

You can secure a PDF using any of the following security methods:

- Add passwords and set security options to restrict opening, editing, and printing PDFs.
- Encrypt a document so that only a specified set of users has access to it.
- **NOTE: the passwords control who can open the document or change the restrictions, the restrictions cannot be bypassed using a password. RCC**



From the author of

Adobe Acrobat 9 Classroom in a Book

<http://www.peachpit.com/articles/article.aspx?p=1272495>

Creating Digital Signatures

For this exercise, you'll use a self-signed digital ID, which is often adequate for signing documents within a corporate environment. In the Security preferences, you can set the appearance of your digital signature, select your preferred digital signature signing method, and determine how digital signatures are verified. Before you open a signed document, you should also set your preferences to optimize Acrobat for validating signatures.

1. Start Acrobat.
2. Choose Edit > Preferences (Mac OS: Acrobat > Preferences), and select Security in the left pane. You may need to scroll down the list.

Adding Images to Your Digital Signatures

First you'll add the company logo to your signature block.

1. In the Preferences dialog box, click New to open the Configure Signature Appearance dialog box. This is where you can personalize your digital signature by adding a graphic. For the moment, the Preview pane shows the default digital signature appearance, which is text-based (see Figure 1).



Figure 1

First you'll name the appearance of your signature and then add your corporate logo to the signature block.

2. In the Title text box, enter a name for the appearance of your signature. We entered Logo because we're going to add our corporate logo to the signature line. You should use a name that's easy to associate with the contents of the signature appearance. You can create several digital signatures for yourself.
3. In the Configure Graphic section of the dialog box, select the Imported Graphic option, and click File (see Figure 2).



Figure 2

4. In the Select Picture dialog box, click Browse, and select the Clarity_Logo.pdf file in the Lesson08 folder. Click Select, and then click OK to return to the Configure Signature Appearance dialog box (see Figure 3).

NOTE

Supported file types are listed in the Files of Type (Mac OS: Show) menu.



Figure 3

Now you'll specify the information to be included in the text block of your signature. You'll include your name, the reason for signing the document, and the date.

5. In the Configure Text area of the Configure Signature Appearance dialog box, leave Name, Date, and Reason selected. Deselect all the other options (see Figure 4).



Figure 4

6. When you're happy with the preview of your signature block, click OK.
7. In the Preferences dialog box, select "View documents in preview document mode when signing."
8. Click Advanced Preferences, and click the Creation tab. Select the "Show reasons when signing" option, and click OK (see Figure 5).



Figure 5

Signing in Preview Document Mode

Use the Preview Document mode when you want to analyze a document for content that may alter the appearance of the document after you sign it. Such content may include transparency, scripts, fonts, and other dynamic content that can alter a document's appearance. The Preview Document mode suppresses this dynamic content, allowing you to view and sign the document in a static and secure state.

When you view a PDF in Preview Document mode, a document message bar lets you know whether the PDF complies with the PDF/SigQ Level A or Level B specification. Level A indicates that the document contains no dynamic content that can alter its appearance. Level B indicates that the document contains dynamic content that can be suppressed during signing. If the document doesn't comply with Level A or B, you may want to refrain from signing the document and contact the document author about the problem.

You can use Preview Document mode to check the integrity of a document at any time.

Acrobat automatically runs the Document Integrity Checker, which checks for Qualified Signatures conformance, before entering the signature preview mode.

You opt to use the Preview Document mode in the Security preferences.

Selecting a Signing Method

Now you'll specify a default signing method.

1. Click the Advanced Preferences button in the Security pane of the Preferences dialog box again.

On the Verification tab of the Digital Signatures Advanced Preferences dialog box, notice that "Require certificate revocation checking to succeed whenever possible during signatures verification" is selected (see Figure 6). This option ensures that certificates are always checked against a list of excluded certificates during validation.



Figure 6

2. Make sure that the first verification option is selected. ("Use the document-specified method. Prompt if it is not available.") You'll be prompted if you don't have the necessary software when you try to open a document.

Also on the Verification tab is a pop-up menu allowing you to choose the default method for verifying signatures. This menu is dimmed unless you change the verification method by selecting a different radio button. On the Creation tab, you set the default method to be used when signing and encrypting documents.

3. Click the Creation tab and check that Adobe Default Security is selected for the "Default method to use when signing and encrypting documents" option.

On Windows, you also have a Windows Integration tab where you can specify whether identities from Windows certificates can be imported and whether all root certificates in the Windows certificates can be trusted. We recommend that you leave the default settings on this tab.

4. Click OK, and click OK again to close the Preferences dialog box.

Creating Digital IDs

A digital ID is like a driver's license or passport. It proves your identity to people with whom you communicate electronically. A digital ID usually contains your name and email address, the name of the company that issued your digital ID, a serial number, and an expiration date.

A digital ID lets you create a digital signature or decrypt a PDF document that has been encrypted. You can create more than one digital ID to reflect different roles in your life. For this section of the exercise, you'll create a digital ID for T. Simpson, Director of Advertising.

1. Choose Advanced > Security Settings.
2. In the Security Settings dialog box, select Digital IDs in the left pane. Then click the Add ID button (see Figure 7).



You'll create a self-signed digital ID. With a self-signed ID, you share your signature information with other users by using a public certificate. (A certificate is a confirmation of your digital ID and contains information used to protect data.) While this method is adequate for most unofficial exchanges, a more secure approach is to obtain a digital ID from a third-party provider.

3. In the Add Digital ID dialog box, select "A new digital ID I want to create now." Click Next.

If you're working in Mac OS, skip to step 5. If you're working in Windows, you'll choose where to store your digital ID. The **PKCS #12** digital ID file option stores the information in a file that you can share with others. A Windows default certificate digital ID is stored in the Windows certificate store. Because you want to share your digital ID with colleagues, you'll use the PKCS #12 option.

4. Make sure that New PKCS #12 Digital File ID is selected, and click Next.

Now you'll enter your personal information.

5. Enter the name you want to appear in the Signatures tab and in any signature field that you complete, and enter a corporate or organization name (if necessary) and an email address. Example: T. Simpson, Director for the name, Clarity for the organization name, and clarity@xyz.net for the email address. Make sure that you select a country/region. We used the default US - United States.
6. Choose a key algorithm to set the level of security. We chose the default 1024-bit RSA. Although 2048-bit RSA offers more security protection, it's not as universally compatible as 1024-bit RSA.

Now you'll specify how the encryption is applied. You can use the digital ID to control digital signatures, data encryption (security), or both. When you encrypt a PDF document, you specify a list of recipients from your trusted identities, and you

define the recipient's level of access to the file—for example, whether recipients can edit, copy, or print the files. You can also encrypt documents by using security policies.

For this exercise, you'll choose digital signatures.

7. From the "Use digital ID for" drop-down list, choose Digital Signatures, and then click Next (see Figure 8).



Figure 8

Now you'll save and safeguard your information.

8. If you want to change the location where your information is stored, click the Browse button and locate the required folder. For this exercise, you'll use the default. Now you must set a password. We used Lotion123 as the password. Reenter your password to confirm it.

NOTE

Remember that the password is case-sensitive. Be sure to make a note of your password and keep it in a safe place. You cannot use or access your digital ID without this password. Your password cannot contain double quotation marks ([dp][dp]) or any of the following characters:

! @ # \$ % ^ & * , | \ ; < > _

9. Click Finish to save the digital ID file in the Security folder (see Figure 9).



Figure 9

Your new digital ID appears in the Security Settings dialog box. In Windows, select the digital ID to see its details. In Mac OS, double-click it to view the certificate details. When you've finished checking your digital ID, click Close to close the dialog box.

Sharing Certificates with Other People

Your digital ID includes a certificate that other people need in order to validate your digital signature and to encrypt documents for you. If you know that others will need your certificate, you can send it in advance to avoid delays when exchanging secure documents. Businesses that use certificates to identify participants in secure workflows often store certificates on a directory server that participants can search to expand their list of trusted identities.

If you use a third-party security method, you usually don't need to share your certificate with others. Third-party providers may validate identities using other methods, or these validation methods may be integrated with Acrobat. See the documentation for the third-party provider.

When you receive a certificate from someone, that person's name is added to your list of trusted identities as a contact. Contacts are usually associated with one or more certificates and can be edited, removed, or reassociated with another certificate. If you trust a contact, you can set your trust settings to trust all digital signatures and certified documents created with that certificate.

You can also import certificates from a certificate store, such as the Windows certificate store. A certificate store may contain numerous certificates issued by different certification authorities.

Now you'll sign the advertisement and return it to the agency.

Signing the Advertisement

Because you want the advertising agency to know that the changes to this advertisement are approved and no additional changes have been made since the time you approved it, you'll create a visible signature field and sign the document.

1. Click the Sign button on the Tasks toolbar, and choose Place Signature from the menu.
2. Acrobat reminds you that you need to create a signature field. Click OK to close the alert box, and drag to create a signature field. We dragged a signature field in the area below the headline (see Figure 10).



Figure 10

Acrobat automatically switches into the Preview mode, which analyzes the document for content that may alter the document's appearance and then suppresses that content, allowing you to view and sign the document in a static and secure state.

3. In the preview toolbar, click Sign Document.
4. In the Sign As text box in the Sign Document dialog box, enter the password associated with the ID. We entered Lotion123 (see Figure 11).
5. For Appearance, select Logo.
6. If desired, add a reason for signing the document.
7. Click Sign to apply your signature, and click Save to save the signed file.



Figure 11

The recipient of the signed document will need your signer's certificate to validate the digital signature (see [Figure 12](#)).



Figure 12

Modifying Signed Documents

Now you'll add a comment to the signed document to see how the digital signature information changes. But first you'll look at the signatures panel to see what a valid signature looks like.

1. Click the Signatures button in the navigation pane to display the Signatures panel. If necessary, drag the right margin of the Signatures panel so that you can see all of the signature information. Expand the signature line, and expand both the "Signature is valid" and "Signature Details" entries (see [Figure 13](#)).



Figure 13

Now you'll add a note to the advertisement and see how the addition changes the digital signature.

2. Choose Tools > Comment & Markup > Sticky Note.
3. Click anywhere on the document page to add a note. We added a note saying Good work (see [Figure 14](#)).



Figure 14

The signature status is changed by the addition of a note. If necessary, expand the signature again to see the status.

As soon as you add the note, that fact is recorded in the Signature panel.

TIP

Use the Signature panel to review the change history of a document or to track changes when a document is signed using multiple digital signature IDs.

Now you'll validate the signature.

4. Right-click (Mac OS: Control-click) the signature box in the document pane, and choose Validate Signature (see [Figure 15](#)).



Figure 15

5. The alert box explains that although the signature is valid, a change has been made. Click Close to close the warning box (see Figure 16).



Figure 16

6. Right-click (Mac OS: Control-click) the signature box in the document pane, and choose View Signed Version. This option allows you to recover your unchanged file. If a document has signatures on multiple versions of the document, for example, you can view any previously signed version of the document by selecting the signature in the Signatures tab and then choosing View Signed Version from the Options menu.
7. Close both files. You don't need to save your work.

TIP

Right-click (Mac: Control-click) the signature box in the document pane, and choose Show Signature Properties to resolve any issues with the signature.