Adobe External Best Practices Guide for Using Digital Signatures

This guide provides procedures for signing and validating Digital Signatures in compliance with Adobe's legal requirements.

Getting Started

Adobe has adopted a Digital Signature policy to accelerate its contracting processes and reduce contracting costs for both parties. Adobe's digital contracting process is designed around the use of the free Adobe Reader for the application of digital signatures on both sides. ***NOTE:*** *This document contains an approval Digital Signature, so that it can be used to practice validation procedures described in this guide.*

Digitally signed by John B. Harris
DN: email=jbharris@adobe.com, c=US, st=California, l=San Jose, o=Adobe Systems Incorporated, cn=John B. Harris
Date: 2009.11.13 16:02:56 -05'00'

Digital Signature Process Requirements

- You must have installed Adobe Acrobat or Reader version 9.2 or greater.
- You must Digitally Sign the document using either a Certified Document Services (CDS) Digital ID obtained from a CDS Provider or a digital ID from an AATL member, for more information, refer to Obtaining an Approved Digital ID.
- You must make sure the USB token or other hardware device containing your CDS Digital ID is plugged into your computer before opening a file to be Digitally Signed.
- You must always be online when signing a document.

- If you have changed any Acrobat or Reader Digital Signature preferences since installation, you must reset them to match those outlined in Checking Your Signing and Validating Environment.

What Contracts May Be Digitally Signed

Provided the requirements of this Best Practices document are met, Adobe's Digital Signature Policy allows for any type of contract approved by Adobe Legal and executed within North America to be Digitally Signed.

Adobe also allows a document containing a Digital Signature to be printed and **wet** signed (signed by hand) by both parties to the agreement if the following conditions are met:

1) The Digital Signature must be accompanied by a scanned representation of the signer's wet ink signature

2) Your organization does not allow Digital Signatures or does not have an appropriate approved Digital ID.

Obtaining an Approved Digital ID

A Digital ID is an electronic representation of certain information, associated with a person or entity, which contains a credential used for Digitally Signing a document.

The Adobe Digital Signature policy requires the use of an Adobe CDS or Adobe Approved Trust List (AATL) Digital ID to Digitally Sign documents. While there are several types of Digital IDs available (Individual Digital ID, Organization Digital ID [Desktop] and Organization Digital ID [Server]), Adobe Digital Signatures Best Practices requires that you use an Individual Digital ID from the CDS or AATL programs. For more information, contact your Adobe representative.

Digital Signatures Workflow

To digitally sign a document:

TASK

1. Ensure your settings are configured according to Validating an Approval Digital Signature.
2. Validate all approval signatures according to Checking Your Signing and Validating Environment.
3. Digitally sign the document Digitally Signing a PDF Document.
4. Return the document to Adobe.

RESULT:

Adobe will then digitally sign the document and return a fully Digitally Signed version of the contract to your organization.

Digitally Signing a PDF Document

The following procedure outlines the steps to Digitally Sign an electronic document in place of a hand written signature on paper. The Policy requires that legal agreements be approved and prepared by Adobe Legal for Digital Signatures before organizations can sign the agreement with an approved Digital ID.

To digitally sign a document:

TASK

1. 1.Make sure you have followed the guidelines specified in Checking Your Signing and Validating Environment
2. Open the document, while online, using Adobe Acrobat or Reader 9.2 or higher.
3. Find and click the Digital Signature field to sign the document.
4. The **Apply Digital Signature – Digital ID Selection** dialog box will appear. Select your CDS or AATL Individual Digital ID and your name will appear. Click **OK**.

   ADDITIONAL INFORMATION: You must use an Individual Digital ID when applying a Digital Signature for approval.
5. The **Apply Digital Signature to Document** dialog box will appear. Enter the password for your Digital ID. Make sure the Reason for Signing field is blank (if displayed), then click **Sign** and **Save As** (the reason for signing should be explained by the document itself).
6. You should see your approval Digital Signature appear on the document.

7. Verify that your Digital Signature was applied in compliance with Adobe requirements by following the procedure in Validating an Approval Digital Signature.

   ADDITIONAL INFORMATION: You should always verify your own signatures. For example, if you were offline at the time you Digitally Signed, the Digital Signature would not be compliant.

8. Your document is now ready to be sent back to Adobe.

Validating an Approval Digital Signature

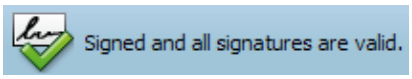
To verify a Digital Signature, you need to use the Signature tab on the left side of the document. It lists all signatures in the document. If you don't see this tab, click the icon on the left hand side that looks like a pen.

NOTE: *You should validate all Digital Signatures on a document before you proceed. Furthermore, you should check your own Digital Signature for correctness using the following procedure.*

To verify that a Digital Signature is compliant:

TASK

1. While online, open the document using Acrobat or Reader 9.2 or higher. When you open the document, you should see a green checkmark at the top of the window with the text **Signed and all signatures are valid**.

2. Click the **Signature Panel** button at the right-hand side of that blue information bar to open the Signature Panel (or click the pen icon on the left-hand side of the window).

3. Validate the following:

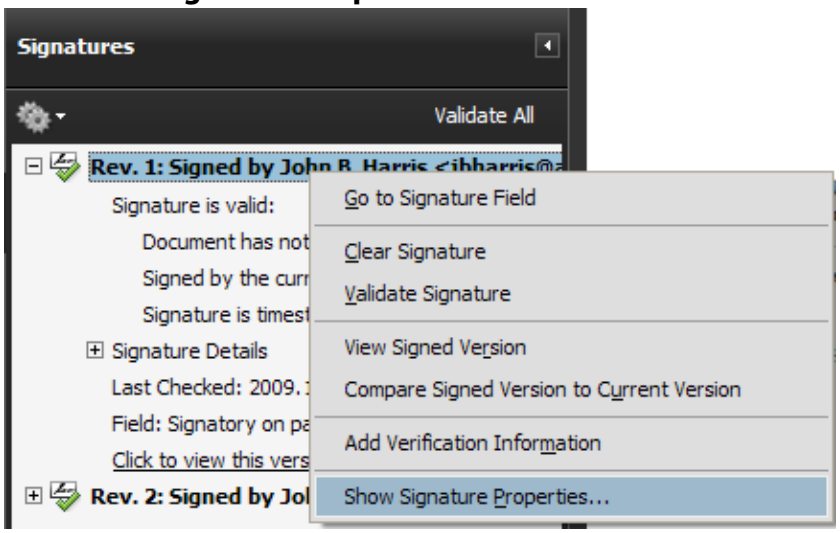
   a All signatures should have green checkmarks next to them.

   b All signatures should say **signed by** different persons.

   c The Digital Signature should be recognizable and **not** be a company or organizational name as these names are not acceptable.

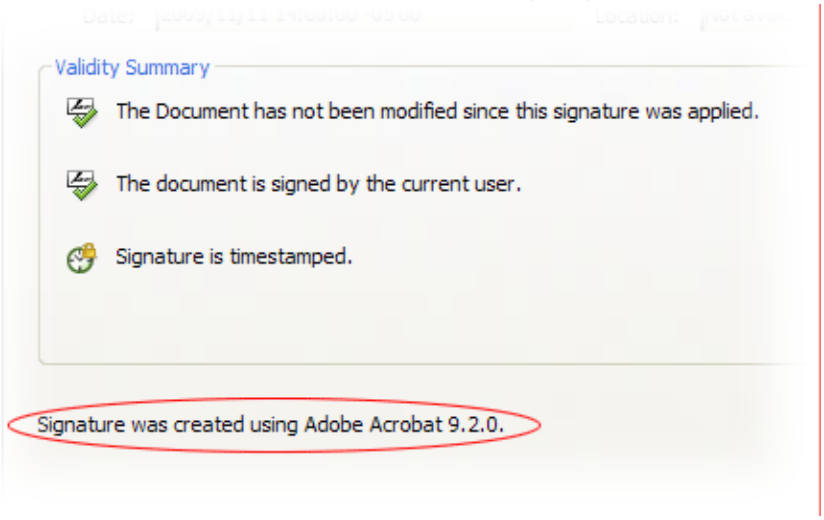
   ADDITIONAL INFORMATION: Refer to the sample signature document for a correct example.

4. Right-click the first Digital Signature in the signature panel, and then select **Show Signature Properties**.



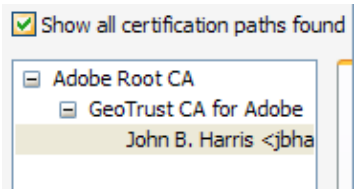
5. In the Signature Properties dialog box, be sure that it says "Signature was created using Adobe Acrobat 9.2.x" or "Signature was created using Adobe Reader 9.2.x."

   ADDITIONAL INFORMATION: The version number must be 9.2 or higher. If this states anything different, then please contact the signer and be sure to refer them to the 9.2.x version requirement when signing.



6. Click the **Show Certificate** button.

7. Ensure that the family is one that is trusted according to Adobe's requirements.



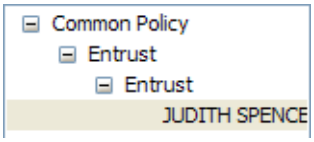
ADDITIONAL INFORMATION: In this Digital Signature, the John B Harris Digital Signature is from the Adobe Root CA family. This is a family we allow pursuant to Adobe's requirements, so this Digital Signature is valid.

Usually, the family member (in this example Adobe Root CA) can be anywhere in this family tree (hierarchy), except the bottom one (the signer him- or herself); however, the family member Adobe Root CA will always be at the top.

Other family members include:

- Common Policy
- DigiNotar Root CA X3
- GlobalSign DocumentSign CA
- KEYNECTIS ICS CA
- Staat der Nederlanden Root CA
- Staat der Nederlanden Root CA – G2
- SwissSign Platinum CA – G2
- TC TrustCenter CA 7:PN
- TC TrustCenter CA 8:PN
- VeriSign Class 3 SSP Intermediate CA

For example, if the family member is Common Policy, the hierarchy may appear as follows.



8. Select the **Revocation** tab.

9. Ensure that the response was embedded in the document. If the term **embedded** is not included in the Details section, complete steps **a** through **d**.

   a Close **Certificate Viewer** and **Signature Properties** windows.

   b Open the **Signature Panel**, and then right-click the Digital Signature that did not have information embedded.

   c Select Add Verification Information. If you are successful, you will receive a dialog box stating **Successfully added selected signature verification information**.

   d Navigate back to the **Revocation** tab and ensure that **embedded** is in the Details section. If it is not, send the document back to the sender and request that the sender confirm his/her Acrobat /Reader settings against this External Best Practices Guide, especially Appendix A of this Guide.

Checking Your Signing and Validating Environment

Every time you need to digitally sign a document you must do the following:

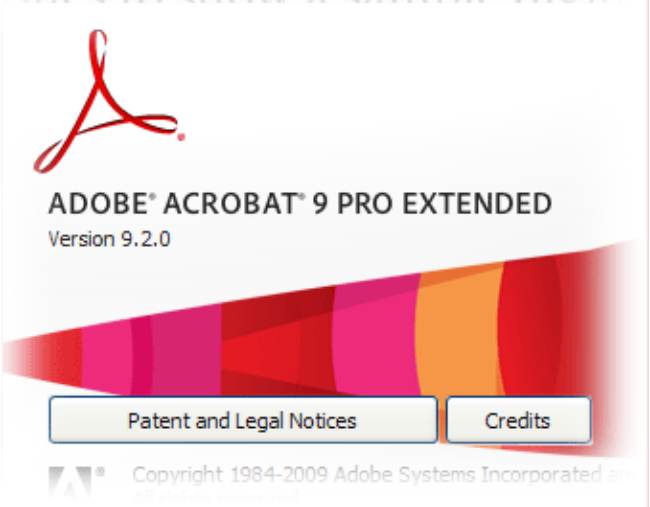
- Use Adobe Acrobat or Reader 9.2 or higher.

- Be logged into ADOBENET when signing the document. You can be inside or outside of the Adobe firewall, but you must never digitally sign a document when offline.
- Ensure the hardware device containing your CDS Digital ID is plugged into your computer before you open the file to be Digitally Signed.
- If you have changed any of your Acrobat or Reader Digital Signature preferences, you must reset them to match those below.

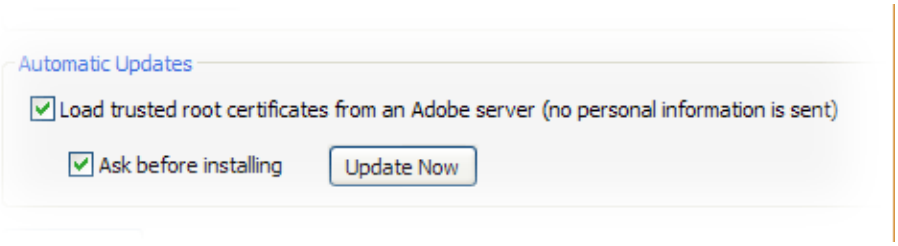
TASK

1. Confirm that you are currently using the latest version of Acrobat or Reader. To do so, launch Acrobat or Reader. **Select Help > About Adobe Acrobat**.

   STEP RESULT: You will see this dialog or one similar. Ensure it states v9.2.0 or above.

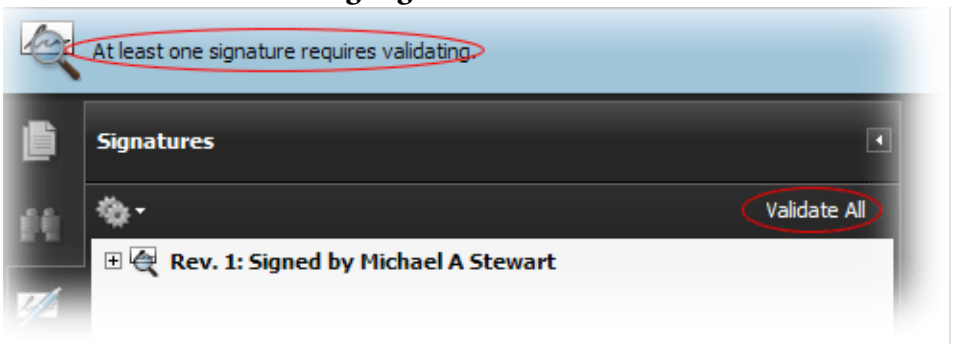


2. Ensure you have the latest version of the **Adobe Approved Trust List**. Select the Edit Menu (on Windows) or the Acrobat Menu (on Mac), and then select **Preferences** . Scroll down the Catetories and select **Trust Manager**. Ensure **Load trusted root certificates from an Adobe server** is selected. Click the **Update Now** button to download the latest version of the Trust List. Click **Yes** to allow the download to occur.



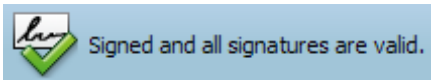
   STEP RESULT: To be sure that worked, download the PDF. If you see a green checkmark at the top of the screen, you're ready to begin.

*NOTE: If you see **At least one Digital Signature requires validating**, Click the **Signature Panel** button, and then click the **Validate All** button. Select **Do not show this message again** and then click **Yes**.*



The document will then go through a validation process. Click **OK** to complete validating all signatures.

At this point, you should see:

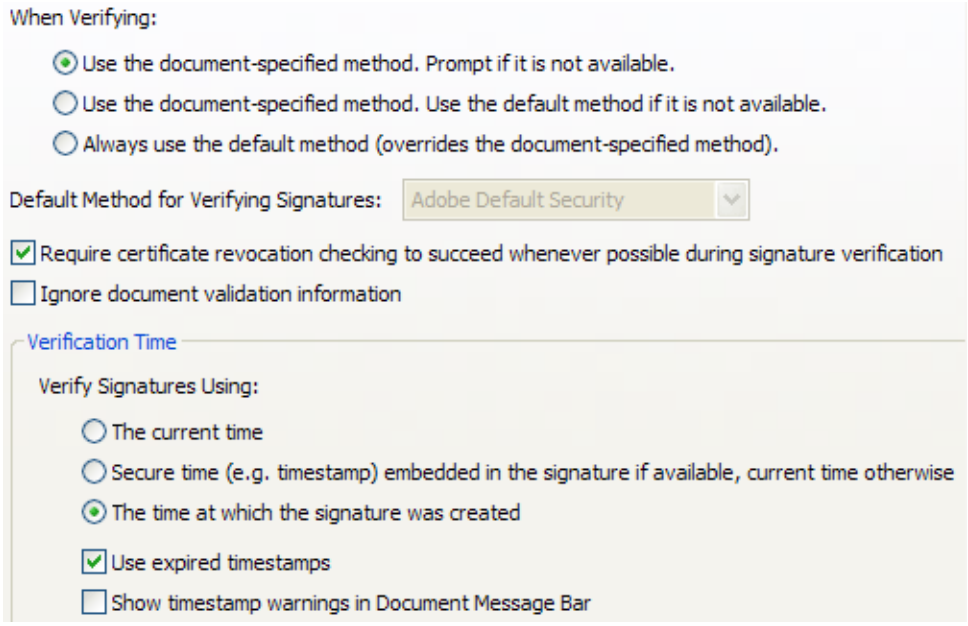


3. Ensure that your software settings are set correctly.

   a Select **Edit > Preferences**.

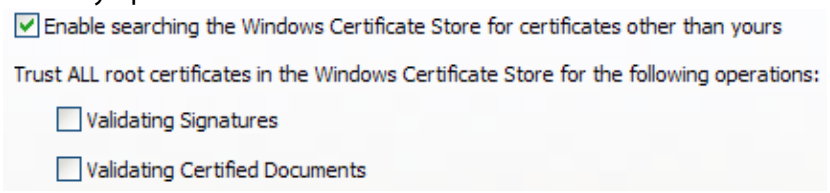
   b Select **Security** from the left side and then click the **Advanced Preferences** button.

   c Select the **Verification** tab and select the following options only:



   d Select the **Creation** tab. Ensure the **Include signature's revocation status when signing** checkbox is selected.

   e Select the **Windows Integration** tab. Ensure **Enable searching the Windows Certificate Store for certificates other than yours** is the only option selected.



   f Click **OK**.