



INSTALLATION WINDOWS



K.SIGN® RGS 2* et EBICS-TS

Installation en Environnement Windows® de K.Sign® réglementé

Auteur : Dominique Manenc

Date : 10/08/2011

Protecteur d'identité
Protecteur de liberté
dans un monde connecté



INSTALLATION K.SIGN RGS 2* ENVIRONNEMENT WINDOWS®

Version du document :	1.4	Nombre total de pages :	15
Statut du document :	<input type="checkbox"/> Projet	<input checked="" type="checkbox"/> Version finale	
Rédacteur du document :	DM	KEYNECTIS	

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

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérfié par
10/08/2011	1.4	DM	Corrections orthographiques	DM
24/06/2011	1.3	DM	Corrections pop-up	DM
20/06/2011	1.2	DM	Mises à jour des liens et URL nouveau site web	DM
03/03/2011	1.1	DM	Ajout pop-up AC Racine	DM
01/03/2011	1.0	DM	Création à partir de K.Sign for PDF V2.1	DM

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



SOMMAIRE

1	Présentation de KSign®	4
1.1	Description	4
1.2	Usage et type de signature	4
2	Avant de demarrer l'installation	4
2.1	Logiciel et matériel nécessaire.....	4
2.2	Utilisateurs de Microsoft Vista®.....	5
3	Installer K.sign® sur mon PC avec Microsoft windows	7
3.1	Etape 1 réception des éléments	7
3.2	Etape 2 installation des drivers Gemalto	7
3.3	Etape 3 Modifier le code PIN	8
3.4	Etape 4 Vérifier l'installation.....	8
4	Révoquer votre certificat	11
5	Support a l'installation	11
6	Annexe	12
6.1	Paramétrage d'une signature électronique dans ADOBE READER 9	12
6.2	Modifier l'apparence de votre signature dans les documents	13
6.3	Modifier les contrôles des documents avant signature.....	14
6.4	Modifier les paramètres de saisie au moment de la signature	14
6.5	Bibliographie	15



1 PRESENTATION DE KSIGN®

1.1 Description

Vous venez de recevoir une clef K.Sign® RGS 2* vous permettant de mettre en œuvre la technologie de signature de documents (PDF, XML, EBICS-TS etc.) la signature de vos emails et l'authentification par certificat.

Proposée sous forme d'un support USB personnalisé avec un certificat Electronique, K.Sign® permet de réaliser des signatures à valeur légale par une personne physique conformément au **Référentiel Général de Sécurité (RGS)** de niveau 2* et aux recommandations du CFONB (PAC).

1.2 Usage et type de signature

K.Sign® peut être utilisé avec des logiciels de signature du marché qui réaliseront votre signature électronique.

Keynectis a ainsi validé l'apposition de signature électronique sur :

- Vos documents PDF en utilisant les produits proposés par Adobe (Acrobat & Reader R9 et R10),
- Vos documents Windows® Office® 2010 avec les produits proposés par Microsoft®,
- Tous les types de documents (XML Image/son Open Office etc.) avec les produits proposés par Lexpersona (ou KEYNECTIS),
- Vos flux d'échange Financier avec les protocoles EBICS-TS.

2 AVANT DE DEMARRER L'INSTALLATION

2.1 Logiciel et matériel nécessaire

2.1.1 Logiciel pilote du support cryptographique USB:

L'utilisation du support USB GEMALTO nécessite sa reconnaissance par votre Système d'exploitation Microsoft Windows, par l'installation d'un driver. Vous trouverez à l'adresse suivante les pré-requis techniques pour son installation (Les mêmes drivers sont utilisés quelque soit le K.Sign® (RGS ou Bureautique) que vous utilisez :

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

Le support 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 (Uniquement en anglais) permettant son Installation et son suivi à l'URL Suivante

http://www.keynectis.com/PDF/FR/Ressources/Classic_Client_User_Guide.pdf



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

2.1.2 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.

2.1.3 Système d'exploitation :

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

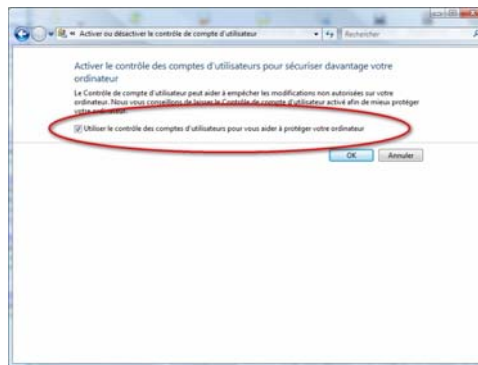
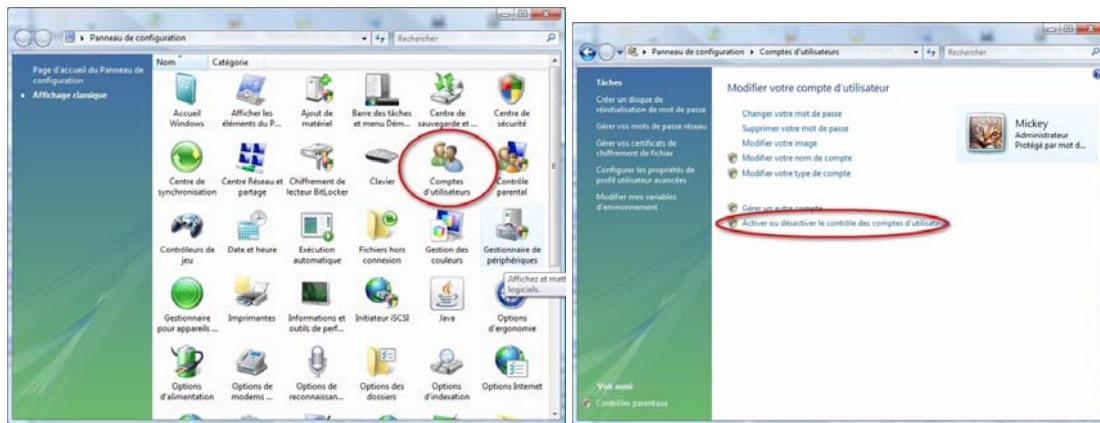
Système d'exploitation	Bits
Microsoft Windows 2000 Professional (avec le SP4)	32
Microsoft Windows XP Home (jusqu'à SP2)	32
Microsoft Windows XP Professional (jusqu'au SP2)	32 and 64
Microsoft Windows Server 2000	32
Microsoft Windows Server 2003	32 and 64
Microsoft Windows Vista	32 and 64
Microsoft Windows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

2.1.4 Compatibilité avec d'autres usages

- Citrix Metaframe® Presentation Server and Citrix Metaframe® Presentation Server V4 (nous consulter)
- 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® RGS 2* KEYNECTIS vous a fait parvenir directement et via son Autorité d'Enregistrement Délégée (AED) les éléments suivants :

-Votre support USB KSIGN® via AED ;

-Un Document PIN MAILER Caviardé contenant le code PIN d'accès à votre clef USB (Par la poste).

Si vous n'avez pas reçu tous ces éléments contactez votre AED ou le service clients de KEYNECTIS par email : 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 en utilisant le PSW de protection du fichier ZIP suivant : 642233 et en extraire le document d'installation.

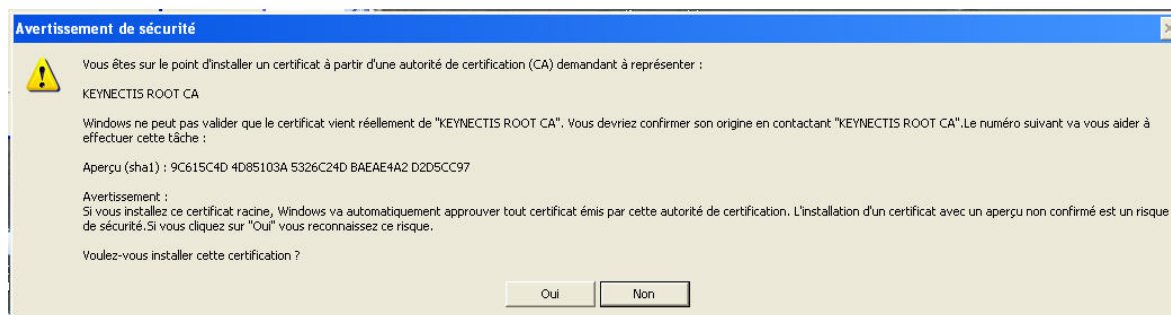
Vous pouvez utiliser l'installation automatique sauf si votre poste est déjà équipé d'un autre lecteur de carte à puce.

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

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 (en bas à droite) donnant accès à l'outil de gestion de la clef K.Sign et la documentation sur votre PC directement via l'interface de gestion de votre carte USB.

Lors de la première installation la clef USB va demander l'installation d'un nouvelle Autorité de confiance racine via la pop-up ci-dessous. **Répondre OUI**





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 documents. Elle a été initialisée avec un Code PIN dont la valeur vous est précisée dans le courrier d'accompagnement (Pin Mailer Caviardé) et dont vous êtes le(a) seul(e) à avoir connaissance.

La clef K.Sign® vous a été affectée personnellement, il est de votre responsabilité de la protéger au moyen du code PIN en veillant à sa confidentialité.



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 Vérifier l'installation

Pour vérifier la bonne installation de la clef K.Sign® dans votre environnement, il est conseillé de procéder à la signature électronique d'un document PDF.

Vous allez pouvoir immédiatement signer électroniquement **CE** document au moyen d'un des logiciels suivants :

- Acrobat® Standard ou Pro Release 9 ou Release x
- Adobe Reader® Release 9 ou release x

En cliquant dans la zone de signature ci dessous.



Remarques:

Si votre poste est équipé de la version 8 de ces 2 produits, vous allez pouvoir signer techniquement le document mais la visualisation de la signature sera en erreur.

Si vous utilisez la version 7 de ces produits merci de contacter service.clients@keynectis.com pour l'application d'un PATCH permettant le support de l'horodatage dans les signatures.

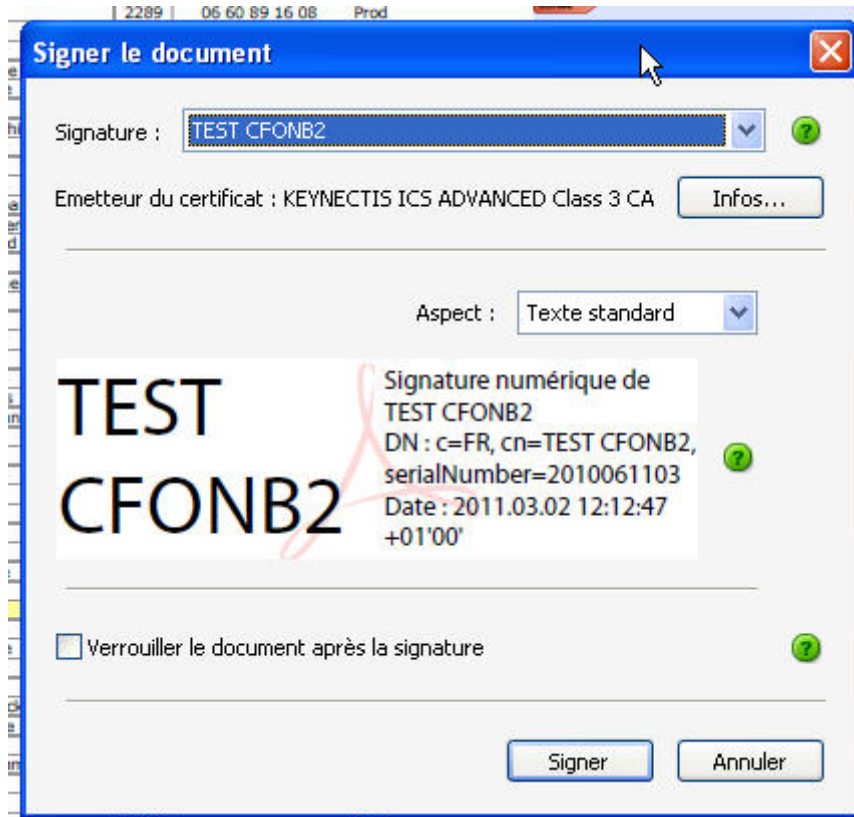
Si votre poste n'est pas équipé d'un de ces produits vous pouvez télécharger gratuitement Adobe Reader® X à l'adresse suivante



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

Vous pouvez aussi conserver votre version d'Acrobat (7 et 8) et télécharger Adobe Reader X ils cohabitent très bien.

1) La fenêtre suivante apparait :



2) Vérifier que l'identification numérique correspond au certificat K.Sign® qui vous a été remis

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

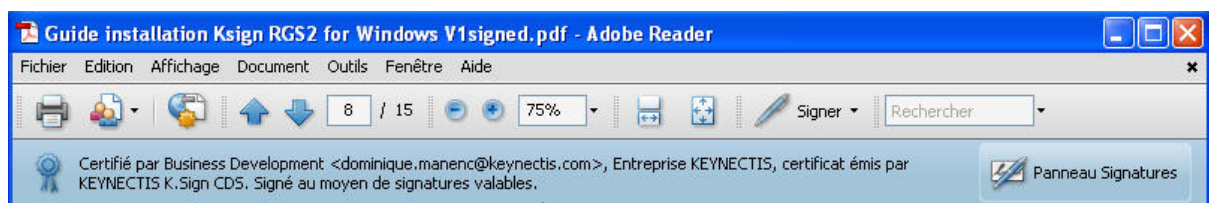
Les certificats K.Sign se caractérisent par l'information : **EMETEUR de Certificat : KEYNECTIS ICS ADVANCED Class 3 CA**

Puis cliquez sur le Bouton Signer et répondez aux questions dans les pop-up (1^{er} fois)

3) Enregistrez le fichier dans le répertoire de votre choix

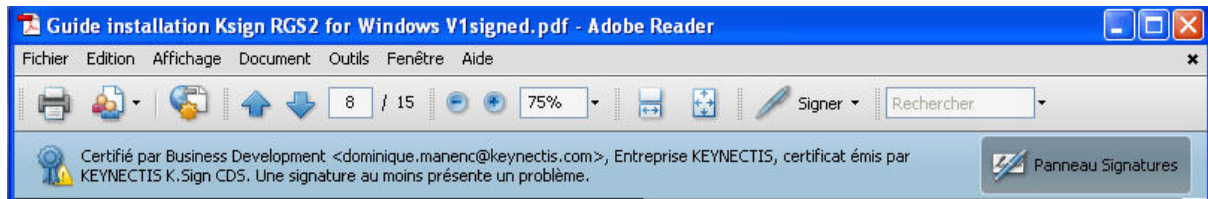
4) Entrez le code PIN de votre clef K.Sign®

Le bandeau d'information de votre Adobe Reader doit alors afficher le message suivant :



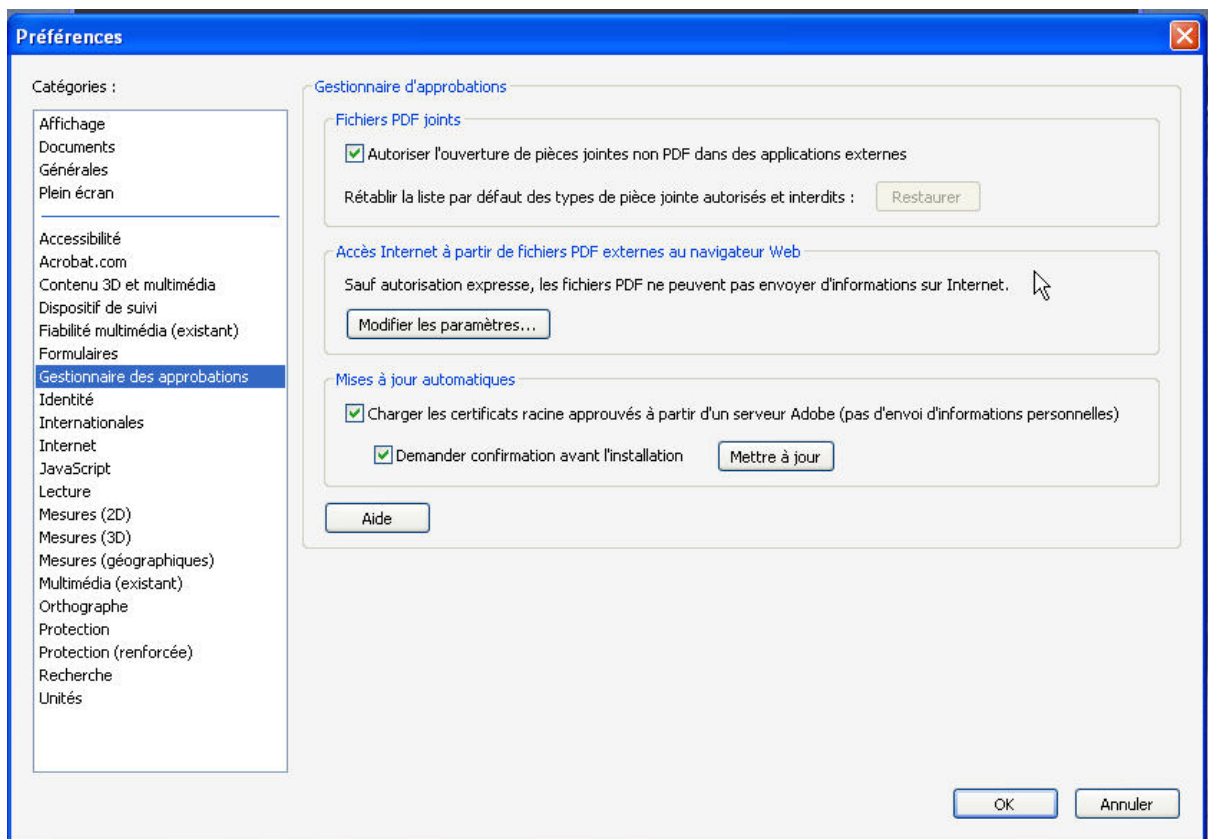


Si le message ci-dessous avec un triangle jaune apparaît l'installation est correcte mais votre logiciel Adobe n'est pas à jour.



Pour que la validation de votre signature soit automatiquement réalisée par Adobe Reader vous devez utiliser un logiciel Adobe Reader 9 ou X Uniquement et avoir accepté la mise à jour des certificats de confiance distribué par la société ADOBE lors de l'installation.

Vous pouvez mettre à jour cette liste simplement en allant dans l'onglet du panel Edition /Préférences/gestionnaire des approbations :



Dans la zone mise à jour automatiques cliquez sur mettre à jour. Vous pouvez fermer puis rouvrir le document avec adobe Reader 9 ou X.



4 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 votre AED.

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 publication la liste de révocation (Révocation effective au plus tard 24 heures après la demande).

La révocation d'un certificat n'a aucun impact sur les documents signés préalablement dont la signature reste valide **si le logiciel de signature** a mis en œuvre le procédé d'auto portance et d'horodatage (La liste des produits assurant cette fonctionnalité est disponible auprès de KEYNECTIS).

Deux procédures de révocation sont mises à votre disposition :

Procédure 1: Appelez ou envoyez un email à votre AED 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/K-SIGN/KEYNECTIS-KSIGN/ICS-KSIGNRGS2-PRO:>

Attention à bien ressaisir l'adresse URL qui se termine par :

5 SUPPORT A L'INSTALLATION

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/signature_electronique/faq

En cas de problème d'installation n'hésitez pas à consultez votre fournisseur de la clef K.Sign®.



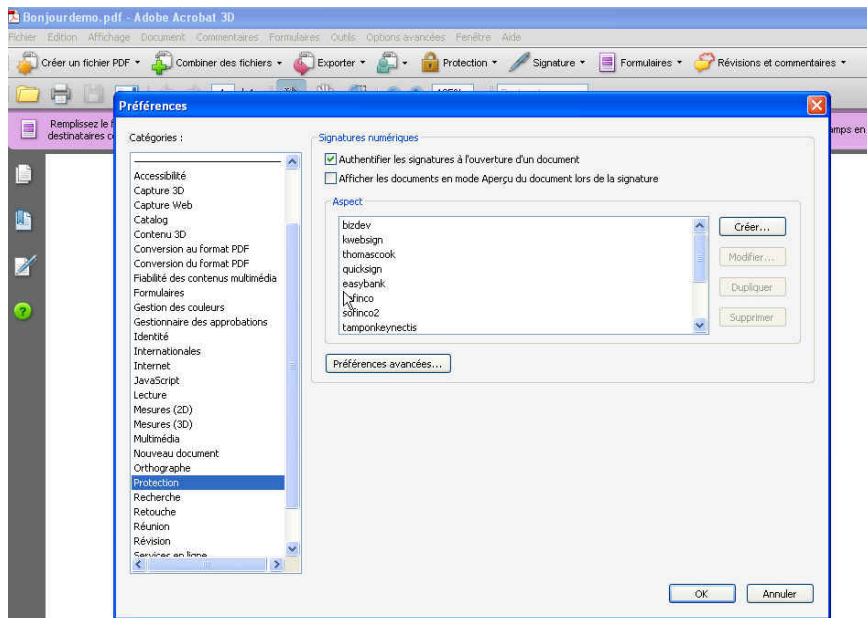
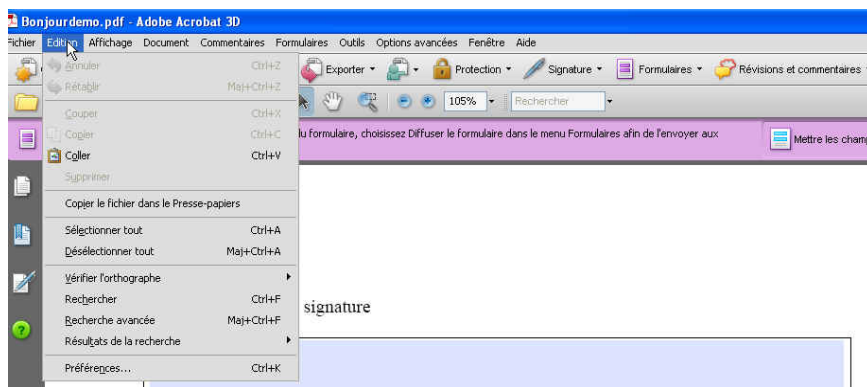
6 ANNEXE

6.1 Paramétrage d'une signature électronique dans ADOBE READER 9

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

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





6.2 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.





6.3 Modifier les contrôles des documents avant signature

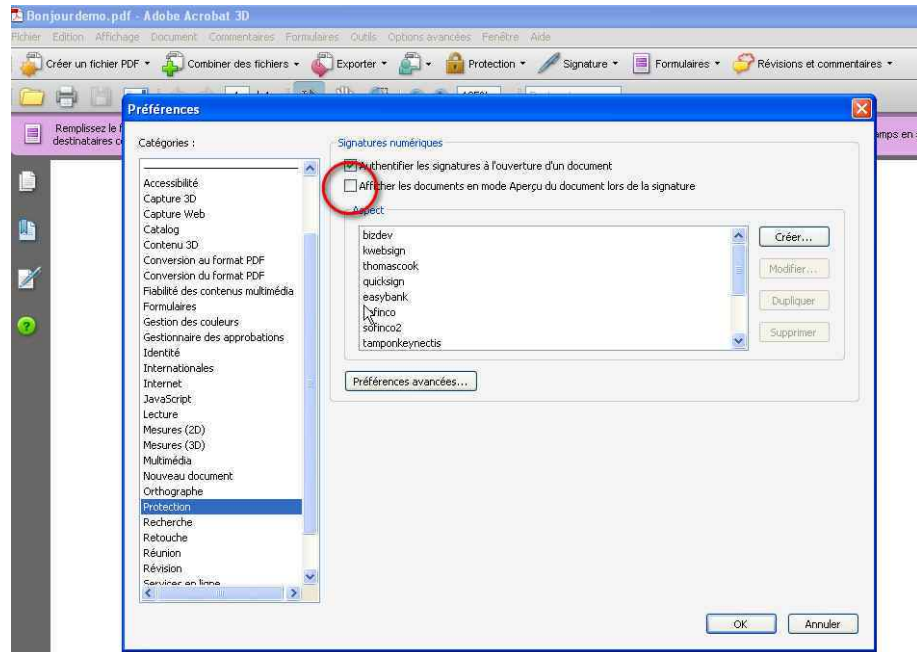
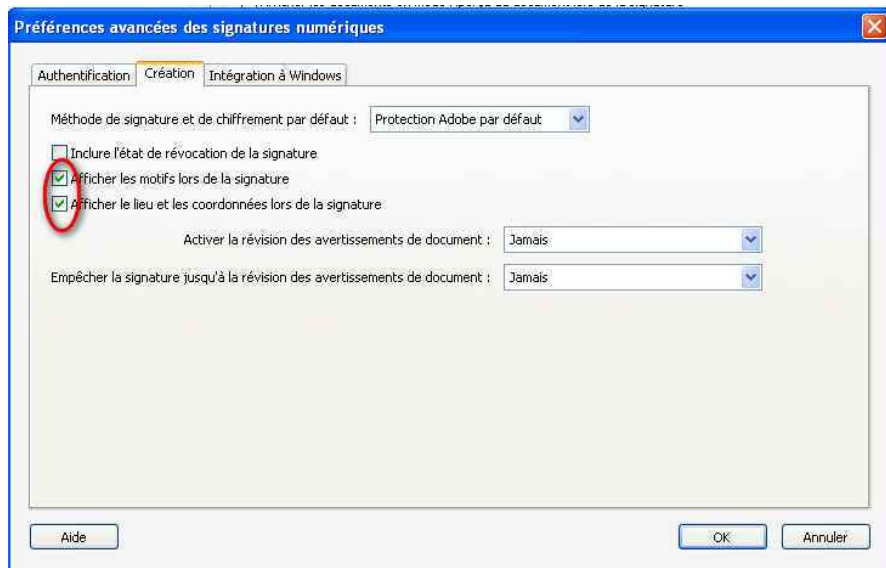


Figure 1: Personnaliser sa signature avec les produits Adobe Avant apposition de votre signature les produits peuvent réaliser un contrôle du type /A (Archivable) /Q Archivable avec données modifiables. Cette option est activable par la case à cocher entourée dans le panel ci-dessus (Afficher les documents en mode aperçu lors de la signature)

6.4 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 :



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 re fermer le logiciel Adobe utilisé vous n'aurez pas à ressaisir le code Pin à chaque signature

6.4.1 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:



Cette image est réalisée sous Acrobat R8, elle peut être légèrement différente dans les autres versions des logiciels Adobe

6.5 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/>.