



# INSTALLATION



K.SIGN® Bureautique

INSTALLATION environnement Windows®



Protecteur d'identité  
Protecteur de liberté  
dans un monde connecté





## K.SIGN BUREAUTIQUE INSTALLATION ENVIRONNEMENT WINDOWS®

---

Version du document :	2.2	Nombre total de pages :	18
Statut du document :	<input type="checkbox"/> Projet	<input checked="" type="checkbox"/> Version finale	
Rédacteur du document :		KEYNECTIS	

Liste de diffusion :	<input checked="" type="checkbox"/> Externe	<input checked="" type="checkbox"/> Interne KEYNECTIS	
	CLIENT		KEYNECTIS

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérfié par
24/03/2010	2.0	DM	Mise à jour AE Déléguee	KEYNECTIS
29/03/2010	2.1	DM	Charte graphique	KEYNECTIS
20/06/2011	2.2	DM	mise à jour Bureautique	KEYNECTIS

Ce document est horodaté et certifié au moyen d'une signature électronique par le département « Business développement » pour la Société KEYNECTIS.



## SOMMAIRE

<b>1</b>	<b>Présentation de KSign®</b>	<b>4</b>
1.1	Description .....	4
1.2	Usage et type de signature .....	4
<b>2</b>	<b>Avant de demarrer l'installation</b>	<b>5</b>
2.1	Logiciel et matériel nécessaire.....	5
2.2	Utilisateurs de Microsoft Vista®.....	6
<b>3</b>	<b>Installer K.sign® sur mon PC avec Microsoft windows</b>	<b>8</b>
3.1	Etape 1 réception des éléments .....	8
3.2	Etape 2 installation des drivers Gemalto .....	9
3.3	Etape 3 Modifier le code PIN .....	9
3.4	Etape 4 Accuser réception et vérifier l'installation .....	10
<b>4</b>	<b>Parametrage d'une signature électronique</b>	<b>14</b>
4.1	Modifier l'apparence de votre signature dans les documents .....	15
4.2	Modifier les contrôles des documents avant signature.....	16
4.3	Modifier les paramètres de saisie au moment de la signature .....	16
<b>5</b>	<b>Révoquer votre certificat</b>	<b>17</b>
<b>6</b>	<b>Support a l'installation</b>	<b>17</b>
6.1	Accéder au service clients KEYNECTIS.....	17
6.2	Accéder à la liste des questions les plus fréquentes .....	17
6.3	Bibliographie .....	18



## 1 PRESENTATION DE KSIGN®

### 1.1 Description

Vous venez de recevoir une clef K.Sign® Bureautique vous permettant de mettre en œuvre la technologie de signature de documents de la société Adobe Systems Incorporated (Adobe) appelée Certified Document Services (CDS). Si vous avez choisi une clef K.Sign® réglementé (RGS) consultez le document d'installation K.Sign Réglementé.

Proposée clef en main, cette solution intègre l'ensemble des éléments permettant de réaliser une signature à valeur légale par une personne physique ou une personne morale.

K.Sign® Bureautique vous apporte:

1. **Un moyen d'identification électronique du signataire** au travers d'un certificat X509, reconnu universellement par tous les produits de la gamme Adobe,
2. **Un outil de signature électronique**, matérialisé par une clé USB cryptographique, permettant la signature de certification (Adobe Acrobat®) ou la signature d'approbation (Adobe Reader® extension),
3. **La compatibilité avec Adobe Reader® V7+** disponible sur tous les types d'environnements – Microsoft Windows, Linux, Apple Macintosh - et dans toutes les langues, pour la vérification des signatures,
4. **Un format de conservation dans le temps** grâce au couplage de l'outil de signature aux services d'horodatage (TSP RFC3161) et de vérification des certificats OCSP (Online Certificate Status Protocole) fournis par KEYNECTIS (création d'un document PDF signé « auto portant » disposant des fonctions d'intégrité et de non répudiation sans altération dans le temps et ce de manière totalement transparente pour les utilisateurs).

### 1.2 Usage et type de signature

Le document PDF est un format ISO ayant la particularité d'être accessible par l'ensemble des ordinateurs du marché. Son succès est également lié à son format qui respecte la continuité d'usage dans la dématérialisation des documents papier.

Dans le souci d'adaptation aux nouveaux besoins associés à l'usage de l'internet et de la dématérialisation des procédures métiers, Adobe a implémenté la signature électronique au sein du format PDF lui-même permettant de donner à un document électronique :

- La même valeur qu'un document papier,
- La même ergonomie qu'un document papier signé (signature et vérification de la signature sont indissociables).

Signification des codes de vérification ou validité générés par les outils Adobe du marché.

Signature  
d'approbation valide



Signature de  
Certification Valide



Validité d'identité de l'auteur de la  
signature NON reconnue



Signature  
invalide






En utilisant K.Sign® vous pouvez signer tous vos documents PDF en utilisant les deux types de signatures proposés par Adobe :

Signature de certification symbolisée par le « Blue Ribbon » .

- Applicable en mode visible (Associée à une représentation graphique) ou invisible elle génère dès l'ouverture du document l'affichage d'un bandeau d'information sur la signature du document.
- Utilisée pour donner à un document une garantie d'intégrité apportée par son auteur elle sera obligatoirement la première appliquée dans le cadre d'un document soumis à de multiples signatures d'approbation.
- La signature de certification est appliquée uniquement avec Adobe Acrobat (V 7+).

Signature d'approbation symbolisée par le stylo .

- Applicable en mode visible (Associée à une représentation graphique) elle ne provoque pas l'affichage d'un bandeau d'information (sauf pour V9.0).
- Utilisée pour la signature de formulaire avec champ de signature spécifique, de document PDF natif (Positionnement manuel du champ de signature) et les documents à multi-signatures elle amène la garantie d'intégrité aux champs modifiés dans un formulaire par le signataire.
- La signature d'approbation est applicable avec Adobe Reader® (Document possédant la fonction Reader extension) et avec Adobe Acrobat® (V 7+).

## 2 AVANT DE DEMARRER L'INSTALLATION

### 2.1 Logiciel et matériel nécessaire

#### 2.1.1 Logiciel nécessaire à l'utilisation de K.Sign® avec Adobe Acrobat Reader®

Vous pouvez signer des documents PDF (Document et formulaire possédant la fonction Reader Extension) avec les logiciels Adobe Acrobat Reader®. Vous trouverez sur le site ci-dessous les pré-requis techniques pour leur installation :

<http://www.Adobe.com/products/reader/productinfo/systemreqs/>

#### 2.1.2 Logiciel nécessaire à l'utilisation de K.Sign® avec Adobe Acrobat®

Vous pouvez signer des documents PDF (Document et formulaire) avec les logiciels Adobe de la famille Acrobat® (Acrobat standard Edition, Acrobat PRO Edition, Acrobat 3D édition à partir de la version 7). Vous trouverez sur le site ci-dessous les pré-requis techniques pour leur installation

<http://www.Adobe.com/products/acrobatpro/productinfo/systemreqs/>

#### 2.1.3 Matériel et logiciel nécessaire à l'installation du jeton USB Gemalto

L'utilisation du jeton USB GEMALTO nécessite sa reconnaissance par votre Système d'exploitation Microsoft Windows, Apple Macintosh ou LINUX par l'installation d'un driver. Vous trouverez à l'adresse suivante les pré-requis techniques pour son installation :

<http://www.keynectis.com/caracteristiques-techniques-de-ksign>



Le jeton USB est constitué d'une carte cryptographique de type Carte TPC IM CC installé dans un lecteur USB référencé USB Shell TOKEN par la société GEMALTO. Vous trouverez une documentation vous permettant de télécharger le middleware et sa documentation permettant son usage dans le cadre des signatures électroniques.

Pour toute installation du composant Classic client 6.0 standard édition vous devez avoir les droits d'administration sur l'ordinateur.

#### **2.1.4 Matériel :**

L'ordinateur individuel compatible PC doit avoir au minimum:

- 50 MB d'espace disque libre
- Un processeur Pentium II 200 MHz ou équivalent
- Une carte graphique VGA supportant au moins 256 couleurs.

#### **2.1.5 Système d'exploitation :**

Classic Client 6.0 est livré sous 2 versions, une version 64-bit du système d'exploitation et une version 32-bit du système d'exploitation. Il est nécessaire d'installer la version appropriée à votre Système d'exploitation en suivant le tableau ci dessous :

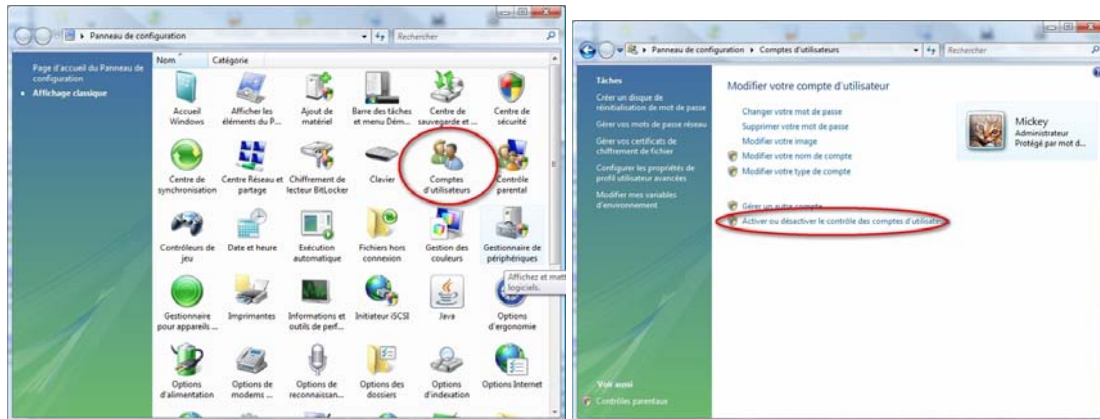
<b>Système d'exploitation</b>	<b>Bits</b>
Microsoft Windows 2000 Professional (avec le SP4)	32
Microsoft Windows XP Home (jusqu'au SP2)	32
Microsoft Windows XP Professional (jusqu'au SP2)	32 and 64
Microsoft Windows Server 2000	32
Microsoft Windows Server 2003	32 and 64
Microsoft Windows Vista	32 and 64
Microsoft Windows Seven	32 and 64

#### **2.1.6 Compatibilité avec d'autres usages**

- Citrix Metaframe® Presentation Server and Citrix Metafram® Presentation Server V4
- Microsoft Terminal Services Windows 2003.

## **2.2 Utilisateurs de Microsoft Vista®**

Si vous avez un problème d'installation dans l'environnement Microsoft Vista avec le Middleware Classic Client vous pouvez probablement le résoudre en modifiant le UAC (Contrôle de compte utilisateur) au sein du panneau de configuration Microsoft Vista.



Une fois le middleware installé n'oubliez pas de repositionner l'UAC sur sa position initiale.



### 3 INSTALLER K.SIGN® SUR MON PC AVEC MICROSOFT WINDOWS

#### 3.1 Etape 1 réception des éléments

A l'issue de la fabrication de votre clef K.Sign® KEYNECTIS vous a fait parvenir les éléments suivants :

- Votre clef USB KSIGN
- Un Document PIN MAILER Caviardé contenant le code PIN d'accès à votre clef USB
- Un Email ci-dessous vous indiquant les URL importantes à consulter

Cher Client

Votre demande de certificat KSIGN a été validée par le Service Clients de KEYNECTIS :

Nom commun : .

Email :

Organisation :

Département :

Titre :

Ville/Localité :

Etat/Province :

Pays : France.

Code de révocation : xxxxxx.

Vous pouvez dès à présent télécharger et sauvegarder le kit d'installation de votre clé K.Sign, indispensable à la génération de votre certificat, depuis l'adresse suivante :

<http://www.keynectis.com/fr/signature-electronique/caracteristiques-techniques.html>

Vous pouvez télécharger les documents d'installation et d'utilisation de la clef K.Sign depuis l'adresse suivante:

<http://www.keynectis.com/fr/support-informations.html>

A la fin de l'installation, merci de télécharger le document PDF d'Acceptation K.sign depuis l'adresse

<http://www.keynectis.com/static/content/common/ksign/AcceptationKsign.pdf>

de le signer électroniquement avant de le retourner en pièce jointe par email à :

[service.clients@keynectis.com](mailto:service.clients@keynectis.com)



Si vous n'avez pas reçu tous ces éléments contacter le service clients de KEYNECTIS par email : [service.clients@keynectis.com](mailto:service.clients@keynectis.com)

### 3.2 Etape 2 installation des drivers Gemalto

Vous devez télécharger le kit d'installation du Token accessible sur le site de KEYNECTIS à l'URL suivante :

<http://www.keynectis.com/caracteristiques-techniques-de-ksign>

et l'enregistrer sur votre ordinateur

Procédez à l'expansion du fichier .Zip et en extraire le document d'installation. Vous pouvez utiliser l'installation automatique sauf si votre poste est déjà équipé d'un autre lecteur de carte à puce.

Suivez la procédure d'installation du chapitre 1 « Installation » du document que vous pouvez télécharger à l'URL :

[http://www.keynectis.com/PDF/FR/Ressources/Classic\\_Client\\_User\\_Guide.pdf](http://www.keynectis.com/PDF/FR/Ressources/Classic_Client_User_Guide.pdf)

Lorsque l'installation est terminée l'insertion de la clef USB se traduit par la reconnaissance automatique des drivers , l'allumage continu de la clef USB et l'apparition d'une Icône donnant accès à la documentation sur votre PC directement via l'interface de gestion de votre carte USB

### 3.3 Etape 3 Modifier le code PIN

La clef K.Sign® qui vous a été affectée contient tous les certificats permettant son utilisation pour la signature de document PDF avec les produits ADOBE. Nous consulter si vous désirez bénéficier d'autres fonctionnalités. Elle a été initialisée avec un Code PIN dont la valeur vous est précisée dans le courrier d'accompagnement (PinMailer Caviardé) . Il est important que vous procédiez à son initialisation avant de générer vos bichés de sécurité et de télécharger votre certificat de signature associé.

La clef K.Sign® vous a été affectée personnellement, il est de votre responsabilité de la protéger au moyen des deux codes PIN (Utilisateur et Administrateur) que vous pouvez choisir au moyen de la « Toolbox » Gemalto.



Remarque sur l'utilisation de la clef K.sign® comme container de sécurité :



La clef K.sign® peut être utilisée pour stocker d'autres certificats afin de leur conférer une portabilité sécurisée. Nous vous renvoyons aux fonctions d'importation de certificats telles que décrites au chapitre 4 (User Tasks, Managing Certificates) du document : [Classic\\_Client\\_User Guide.pdf](#)

### 3.4 Etape 4 Accuser réception et vérifier l'installation

Pour vérifier la bonne installation de la clef K.Sign®, il est obligatoire de procéder à la signature électronique du document d'acceptation de la clef K.Sign® et de le retourner par email au [service.clients@keynectis.com](mailto:service.clients@keynectis.com).

Vous avez reçu par email les instructions pour obtenir un document PDF intitulé AcceptationKsign.pdf que vous allez pouvoir immédiatement signer électroniquement au moyen d'un des logiciels suivants

-Acrobat® Standard ou Pro Release 8 ou Release 9

-Adobe Reader® Release 8 ou release 9

Le document à signer est téléchargeable à l'URL suivante :

<http://www.keynectis.com/PDF/FR/Ressources/AcceptationKsign.pdf>

#### **Remarques:**

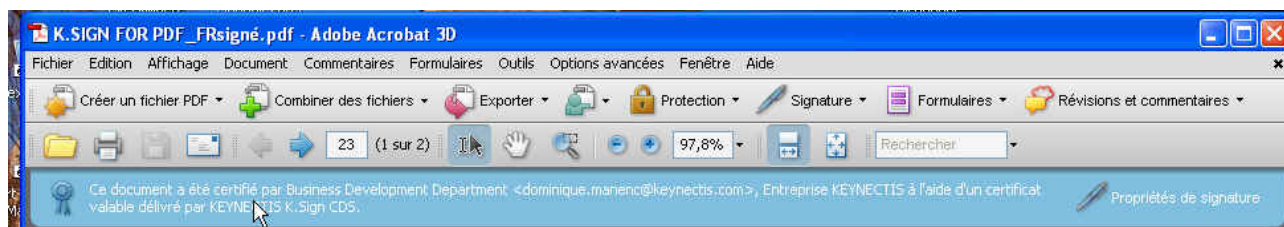
Si votre poste est équipé de la version 7 de ces 2 produits, merci de contacter [service.clients@keynectis.com](mailto:service.clients@keynectis.com) pour l'application d'un PATCH permettant le support de l'horodatage dans les signatures

Si votre poste n'est pas équipé d'un de ces produits vous pouvez télécharger gratuitement Adobe Reader® 9 à l'adresse suivante :

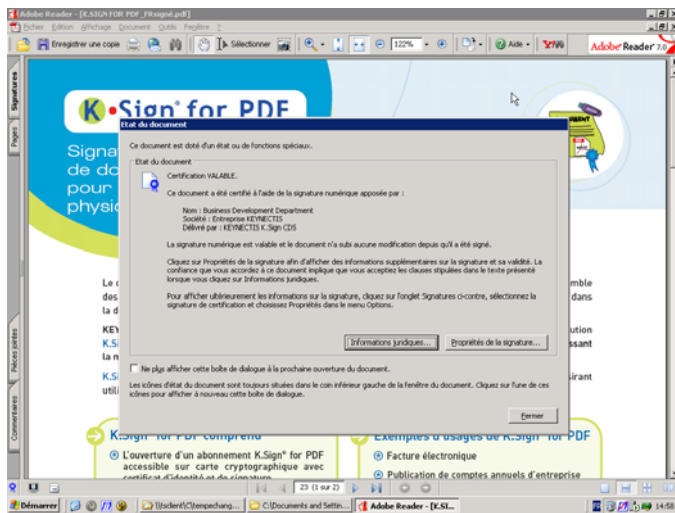
<http://www.keynectis.com/caracteristiques-techniques-de-ksign>

#### **3.4.1 Vérification de signature sur votre poste :**

L'ouverture du document provoque l'affichage du bandeau de validation suivant (R8 et R9)



Ou l'affichage du panel état du document en version 7



### 3.4.2 Signer le document d'acceptation

1) Après vérification de l'information de signature de certification et de l'ensemble des champs vous identifiant cliquez sur le champ signature.



MOD\_K.sign Acceptation Unitaire de remise signed V1.0.pdf - Adobe Acrobat 3D

Fichier Edition Affichage Document Commentaires Formulaires Outils Options avancées Fenêtre Aide

Créer un fichier PDF Combiner des fichiers Exporter Protection Signature Formulaires Révisions et commentaires

1 / 1 105% Rechercher

Ce document a été certifié par Departement Business Development <dominique.manenc@keynectis.com>, Entreprise KEYNECTIS à l'aide d'un certificat valable délivré par KEYNECTIS K.Sign CDS. Remplissez le formulaire suivant: Si vous êtes l'auteur du formulaire, choisissez Diffuser le formulaire dans le menu Formulaires afin de l'envoyer aux destinataires concernés.

Document de remise et d'acceptation d'utilisation  
Des Certificats de signature K.Sign de KEYNECTIS.

Je, soussigné, **Dominique manenc**

Dé la société : **Keynectis**

Dont le n° de SIREN est : **478217318**

Certifie avoir reçu un kit de signature K.sign N° **DBID033**

Je déclare avoir pris connaissance et accepter les termes et conditions d'utilisation de ces Certificats de type « CDS Usage2 » décrits dans la CPS publiée à l'adresse suivante :

[http://www.keynectis.com/PC/CPS\\_KEYNECTISCDS\\_CA\\_05112007\\_GB-V1.pdf](http://www.keynectis.com/PC/CPS_KEYNECTISCDS_CA_05112007_GB-V1.pdf)

Je m'engage à utiliser ce certificat uniquement avec les outils de signature de la société ADOBE (Live cycle, Acrobat et Reader).

Ma signature électronique avec horodatage de ce document est la preuve de la remise du certificat\*.

2) Une des deux fenêtres suivantes apparait :

Signer le document

ID numérique: Departement Business Development

Identification Numérique

Signature de transaction, Signature de document, Chiffrement de clé

2011/04/08 15:44:56 +0200

KEYNECTIS K.Sign CDS

Aspect: Texte standard

Departement Business Development

Signature numérique de Departement Business Development

CN: cn=K, o=Intégraparc, ou=KEYNECTIS, ou=0002-471217318, ou=ClientPCRay Dablu 0033, ou=Departement Business Development

Date: 2008.10.08 17:07:38 +0200

Nom: manenc

Adresse électronique: jmanenc@keynectis.com

Emploiement: jmanenc

Coordonnées: manenc

Actualiser les ID Signer Annuler

Signer le document

ID numérique: Departement Business Development

Identification Numérique

Signature de transaction, Signature de document, Chiffrement de clé

2011/04/08 15:44:56 +0200

KEYNECTIS K.Sign CDS

Aspect: Texte standard

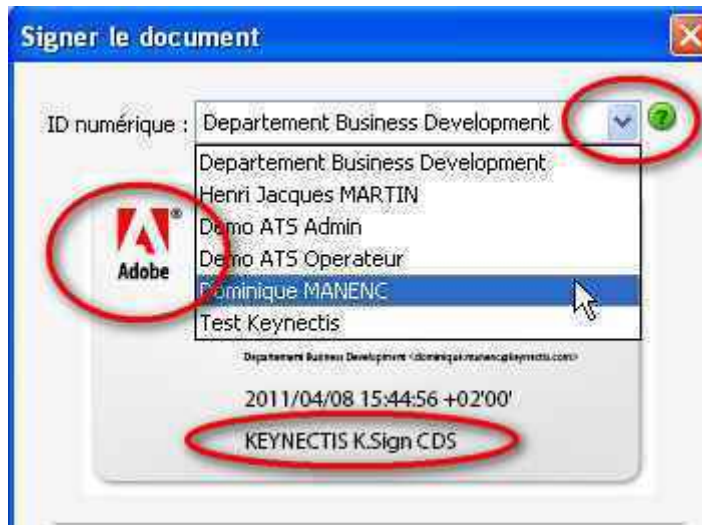
Departement Business Development

Signature numérique de Departement Business Development

CN: cn=K, o=Intégraparc, ou=KEYNECTIS, ou=0002-471217318, ou=ClientPCRay Dablu 0033, ou=Departement Business Development

Date: 2008.10.08 18:00:38 +0200

Actualiser les ID Signer Annuler



3) Vérifier que l'identification numérique correspond au certificat K.Sign®. Cela se traduit par l'affichage

-du logo Adobe dans la partie supérieure de l'encadrement

-du label KEYNECTIS K.Sign® CDS comme ci-dessous.

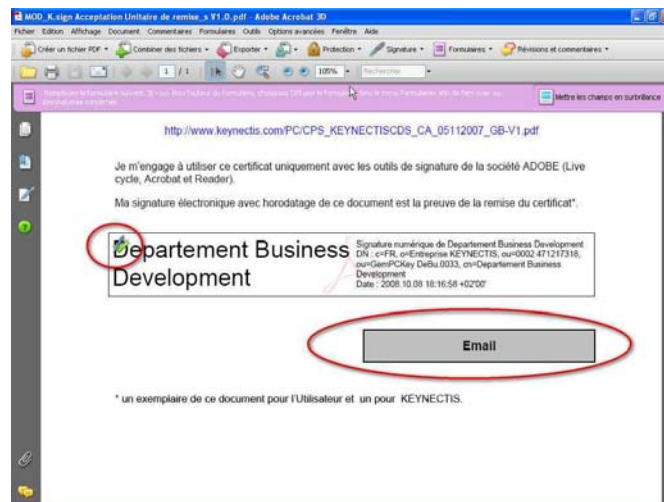
Si ce n'est pas le cas choisissez l'ID numérique dans la fenêtre ID Numérique comme ci-dessous :

Puis cliquez sur le Bouton Signer

4) enregistrez le fichier dans le répertoire de votre choix

5) Entrez le code PIN de votre clef K.Sign®

6) Cliquez sur le bouton Email pour provoquer l'envoi de ce document de façon automatique à destination de [service.clients@keynectis.com](mailto:service.clients@keynectis.com)





## 4 PARAMETRAGE D'UNE SIGNATURE ELECTRONIQUE

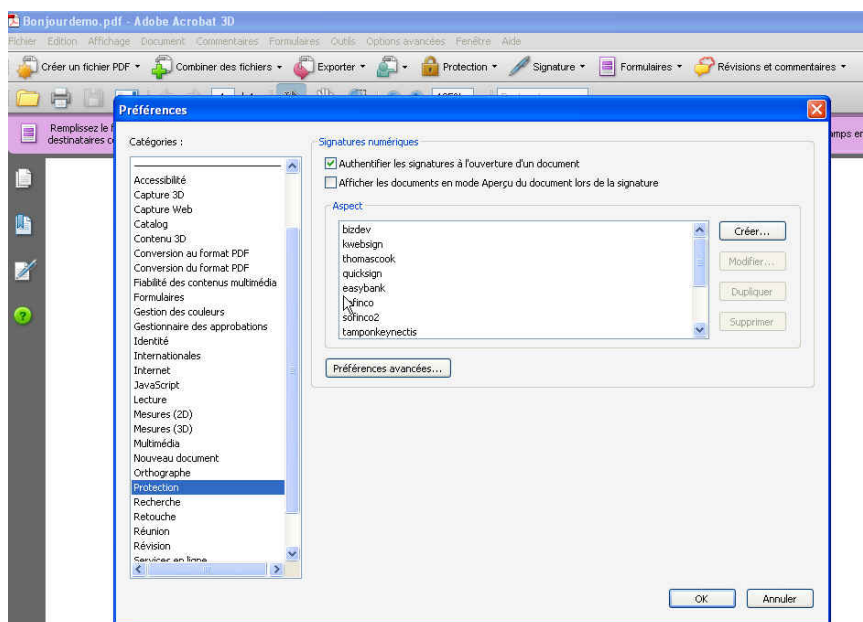
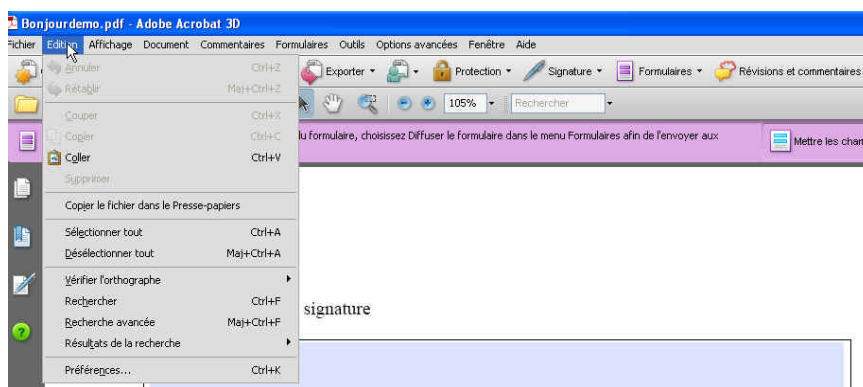
La signature du document est réalisée sur votre poste de travail via les produits ADOBE Acrobat® ou Reader® (si le PDF possède les droits Avancés de modification appelés reader extension).

Les produits Adobe permettent par paramétrage de modifier l'aspect de votre signature dans les documents PDF que vous désirez Signer.

Vous pouvez visionner à l'adresse suivante une vidéo de la réalisation d'une signature avec ces produits

<http://www.Adobe.com/products/acrobat/tutorials/signingdocs/index.html>

Les paramètres sont accessibles au moyen du panel Edition /Préférences/protection ;





#### 4.1 Modifier l'apparence de votre signature dans les documents

Vous pouvez modifier l'aspect de votre signature électronique telle qu'elle sera présentée dans le document (Cas d'une signature visible). Cette opération est réalisée au moyen du bouton Créer du panel Ci-dessus.

Vous pouvez créer autant de représentation de votre signature que vous le désirez en leur donnant un nom différent puis les modifier/supprimer en utilisant ce panel.

Ce panneau se modifie dynamiquement chaque fois que vous modifiez une case à cocher

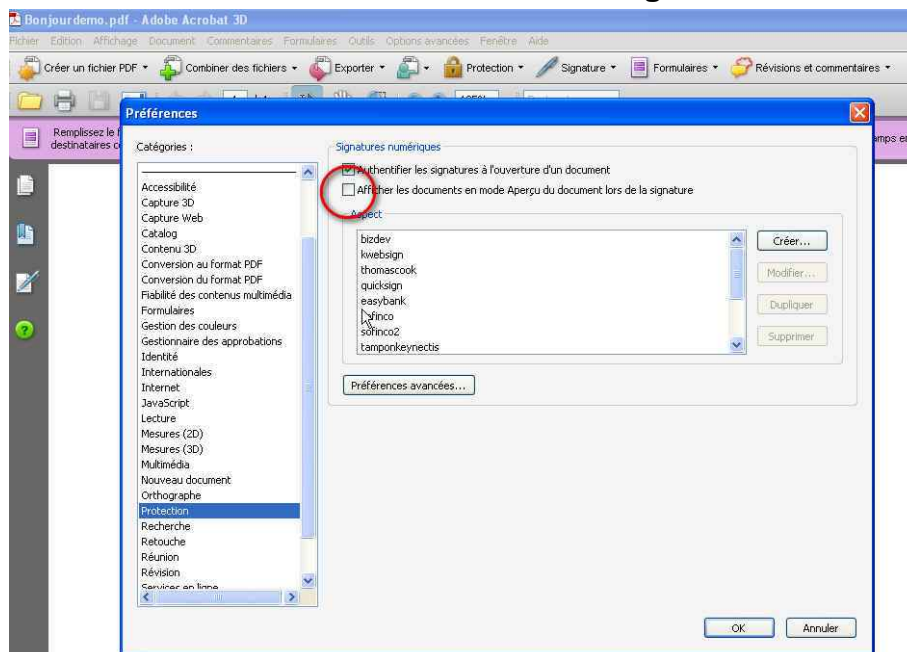
Quand la signature correspond à vos souhaits remplissez le champ titre et cliquez sur OK votre apparence de signature sera conservé par le logiciel et sera modifiable à tout moment.

Attention si vous désirez insérer un LOGO dans votre signature vous devez le fournir en format PDF.





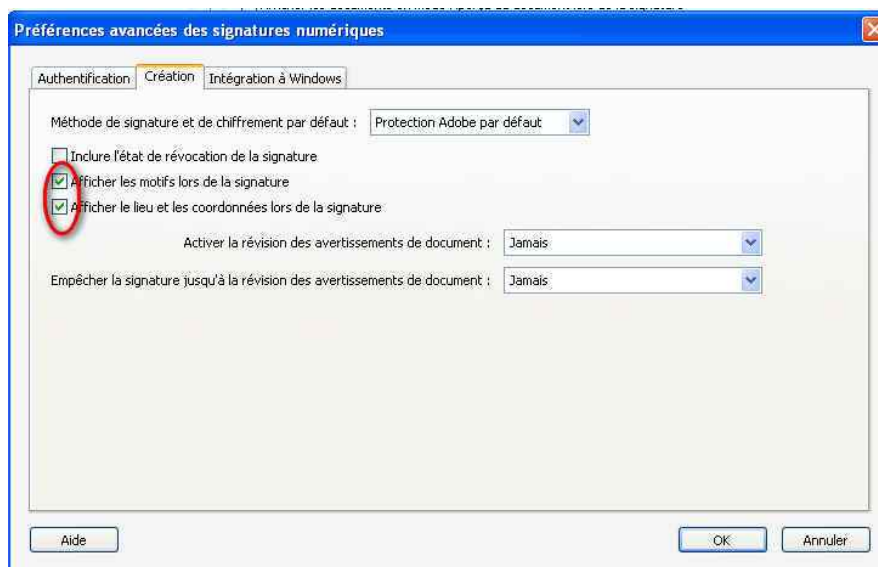
## 4.2 Modifier les contrôles des documents avant signature



Avant apposition de votre signature les produits peuvent réaliser un contrôle du type /A (Archivable) /Q Archivable avec données modifiables. Cette option est activable par la case à cocher entourée dans le panel ci-dessus (Afficher les documents en mode aperçu lors de la signature)

## 4.3 Modifier les paramètres de saisie au moment de la signature

Si vous avez décidé de faire apparaître dans votre signature les informations optionnelles de lieu et de coordonnées vous devez au moyen du bouton préférence « Avancée » onglet « Création » cocher les deux cases comme ci-dessous.





## 5 RÉVOQUER VOTRE CERTIFICAT

Si pour une raison quelconque (perte, vol etc;) vous n'êtes plus en possession de votre clef K.Sign vous pouvez faire une demande de révocation de votre certificat auprès de KEYNECTIS.

La révocation du certificat vous protège contre l'utilisation par un tiers qui aurait connaissance de votre code PIN de votre identité. La révocation d'un certificat interdit son usage à partir de la date de révocation (Révocation effective le même jour à minuit).

La révocation d'un certificat n'a aucun impact sur les documents signés préalablement dont la signature reste valide grâce au procédé d'autoportance et d'horodatage mis en œuvre par la signature K.Sign for PDF.

Deux procédures de révocation sont mises à votre disposition :

**Procédure 1:** Appelez ou envoyez un email au service clients de KEYNECTIS qui procédera à la révocation durant les jours et heures ouvrés indiqués dans les conditions générales de vente.

**Procédure 2:** Connectez vous à l'URI ci dessous et procédez vous même à la révocation en indiquant le code de révocation qui vous a été remis dans le mail de mise à disposition initiale de votre clef K.Sign.

<https://kregistration-user.certificat2.com/eCommerce/KSSL/KSIGN:IHM>

## 6 SUPPORT A L'INSTALLATION

### 6.1 Accéder au service clients KEYNECTIS

Le service clients de KEYNECTIS est joignable conformément aux informations indiquées dans le site Web <http://www.keynectis.com/support>

### 6.2 Accéder à la liste des questions les plus fréquentes

Ci-dessous quelques remarques concernant l'usage de K.sign® mais vous trouverez d'autres informations techniques sur le site Web de KEYNECTIS :

<http://www.keynectis.com/fr/faq>

Votre logiciel Adobe conserve le dernier format de signature que vous avez utilisé vous évitant ainsi de remplir tous les champs à chaque signature.

Si vous signez plusieurs documents sans refermer le logiciel Adobe utilisé vous n'aurez pas à ressaisir le code Pin à chaque signature

#### 6.2.1 Usage de K.sign® avec de multiple certificats

Lorsque votre ordinateur possède plusieurs certificats il est possible qu'Adobe vous propose un certificat qui ne soit pas celui de K.sign®. Pour s'assurer que vous allez signer avec le bon certificat vous devez voir l'information suivante quand vous sélectionnez le certificat dans la liste déroulante :



### 6.3 Bibliographie

Si vous désirez plus d'informations sur les logiciels Adobe et la signature électronique que nous utilisons consultez le site <http://www.adobe.com/devnet/acrobat/security.html>.

Si vous désirez plus d'information sur les clefs USB de Gemalto et leur utilisation technique consultez <http://support.gemalto.com/>.