

Using PGP TrustCenter's Digital Certificates with Adobe Acrobat v6 and Adobe Reader

To use any of the security features in Adobe Acrobat and Reader, you must first obtain a digital certificate. If you do not already have a digital certificate, please visit PGP TrustCenter's website at <http://www.pgptrustcenter.com/digital-certificate-solutions>

About Digital Signatures

You can digitally sign a document for many of the same reasons you might sign a paper document. A digital signature is used to authenticate digital information — such as documents, e-mail messages, and macros — by using computer cryptography. Digital signatures help to establish the following assurances:

- **Authenticity:** The digital signature helps to assure that the signer is who he or she claims to be.
- **Integrity:** The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation:** The digital signature helps to prove to all parties the origin of the signed content. "Repudiation" refers to the act of a signer's denying any association with the signed content.

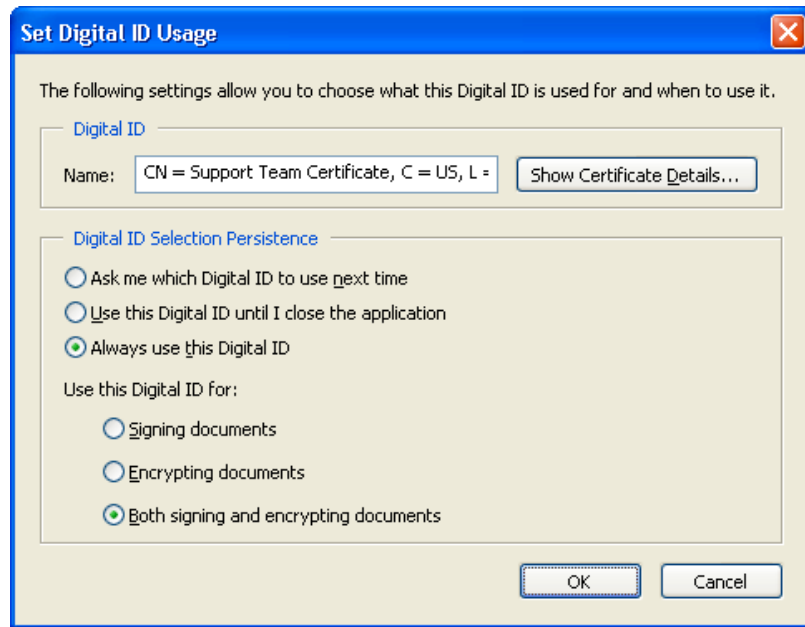
To make these assurances, the content creator must digitally sign the content by using a signature that satisfies the following criteria:

- The digital signature is valid (legitimate, current, and not expired or revoked).
- The certificate associated with the digital signature is current (not expired).
- The signing person or organization, known as the publisher, is trusted.
- The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority (CA) such as PGP TrustCenter.

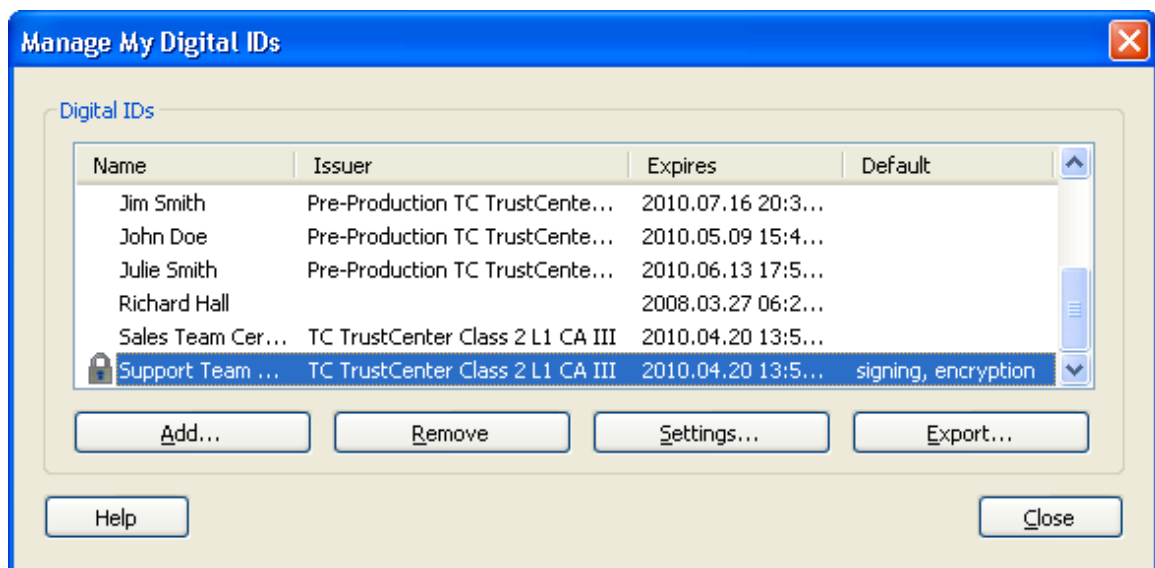
Selecting your default Adobe Digital ID

After you have your digital certificate with private keys installed, you can set it as your default signing certificate in Adobe Acrobat by following these steps:

1. From the Advanced menu, click Manage Digital IDs, and then My Digital ID.
2. Either highlight an existing certificate that is shown, or select the Add button to load a certificate that is stored elsewhere.
3. Press the Settings button and choose to "Always use this Digital ID" and "Both signing and encrypting documents". Click OK.



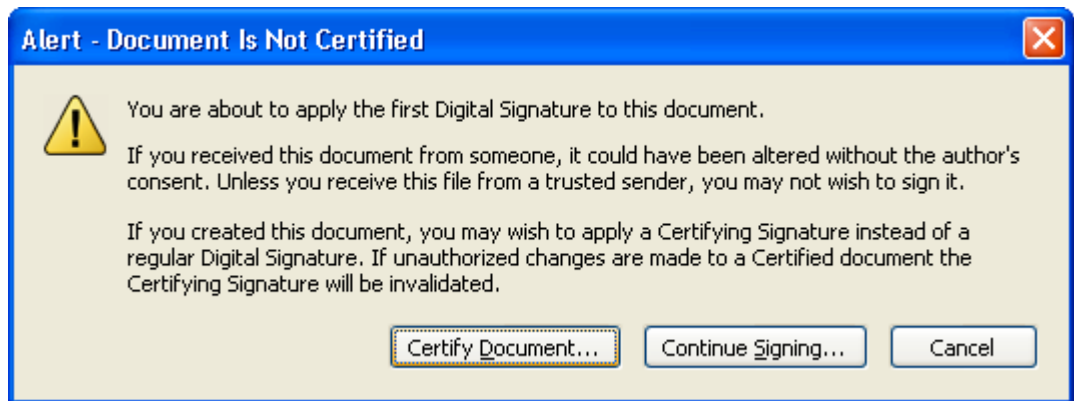
4. Your PGP TrustCenter certificate should now be listed as the default Digital ID for Adobe. Click on the Close button to finish.



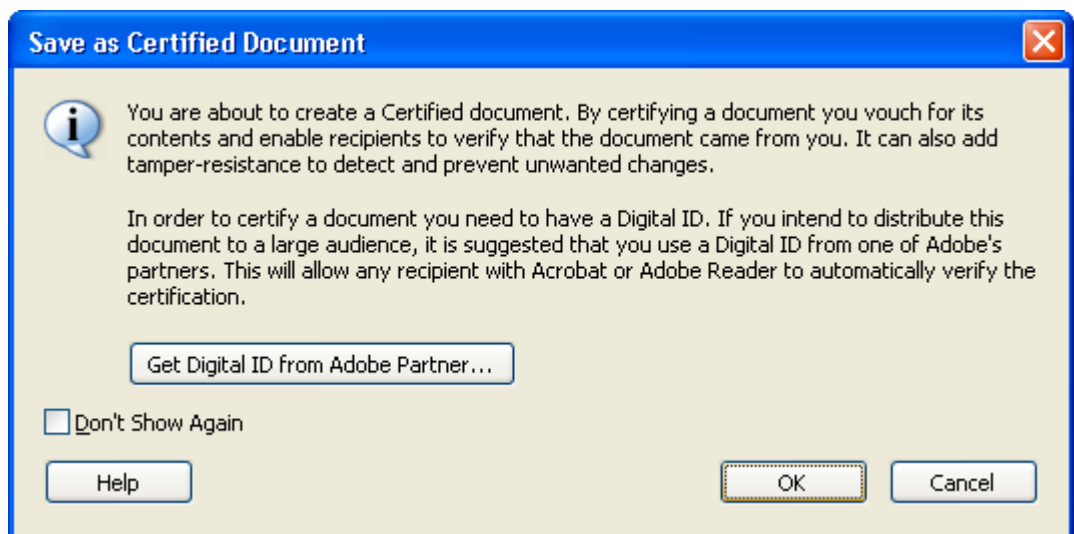
Digitally Signing PDFs with Adobe Acrobat v6

After you have your digital certificate with private keys installed, you can digitally sign your PDFs by following these steps:

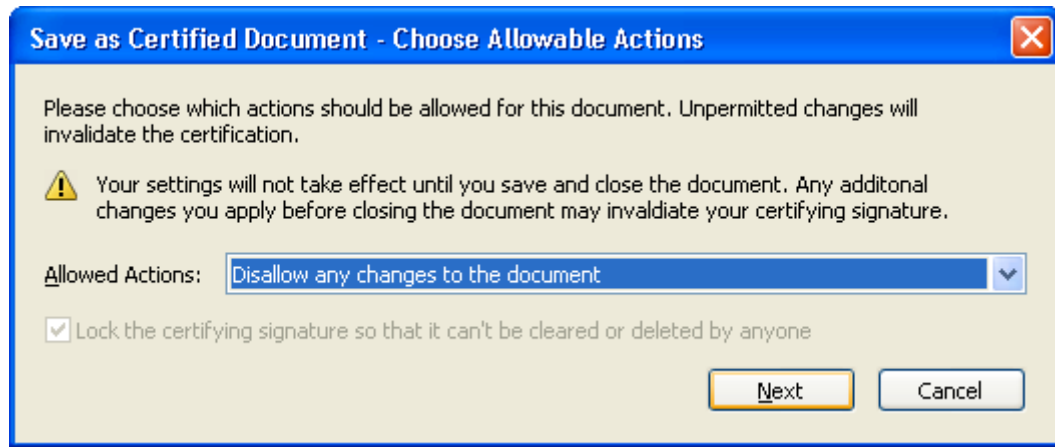
1. Once you have created a PDF, from the Document menu, click Digital Signatures, and Sign this Document.
Alternatively, you may click the "Sign" button and choose Sign this Document.
2. Select to either to Certify Document or Continue Signing.
NOTE: Just signing the document will simply prove who the document is from, while certifying the document will also ensure that the document has not been tampered with. If this is a new document authored by you, it is recommended that you select Certify Document.



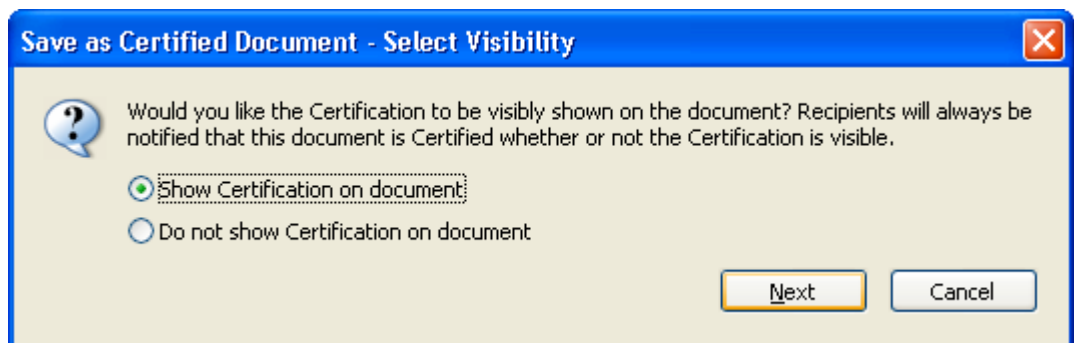
3. Click OK when the message about certifying documents is displayed.



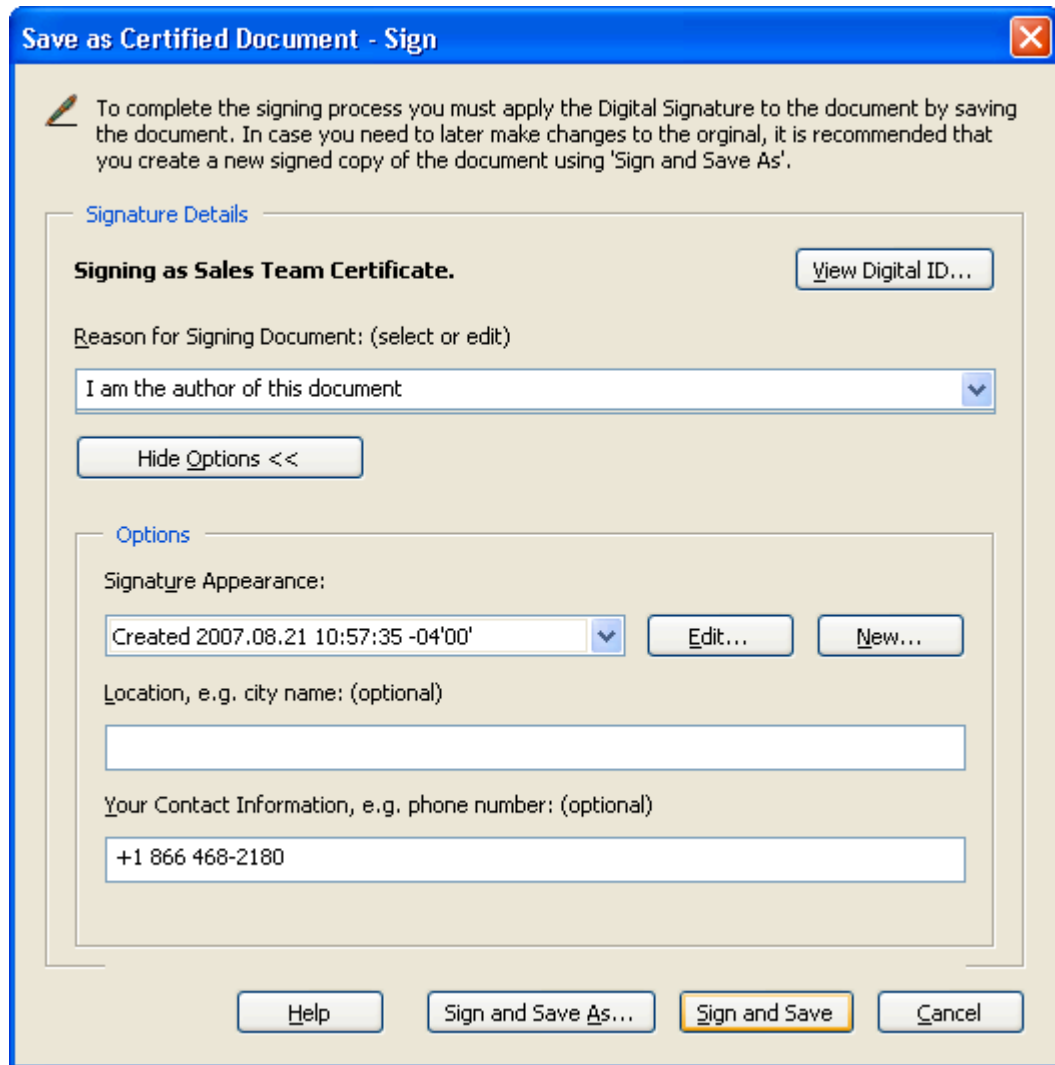
4. Now Choose the desired allowed actions for this document and click next.



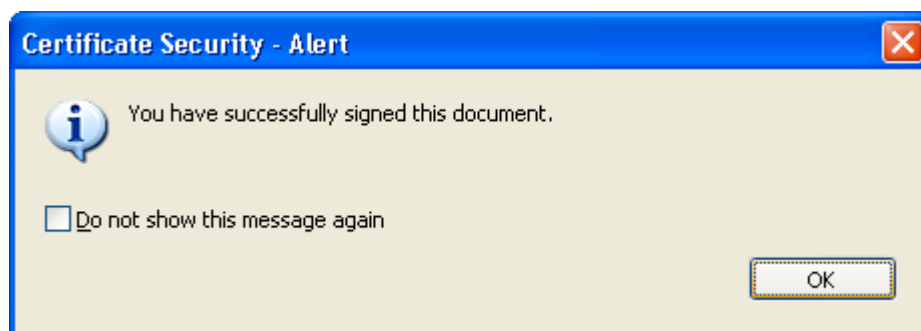
5. Select whether or not to show the digital signature certification on the saved PDF file. In this example we will choose to show the certification. Select Next when finished.



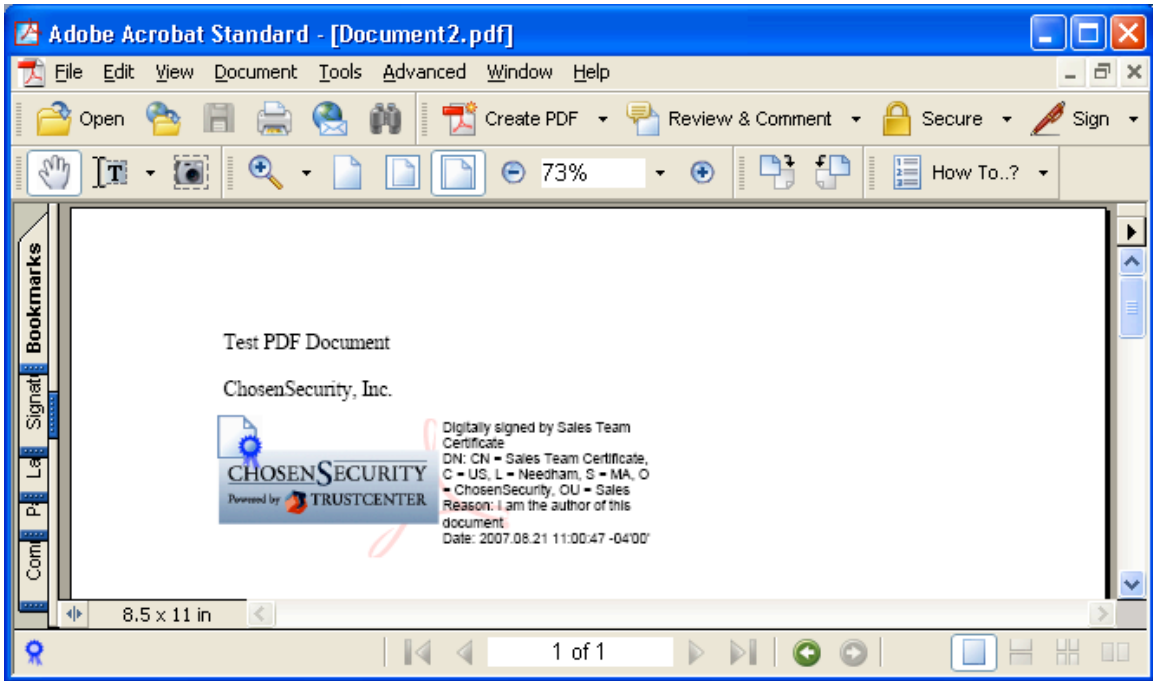
6. A message will then be displayed telling you to use the mouse to define the location for this signature. Click OK and then draw the desired place on the document where the digital signature should be displayed
7. Select the reason for signing this document. Press the Show Options button. In the Options section, press the New button for Signature Appearance. Here you will have options for which fields of your digital certificate to display, as well as the option to add a graphic such as a company logo, a picture or a graphic of an actual signature. Click OK, and then complete any additional information desired. Click on Sign and Save when finished.



8. A message is then displayed informing you that you have now successfully signed this document. Click OK to acknowledge this.



9. The document should now display the signature within the body. A valid signature will display a blue ribbon in the lower left-hand corner of the document.



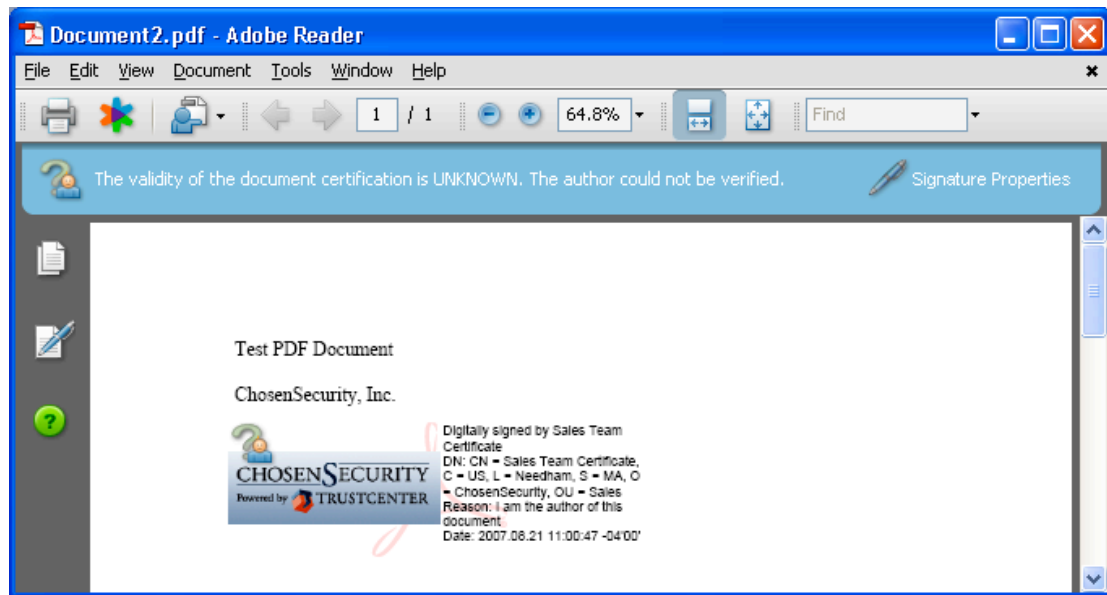
10. You can now distribute this trusted document, and anyone that has your public key, and use of Adobe Acrobat v6.0 or Adobe Reader 6.02 and higher, will be able to verify that it is actually from you and ensured that this file has not been tampered with or altered.

Verifying a Digitally Signed Document

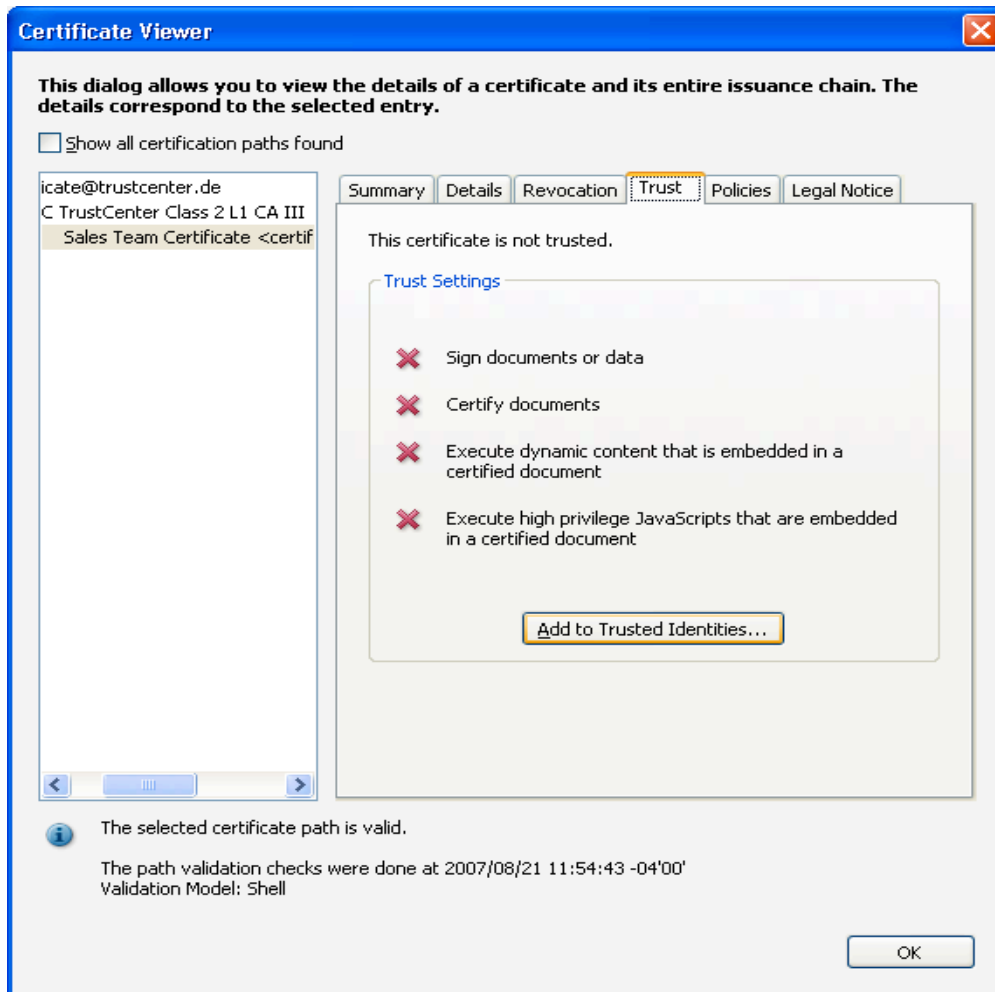
Informational Note: Anyone using Adobe Reader version 6 or lower will still be able to view a digitally signed PDF, but there will be no actual signature verification; a warning message will be displayed informing you of such and will request for you to upgrade Reader. Signature verification was included with Adobe Reader version 6.02 and higher.

In order to verify signatures with Adobe Reader or Acrobat, you need to maintain a list of trusted identities. By default, Adobe Reader will only trust signatures from those users that you have already added to your trusted identities list (unless this is a CDS document already verified by Adobe). For use with Adobe Reader v8, please perform the following steps:

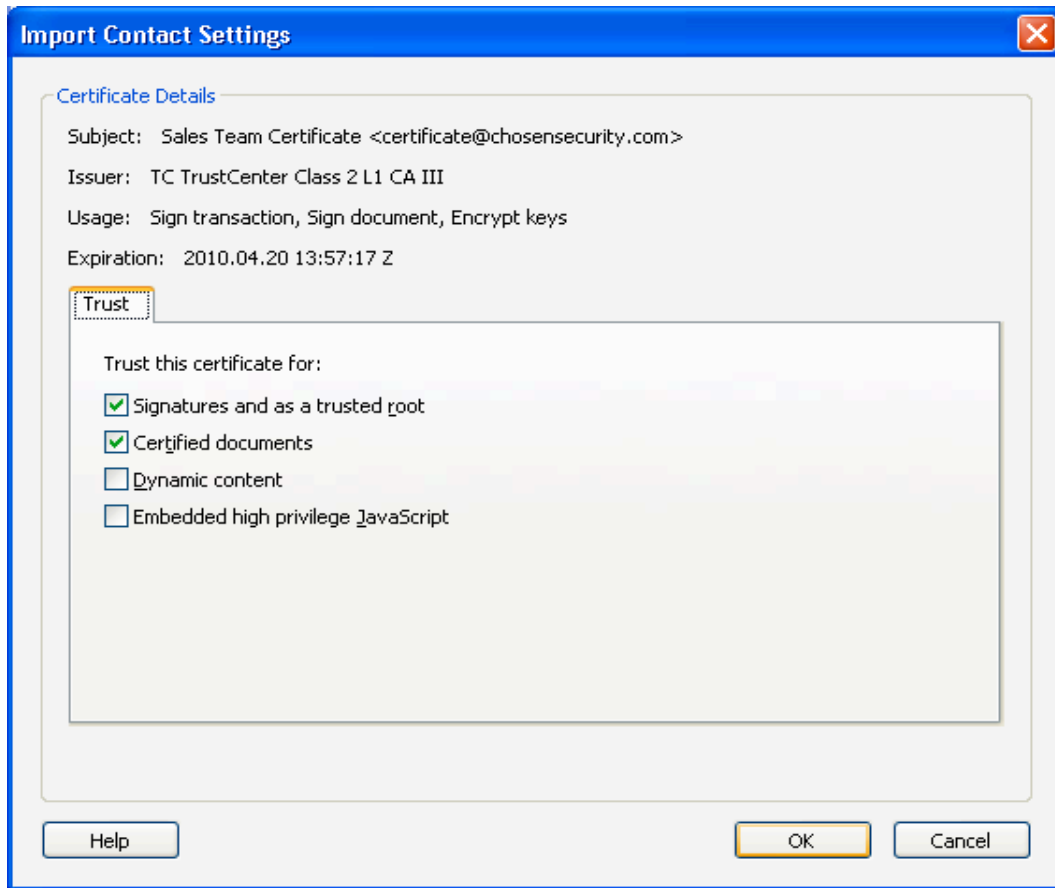
1. When you first open a signed document from someone that is not in your list of trusted identities, a message will appear stating that the author could not be verified. Click on "Signature Properties" in the upper right-hand corner. Alternatively, you can click on the question mark symbol within the signature of the signed document.



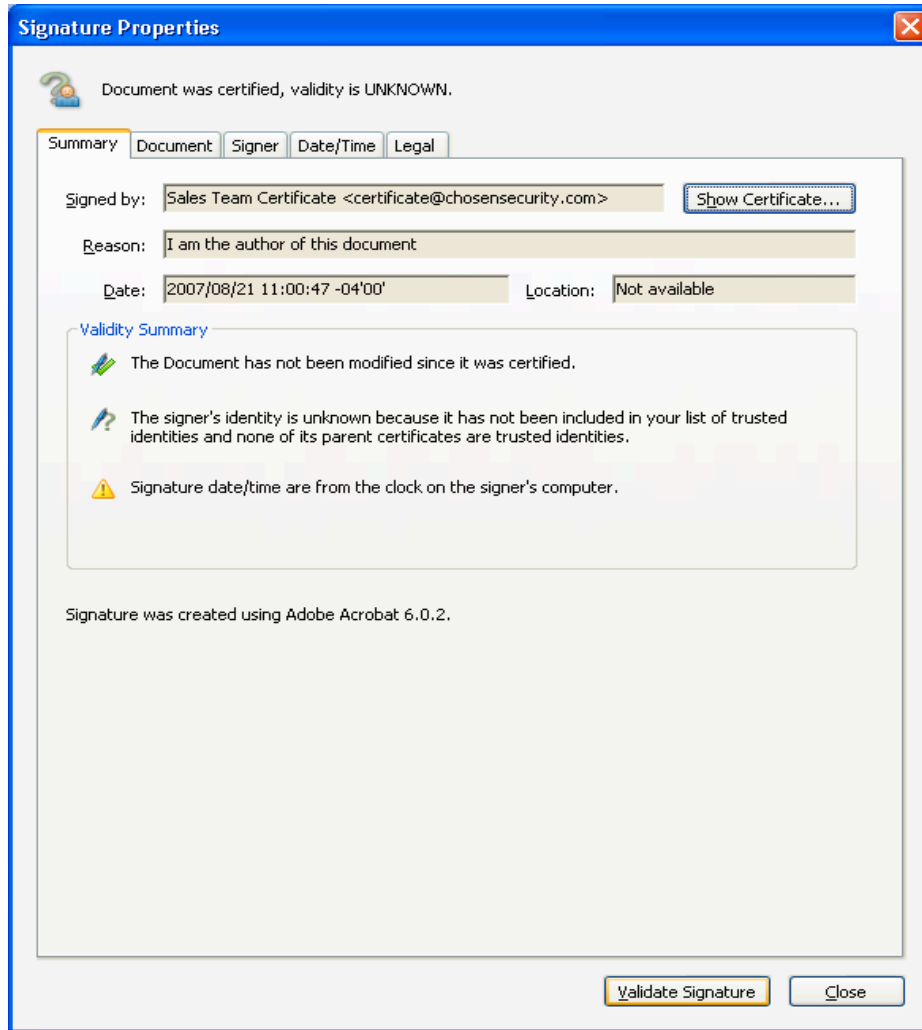
2. Within the Signature Properties dialog, click the "Show Certificate" button, and then select the "Trust" tab.
3. A message displays "The certificate is not trusted". Click the "Add to Trusted Identities" button. This should only be done if you believe this to be from someone that you trust.



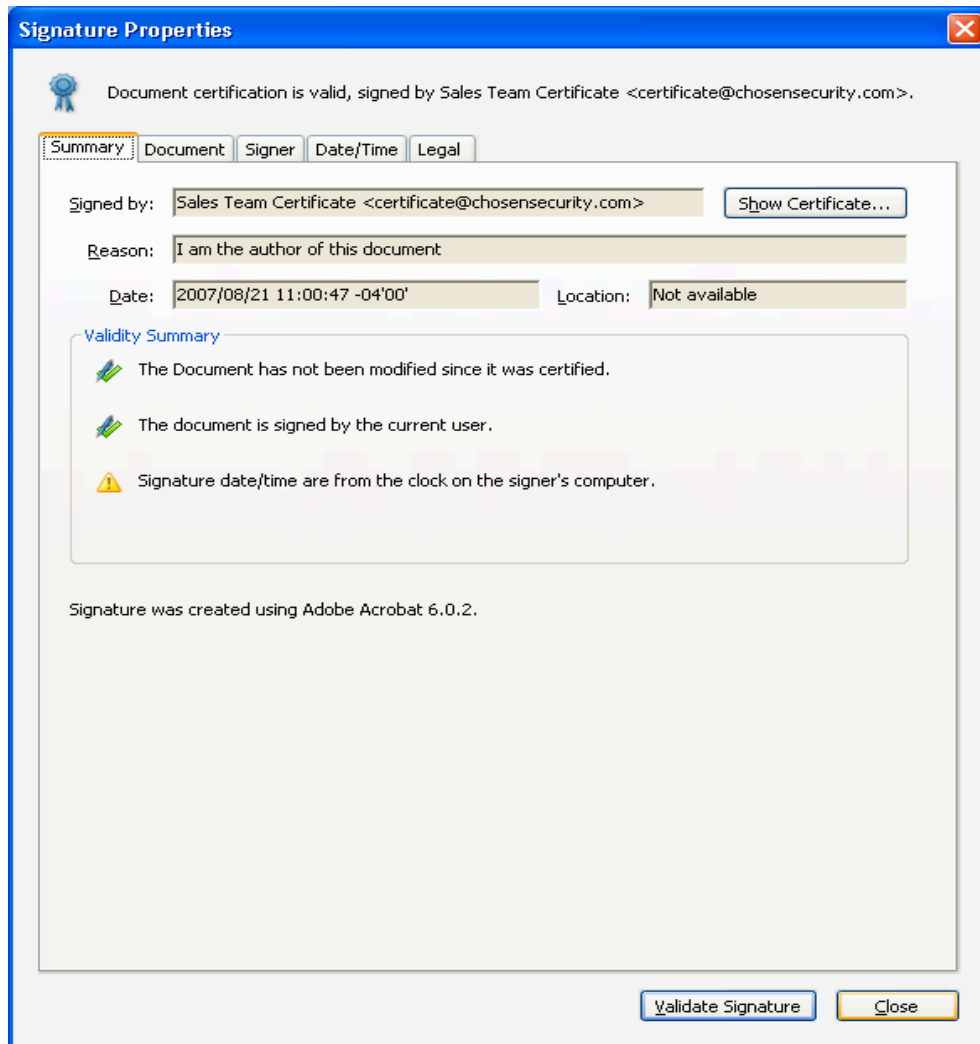
4. The Trust defaults should be set to "Signatures and as a trusted root" and "Certified documents". Click OK.



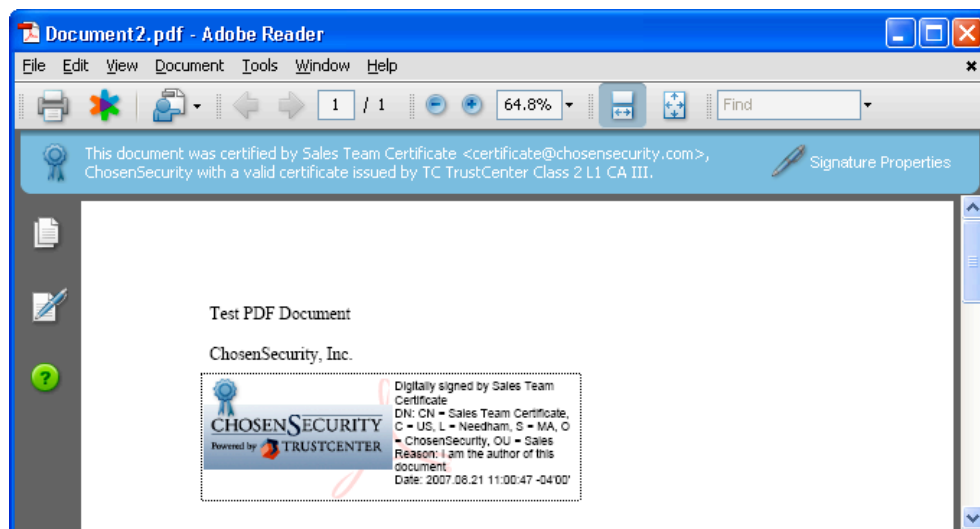
5. When brought back to the Signature Properties dialog, click on the "Validate Signature" button in the lower-right.



6. The signature should now show as valid and any correspondence with this user will now be trusted. Click on Close when finished.



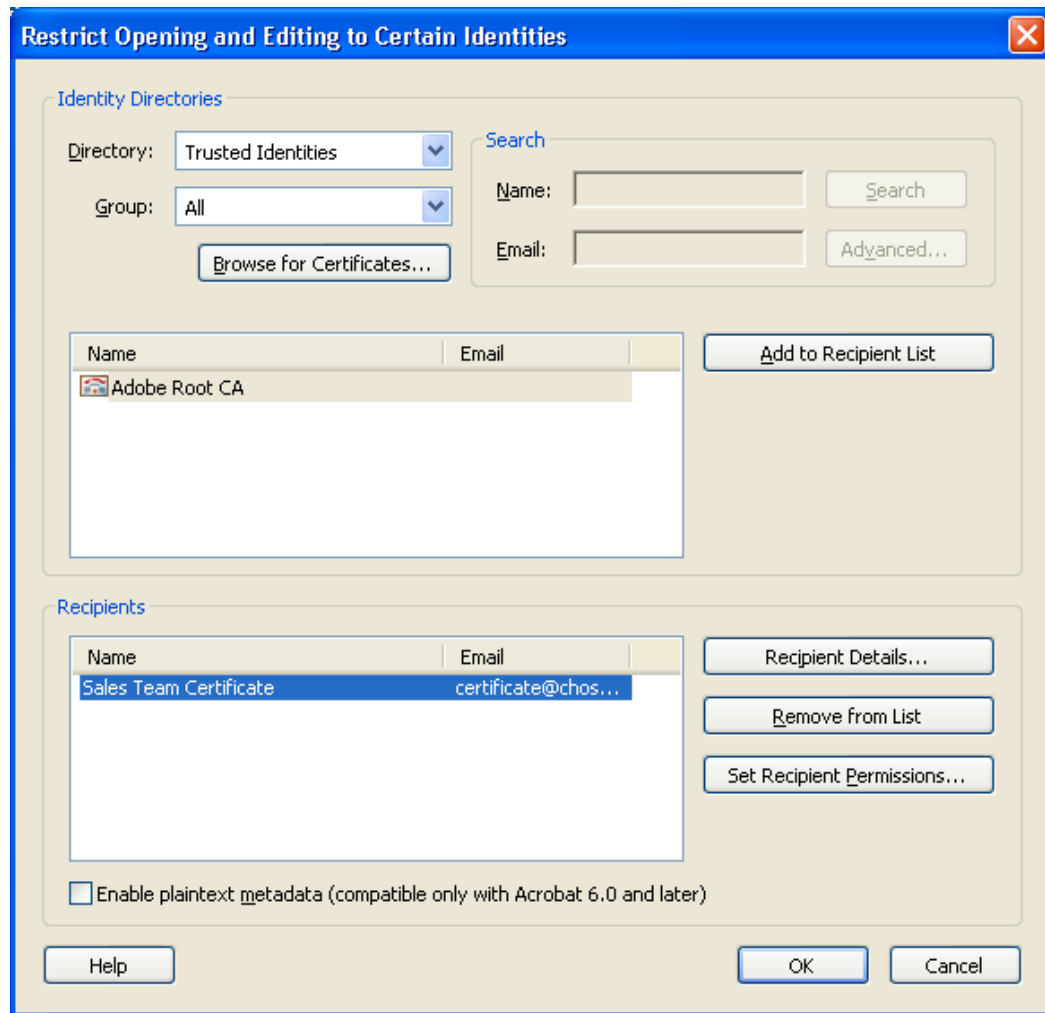
7. The PDF will now display with a certified signature by a valid certificate. All future correspondence with this user will now be accepted as valid and verifiable.



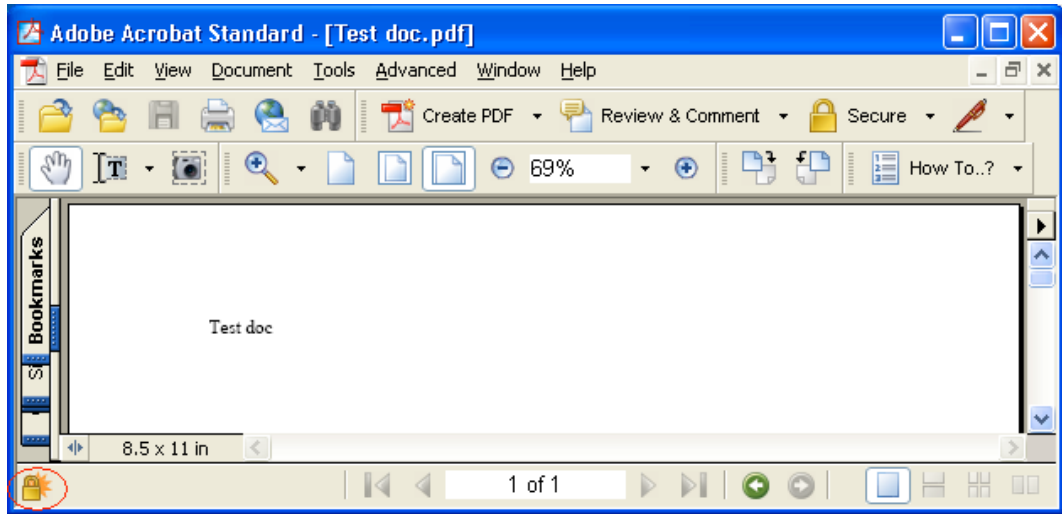
Encrypting PDFs with Adobe Acrobat v6

Encrypting PDFs provides for document control and can ensure that only the desired recipients may open the document. To encrypt a PDF file, you will need access to the public keys of all users in which you wish to provide the encrypted PDF to. Follow the steps outlined:

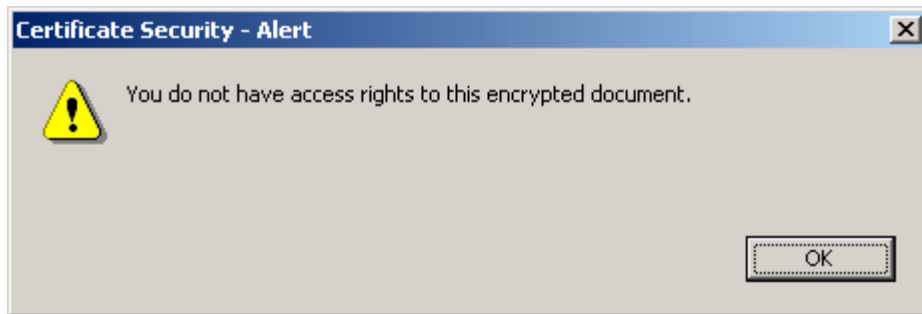
1. Open a new PDF in Adobe Acrobat v6. From the Document menu, select Security, and then Encrypt for Certain Identities Using Certificates.
Alternatively, you can select the "Secure" icon and choose Encrypt for Certain Identities Using Certificates.
2. A screen is displayed which allows you to select recipients from your list of Trusted Identities. If you would like to add a recipient, you can select the "Browse for Certificates" button to import additional certificates. Once the certificate has been imported, highlight it and press the Add to Recipient List button. When all recipients have been selected, click on OK.



3. You will next see a message notifying you that the security settings will not be applied until the document has been saved and closed. Click OK to acknowledge.
4. When the document is saved, a gold padlock will appear in the lower left-hand corner of the PDF to show that it is now encrypted. Now you can safely distribute this PDF and any recipient on the list will be able to open this file with Adobe Reader v6.02 and higher, or Adobe Acrobat v6.0 and higher.



5. The Adobe software will perform a check whenever an encrypted PDF is accessed to see if any of the recipient's certificates are present on that computer. If it is not, then access to the file will be prohibited.



6. The status of an encrypted PDF can be displayed by clicking on the gold padlock icon in the lower left-hand corner of the document.

