



# INSTALLATION



K.SIGN® for PDF

INSTALLATION environnement Windows®

Auteur : Dominique Manenc

Date : 01/04/2010



Protecteur d'identité  
Protecteur de liberté  
dans un monde connecté





## **K.SIGN INSTALLATION ENVIRONNEMENT WINDOWS®**

<b>Version du document :</b>	2.1	<b>Nombre total de pages :</b>	16
<b>Statut du document :</b>	<input type="checkbox"/> Projet	<input checked="" type="checkbox"/> Version finale	
<b>Rédacteur du document :</b>		KEYNECTIS	

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

<b>Historique du document :</b>				
Date	Version	Rédacteur	Commentaires	Vérfié par
24/03/2010	2.0	DM	Mise à jour AE Déléguée	KEYNECTIS
29/03/2010	2.1	DM	Charte graphique	KEYNECTIS

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



## CONTENTS

<b>1</b>	<b>Presentation of K.Sign®</b>	<b>4</b>
1.1	Description .....	4
1.2	Usage and signature type .....	4
<b>2</b>	<b>prior to installation</b>	<b>5</b>
2.1	Software and hardware pre-requisites .....	5
2.2	Microsoft Vista® users .....	6
<b>3</b>	<b>Installing K.sign® on my PC with Microsoft windows</b>	<b>7</b>
3.1	Step 1 Cecheck received elements .....	7
3.2	Step2 Installing GEMALTO Classic Client driver .....	8
3.3	Step 2 Modifying the PIN code .....	8
3.4	Step 4 Acknowledging receipt and verifying installation .....	8
3.5	Using K.Sign® with multiple certificates .....	11
<b>4</b>	<b>configuring a digital signature</b>	<b>11</b>
4.1	Modifying the appearance of your signature in documents .....	12
4.2	Modifying pre-signature document controls .....	14
4.3	Enabling reasons and location parameters when signing .....	14
<b>5</b>	<b>revoking a certificate</b>	<b>15</b>
<b>6</b>	<b>installation Support</b>	<b>16</b>
6.1	KEYNECTIS customer service .....	16
6.2	Frequently asked questions .....	16
6.3	Bibliography .....	16



## 1 PRESENTATION OF K.SIGN®

### 1.1 Description

You have just received a K.Sign® key allowing you to use the Adobe Systems Incorporated (Adobe) document signing technology called Certified Document Services (CDS).

This turnkey solution provides all the necessary components enabling a private individual or legal entity to produce a legally binding signature.

K.Sign® for PDF offers:

1. **A means of digitally identifying signatures** using an X509 certificate, universally recognized by the full range of Adobe products.
2. **A digital signature tool**, in the form of a cryptographic USB token, that can be used to create certification signatures (Adobe Acrobat®) and approval signatures (Adobe Reader® extension).
3. **Compatibility with Adobe Reader® V7+**, available on all environments (Microsoft Windows, Linux, Apple Macintosh) and in all languages, for signature verification.
4. **A long-term archiving format**, because it combines a signing tool with time stamping (TSP RFC3161) and OCSP (Online Certificate Status Protocol) certificate verification services provided by KEYNECTIS (creation – in a way that is totally transparent for users – of a signed, “self-contained” PDF document with integrity and non-repudiation functions that are unalterable over time).

### 1.2 Usage and signature type

PDF is an ISO format that offers the advantage of being accessible by all computers currently on the market. The PDF format also owes its success to the fact that it enables documents to be preserved and used in the long-term, thus reducing the need for paper documents.

In order to adapt to new needs resulting from the use of the Internet and paperless business procedures, Adobe has integrated digital signatures within the PDF format itself, thus providing an electronic document that offers:

- The same legal value as a paper document
- The same ease of use as a signed paper document (the signature and its verification cannot be dissociated).

Meaning of verification and validity codes generated by Adobe tools currently on the market

Valid Approval  
Signature



Valid Certification  
Signature



The validity of the document is unknown.  
The author could not be verified.




Invalid  
signature






With K.Sign®, you can sign all of your PDF documents using the two types of signature available from Adobe:

Certification signature, symbolized by the “Blue Ribbon” .

- Applicable in visible mode (displaying an icon) or invisible mode. Generates an information bar about the document’s signature when the document is opened.
- Used by a document’s author to guarantee document integrity, this signature is the first to be applied to documents requiring multiple approval signatures.
- The certification signature is only applied with Adobe Acrobat (V 7+).

Approval signature, symbolized by the pen .

- Applicable in visible mode (displaying an icon) or invisible mode. Does not generate an information bar (except for V9.0).
- Used to sign forms with specific signature fields, native PDF documents (manual positioning of signature field) and documents requiring multiple signatures, this signature guarantees the integrity of fields modified by the signer in a form.
- The approval signature is applicable with Adobe Reader® (document with Reader Extension function) and with Adobe Acrobat® (V 7+).

## 2 PRIOR TO INSTALLATION

### 2.1 Software and hardware pre-requisites

#### 2.1.1 Software required to use K.Sign® with Adobe Acrobat Reader®

You can sign PDF documents (documents and forms with Reader Extension function) using Adobe Acrobat Reader® software. You will find the list of the technical pre-requisites for installation on the following website:

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

#### 2.1.2 Software required to use K.Sign® with Adobe Acrobat®

You can sign PDF documents (documents and forms) with Adobe software products from the Acrobat® range (Acrobat Standard Edition, Acrobat PRO Edition, Acrobat 3D Edition starting from Version 7). You will find the list of the technical pre-requisites for installation on the following website:

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

#### 2.1.3 Hardware and software required to install the Gemalto USB token

In order to use the GEMALTO USB token, you must install a driver on your operating system (Microsoft Windows, Apple Macintosh or LINUX) so it will recognize the token. You will find the list of the technical pre-requisites for installation on the following website:

<http://www.keynectis.com/en/digital-signature/technical-features.html>

The USB token is composed of a cryptographic card, such as the TPC IM CC card, installed in a USB driver referenced as “USB Shell TOKEN” by GEMALTO. It was delivered to you with an installation CD or documentation enabling you to download the middleware required when using it with digital signatures.

To install the GEMALTO Classic Client component, you must have administration rights on the computer.



### 2.1.4 Hardware

Each individual compatible PC must have at least the following:

- 50 MB of available drive space
- A Pentium II 200 MHz or equivalent processor
- A VGA graphics card supporting at least 256 colors

### 2.1.5 Operating system

GEMALTO Classic Client is available in two versions: one for 64-bit Operating Systems and one for 32-bit Operating Systems. You may use the table below to determine which version is appropriate for your OS.

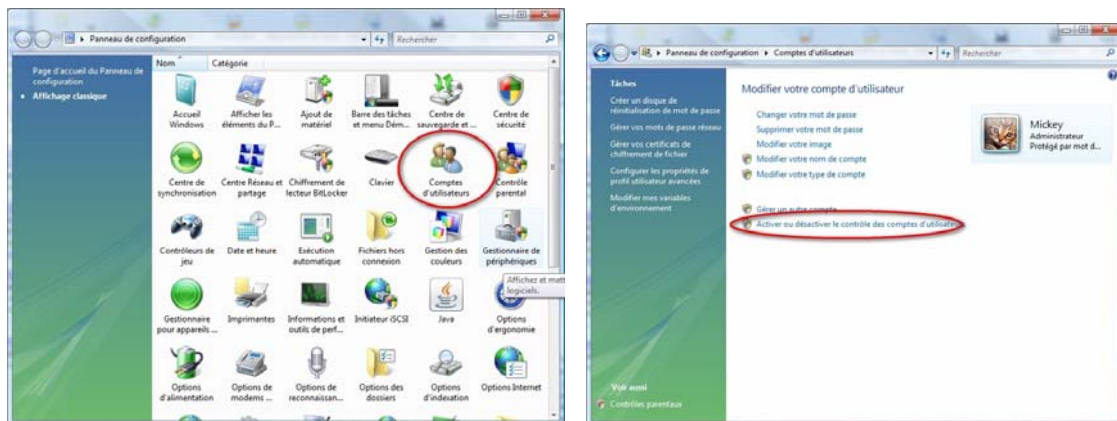
Operating System	Bits
Microsoft Windows 2000 Professional (with SP4)	32
Microsoft Windows XP Home (up to SP2)	32
Microsoft Windows XP Professional (up to SP2)	32 and 64
Microsoft Windows Server 2000	32
Microsoft Windows Server 2003	32 and 64
Microsoft Windows Vista	32 and 64

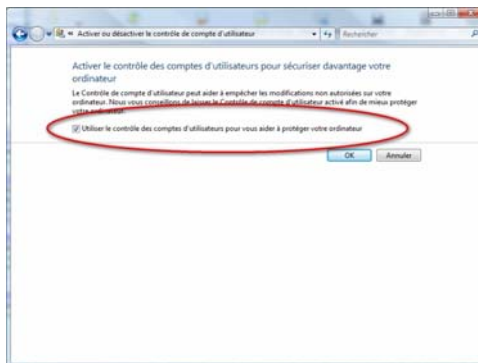
### 2.1.6 Compatibility with other usages

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

## 2.2 Microsoft Vista® users

Any problems encountered while installing GEMALTO Classic Client in your Microsoft Vista environment can probably be resolved by modifying the UAC (User Account Control) in the Microsoft Vista configuration panel.





Once the middleware has been installed, remember to reset the UAC to its initial position.

### 3 INSTALLING K.SIGN® ON MY PC WITH MICROSOFT WINDOWS

#### 3.1 Step 1 Cecheck received elements

You have received the following information through two different channels:

- Your K.Sign® key
- Your confidential PIN mailer.
- An email from KEYNECTIS customer service informing you that your request has been validated and providing list of master URL and revocation code if necessary.

Dear Customer

Your request for K.Sign certificate has been validated by Service Clients de KEYNECTIS :

Common Name: .

Email :

Organisation :

Department :

Title :

City :

State :

Country:

Revocation code : xxxxxx.

You can download and save the installation kit for your USB KEYB now at the following URI:

<http://www.keynectis.com/en/support-information.html> and

At the end of tinstallation,please download the Acceptance PDF forms at the following URI :

<http://www.keynectis.com/static/content/common/ksign/MOD KSign Agreement for delivery GB s.p df>

Then sign it with your K.Sign and email it as attachment file to : [service.clients@keynectis.com](mailto:service.clients@keynectis.com)



If you have not received all 3 elements, email to service clients de KEYNECTIS:

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

### 3.2 Step2 Installing GEMALTO Classic Client driver

Download the installation kit available on the KEYNECTIS website:

<http://www.keynectis.com/en/digital-signature/technical-features.html>

Select the 32- or 64-bit kit based on your OS and save it on your computer.

Unless your computer is already equipped with a smartcard drive, expand the .zip file and use the automatic installation function by double-clicking the Classic\_Client\_User\_setup.msi file.

After rebooting your PC and inserting the K.Sign® USB key, your environment should automatically recognize the key (new component installation) and the green light should be permanently illuminated on the USB token. Using Gemalto toolbox program provides you access to Key management functions..

### 3.3 Step 2 Modifying the PIN code

The K.Sign® key attributed to you does not contain any certificates and was initialized with a PIN code provided in the confidential mailer you received. It is important that you initialize the PIN code prior to generating your key pairs and to downloading the related signature certificate.

The K.Sign® key has been personally attributed to you. It is your responsibility to protect it using two



About using the K.Sign® key as a security container: the K.Sign® key can be used to store other certificates to enable secure portability. For further information, please see the section on certificate import functions described in Chapter 4 (User Tasks, Managing Certificates) of the document entitled [Classic\\_Client\\_User\\_Guide.pdf](#).

### 3.4 Step 3 Acknowledging receipt and verifying installation

To ensure your K.Sign® key has been properly installed, you must digitally sign the K.Sign® acceptance document and return it by email to: [service.clients@keynectis.fr](mailto:service.clients@keynectis.fr).

Download the PDF entitled AcceptationKsign.pdf from the following address:

<http://www.keynectis.com/en/support-information.html>

Then digitally sign the document using one of the following software products:

- Acrobat® Standard or Pro Release 8 or Release 9



- Adobe Reader® Release 8 or Release 9

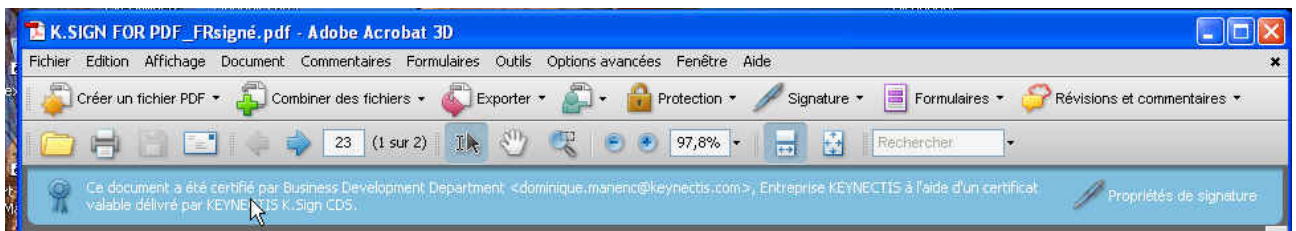
### **Important:**

If your computer is equipped with Version 7 of any of these products, please contact [service.clients@keynectis.fr](mailto:service.clients@keynectis.fr) to receive a patch enabling your signatures to support the time stamping function.

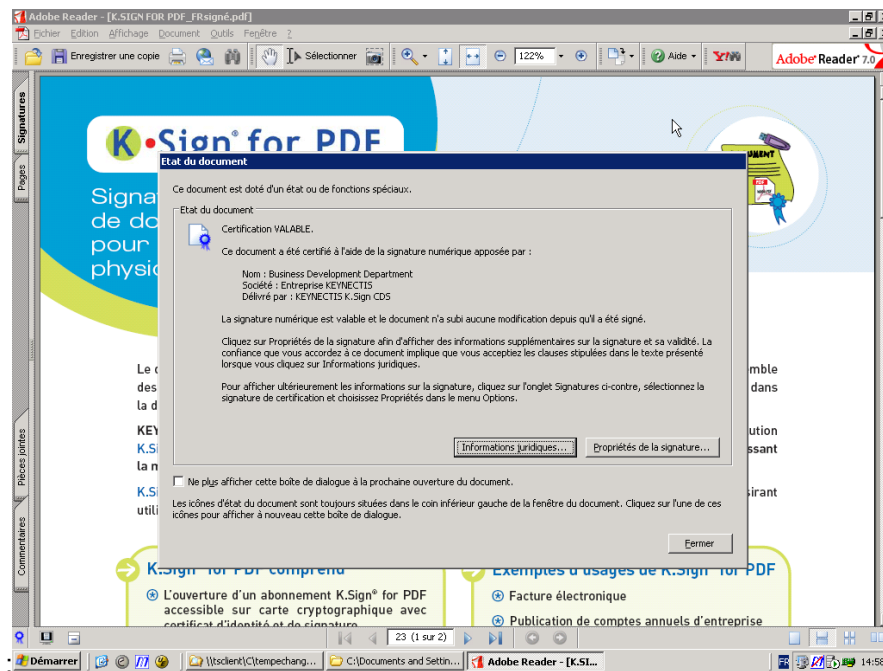
If your computer is not equipped with any of these products, you can download Adobe Reader® 8 or 9 free of charge from the following address: <http://www.adobe.com/fr/products/reader/>.

### **3.4.1 Signature verification on your computer**

After opening the document, the following validation banner will be displayed (R8 and R9):

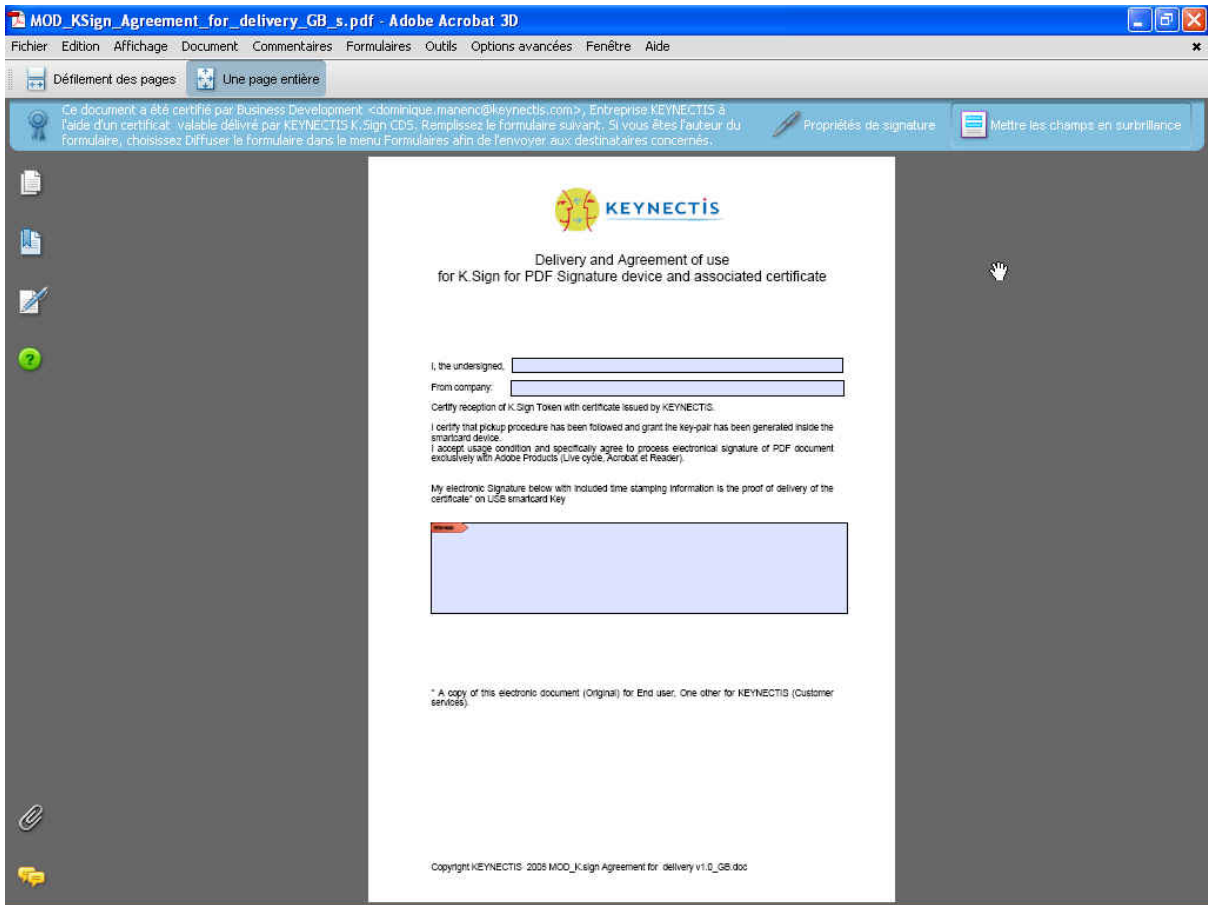


For Version 7, the following document status window will be displayed

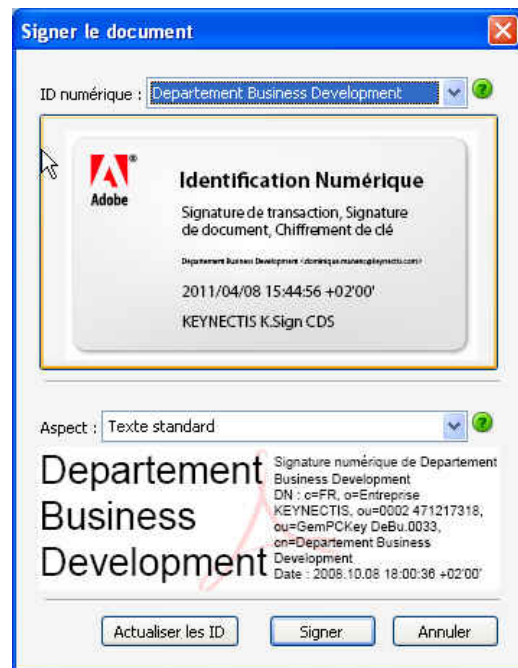


### **3.4.2 Signing the acceptance document**

1) After verifying the certification signature information and completing the fields to identify you, click the signature field.



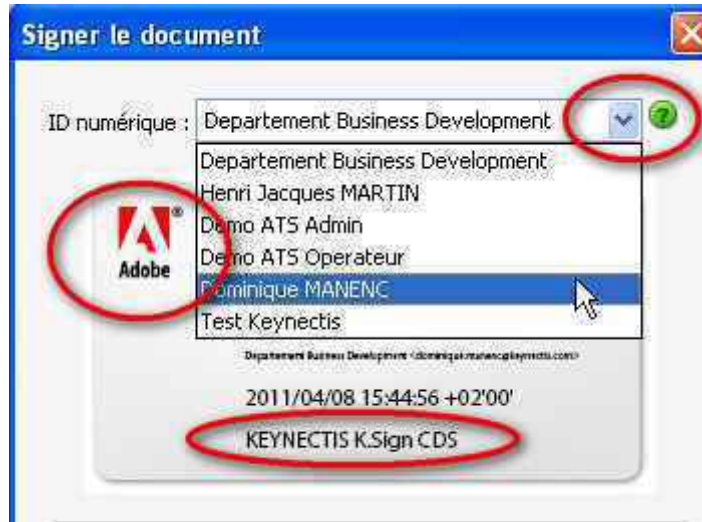
2) One of the following windows will appear:





### 3.5 Using K.Sign® with multiple certificates

When your computer contains several certificates, Adobe might propose a certificate other than the K.Sign® certificate. To make sure you are signing the right certificate, you should see the following information when you select the certificate from the list box:



3) Make sure the digital ID matches the K.Sign® certificate. This means that:

- the Adobe logo is displayed in the upper part of the frame
- the KEYNECTIS K.Sign® CDS label is displayed as above

If these items are not displayed, select the digital ID in the Digital ID window as indicated above.

Then click the “Sign” button.

4) Save the file in the directory of your choice.

5) Enter the PIN code of your K.Sign® key.

6) Email the signed PDF to [service.clients@keynectis.com](mailto:service.clients@keynectis.com)

## 4 CONFIGURING A DIGITAL SIGNATURE

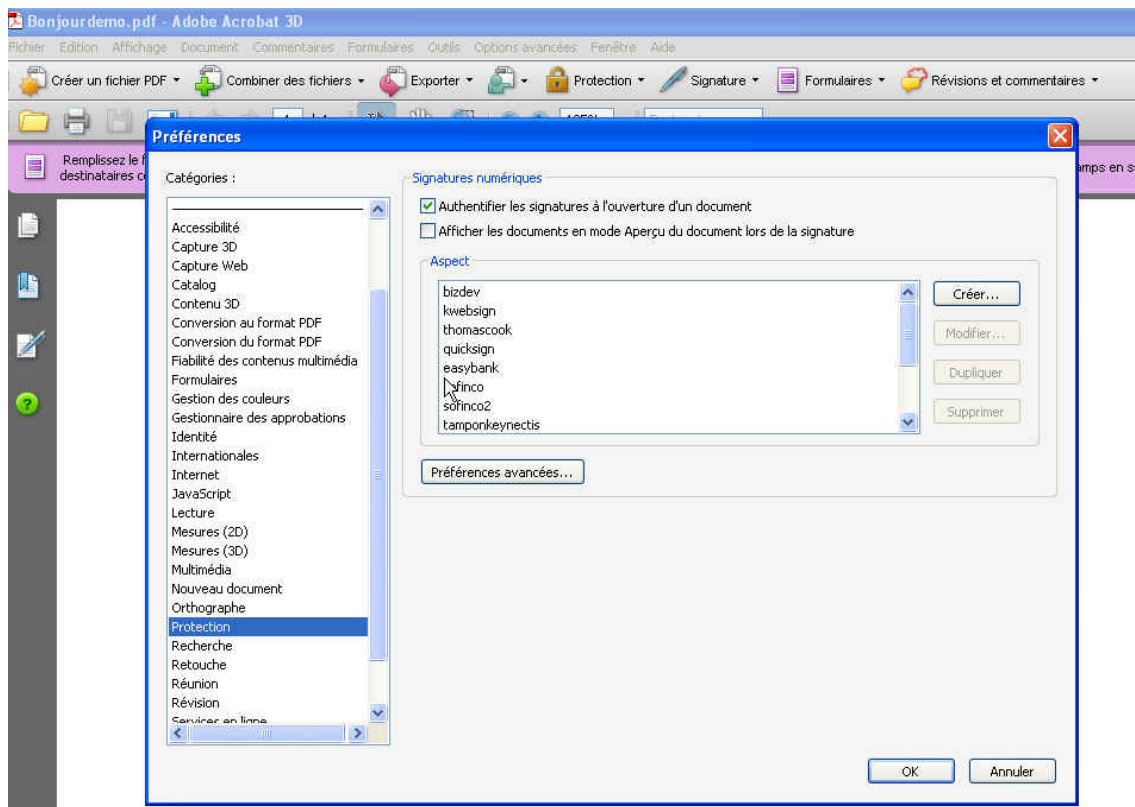
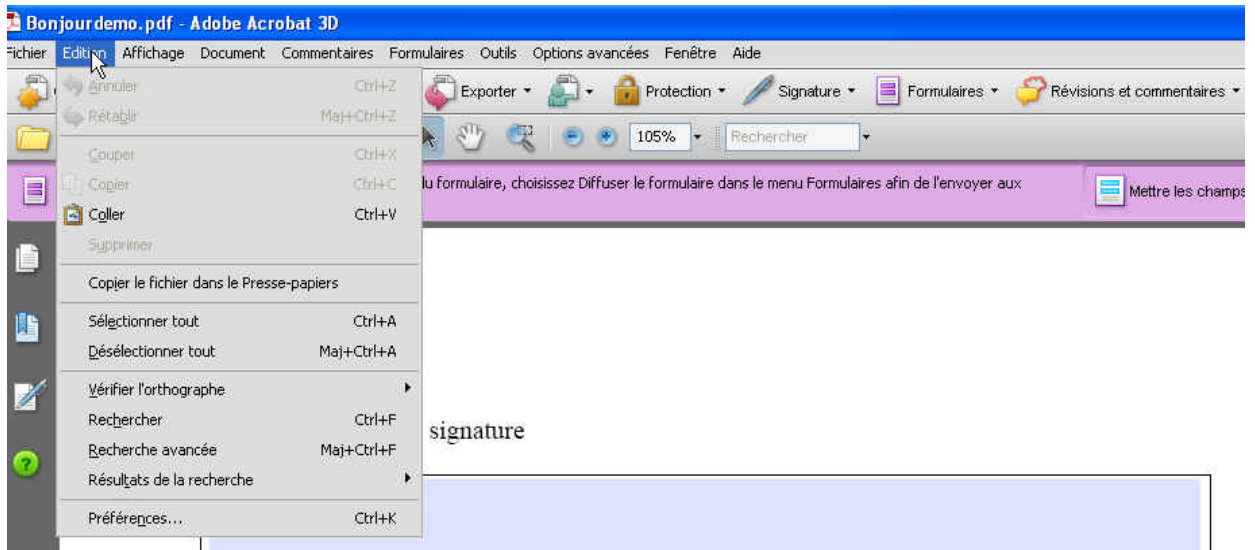
You can sign your documents from your computer using ADOBE Acrobat® or ADOBE Reader® (if the PDF has Reader Extension modification rights).

Adobe products can be configured to allow you to modify the appearance of your signature in the PDF documents you wish to sign.

A video on how to produce a signature with these products can be viewed at the following address:

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

The parameters can be accessed from the Edit/Preferences/Protection menu:



#### 4.1 Modifying the appearance of your signature in documents

You can modify the appearance of your digital signature in your documents (for visible signatures only). To do so, use the “Create” button shown in the window above.

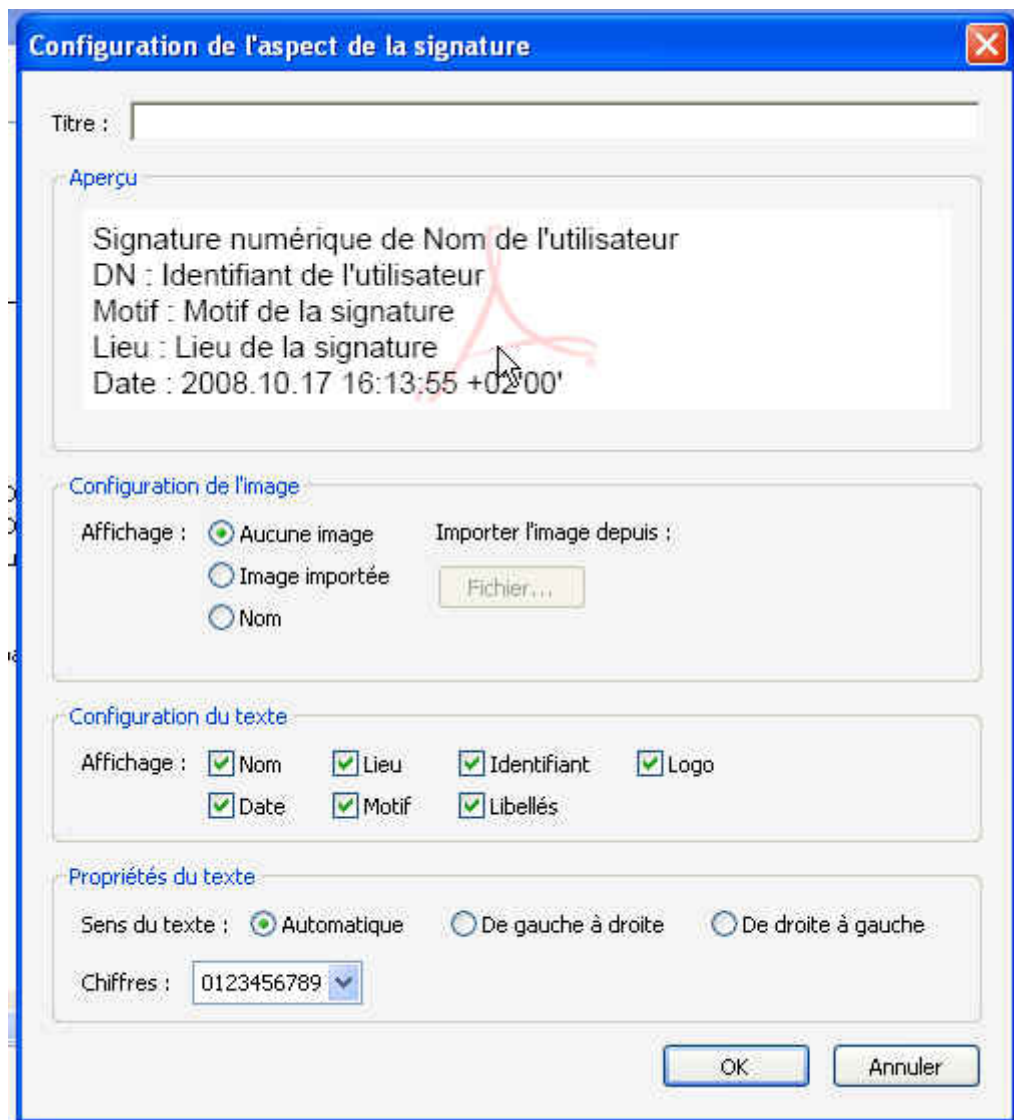


You can create as many different signatures as you wish by saving each signature under a different name. They can then be modified/deleted using the options in this window.

This window is dynamically modified each time you modify a checkbox.

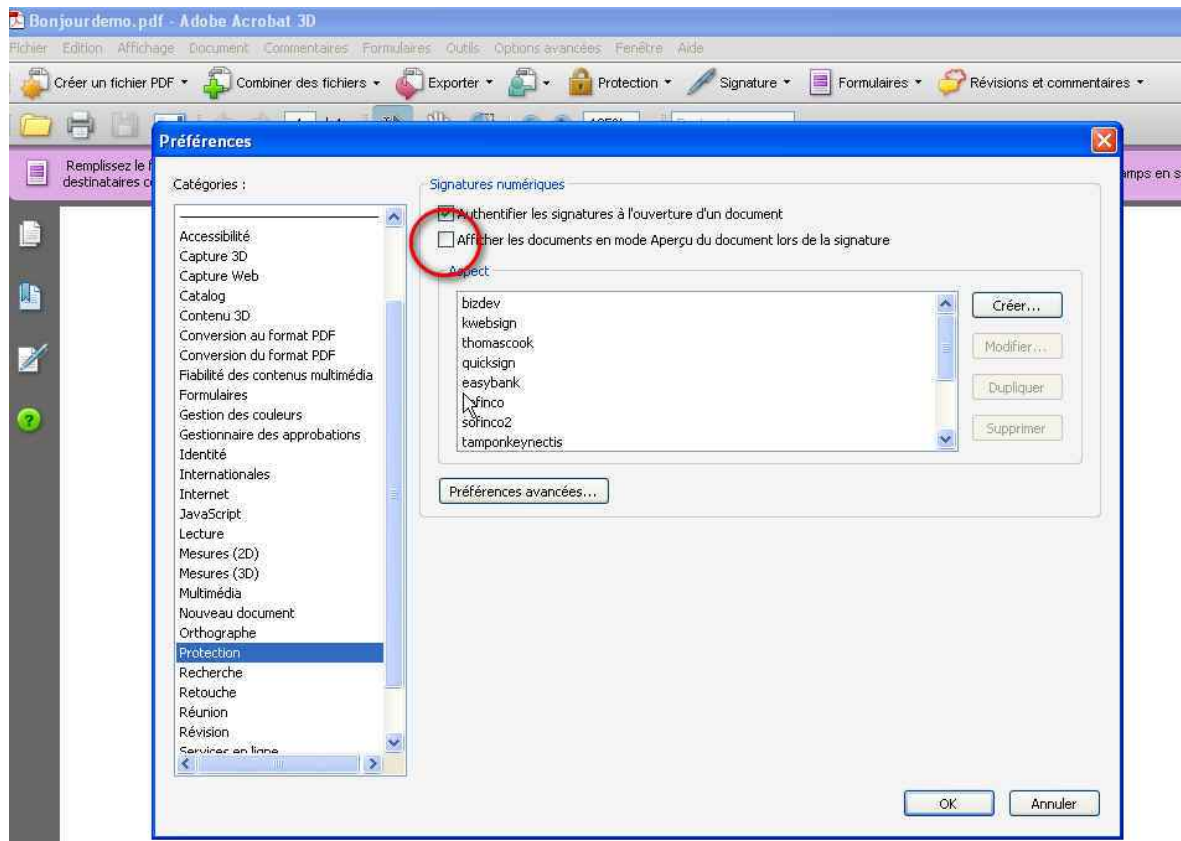
When you have obtained the desired signature, complete the title field and click OK. The software will save your signature and allow you to modify it at any time.

Important: If you want to insert a LOGO into your signature, you must provide it in PDF format.





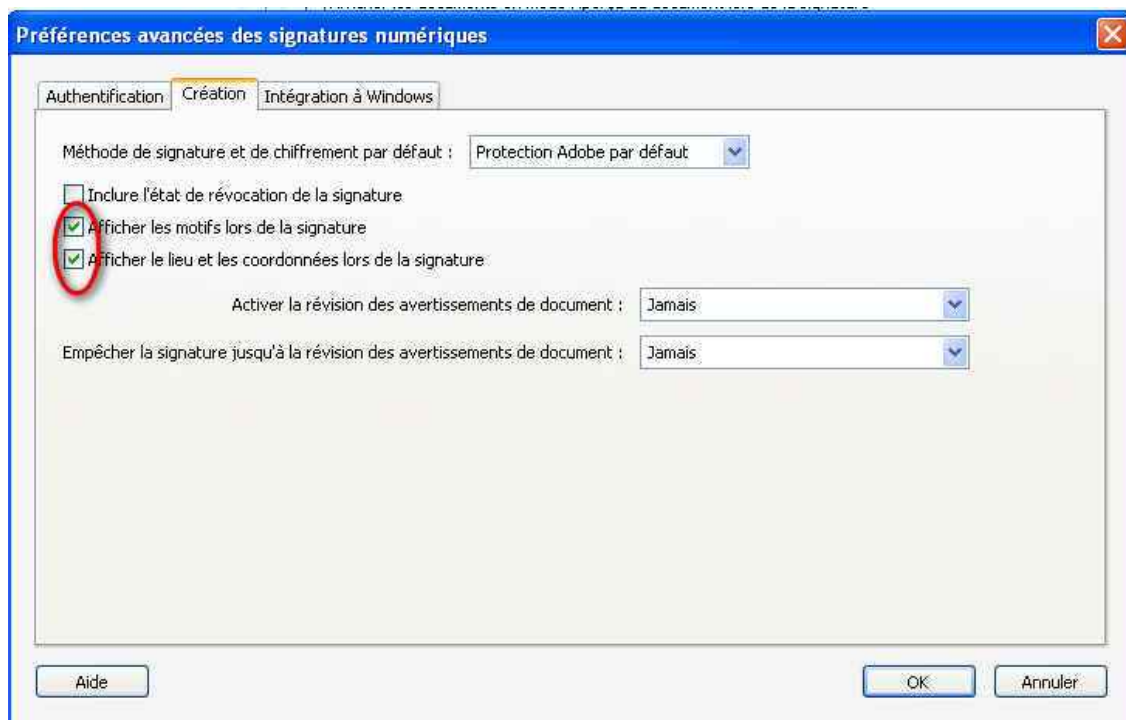
## 4.2 Modifying pre-signature document controls



Before applying your signature, the products can perform two types of control: type /A (Archivable) or type /Q (Archivable with modifiable data). This option can be activated using the checkbox circled in the window above (View documents in preview mode when signing).

## 4.3 Enabling reasons and location parameters when signing

If you would like optional information concerning your location and contact details to appear in your signature, use the “Advanced preferences” button (“Creation” tab) to select the two checkboxes as shown below:



## 5 REVOKING A CERTIFICATE

If, for various reasons (loss, theft, etc.) you are no longer in possession of your K.Sign key, you can request that it be revoked by KEYNECTIS.

Revoking a certificate prevents third parties from using it and from gaining access to your PIN code.

Revoking a certificate prohibits producing a signature with the certificate, starting from the revocation date.

Revoking a certificate has no impact on signatures previously signed with your K.Sign key, because signed documents are self-contained and time stamped.

You may choose from two revocation procedures:

**Procedure 1:** Call or send an email to KEYNECTIS customer service, which will revoke your certificate during the business hours indicated in the General Terms of Sale.

**Procedure 2:** Connect to the following URL, complete one of the fields in the form (Email) and enter the revocation code you chose (and saved) when you purchased your K.Sign key:

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



## 6 INSTALLATION SUPPORT

### 6.1 KEYNECTIS customer service

KEYNECTIS customer service can be reached as indicated on the KEYNECTIS website:

<http://www.keynectis.com/en/support-information.html>

### 6.2 Frequently asked questions

In addition to the information about using K.Sign® provided below, further technical information is available on the KEYNECTIS website: <http://www.keynectis.com/en/digital-signature/cds-faq.html>

Your Adobe software saves the most recent signature format used, meaning you do not have to complete all the fields each time you use your signature.

If you sign several documents without closing your Adobe application, you will not have to enter your PIN code each time you use your signature.

### 6.3 Bibliography

For further information about Adobe software products and the digital signature we use, please visit the Adobe website at the following address: <http://www.adobe.com/devnet/acrobat/security.html>.

For further information about the Gemalto USB keys and how they are used, please visit <http://support.gemalto.com/>.