



Adobe Acrobat & Reader 8 have been **certified** to comply with the SAFE standard. This guide describes how to set up Acrobat and Reader to best support the technical and user interface requirements of the SAFE standard.



Adobe® Acrobat® & Reader® SAFE Configuration Guide

Configuring Adobe Acrobat and Reader to support the SAFE (Signatures and Authenticity for Everyone) standard

This document is a guide to configuring Adobe Acrobat and Reader 8 in a SAFE environment. It can be used by individuals who wish to enable SAFE signature support for Acrobat on their own computers, or may also be used by system administrators who are preparing Acrobat or Reader for enterprise deployment within their organizations. This guide is not a substitute for the SAFE technical specifications, but is intended as an Acrobat & Reader-specific supplement to those specifications. There are many factors, both technical and procedural, that are outside the scope of this document, that must be considered to successfully implement SAFE-enabled applications and processes. Please refer to the SAFE specifications and certificate policies for more information (available at <http://www.safe-biopharma.com/>).

This Configuration Guide provides information on directly user-modifiable settings that are available in Acrobat and Reader 8. These settings (and others) may also be configured for deployment in an enterprise environment by using the Adobe Customization Wizard (more information is available at: <http://www.adobe.com/support/downloads/detail.jsp?ftplID=3564>).

Note on Adobe Acrobat and Adobe Reader 8 Signature Functionality

For those organizations that deploy Adobe Acrobat or Reader, it's very important to understand the differences in functionality between *Adobe Acrobat* and *Adobe Reader* and the options for Acrobat and Reader deployment. There are distinct differences in functionality between Acrobat and Reader - particularly with regard to digital signatures. *Adobe Reader* is Adobe's freely available PDF viewing application. It does not enable the authoring or modification of PDF files, and it does not natively include the ability to digitally sign documents (with one notable exception - *Adobe LiveCycle Reader Extensions* - see below). Reader only includes the capability to *verify* existing signatures. *Adobe Acrobat* is the fully-functional PDF creation and editing application that allows users to generate and modify PDF files. Users of Acrobat can both create and verify digital signatures.

Enabling Digital Signatures in Reader with Adobe LiveCycle Reader Extensions

To enable the creation of digital signatures with the free Adobe Reader, organizations may choose to use Adobe LiveCycle Reader Extensions. LiveCycle Reader Extensions is an enterprise tool that allows organizations to “switch on” features in Adobe Reader on a document-by-document basis. When LiveCycle Reader Extensions are used with a PDF document, end-users with only the free Adobe Reader will be able to digitally sign that document (other features, including advanced form filling and commenting are available too). LiveCycle Reader Extensions can be a very effective way of enabling digital signatures for large numbers of users without requiring individuals to each have a license for Adobe Acrobat Standard or Professional. For more information, visit: <http://www.adobe.com/products/livecycle/readerextensions/>

Obtain and Install a SAFE Digital Identity

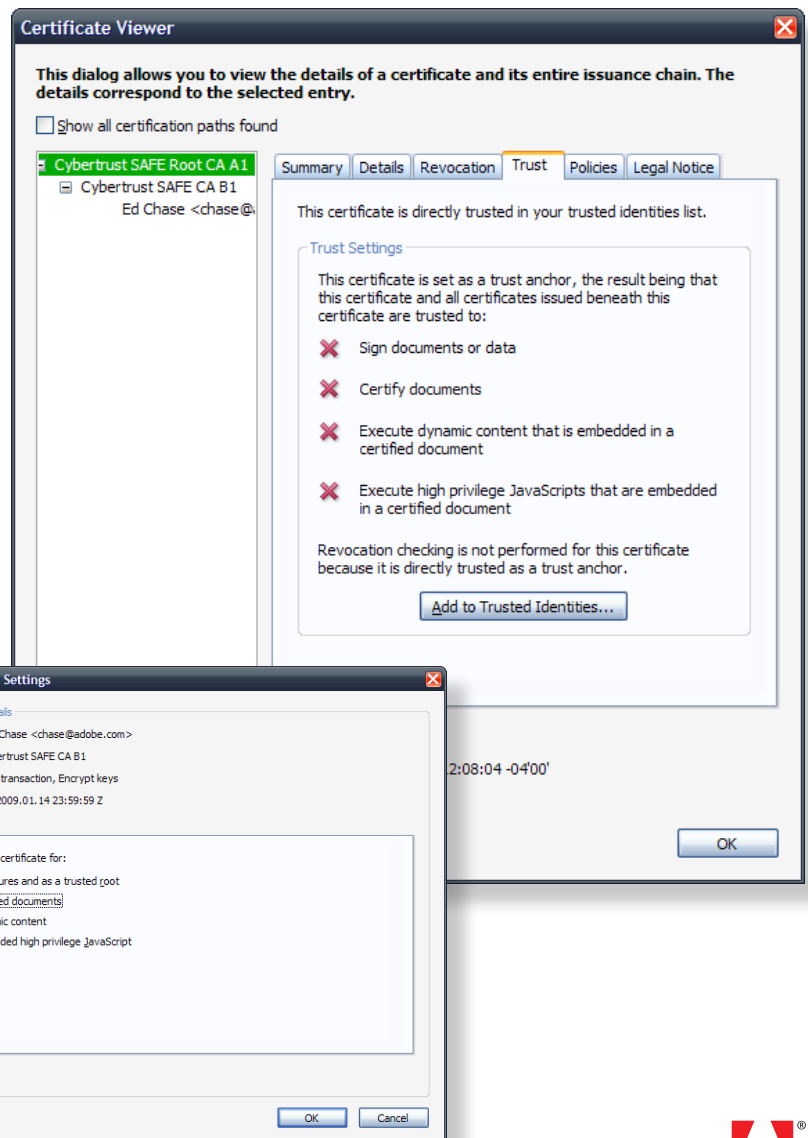
Before you can create SAFE digital signatures with Acrobat or Reader, you will need to obtain a SAFE Digital ID in accordance with the SAFE policies and procedures (not covered in this document, visit: <http://www.safe-biopharma.com> for more information). You may also need to configure additional software and hardware if you are using smart card hardware tokens. See **“Using third party digital identities” in the Acrobat & Reader Help Documentation** for more information on installing and configuring digital IDs. Installation of hardware components like smart card readers or hardware tokens is not covered here and is typically found in the documentation provided with those products.

Establishing Trust

Once you have installed your SAFE digital ID and any required hardware devices, the next step is to verify that you have configured Acrobat to **trust** SAFE digital signatures. Even if you don’t use a SAFE digital ID, these steps can also help you set up Acrobat to accurately verify the validity of any SAFE signatures that you may receive. There are several ways to set up trust in Acrobat - you should only need to use **one** of the methods below:

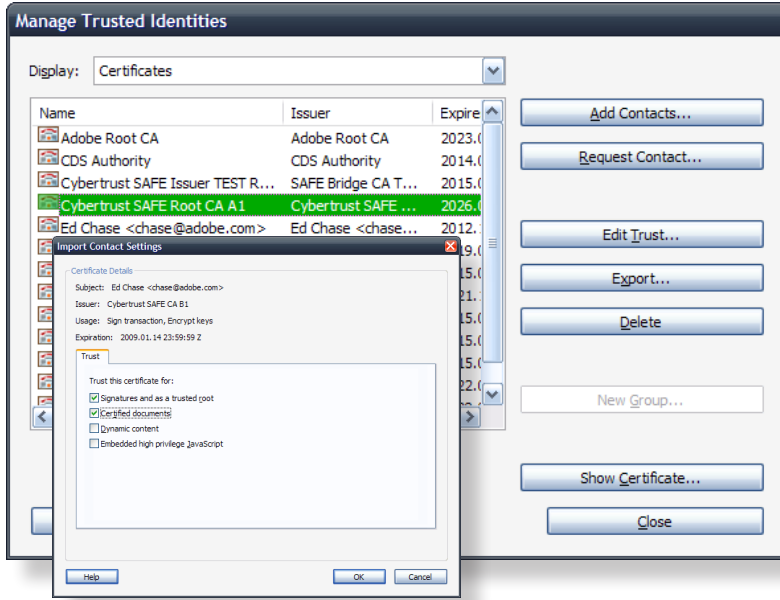
If you have a document from another user that has been signed with a SAFE signature, you can use it to add trust for the SAFE Root Certificate (NOTE: You can also use this method if you don’t have a SAFE digital ID but wish to verify the signatures of other users):

1. Open the PDF document containing the SAFE signature
2. Click the signature - it display a Question-Mark (“?”) status icon indicating unknown trust
3. Click Signature Properties, and then click “Show Certificate”
4. In the list of certificates in the left pane in the **Certificate Viewer Dialog (left)**, select the “Cybertrust SAFE Root CA A1”
5. Select the “Trust” tab and click the “Add to Trusted Identities” button
6. In the “Import Contact Settings” dialog, check at least the boxes for “Signatures and as a trusted root” and “Certified documents”
7. Click “OK”, then Click “OK” in the “Certificate Viewer” dialog, then click “Close” in the “Signature Properties” dialog to return to the document
8. Click on the SAFE signature, and it should now validate with a green check mark



...or add trust for the SAFE Root Certificate using the “Trusted Identity Manager” in Acrobat or Reader:

1. In Acrobat, select from the menu: “Advanced>Manage Trusted Identities”. If you are using Reader, select: “Document>Manage Trusted Identities”
2. In the “Display” drop-list at the top of the page, the default selection is “Contacts”, change the selection to “Certificates”
3. Select the “Cybertrust SAFE Root CA A1” from the list (if this certificate is not present in the list, use one of the other methods listed here)
4. With the “Cybertrust SAFE Root CA A1” selected, click the “Edit Trust” button
5. The “Edit Certificate Trust” dialog will appear
6. In the “Edit Certificate Trust” dialog, check at least the boxes for “Signatures and as a trusted root” and “Certified documents”
7. Click “OK”, then Click “Close” in the “Manage trusted identities” dialog
8. SAFE signatures should now validate with a green check mark

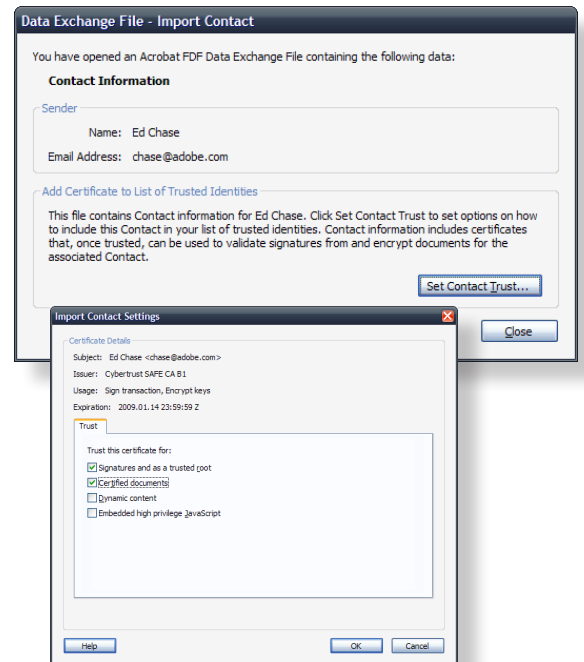


...or add trust using an FDF data exchange file :

1. On the desktop, double-click on a file with the “.FDF” extension that contains the SAFE Root Certificate information (alternately, open the “.FDF” file through the “File>Open” menu in Acrobat or Reader)
2. The “Data Exchange File - Import Contact” dialog will appear - there are two variations on how this dialog may appear - which variation appears will depend on whether the Data Exchange File has been digitally signed by a contact that is already trusted in Acrobat

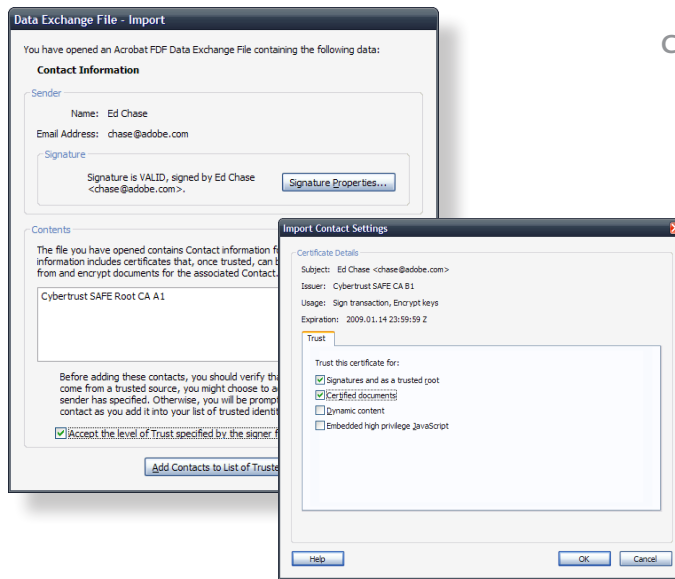
Unsigned Data Exchange Files

1. When you open an Unsigned Data Exchange file, a dialog will appear describing the contents of the file - the dialog will have two buttons: “Set Contact Trust” and “Close”
2. Click the “Set Contact Trust” button which opens the “Import Contact Settings” dialog
3. In the “Import Contact Settings” dialog, check at least the boxes for “Signatures and as a trusted root” and “Certified documents” and click “OK”
4. Click “OK” in the “Import Complete” dialog, then click “Close” in the “Data Exchange File - Import Contact” dialog



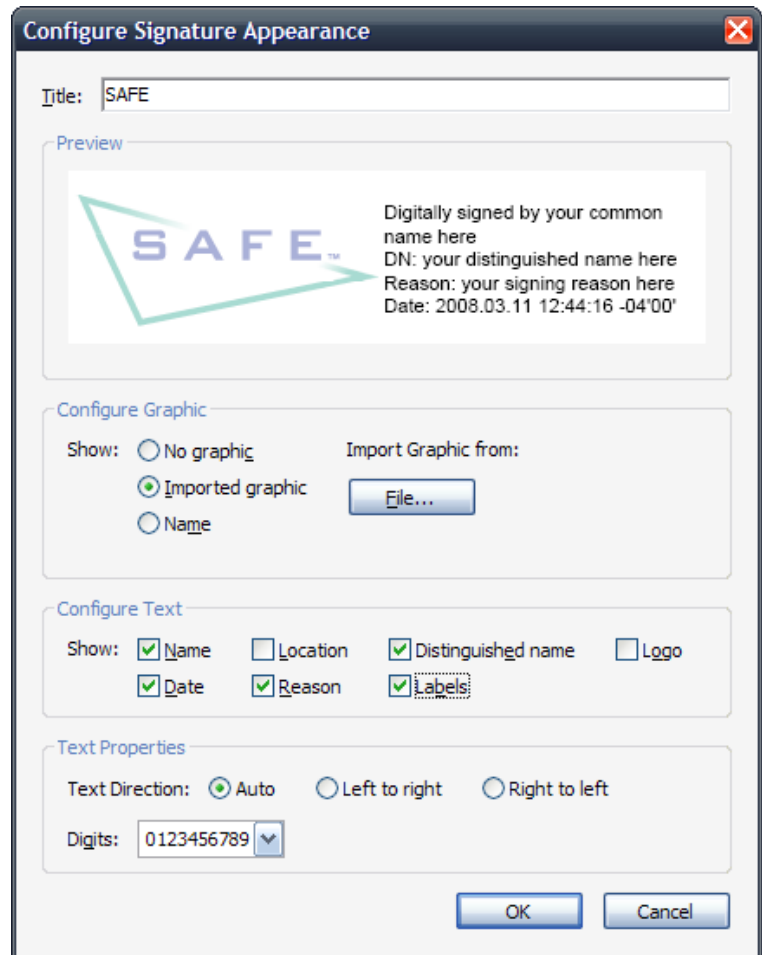
Signed Data Exchange Files

1. When you open a Signed Data Exchange file, a dialog will appear describing the contents of the file - the dialog will have two buttons: "Set Contact Trust" and "Close"
2. Click the "Set Contact Trust" button to open the "Import Contact Settings" dialog
3. In the "Import Contact Settings" dialog, check at least the boxes for "Signatures and as a trusted root" and "Certified documents" and click "OK"
4. Click "OK" in the "Import Complete" dialog, then click "Close" in the "Data Exchange File - Import Contact" dialog



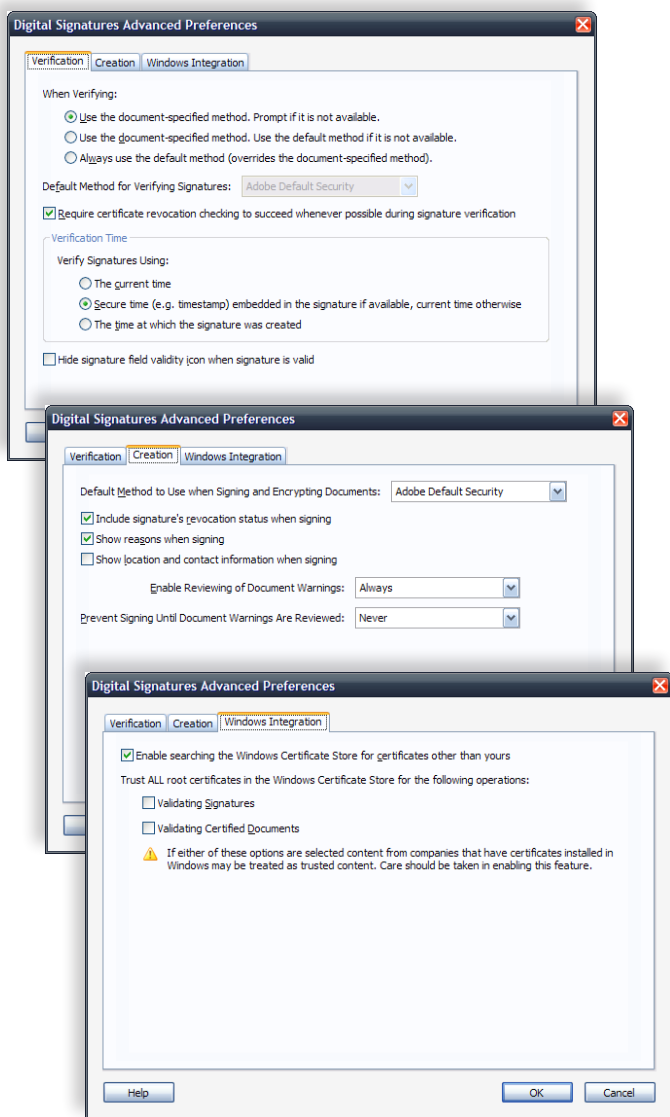
Creating a SAFE Signature Appearance

1. Locate the SAFE.pdf file that contains the SAFE logo (**Attached to this PDF document - open the attachment pane to view**) and save it to your desktop or other convenient location on your hard drive
2. In Acrobat or Reader, select the "Edit>Preferences" menu item
3. Select the "Security" category in the "Preferences" dialog
4. In the "Appearances" section, click the "New" button
5. The "Configure Signature Appearance" dialog will appear
6. In the "Title" field, enter, "SAFE" (using this exact appearance name is particularly important if you choose to use the SAFE plug-in (see below), since that is the name that the plug-in will search for)
7. In the "Configure Graphic" section, select "Imported Graphic", then click the "File" button, in the "Select Picture" dialog, click "Browse" and locate the "SAFE.pdf" file containing the SAFE logo
8. Verify that the image is the correct SAFE logo, then click "OK" to add it to the signature appearance and return to the "Configure Signature Appearance" dialog
9. In the "Configure Text" section of the "Configure Signature Appearance" dialog, check at least the following boxes: "Name", "Distinguished Name", "Labels", "Date", "Reason"
10. Also in the "Configure Text" section, **un-check** the "Logo" box
11. The SAFE standard does not required that the "Location" box be either checked or unchecked
12. Do not modify any settings in the "Text Properties" section unless otherwise directed by your organization
13. Click the "OK" button when complete, the new "SAFE" appearance should now appear in the list of signature appearances



Configure the Signature Preferences

1. In Acrobat or Reader, select the Edit>Preferences menu item
2. Select the “Security” category in the Preferences dialog
3. Ensure that “Verify signatures when the document is opened” is checked
4. Click the “Advanced Preferences” button to open the “Digital Signatures Advanced Preferences” dialog



5. Under the “Verification” tab, be sure that for the “When verifying” setting, “Use the document specified method, prompt if not available” is selected
6. Check the box next to: “Require certificate revocation checking to succeed whenever possible during signature verification”
7. In the “Verification Time” section, select “Secure time”. **NOTE:** You *may* optionally select “The time at which the signature was created” instead. **HOWEVER** - selecting this option will strictly limit the types of signatures that will successfully validate in Acrobat. Using “The time at which the signature was created” will only allow Acrobat to verify signatures that are SAFE-compliant or those of an equivalent level of assurance. If you **ONLY** accept SAFE digital signatures, you may choose select the “The time at which the signature was created” setting for an additional level of verification
8. Ensure that the “Hide the signature field validity icon when signature is valid” is not selected
9. Under the “Creation” tab, be sure that the “Default method to use when signing and encrypting documents” is set to “Adobe default security”
10. Ensure that “Include signature’s revocation status when signing” is checked
11. Ensure that “Show reasons when signing” is checked
12. All other settings in this tab are optional
13. Under the “Windows Integration” tab, be sure that “Enable searching the Windows Certificate Store for certificates other than yours” is selected
14. The two settings under “Trust ALL root certificates in the Windows Certificate Store for the following operations” are optional. It is **NOT** recommended that you check either of these boxes unless specifically directed to do so by your organization. Without proper system configuration, checking these boxes may result in inadequate or incorrect verification of SAFE signatures
15. When all settings have been configured in the “Digital Signatures Advanced Preferences” dialog, click the “OK” button to accept the changes and return to the “Preferences” dialog, click “OK” to close the “Preferences” dialog

Creating a SAFE signature

Now that you’ve configured Acrobat, you’ll need to create a test signature to perform a few final configurations and verify your settings. Also, it’s important that you create a test signature since some **additional settings need to be made only the first time** you sign a document with your SAFE digital ID.

1. Close all dialog boxes
2. Ensure that your computer has access to the internet (Acrobat needs to connect to the SAFE servers to verify your digital ID when you create a signature)
3. Insert your SAFE token or smart card
4. Open a blank or test document in Acrobat (be sure that there are no security restrictions on the test document)

5. From the menu, select "Advanced> Sign & Certify>Place Signature" (alternately, select "Place Signature" from the "Sign" toolbar menu, or select the "Digital Signature Tool" from the "Forms" toolbar)
6. With the mouse, draw the signature field in the location you would like the signature to appear - make sure that it is large enough to view the signature appearance - most visible signature fields should be a **minimum** of one inch tall by two inches wide to be easily viewable
7. Once you've drawn the signature field, the "Sign Document" dialog will appear
8. In the "Digital ID" field, select your SAFE digital ID
9. In the "Appearance" section, select "SAFE" (when selected, the SAFE appearance should be visible in the signature preview)
10. In the "Reason" section, **type** in the following statement **exactly** as it appears here: **"I intend this signature to be legally binding per my executed SAFE user agreement"**. You will only need to manually type this statement in the **first** time you create a SAFE signature on this computer, once it is entered, you will be able to select it from the list for subsequent signatures. Your organization may also apply different wording around this statement as required for some transactions. **NOTE:** If the "Reason" field does not appear, verify that the signature preferences have been correctly configured in the previous section
11. Click the "Sign" button to create the signature. You will be prompted to enter your passphrase to access your digital ID - when you successfully enter your passphrase, the signature creation process will complete
12. Once the signature is created, it should appear on the document, in the signature field you created, with a green check mark icon indicating that it is valid
13. Select the signature with the mouse, and click the "Signature Properties" button, the "Signature Properties" dialog will appear
14. In the "Signature Properties" dialog, click the "Show Certificate" button, the "Certificate Viewer" dialog will appear
15. Ensure that the "Cybertrust SAFE Root CA A1" appears in the left pane
16. In the "Certificate Viewer" dialog, select the "Revocation" tab, ensure that in the "Details" section, the first paragraph reads: "The selected certificate is considered valid because it has not been revoked as verified using the Online Certificate Status Protocol (OCSP) response that was embedded in the document."



Troubleshooting

Below are some basic tips for troubleshooting problems with SAFE configuration in Acrobat:

If you can't create a signature at all

- Verify that you are using **Adobe Acrobat Standard or Professional (versions 7 or later)**, or if you are using **Adobe Reader**, you can not **create signatures**, but can only **verify** signatures for most documents. To sign with Reader, you'll need a special type of PDF file that has been "**Reader-Extended**" by Adobe Acrobat Professional or Adobe LiveCycle to provide signing functionality in Reader

If your SAFE digital ID does not appear in the "Digital ID" list

- Verify that your SAFE digital ID is securely inserted
- Verify that all hardware and software drivers for your token are installed and functioning (consult your token vendor's documentation for additional support)
- Also verify that all configuration settings above are accurate and complete in Acrobat

If the signature appears but does NOT have a green check mark icon - instead it has a question mark or other icon.

- Acrobat may not be configured correctly to trust the SAFE root CA. Verify that you have followed the steps in the "Establishing Trust" section of this document
- Alternately, your organization may have it's own trust relationship between it's own Root certificate and the SAFE bridge CA, in which case, you may need to add the cross-certificates for your organization. Contact your organization's IT staff for more information.

If the details section in the Revocation tab does not read: "The selected certificate is considered valid because it has not been revoked as verified using the Online Certificate Status Protocol (OCSP) response that was embedded in the document."

- Verify your preferences in accordance with the "Configuring the Signature Preferences" section of this document
- Also verify that Acrobat can access the internet. In some older Proxy Server environments, Acrobat may not be able to access the internet. If this is the case, additional configuration may be needed to your Proxy Server to allow Acrobat to process revocation checks

Optional - Install the Adobe SAFE Plug-In

You may also wish to install the Adobe SAFE Plug-In. The plug-in is not required to create SAFE signatures, but provides a simpler user interface and a helpful toolbar button for easy signature creation. System Administrators may also choose to install the SAFE plug-in automatically with other SAFE elements using the Adobe Customization Wizard. **NOTE:** All other configurations in this document **must** still be performed when you are using the plug-in - the plug-in provides only an alternate user interface for the signature process. Be sure to read the included plug-in license agreement before installing the plug-in. The SAFE plug in is a free JavaScript code sample and is not supported directly by Adobe. Please contact your System Administrator for assistance.

To install the plug-in directly:

1. Copy the SAFESign.js file (**Attached to this PDF document - open the attachment pane to view**) to the Adobe JavaScripts folder located in either (a) or (b) location below.
 - a. For Acrobat Standard or Professional, the default location for the JavaScript folder is: "<drive letter>\Program Files\Adobe\Acrobat 8.0\Acrobat\Javascripts"
 - b. For Adobe Reader, the default location for the Javascript folder is: "<drive letter>\Program Files\Adobe\Reader 8.0\Acrobat\Javascripts"
2. Close and re-open Acrobat/Reader - the SAFE Sign button should now appear in the toolbar

System Administrators may also choose to install the SAFE plug-in automatically with other SAFE elements using the Adobe Customization Wizard. Visit <http://www.adobe.com/support/downloads/detail.jsp?ftplID=3564> for more information.

To use the SAFE plug-in:

1. Open a document with a signature field or create a signature field with the Digital Signature Field tool on the Forms toolbar in Acrobat
2. Click the "SAFE Sign" button on the toolbar
3. The plug-in will prompt you to select a signature field
4. On the first use ONLY, the plug-in may prompt you to select your SAFE digital ID and SAFE signature appearance - select your SAFE digital ID and signature appearance (you can edit these later by clicking the "Configure" button)
5. Click the "Sign" button to create the signature



Adobe helps people create, manage, and deliver the highest quality digital content in the world.
Better by Adobe.™

Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, Clearly Adobe Imaging, the Clearly Adobe Imaging logo, Illustrator, ImageReady, Photoshop, and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Microsoft, Windows, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2008 Adobe Systems Incorporated. All rights reserved.
Printed in the USA.