

## Applying Custom Formatted Digital Signatures with Acrobat 7

### Introduction

In certain lines of business, such as engineering and surveying, there is a requirement for a seal to be applied to a document when it is approved. Digital signatures can provide a mechanism with stronger trust and assurance than a sealed paper document, while providing potential process improvements such as:

- Reducing or removing paper from the workflow
- Creating an approval process flow to ensure the appropriate parties see and act upon the document at the correct time
- Providing a strong third-party attestation of a time and date where the document existed, and/or was approved

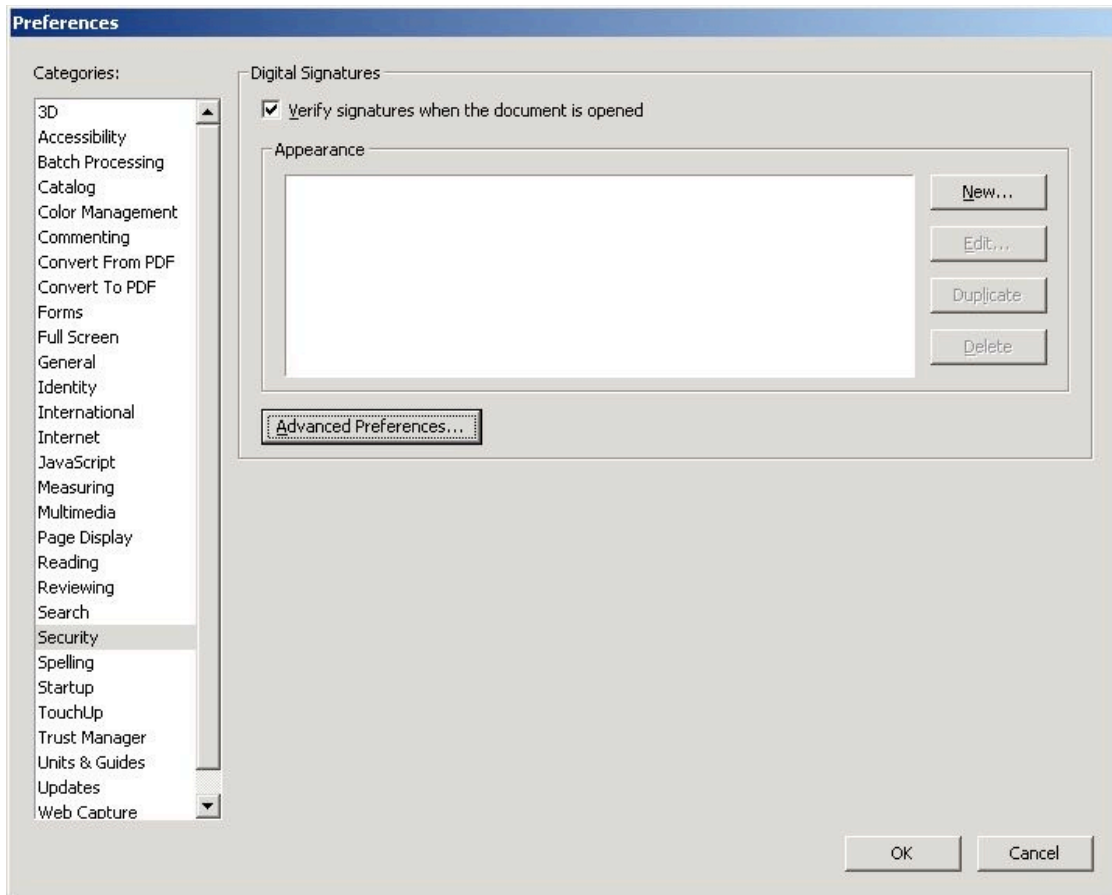
This document discusses how to set up Adobe Acrobat 7 to apply digital signatures which still have the “look” of a seal or an inked signature (provided you have an image file of the seal or signature) and some basics on applying digital signatures. The process is similar in other versions of Acrobat, although it is only available in Acrobat Standard, Professional, 3D, or Extended (not Reader).

This document does not cover how one would obtain a digital identity from their own public key infrastructure (PKI) or a service provider. For more information on that, please contact us using the information at the end of this whitepaper.

### Setting Up Your Digital Identities

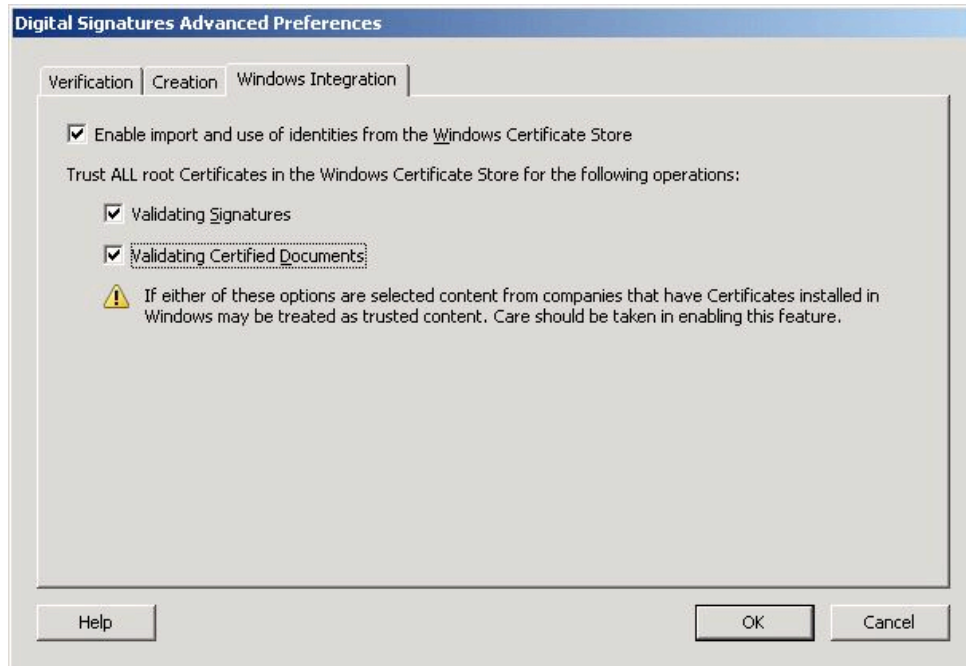
The first step in signing a document is setting up Adobe to recognize and trust your digital identities. This document assumes that your identities are set up in the Microsoft Windows Certificate Store which can be accessed from Tools->Internet Options, Content->Certificates in Internet Explorer.

First go to Edit->Preferences and select Security from the side menu. Ensure that “Verify Signatures when the document is opened” is checked.



**Figure 1 - Security Preferences**

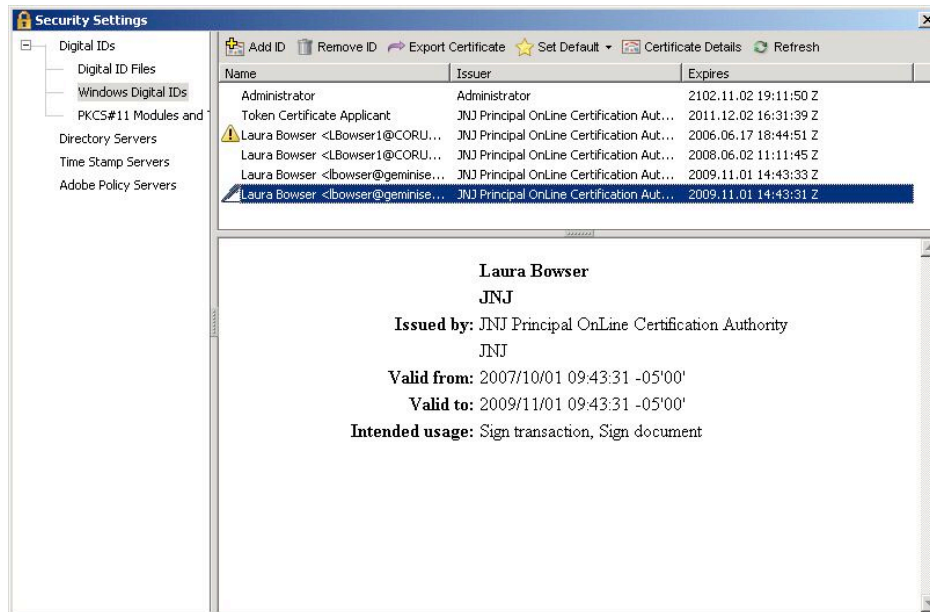
Then press the “Advanced Preferences” button to open the advanced security preferences. Make sure that all options are checked. This will allow Adobe Acrobat to use the Windows Certificate Store for certificates.



**Figure 2 - Advanced Security Preferences**

Close the Advanced Preferences Dialog, and the Preferences Dialog.

From the main menu, select Advanced->Security Settings. You should find your certificate under Windows Digital IDs. If there is a caution icon next to your Digital ID, it is not considered valid, and cannot be used to sign PDFs. You may have multiple Digital IDs, and later you will be required to choose which Digital ID to use for signing a document.



**Figure 3 - Security Settings**

After ensuring your digital ID appears in this list, you can close the Security Settings window.

## Creating a Custom Signature Appearance

In order to place an electronic image on the digital signature, you need to create a custom signature appearance. From the main menu, select Edit->Preferences, and then Security on the side menu. There will be a list of existing signature appearances. Click on “New” to create a new signature appearance, and you will see a dialog similar to Figure 4.

Give this signature appearance an appropriate title. Under Configure Graphic, you should select “Imported Graphic” and then click on the File button to select the file that contains the graphic. Under Configure Text, you should select those elements that are important for display with your signature. In this case, Name, Date, Reason, the Adobe logo, and Labels are chosen. The Preview updates with each choice, so you can see how the signature will look on the document.

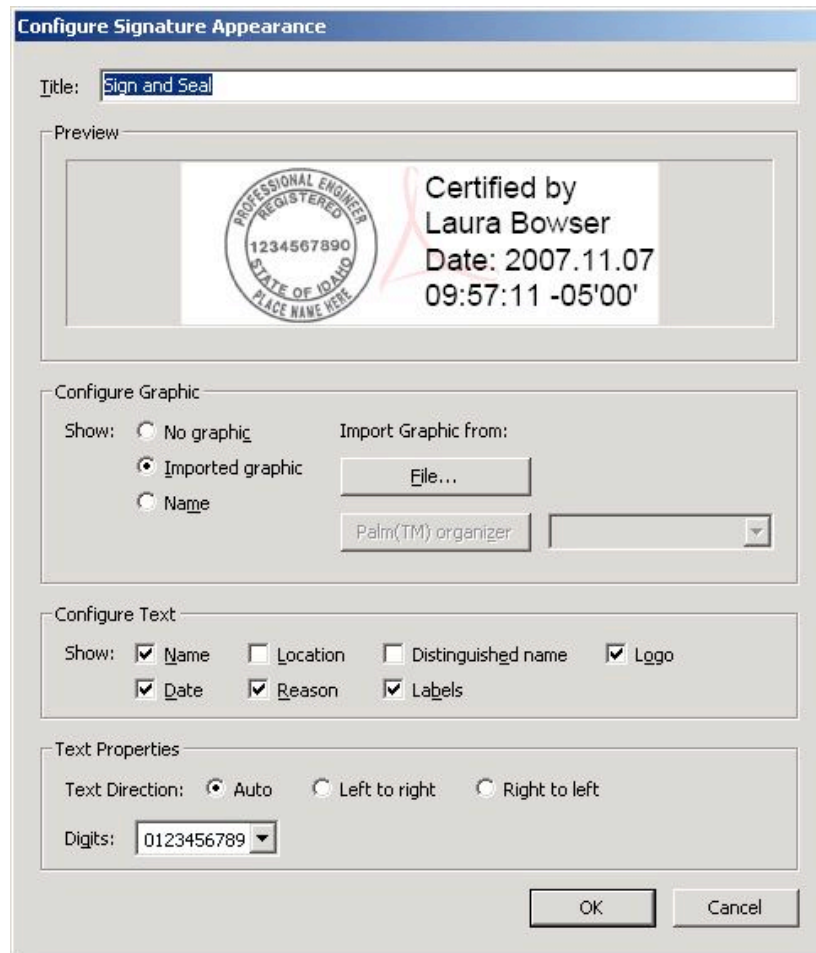


Figure 4 - Custom Signature Appearance

Once you are happy with the way the signature will look, click OK. You can now use this signature appearance to sign PDFs.

## Signing a Document

Create or open a PDF document that will be signed. From the top icon menu, select Sign->Sign this Document. If you plan on having multiple people digitally sign the document, you will want to select “Create a blank signature field” and create signature fields for each expected signature.

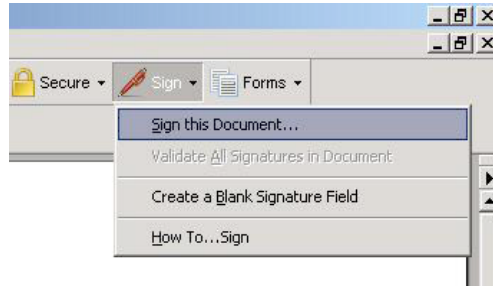


Figure 5 - Signing Menu

This will bring up a dialog asking you to whether you want to Sign or Certify the document. Certifying the document “locks” the document such that no one else can modify it (except comments and form fill-ins). If you are the author, it is suggested that you select “Certify Document”.



Figure 6 - Certification Options

When you choose to certify a document, you can set what types of actions are allowed without making the digital signature invalid. If you are the only signer of the document, it is recommended that you “Disallow and changes to the document”. If the document needs other signatures such as for final approval, you must create other signature fields before certifying the document, and select “Only allow form fill-in actions on this document” as the allowed action. If you would like people to comment on the document, you can also “Only allow commenting and form fill-in actions on this document”. In this example, we will disallow any changes to the document.

Once you’ve selected the allowed actions, Acrobat will ask you if you want to show the certification visibly on the document. In order for the digital signature to be placed on the document along with a seal or logo, select “Show Certification on document”.

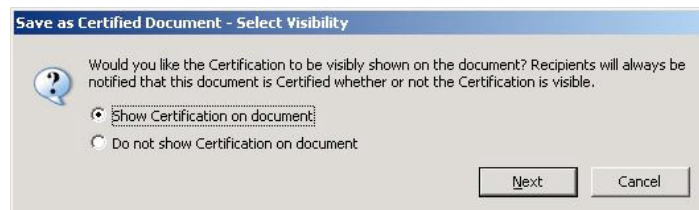


Figure 7 - Visible Certification

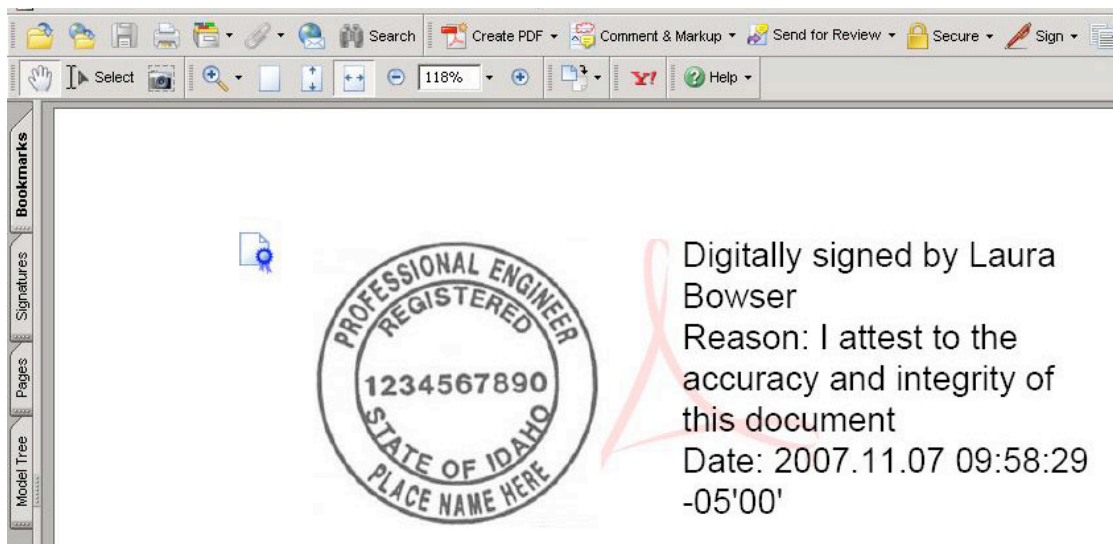
At this point, you will be asked to click and drag the area on the document where you would like the visible digital signature to appear. If there is a defined area to sign the document, you should “draw” the signature area over the document where the signature should be visible.

Once you have drawn your signature area you will see the Save as Certified Document dialog. If you have not signed a document before, you may be asked to select the Digital ID you want to use for signing. Click on “Show Options”, and under Signature Appearance, select the custom appearance you created in section 0.

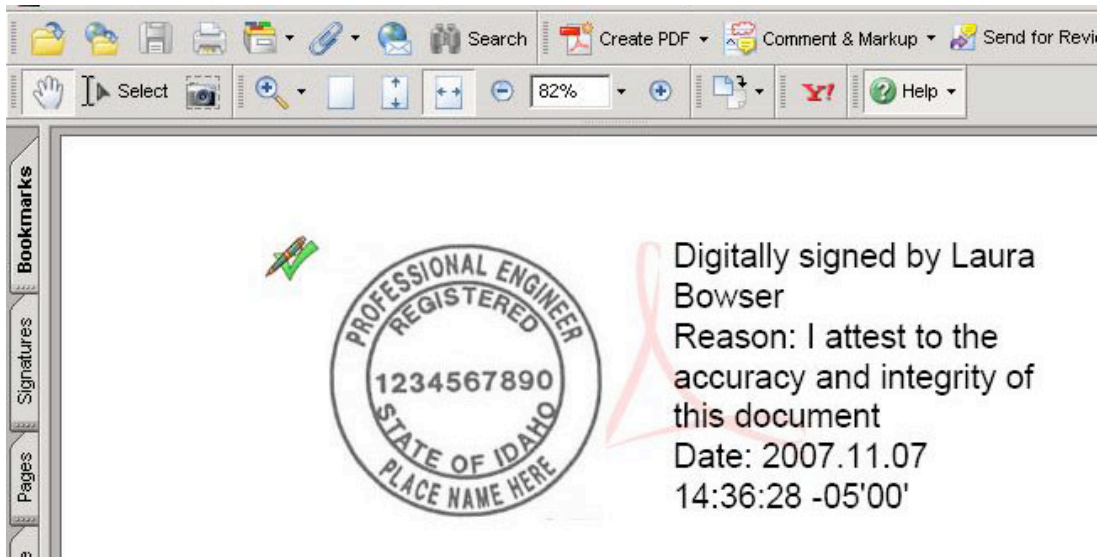
If you have a reason for signing the document, or you are subject to laws or regulations which require you to give a reason, you can select one from the drop down box. From a technical standpoint, a reason is not required for a digital signature, but reasons are sometimes required by policy.

When you have selected your reason, signature appearance, and (if desired) the location and contact information, click on “Sign and Save” or “Sign and Save As...” to save the document.

If your Digital ID needs a passphrase to be unlocked, the system will ask for one. Otherwise, you will be shown your signed document. In the upper left of the signature area will be a blue ribbon (as in Figure 8). This means that the certifying digital signature is valid. If you did not certify the digital signature, then a green check mark will be shown (as in Figure 9).



**Figure 8 - Certified Document**



**Figure 9 - Signed Document**

When other individuals who trust your Digital ID issuer open the document, they will be able to verify the signature. When a signature is verified, it means that the Digital ID used to sign the document is valid (not expired and not revoked), **and** that the document has not been modified since the signature was made.

This digital signature will be visible on any printouts, but digital signatures should only be trusted when they can be verified in their electronic form.

## **For More Information**

If you have any questions about the contents of this document, or are interested in learning more about digital signatures, or ways to reduce paper and improve processes in your organization, please contact:

Peter Hesse ([pmhesse@geminisecurity.com](mailto:pmhesse@geminisecurity.com))

Laura Raderman ([lraderman@geminisecurity.com](mailto:lraderman@geminisecurity.com))

Gemini Security Solutions, Inc.

4451 Brookfield Corporate Dr. Suite 200

Chantilly, VA 20151

703-378-5808

<http://geminisecurity.com>

## ***About Gemini Security Solutions***

Gemini Security Solutions, Inc. provides impartial information security consulting services that ensure the confidentiality, integrity, and availability of critical business information and resources. Our value is centered on our ability to deliver the right expertise and the right experience, at the right time.

Founded in 2001, and with decades of experience, our certified team of experts assists organizations to assess and deliver security solutions in compliance with business strategy, policy and regulatory requirements. Our services include risk analysis and management, regulatory compliance, identity access and management, operations security, and security software development.

Gemini Security Solutions is focused on providing big business experience with a small business approach. Working with you every step of the way, Gemini Security Solutions enables secure business operations with vigor, agility and a commitment to excellence.