AdobePress

Understand the Basics of Digital Signatures in Adobe Acrobat X

Date: May 31, 2011 By Brian Wood.

Digitally signing a document can be simple or complex, depending on how you approach it and what you expect from it. Adobe expert Brian Wood explores the generic process for digitally signing a PDF document using Acrobat X and what you can expect.

Understand the Basics of Digital Signatures

When I started working with PDFs, I remember wanting to send the file to someone and ensuring that the document didn't change and that content couldn't be removed, among other things. So I started looking into the different security features that can be added to a PDF in Acrobat. There seemed to be about a billion at first glance. Actually, generally, security on a PDF can be broken down into a few options found within Acrobat X:

- Password security (the simplest method)
- Digitally signing a document
- Certifying a document
- Using Adobe LiveCycle Rights Management

Password security is the security method most of us use when we want to ensure that content can't be copied from our PDF (among other things). Certifying a document via encryption indicates that you approve of the contents of the PDF, and only the first person to sign the document can certify it (usually the initiator). When you certify the document, you can also specify what changes can be made to the document in order for it to remain certified.

Digitally signing a document can be simple or complex, depending on how you approach it and what you expect from it. In a PDF, most digital signatures are referred to as *approval signatures*, because it's used to identify the person signing it. For most of us individuals and small business owners, it can be used not as an iron-clad legal guarantee, but as a way to see if something changed in the document.

In this article, I explore the generic process for digitally signing a document using Acrobat X and what you can expect. Please know going into this article that I am not going to cover in-depth options such as Certificate Authorities or using Adobe Certified Document Services. There is a lot of great information out there related to more "advanced" methods of signing and certifying signatures. Through the course of the article, I will mention these aspects and point to resources that I have found to be helpful.

So let's get started signing our first document. Here's a list of topics we'll cover:

- Why you might want a digital signature
- How a digital signature process works
- Create a digital ID
- Sign a document
- Discuss verifying a signature

Why Would You Use a Digital Signature?

When larger organizations and agencies distribute documents electronically, it's usually important that recipients of the PDF can verify that the content of the PDF hasn't been changed, that the document is coming from the actual person who sent it, and that an individual who has signed the document cannot deny that they signed it.

The (Generic) Digital Signature Process: What It Takes and How It Works

Here's an overview of how the digital signature process works. Details are covered in the upcoming sections.

1. **Create or obtain a digital ID**. You can create a "self-signed" ID in Acrobat or obtain one from a third-party CA (Certificate Authority). This is what you use to "sign" or encrypt the document. Typically (not always) most of us will create one digital ID and keep it to sign our documents.
2. **Sign the document**. Once a digital ID is obtained and Acrobat knows where it is, you can sign the document. You can also change the appearance of your signature to include an image or other information.
3. **Send it off to the recipient(s)**. This can be done via email or any other method you can think of to get it in someone's hands.
4. **Verify the signature (optional)**. Once the recipient has the PDF, they can verify your signature. This ensures that the document came from you. Even without verifying, they can see if anything had been changed since the initiator signed the document.

Step 1: Create a Digital ID

In order to sign a PDF, you need to have a digital ID. If you don't have one, Acrobat can create a "self-signed" ID for you that is stored on your machine (typically) forever, allowing you to use it any time you need to sign a PDF. You can also utilize either an existing solution within your company (check with IT) or use a third-party company like VeriSign® or Entrust® (among many others) to create and host your digital ID. In this article, I will show you how to create a self-signed digital ID, but in the process, you will also see how you could utilize a digital ID you get elsewhere.

1. Open a PDF that you would like to sign and make sure that before you sign it, you are finished making changes to it.

   NOTE

   After signing, Acrobat will allow you to save the file with another name if you like. That will be good for testing a signature for the first time.

2. Choose View > Tools > Sign & Certify. In the Tools task pane, you will see the Sign & Certify options.

   There are two main ways to create a digital ID in Acrobat:

   - The first time you ever sign a document, you can create a digital ID in the process.
   - Create a digital ID before you decide to sign a document.

   What Exactly Is a Digital ID?

   A digital ID contains information such as your name and email address, the name of the company that issued your digital ID, a serial number, and an expiration date. You usually only have one, like a driver's license, but you can have multiple for different signing circumstances. Essentially, it proves your identity to people that receive a document that you have signed digitally.

Digital IDs are made up of two keys:

- *The public key* that locks, or encrypts, data.
- The *private key* that unlocks, or decrypts, that data.

When you sign PDF documents, the private key applies your digital signature. You distribute the certificate that contains your public key and other identifying information to those who need to validate your signature, verify your identity, or encrypt information for you. Only your private key can unlock information that was encrypted using your certificate, so be sure to store your digital ID in a safe place.

In this article, we will save a little time by signing a document and setting up a digital ID in one step.

3. Click Sign Document in the Tools task pane. A dialog box appears asking you to draw where you would like the signature to appear (see Figure 1).

Figure 1 Click to draw a signature

NOTE

What is the difference between *Sign Document* and *Place Signature*? The Sign Document option can be used if you are signing a document that has a digital signature fillable field already. The Place Signature option is used if you want to sign somewhere besides where a digital signature field is or if there is no digital signature field. You can use Sign Document to add a digital signature even if there is no digital signature fillable field.

TIP

If you want to sign a document and add a reason for signing, location, and contact information when signing (included in the signature), you need to set that first—before signing. Choose Edit > Preferences (Windows) or Acrobat > Preferences (Mac OS) and select the Security category. Click the Advanced Preferences button and select the Creation tab. Select the Show Reasons… and/or Show Location… option and click OK, then OK.

4. In the PDF, navigate to the page where you want to place the signature. Click and drag to draw a signature area (see Figure 2). Make sure that it is big enough to be readily visible and contain some information like your name, date, etc. because you can't edit the size once you are finished. You'll see what I mean shortly.

Figure 2 Click and drag where the signature is to appear

TIP

You can add an image of your actual signature to the signature area. Think about that when you are drawing the signature area.

5. In the Add Digital ID dialog box, select A New Digital ID I Want to Create Now (see Figure 3). Click Next.

Figure 3 Create a new digital ID

If you already created a self-signed ID in Acrobat (we've gone through this process before), you could also just choose the file at this point by selecting A File from My Existing Digital ID From:. If you have a digital ID from a company such as VeriSign or other), you can choose A Roaming Digital ID Accessed Via a Server, and enter the URL of the digital ID that they give you. If you store your digital ID on a smart card or hardware token, connect it to your device to use it for signing documents, and choose A Device Connected to This Computer.

6. Next, you need to decide where to store the digital ID. If you are on Windows, you will see a choice between New PKCS#12 Digital ID File and Windows Certificate Store. If you are on Mac OS, you won't see these options, so you can skip this step. Make sure that New PKCS#12 Digital ID File is selected (Windows only). This allows you to create your digital ID as a .pfx or .p12 file that is saved on your hard drive. If you want to save the digital ID in your certificate store, which means it can be accessed by more than Acrobat, select Windows Certificate Store (see Figure 4). Click Next.

Figure 4 Decide where to store the digital ID

7. Enter your personal information in the next screen (things like full name, email address, etc.; the organizational unit and organization name is not required for the creation of your digital ID). Leave the Key Algorithm option at its default setting. Although 2048-bit RSA is more secure, 1024-bit RSA is more universally accepted. You could also choose what you want to use this digital ID for from the "Use Digital ID For menu. This allows you to sign documents, encrypt data, or both. Leave it at the default setting and click Next (see Figure 5).

Figure 5 Enter your personal information

NOTE

Enable Unicode Support is for extended characters (things like #, &, ^, etc.). If you select this option, you can type the Unicode values in the boxes that appear to the right of the original fields.

8. Next, you need to decide where to store the actual digital ID file. If you leave it in the default folder, Acrobat can easily find it; however, you can choose a different location if you like because you can later tell Acrobat where it is when you go to sign a document. Enter a strong password and click Finish (see Figure 6).

Figure 6 Decide where to store the digital ID

TIP

Make note of the folder where the digital ID is stored. You may want to make a copy of it and store it somewhere safe.

NOTE

Acrobat stores the digital ID information in a file, which has a .pfx extension in Windows and .p12 in Mac OS. The files can be used interchangeably between operating systems. If you move a file from one operating system to another, Acrobat still recognizes it.

Step 2: Sign the Document

Now that the digital ID is created (you won't have to do that again if you keep the self-signed ID you just created), the next step is to sign the document. The Sign Document dialog box immediately appears after clicking Finish. In there, you can choose which digital ID to use and change the appearance of the signature in the document.

1. In the Sign Document dialog box, make sure that your digital ID name (mine is "Brian Wood") appears in the Sign As menu. Notice that clicking that menu reveals you can make another digital ID. Enter the password you just created.

Figure 7 Edit the Sign As content

2. Click the Info button, and you will see all of the information related to the digital ID you just created (see Figure 8). Click OK.

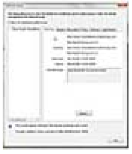

Figure 8 View the certificate created

A preview of what the digital signature will look like in your document shows just below the Appearance menu. You can edit that and then save the appearance so next time you can easily apply it.

3. Choose Create New Appearance from the Appearance menu. In the Configure Signature Appearance dialog box, you need to give this appearance a title so you can choose it later by name (see Figure 9).

Figure 9 Create a new digital ID appearance

4. In the Configure Graphic options, select No Graphic if you want to remove your large name from the signature and select Name for it to appear again. If you want to put a company logo—or better yet, a picture of your actual signature (which is what I do)—you can select Imported Graphic and click the File button to choose it. Of course, you need to have made the image in another application such as Adobe Photoshop. In the Select Picture dialog box, click Browse. Choose the file type (like GIF) from the File Type menu, then select the image and click Open. Click OK in the Select Picture dialog box (see Figure 10). The image will appear in the signature preview now.

Figure 10 Add a graphic to your signature

TIP

If you want the image to have a transparent background, make sure you save the image with transparency using GIF, PDF, or PNG as example file formats. To learn more about setting the appearance of a signature visit, go to the Adobe website and click on the Sample Signatures link.

TIP

Any signature appearances you save using the method above can be accessed later on by choosing Edit > Preferences (Windows) or Acrobat > Preferences (Mac OS) and selecting the Security option on the left of the Preferences dialog box. You can create new appearances in here or delete any existing ones.

5. If you want to have just the image showing, you can deselect what to show in the Configure Text options.
6. In the Text Properties options, choose which way the text is to read, left to right or right to left. You can also choose how the digits appear in the Digits menu (see Figure 11). Click OK.

Figure 11 Finish editing the signature appearance

7. Back in the Sign Document dialog box, the last option you can select is Lock Document After Signing. Select this only if you are the last person to digitally sign this document because it locks all of the fields in the document. Click OK to sign the document.
8. In the Save As dialog box, save the PDF with a different name (advised in some cases) and click Save. The signature will appear on the page (see Figure 12).

Figure 12 The signature as it appears on the page

Now that the document is signed, let's take a look at where you can see that digital ID you created.

1. In the Tools task pane, choose Security Settings from the More Sign & Certify menu. This opens the Security Settings dialog box (see Figure 13). This is the home for your stored digital IDs (that Acrobat knows about) and other features such as timestamp servers and Adobe LiveCycle Rights servers. We are just going to focus on the digital IDs.

   Figure 13 The Security Settings dialog box

2. Select the digital ID listed and click Certificate Details. This shows you the same information as when you clicked the Info button in the Sign Document dialog box. Click on the tabs towards the top of the dialog box to see all of the information available. Click OK.

   Notice that back in the Security Settings dialog box, you can also add another digital ID, delete any listed, change the usage options for a digital ID, and export.

3. With your digital ID selected in the list (it's the only one at this point), click Usage Options. Notice that you can designate when this ID is used. You can even apply more than one usage. For instance, suppose you have multiple digital IDs, and you want to use the selected one for signing, not certifying. Choose Use for Signing and when you digitally sign a document; this ID will be used (see Figure 14).

   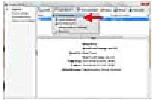

   Figure 14 Set the digital ID usage options

4. Click Export, and you will see a dialog box explaining that you can export your public certificate so that others can validate your signature (see Figure 15). While this can be an important step in some processes, you won't export in this case. Click Cancel and close the Security Settings dialog box.

   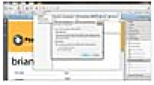

   Figure 15 Export your public certificate (key)

5. Close the Security Settings dialog box.

Notice the blue message bar along the top of the document. This indicates whether the signature is valid or not (since you signed it, this PDF is valid). Click the Signature Panel button in the message bar and you will see information on the left, similar to what you've seen so far (see Figure 16).

Figure 16 The Signature Panel

Step 3: Verify the Signature

Suppose you send this document to someone else. When she opens the PDF file, the blue message bar will appear indicating that at least one signature has a problem. If she was to click on the signature area, a dialog box would appear indicating that the signature validity is unknown (see Figure 17). It indicates that the document hasn't been changed since it was signed (which is good), but that her identity hasn't been added to your list of trusted identities. *What does that mean*?

Figure 17 A signature that is not valid

In order to truly validate a signature, the recipient needs the public certificate (key) to match against the private key data used to sign the document. This public certificate (key) is sent or requested, in a simpler self-sign workflow, via email as an FDF file. The recipient then adds that file to their Reader or Acrobat list of trusted identities (Tools > Sign & Certify > More Sign & Certify > Manage Trusted Identities) and the certificate is stored. Acrobat allows the user to create a list of trusted identities, store her contact and certificate information, and set different trust levels for each identity. Users can obtain and exchange certificates by one of three methods:

- Exchange a public certificate (key) as an FDF file by e-mail or a shared network folder
- Extract data embedded in a signed document
- Search a directory server that contains the required certificates

To learn more about the signature validation process and the different methods you can use, check out the Adobe blogs.

Final Thoughts

Well, there you have it—a simpler self-signing digital signature workflow with Acrobat. Like I stated in the beginning of this article, there are many ways to work with digital signatures, from a simple stamp that has a picture of your signature to using a certificate authority (CA) or other to sign and certify documents.

Because there is so much more we could go over, I wanted to offer some of the great resources that Adobe has available:

- If you are looking for a digital signing solution that allows authors to create Adobe PDF files that automatically certify to the recipient that the author’s identity has been verified by a trusted organization, you need to check out Adobe Certified Document Services.
- If you are looking for all sorts of further information on digital signatures, head over to the Adobe Developer Center.
- Another great resource for digital signatures is the document library over at the Adobe Developer Connection.

1301 Sansome Street, San Francisco, CA 94111