Guide
Configuration of Adobe Reader for document Signature Validation

Document SIGNE_PAPET. Ver. 1.0
Date of application 14/01/2011

Seguridad documental

Table of contents

Introduction

This manual describes how to validate the signatures of documents in PDF format with Adobe Reader or Adobe Acrobat. Signatures can be validated manually or automatically, as described in the following sections of this document, but regardless of the method used, the Root CA certificate from Firmaprofesional and the Subordinate CA certificate from Signe must first be installed, and the application must then be configured to trust the root certificate of the signature certificate.

Install Root CA and subordinate CA Certificates

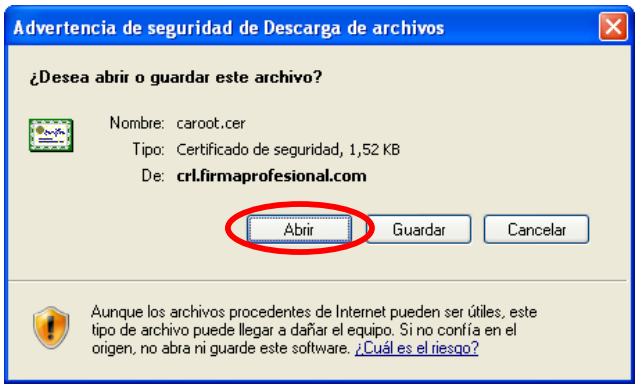
In order to properly verify the electronic signatures in PDF documents, you will need to register the root CA certificate (ROOT CA Firmaprofesional) and Signe's Subordinate CA certificate in your browser. These certificates are:

Firmaprofesional CA Root: http://crl.firmaprofesional.com/caroot.crt
Signe Subordinate CA: http://crl.firmaprofesional.com/signe.crt

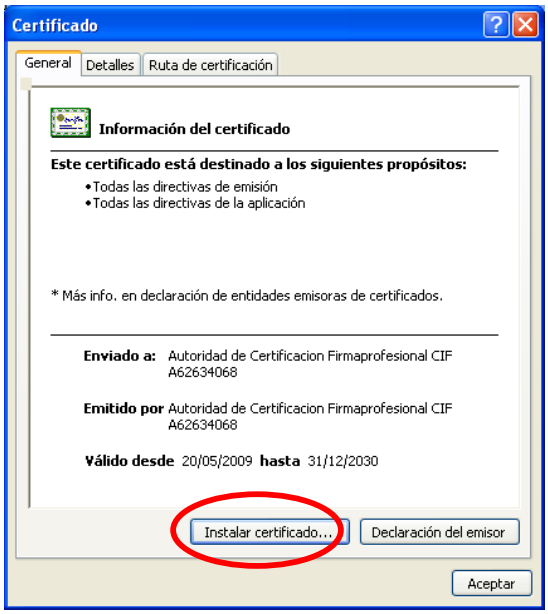
Although the installation process described here has been prepared for Internet Explorer, it may also be used as a guide for other browsers.

1. Click the link "Certificado AC RAIZ Firmaprofesional", which is located at http://crl.firmaprofesional.com/caroot.crt.

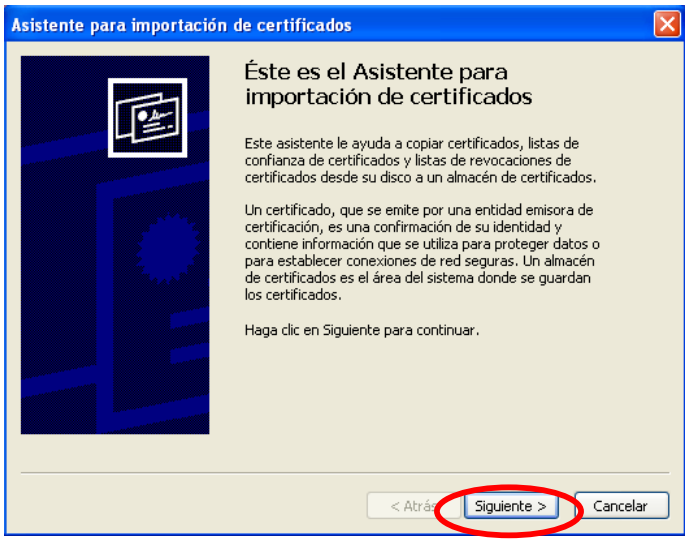
2. A window like the one shown below will open and ask you if you would like to open the file or save it to your computer. Click "Open".



3. A window with the certificate information will then be displayed. Select the "General" tab and click the "Install certificate..." button



4. A new window will open with the “Certificate Import Wizard”. Click Next in this step and the one that follows, and then the Finish button. A message will then be displayed to indicate that the import process was completed successfully.



5. Click OK in the window that displays the certificate information to close it. .
6. Click on the link "Certificado AC Subordinada SIGNE”, which you will find at http://crl.firmaprofesional.com/signe.crt and repeat steps 2 to 5 to install this new certificate.

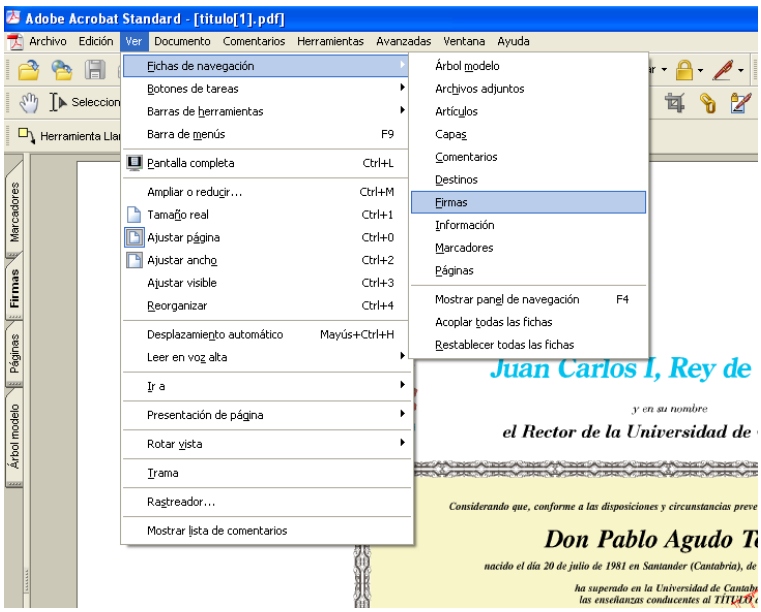
Configure adobe reader to trust the root certificate of the signature certificate

There are several ways to configure trusted identities in Adobe Reader and only one of the following methods needs to be used:

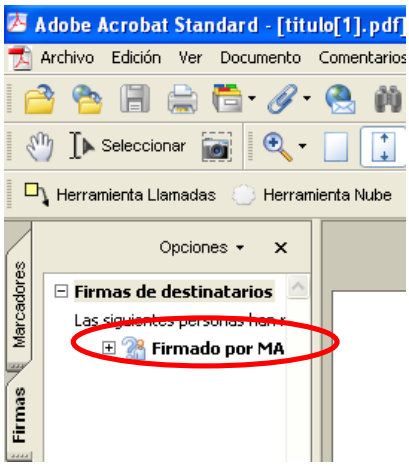
Method one: Trust the root certificate of the signature certificate.

When a signed PDF is opened for the first time, the root certificate of the signature certificate can be added to the trusted identities as follows:

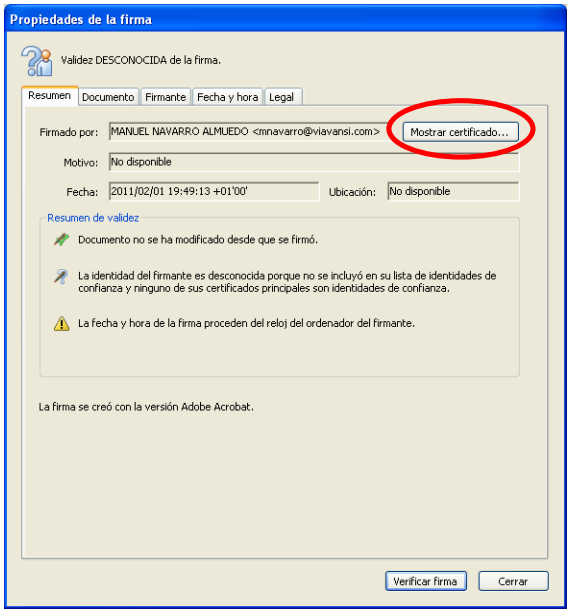
1. Open the document.
2. Select the signature tab, starting from the main menu, “View" > “Signature panel" > “Signatures", or select the “Signatures" tab that is displayed to the left of the document.



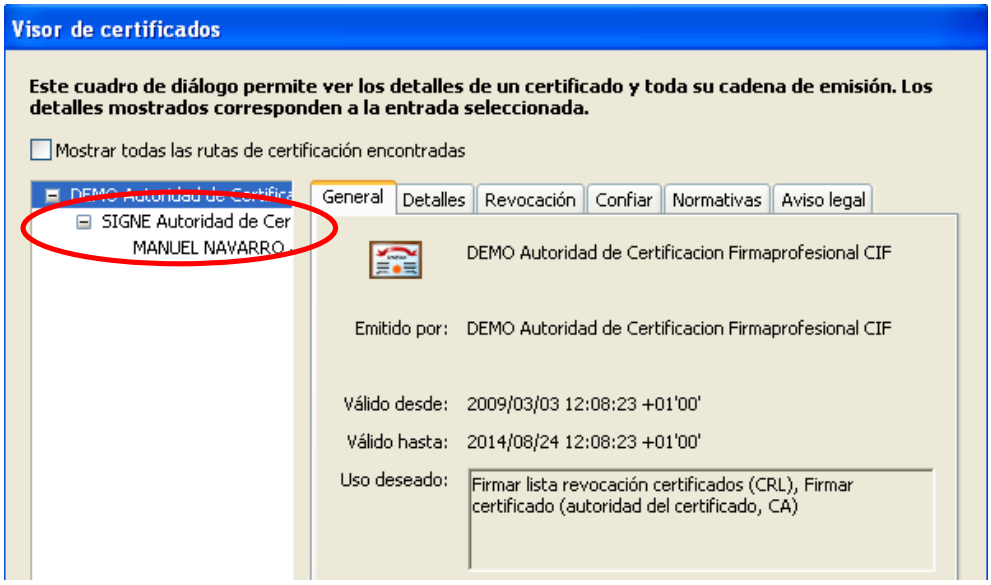
3. Select the signature (the icon  or a similar one will be displayed next to the signature to indicate that the signer's identity is unknown because it has not been included in the list of trusted identities and none of its parent certificates are trusted entities).



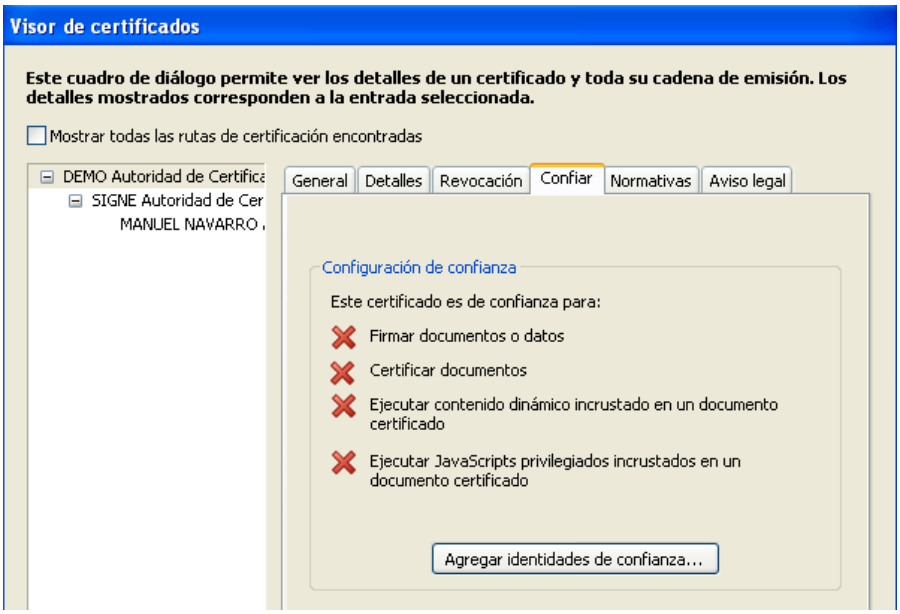
4. Select the signature and right-click and select "Properties" in the drop-down menu. The "Signature Properties" window will open. There are several tabs. Select the first one ("Summary") and click "Show Certificate".



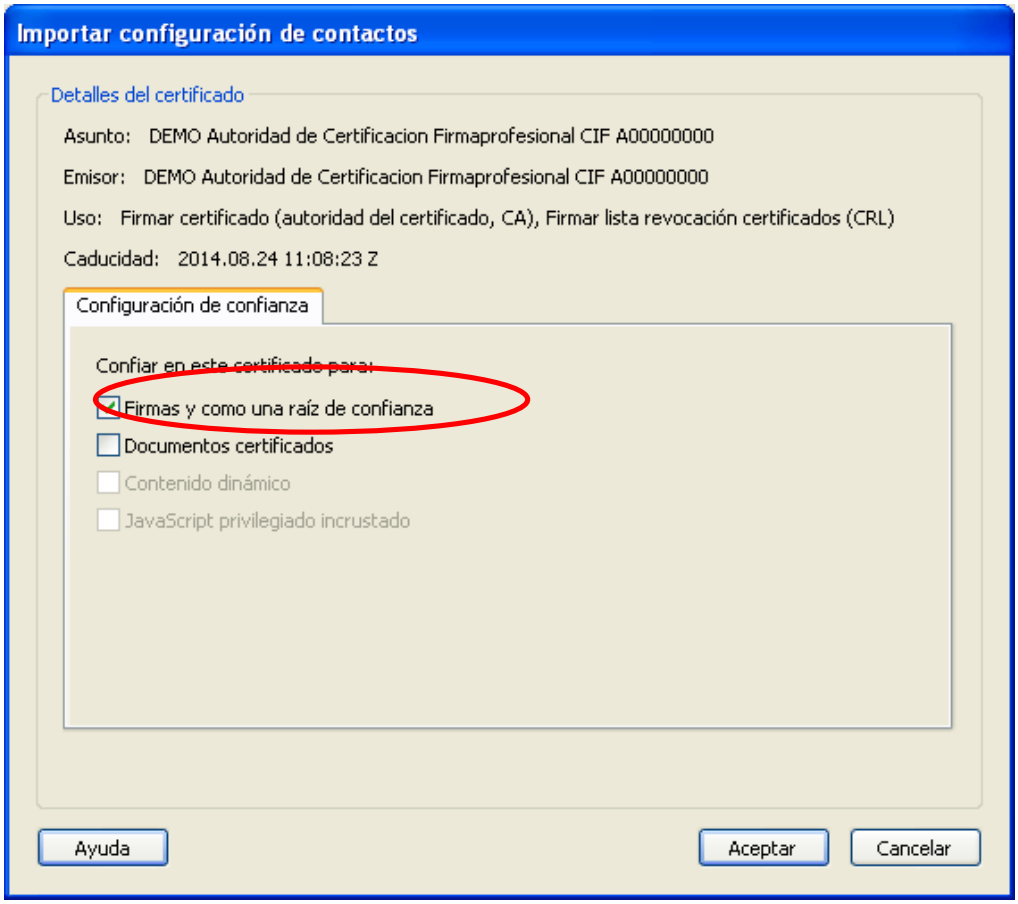
5. A Certificate Viewer window will open, displaying the list of certificates that make up the full certification path in the left panel. Select the root certificate (the first one in the hierarchy).



6. Select the tab “Trust” and click “Add to Trusted Identities”.



7. An import Contact Settings window will open. In The "Trust Settings" section mark the "Signatures and trusted root" box.

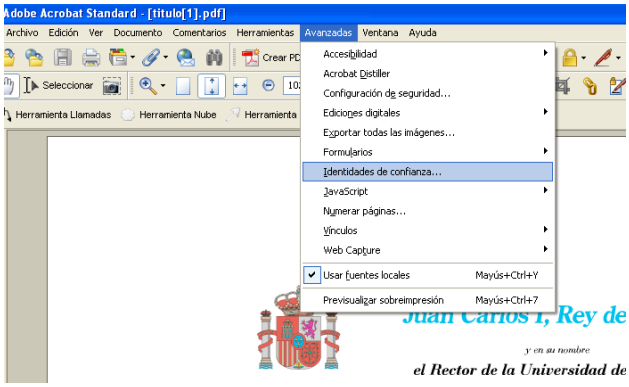


8. Click OK to close the “Import contact settings” window, and then OK in the “Certificate Viewer” window. After the root certificates of the signature certificate have been configured as trusted, click “Close” in the “Signature properties” window.

Method two: Trust the root certificate of the signature certificate

Add the root certificate of the signature certificate to the trusted identities using the Trusted identity manager in Adobe Reader, carrying out the following steps:

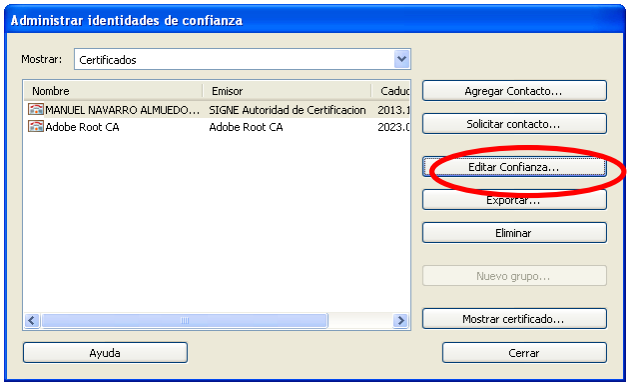
1. In the menu, select “Advanced" > “Trusted identities" if Adobe Acrobat is installed, or “Document" > “Manage trusted identities" if Adobe Reader is installed.



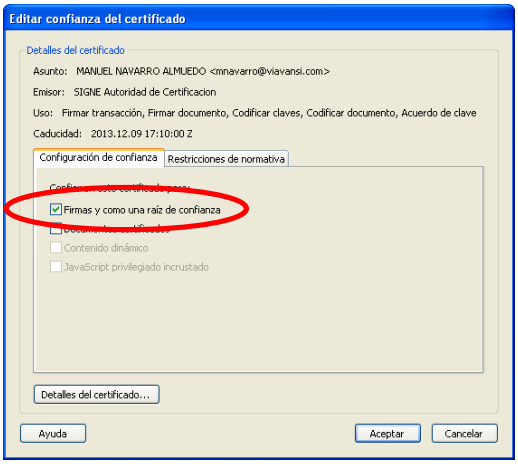
2. At the top of the window, the default option is “Contacts”. Change the selection to “Certificates”.

3. Select the root certificate from the list (if it is not in the list, use the method explained above)

4. With the root certificate selected, click “Edit trust”.



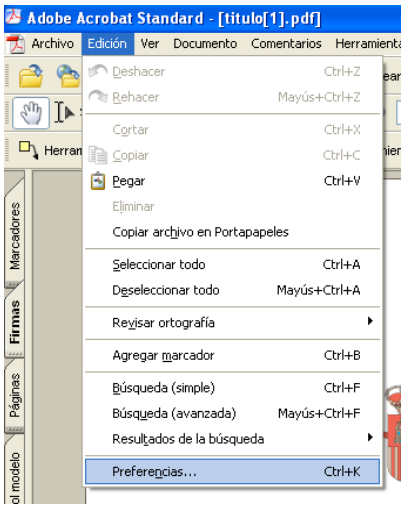
5. In the new window, “Edit certificate trust”, in the “Trust” section, click the “Use this certificate as trusted root” box.



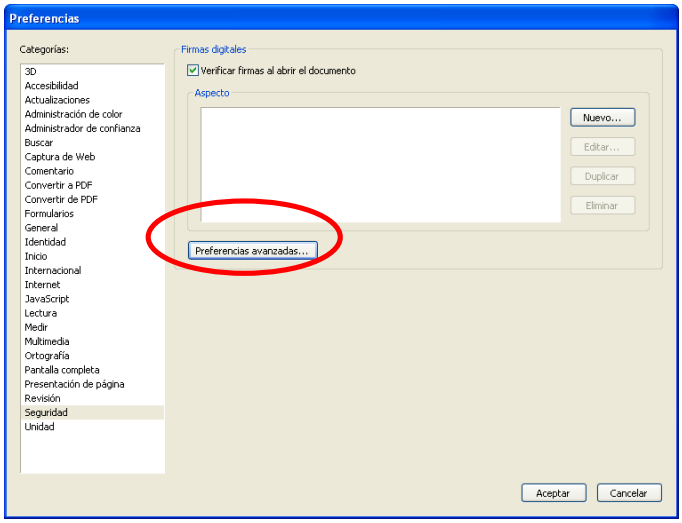
Method three

Method three can be used if the root certificate of the signature certificate and the root certificate of the certificate of the Timestamp Authority are registered in the Microsoft Windows certificate store. It consists of the following steps:

1. In the main menu, select “Edit" > “Preferences".



2. In the next window,select the “Security” option in the left panel.
3. Click “Advanced Preferences” to open the “Advanced preferences for digital certificates”



4. In the “Advanced preferences for digital signatures” select the “Windows Integration” tab and mark the options “Enable searching the Windows Certificate Store for certificates other than yours”, and “Validating Signatures” in the section “Trust ALL certificates in the Windows certificate store for the following options"

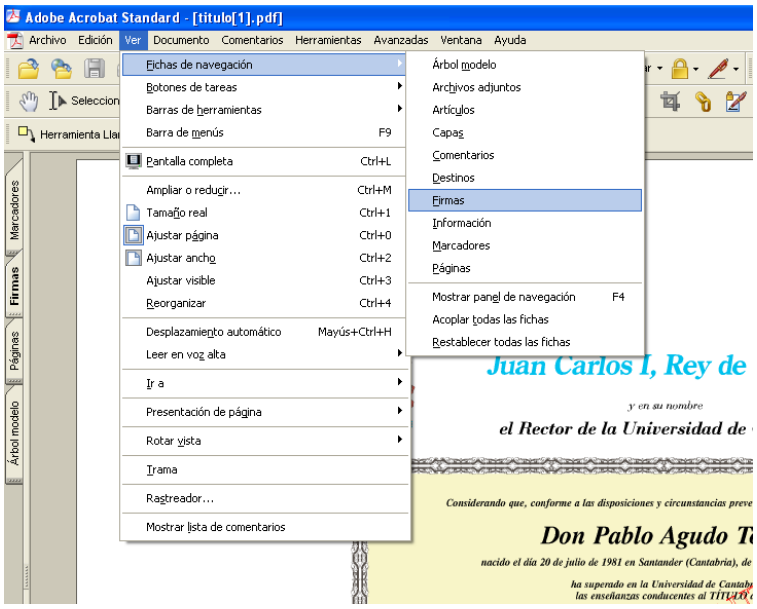
5. Click OK to save the changes and return to the “Preferences” window and then OK to close the window.

Validating digital signatures

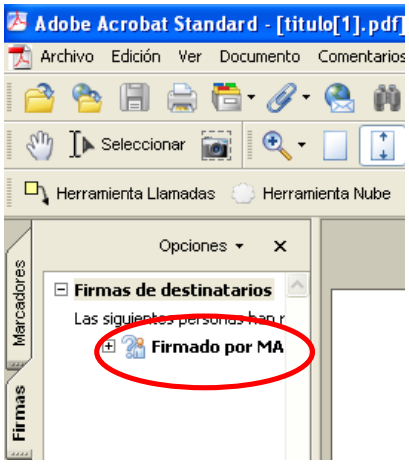
Manual validation

To manually validate a digital signature, follow the steps indicated below::

1. Open the document.
2. Select the signature tab, starting from the main menu, “View" > “Signature panel" > “Signatures", or select the “Signatures" tab that is displayed to the left of the document.



3. Select the signature (if it has not yet been validated, the icon , or a similar icon will be displayed next to the signature).

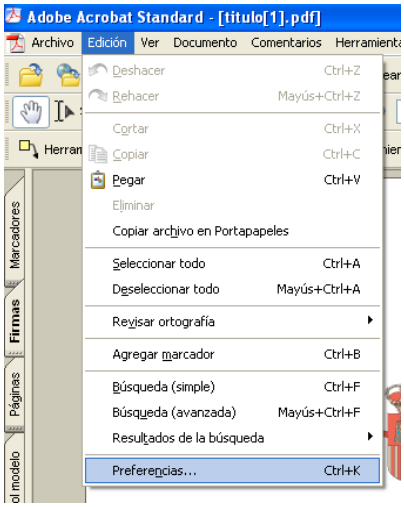


4. Select the signature and right-click and select “Validate signature”.
5. After the signature has been validated, if everything was successful, the icon or a similar one should be displayed next to the signature.

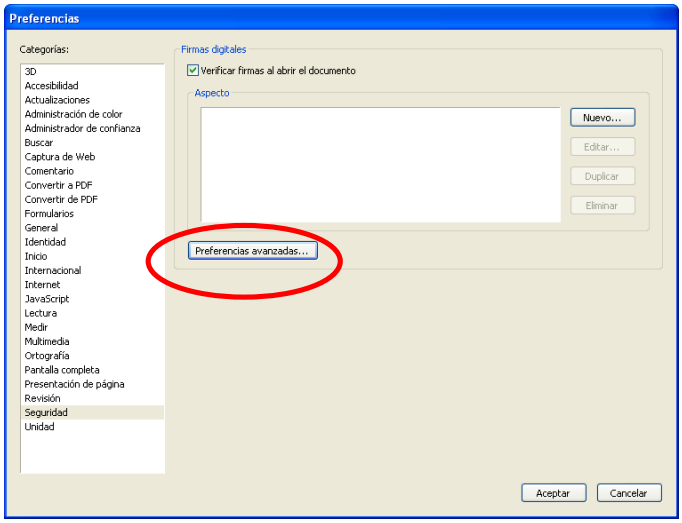
Automatic validation

The application can be configured to validate signatures in PDF documents automatically when they are opened, but keep in mind that this operation takes a bit of time every time the document is opened. To activate automatic validation, configure Adobe Reader’s digital signature preferences as follows:

1. Open the document.
2. In the main menu, select “Edit" > “Preferences".



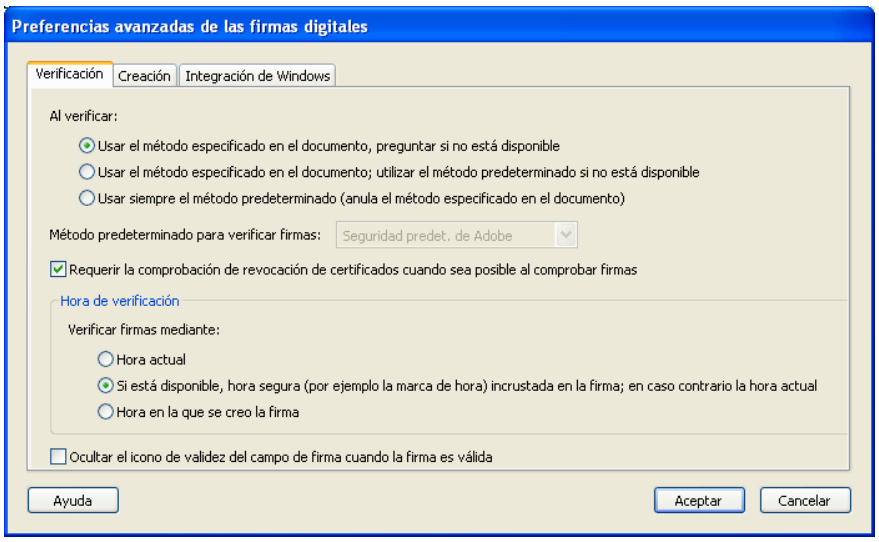
3. In the next window, select the “Security” option in the left panel.
4. Mark the option “Verify signatures when the document is opened”, if it is not already marked.
5. Click “Advanced Preferences” to open the “Advanced preferences for digital certificates”.



6. Select the “Verification” tab and in the “When verifying” option, mark “Use document-specified method. Prompt if it is not available”.

7. Mark the option “Require certificate revocation checking whenever possible during signature verification”.

8. In the “Verification time” box, select the option “Secure time (e.g. timestamp) embedded in the signature if available, current time otherwise”.

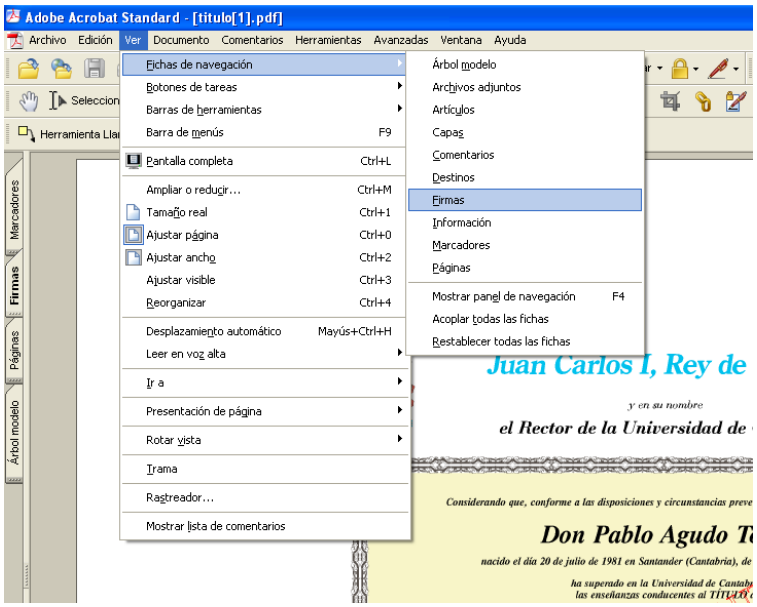


9. Click OK to close the “Advanced preferences of digital signatures window” and then OK again to close the “Preferences” window”.

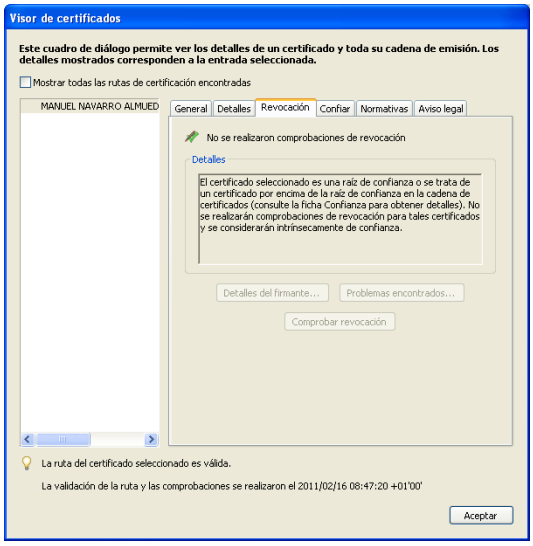
10. The signature will be validated automatically the next time the document is opened.

Verifying electronic signature validity

The validity of a digital signature can be verified starting from the main menu, “View" > “Signature panel" > “Signatures", or select the “Signatures" tab that is displayed to the left of the document. This tab shows a list of all of the document’s electronic signatures along with information on their validity.



To see the details for the signature and the validity of the certificate used to generate it, right-click on the signature and select the “Show Signature properties” in the drop-down menu. A window with several tabs will open. Select the first one (“Summary”) and click “Show Certificate”. A Certificate Viewer window will open. Select the “Revocation” tab. The “Details” tab will display information on the certificate’s revocation status.



Troubleshooting

The signature has the icon  **next to it.**
This normally occurs when the document is opened from a browser. In some cases, if the Adobe Reader application has been configured to validate signatures automatically, the document will have to be reloaded to allow the application to carry out the validation. If it is not configured for automatic verification, validate the signature manually (see the corresponding section of this document).

The icon  **appears next to the signature, rather than the icon** 
This problem is caused when Adobe Reader can't verify the signature. The possible causes and solutions are:

1. If the display properties of the certificate signature on the " Withdrawal " tab, a message is displayed saying that could not be verified because the root certificate is not a trusted entity , review the section "Setting Adobe Reader to trust the root certificate of the signing certificate and the certificate Authority Time Stamping " of this document.

2. In some setups that use proxies, the Adobe Reader settings may need to be changed to allow it to connect to the Internet. In the main menu, select "Edit" > "Preferences" > "Internet", and in the "Internet Options" section, click the "Internet Properties" button. In this case, contact the network administrator.

Una compañía de GRUPO signe

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
comercial@signe.es