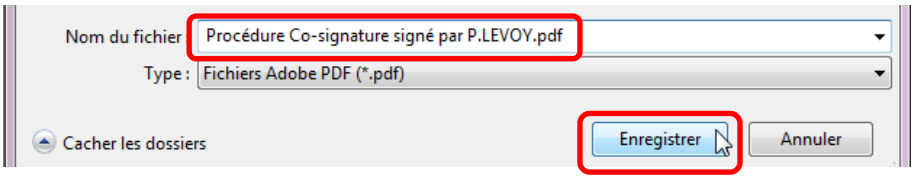
- Faites un cliquer-glisser pour tracer le **cadre** qui contiendra la signature électronique dans le document :



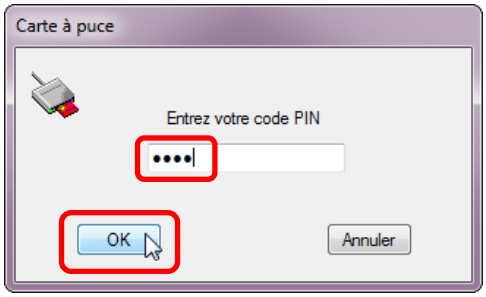
- La *boite de dialogue* **Signer le document** s'ouvre : sélectionnez votre signature électronique dans la *liste* **Signature**, puis cliquez sur le *bouton* **Signer** :



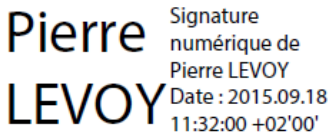
- Acrobat Reader vous propose alors d'enregistrer le document signé :



- Dans la *boite de dialogue* **Carte à puce**, tapez le **code** de votre certificat puis cliquez sur le *bouton* **OK** :

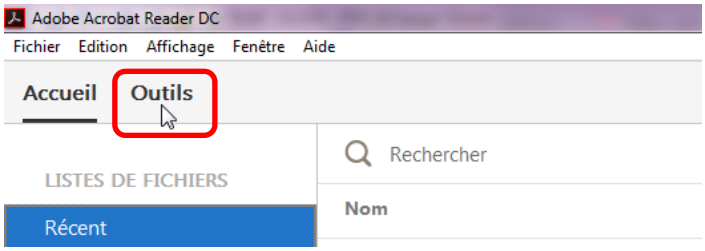


- Après validation, la signature apparaît dans le document signé à l'intérieur du cadre tracé précédemment :

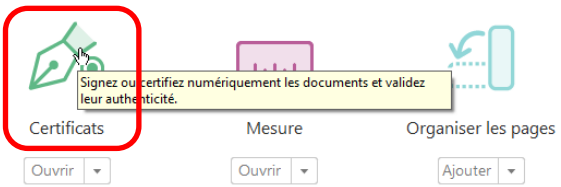


2.2 Procédure pour la version Acrobat Reader DC

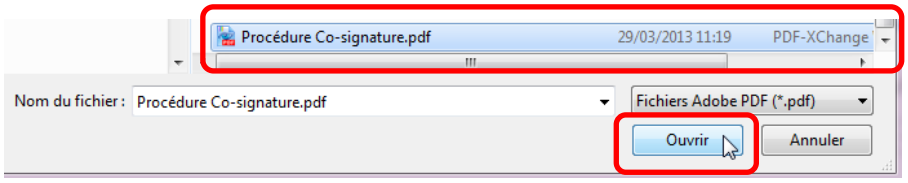
- Si votre certificat RGS** vous a été livré sur une clé cryptographique, branchez cette dernière sur un port USB
- Lancez le *programme* Adobe Acrobat Reader DC
- Cliquez sur la *commande* **Outil** dans la barre d'outils (Si vous ne voyez pas la barre d'outils, pressez la *touche* **F8**) :



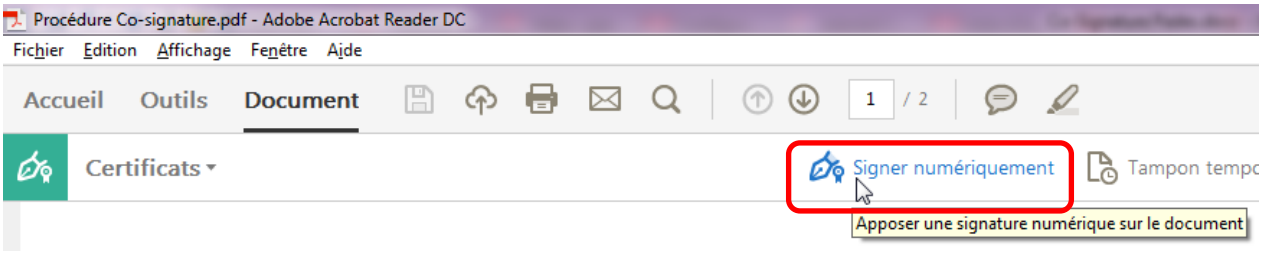
- Cliquez sur le *bouton* Certificats :



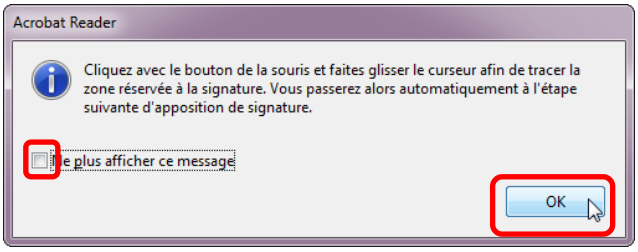
- Une **boite de dialogue** s'ouvre : sélectionnez le *document* **Pdf** que vous souhaitez signer puis cliquez sur le *bouton* **Ouvrir** :



- Dans la *barre d'outils* **Certificats**, cliquez sur la *commande* **Signer numériquement** :

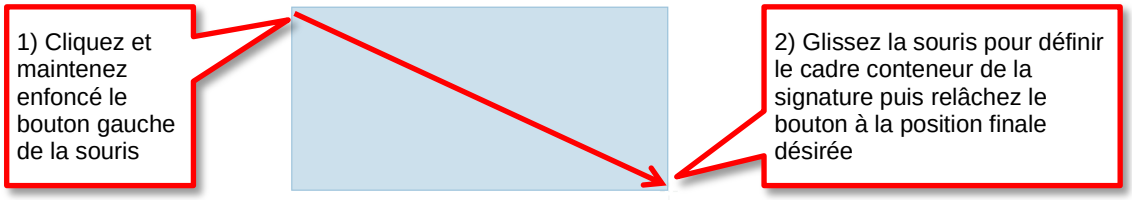


- Si la *boite de dialogue* suivante s'ouvre, vous pouvez cocher *l'option* **Ne plus afficher ce message**, puis cliquez sur le *bouton* **OK** :

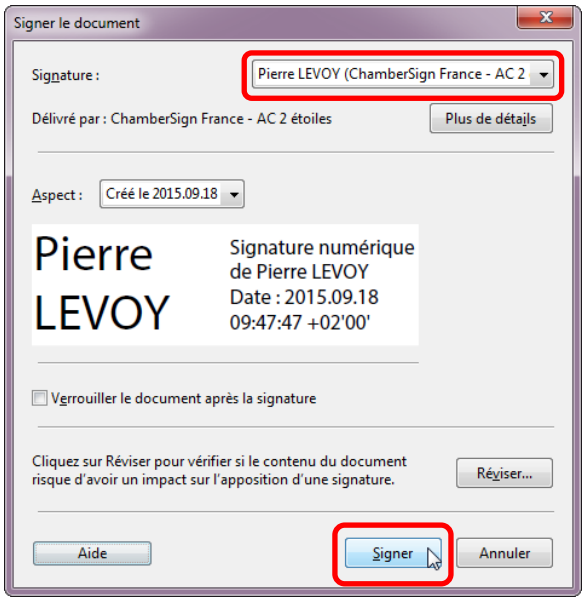


- Eventuellement, faites défiler l'écran pour visualiser la partie du document ou vous souhaitez apposer votre signature.

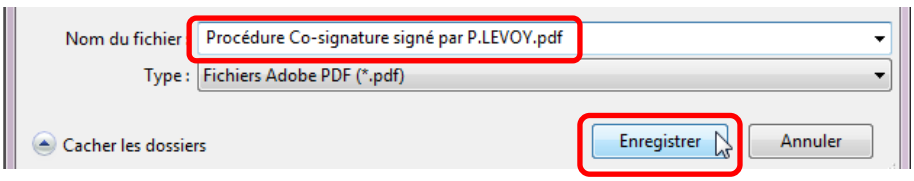
- Faites un cliquer-glisser pour tracer le **cadre** qui contiendra la signature électronique dans le document :



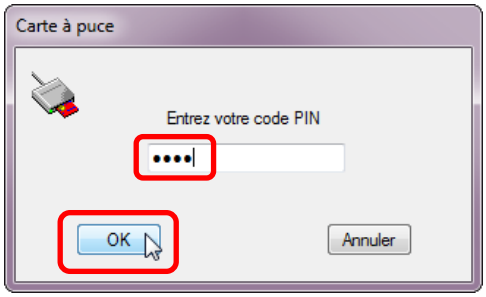
- La *boite de dialogue* **Signer le document** s'ouvre : sélectionnez votre signature électronique dans la *liste* **Signature**, puis cliquez sur le *bouton* **Signer** :



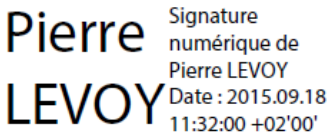
- Acrobat Reader vous propose alors d'enregistrer le document signé :



- Dans la *boite de dialogue* **Carte à puce**, tapez le **code** de votre certificat puis cliquez sur le *bouton* **OK** :



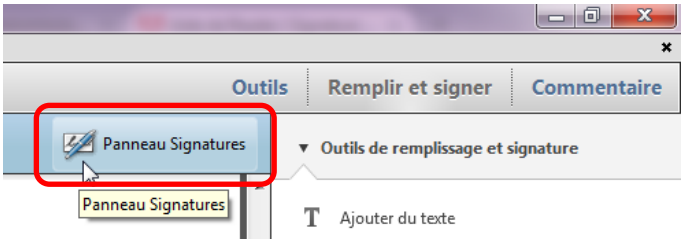
- Après validation, la signature apparaît dans le document signé à l'intérieur du cadre tracé précédemment :



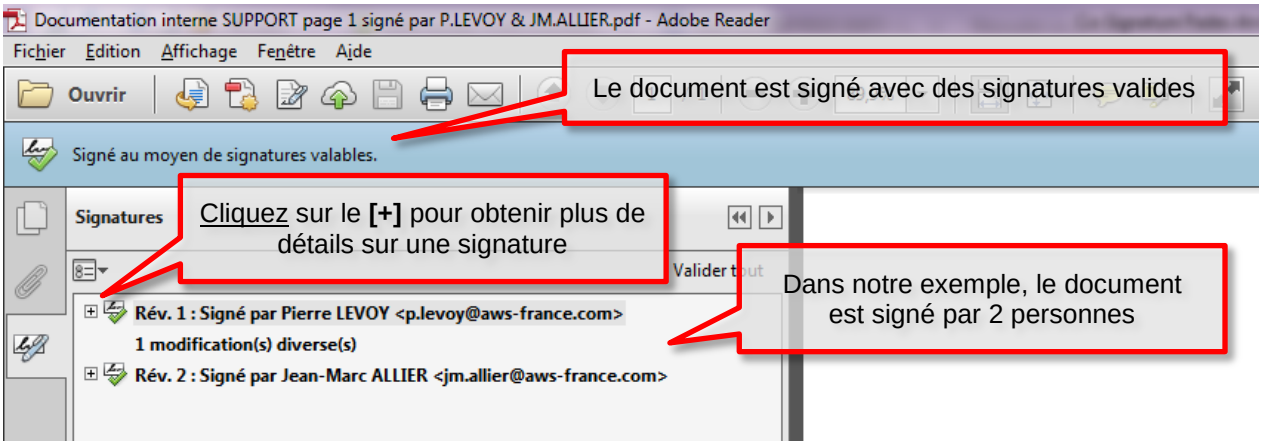
3 VERIFICATION DE SIGNATURE(S) DANS UN DOCUMENT PDF

Cette procédure est valide pour la version Acrobat Reader XI et DC,
seuls quelques icônes ont été modifiées entre ces 2 versions.

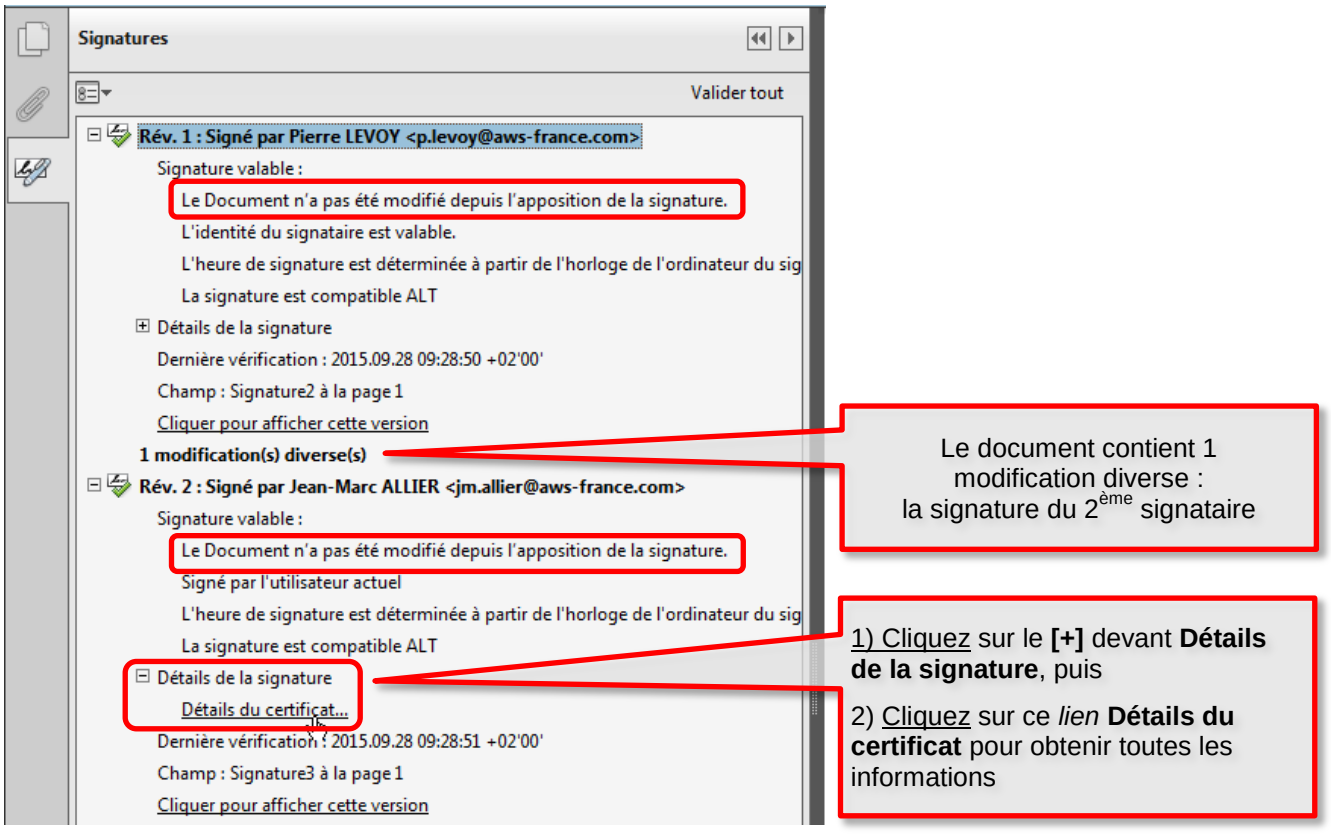
- Ouvrez le *document* **Pdf** dont vous souhaitez vérifier la signature
- Dans le *bandeau* **bleu**, cliquez sur le *bouton* **Panneau Signatures** :



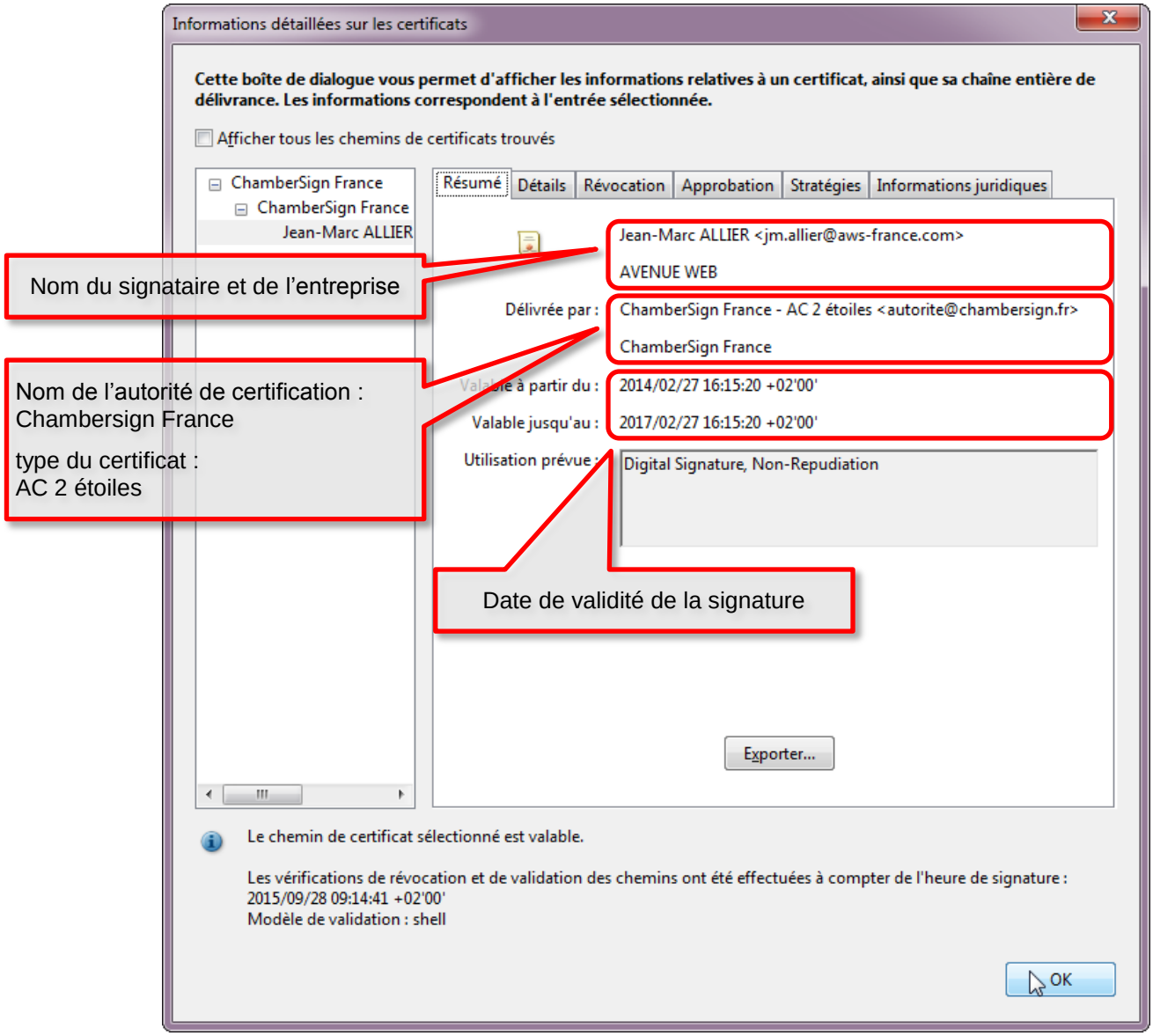
- Le *Panneau* **Signatures** s'affiche :



- Pour avoir plus de détails pour une signature, cliquez sur le **[+]** devant celle-ci :



- Cliquez sur **Détails du certificat** pour obtenir les informations détaillée de la signature électronique :



4 PROCEDURE DE CO-SIGNATURE ET DE DEPOT D'UN PLI DANS LE CADRE D'UN GROUPEMENT

4.1 Préparation des documents à co-signer

Dans le cas de groupement, sous-traitance ou co-traitance, plusieurs candidats doivent signer certains documents, comme par exemple l'acte d'engagement.

Nous vous conseillons de pointer avec soin les documents définitifs à co-signer, et de les placer dans un dossier à part.

4.2 Signature séquentielle

Faites circuler le dossier contenant les pièces à co-signer auprès de tous les signataires.

Chaque signataire signera les documents Pdf selon la procédure adaptée à sa version d'Adobe Acrobat Reader (cf *paragraphes* 2.1 Procédure pour la version Acrobat Reader XI ou 2.2 Procédure pour la version Acrobat Reader DC).

Veillez à :

- ce que chaque signature soit regroupée au même endroit du document afin de faciliter la vérification visuelle des signatures.
- ne pas modifier les documents entre chaque signataire.

4.3 Préparation du pli

Une fois que tous les signataires ont signés :

- Vérifiez que tous les documents ont bien été signés par chaque signataire : reportez-vous au chapitre 3 - Vérification de signature(s) dans un document pdf.
- Replacez les fichiers co-signés dans les dossiers correspondants, à savoir le dossier Candidature ou le dossier Offre

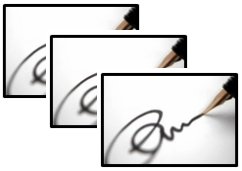
4.4 Dépôt du pli

Le candidat qui dépose le pli doit disposer d'un compte AWS-Entreprise à jour. Il pourra déposer en signant les autres pièces non signées.

Merci de vous référez au manuel utilisateur intitulé « depot_pli_dematerialise.pdf » pour déposer votre pli.

5 ANNEXE 1

5.1 Ce que la signature électronique n'est pas



La signature électronique n'est pas une signature manuscrite numérisée (scannée). Ce type de signature ne présente aucune garantie en termes d'identité du signataire et rend très facile l'usurpation d'identité. Une signature manuscrite scannée peut très facilement être reproduite à l'identique.

En justice, numériser une signature revient à la copier : sur le plan de la preuve, elle équivaut au mieux à un commencement de preuve par écrit.

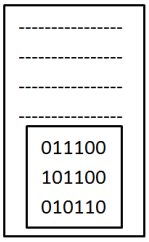
5.2 Ce que la signature électronique est

La signature électronique (parfois appelée signature numérique) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

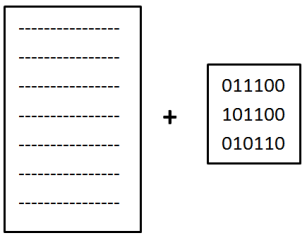
Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères.

5.2.1 Les différentes formes de signature électronique

Il existe différentes formes de signatures électroniques, chacune étant destinée à un usage particulier. Concernant la signature de documents bureautiques, nous retiendront les deux formes suivantes :



La **signature enveloppée** :
la signature est contenue
dans le fichier de données



La **signature détachée** :
les données et la signature sont contenus
dans 2 fichiers distincts.

5.2.2 Les différents formats de signature électronique

Pour des raisons historiques et techniques liés aux différents types de fichiers qu'il est envisageable de signer, plusieurs formats de signature coexistent aujourd'hui sur le marché.

Ils sont regroupés entre 3 grandes familles :

- Binaires
  - PKCS #7
  - CMS, S/MIME
  - **CAdES**
- XML
  - XML-Dsig
  - **XAdES**
- PDF enveloppée (signature interne)
  - PKCS #7
  - **PAdES**

Les signatures de types « avancées » (AdES: Advanced Electronic Signature) standardisées au niveau européen par l'ETSI sont désormais considérées comme le standard du marché.

Ce document présente la signature électronique de documents Pdf selon la norme PAdES.