Digitally Signing PDF Files

The digital signatures feature in Acrobat offers much more than the ability to "sign" a document to indicate that you have read and approved it, for example.

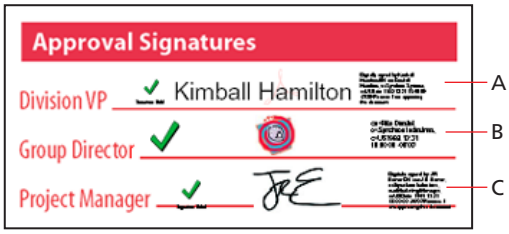
- You can digitally sign a document to ensure that any changes you make to the document are preserved. If any changes are made to the document after you sign it, you can roll back to recover the version that you signed.
- You can verify another person's digital signature to verify that their signature is authentic. The verification process uses a user certificate that the signer makes available to you.
- You can review all the signatures on a document in the Signatures palette, you can retrieve any signed version of a document, and you can use the Compare Two Versions Within a Signed Document command to compare different versions of a signed document.
- You can create different identities (digital signatures) for yourself if you handle documents in more than one capacity.
- You can create a signature that uses or includes a graphic such as your company logo.

The encryption feature also allows you to encrypt a PDF document for distribution to selected recipients. For more information, see "Encrypting PDF files" on page 192.

About using digital signatures

A digital signature, like a conventional handwritten signature, identifies a person or entity signing a document. Unlike traditional signatures on paper, however, each digital signature stores information "behind the scenes" about the person signing and about the exact state of the document when it was signed.

What your signature looks like. A digital signature can have any one of several formats—a handwritten name, a logo or other graphic, or simply text explaining the purpose of the signing. Depending on your signature handler, a signature may even be invisible. (It is important to remember that the appearance of a signature is just its representation on the page and is not the actual electronic signature information.)



Signature formats
A. Text signature **B.** Graphic signature
C. Handwritten name signature

Signing a document. Before you can digitally sign a document for the first time, you must choose a signature handler (if you have more than one installed). If you haven't installed any additional signature handlers, Acrobat Self-Sign Security will be used as the default signature handler. If Acrobat Self-Sign Security is your signature handler, you must also create a password-protected profile within the signature handler before you can sign.

Verifying someone else's signature. When you receive a document signed by a third party, you should verify the signature to ensure that the document was indeed signed by that person and has not been altered since it was signed. To verify the signature of a third party, you need to import their user certificate. They can e-mail you their user certificate, or they can store it in a shared folder from which you can copy it. Similarly, if you send a signed document to a third party, you should e-mail them a copy of your certificate so that they can verify your signature. Alternatively, you can put a copy of your certificate in a shared folder.

Checking a document for changes made since it was signed. Once a document is signed, any changes made since the signing are recorded in the Signatures palette. You can track changes made between signings using the Signatures palette or by comparing signed versions of the document.

Comparing versions of signed documents. You can easily see changes made between two signed versions of a document using the Compare Two Versions Within a Signed Document command. Acrobat will display the pages of the document side-by-side and highlight the differences between the two documents.

Selecting a signature handler

The digital signatures feature in Acrobat uses a signature handler plug-in. You add, verify, and manage your signatures using commands and tools in the Acrobat interface, but the signature handler plug-in determines the nature of the signatures—their appearance on the page, the exact information stored in them, and the attributes and method used for their verification. The flexibility of this structure allows you to use whichever signing method your company or regulations require, with Acrobat providing a consistent and convenient front end.

Acrobat comes with the default signature handler Acrobat Self-Sign Security for basic signing purposes. Self-Sign Security is included in the default Acrobat installation. Third-party signature handlers are available on the Acrobat CD for custom installation (Windows). For information on compatible handlers from third-party vendors, see the Security folder on the Acrobat CD and the Adobe Web site (www.adobe.com).

Setting a default signature handler

You set your default signature handler in the Digital Signatures Preferences dialog box.

To set your default signature handler:

1 Choose Edit > Preferences > General. Click Digital Signatures in the left pane of the Preferences dialog box.

2 Choose a default signature handler. The pop-up menu lists all handlers installed in your Acrobat Plug-ins folder (the default is Acrobat Self-Sign Security).

3 Select Verify Signatures When Document Is Opened to determine if signatures will be verified automatically when a document is opened.

4 Click OK.

About Acrobat Self-Sign Security

Acrobat Self-Sign Security, the default Acrobat signature handler, provides a quick and easy method of signing documents using a private/public key (PPK) system to verify the authenticity of signatures and the integrity of signed document versions. (This is a direct-trust system.) You can also use Acrobat Self-Sign Security to encrypt PDF files, as described in "Encrypting PDF files" on page 192.

In Acrobat Self-Sign Security, each signature is associated with a profile that contains unique security data—a private key and a public key. The private key is a password-protected numerical value that allows the user to sign a document. The *public key* is embedded in the digital signature and is used to mathematically verify digital signatures when the signatures are verified. The private key encrypts a checksum that is stored with a signature when you sign; the public key decrypts the checksum when you verify. (Acrobat Self-Sign Security uses the RSA algorithm for generating private/public key pairs and the X.509 standard for certificates.)

Because other users must have access to your public key to verify your signature, your public key is contained in a *certificate* that can be shared. (See "Managing user certificates" on page 205.) This system of sharing certificates used by Acrobat Self-Sign Security is referred to as *direct-trust*, which means that you share directly with other users rather than going through a third-party agent.

Note: *Acrobat Self-Sign Security does not include a public-key infrastructure with third-party certification and is not intended to serve all signing purposes. See the Security folder on the Acrobat CD or the Adobe Web site (www.adobe.com) for information on signature handlers with more advanced features.*

Setting up profiles in Acrobat Self-Sign Security

Before you can sign documents with Acrobat Self-Sign Security, you must set up a profile—a password-protected file—containing your name, your password, and other basic attributes. You may want to create more than one profile if you sign documents in different roles.

Creating profiles

Your profile file stores your private key (encrypted), your public key (wrapped in a certificate), your list of trusted certificates (certificates of other users), and a time-out value representing when a password is required for signing. The name of the file is the profile name you provide, plus the extension .apf.

Important: *Always make a backup copy of your profile file. If your profile file is lost or corrupted, or if you forget your password, you cannot add or verify signatures with that profile. (See "Backing up your profiles" on page 198.)*

To create a profile:

1 Assuming you are not already logged in to a profile, do one of the following:

- Choose Tools > Self-Sign Security > Log In.
- Choose Tools > Digital Signatures > Sign Document. Click OK in the Digital Signatures Alert dialog box, and drag on the page to create a signature box.

- Select the digital signature tool, and drag to create a signature box.

2 In the Log In dialog box, click New User Profile.

3 In the Create New User dialog box, enter a name for your user profile. Do not use accented characters or any of the following characters: ! @ # $ % ^ & *, double quotation marks, and | \ ; < > _. When you add a signature to a document, this user profile name is the name you'll see in the Signatures palette. It is also the name that will appear in the signature field.

4 Enter a password containing at least six characters. You need to enter the same password in both the User Password and Confirm Password text boxes.

5 Click OK.

6 Click Save. The default location for saving your profile file is the Acrobat Preferences folder (Windows) or the Adobe Acrobat 5.0 folder (Mac OS).

7 Do one of the following:

- Click OK to end the profile creation process.
- Click User Settings to change the profile's password, and password options, to set the appearance of your signature, to configure picture appearances, or to add certificates to your list of trusted certificates.

Backing up your profiles

Acrobat Self-Sign Security does not automatically back up your profiles. You should create a backup file whenever you create a new profile.

To back up your profile:

1 Choose Tools > Self-Sign Security > User Settings. (You must be logged into your profile.)

2 In the User Settings dialog box, select User Information in the left panel.

3 For Profile File, click Backup. Browse to select a location for your backup file, and click OK (Windows) or Backup (Mac OS).

4 Click Close.

Adding graphics to signatures

You can use a picture or a combination of graphics and words as your digital signature. You might want to include your company logo or use an image of your handwritten signature. The amount and type of information that can be contained in a digital signature also means that it can meet legal requirements.

You can also write text on a Palm organizer, store the text as a picture, and then use the picture in a digital signature. Most often, the text is a handwritten signature, but you can also use this feature to create a short handwritten message or a freehand drawing to appear with digital signatures. Acrobat provides an application to use for writing text on your Palm organizer. For information, see the Adobe Web site (www.adobe.com).

To add a picture to a signature:

1 Create or import a picture from any authoring application, place the graphic on a page *by itself*, and convert the file to PDF.

When you use the picture in a signature, Acrobat Self-Sign Security copies only the picture out of the page, not the white space around it. Self-Sign Security crops and scales the picture to fit in the signature field.

2 Log in to Acrobat Self-Sign Security as described in "Logging in to a profile" on page 201, and choose Tools > Self-Sign Security > User Settings**.**

3 Select Signature Appearance in the left pane of the User Settings dialog box, and click New.

4 In the Configure Signature Appearance dialog box, enter a title for the picture. Your current signature is shown in the preview box.

Note: *When you sign a document later, you'll select the picture by its title, so use a short title that describes the image accurately.*

5 For Configure Graphic, select Imported Graphic and click PDF File.

6 In the Select Picture dialog box, click Browse to locate the file. (Your picture file must be in PDF format.) Click OK (Windows) or Open (Mac OS).

Note: *The Palm Organizer button will be grayed out unless Acrobat Self-Sign Security Security detects that Palm Organizer files are present. For information on importing graphics created on Palm Organizers, see the Adobe Web site (www.adobe.com).*

7 In the Configure Text panel, select any text items you want to appear with the picture on document pages:

- Distinguished Name to show the user attributes defined in the profile, which may include common name, organization, and country.
- Labels to display labels such as *Signed by, Date,* and *Reason* with any text in the signature appearance.

8 Click OK in Configure Signature Appearance, and click Close in User Settings.

To edit or delete a picture:

1 Log in to Acrobat Self-Sign Security as described in "Logging in to a profile" on page 201, and choose Tools > Self-Sign Security > User Settings**.**

2 Select Signature Appearance in the left pane of the User Settings dialog box.

3 Do one of the following:

- To edit a picture, select the appropriate name in the right pane, and click Edit. You can change the title, select a different graphic, or change the text items, as described in the procedure for configuring a new picture.
- To delete a picture from the configuration file, select the name of the picture in the right pane, and click Delete.

Changing your password options

You can change both your profile password and how and when Acrobat Self-Sign Security prompts for a password.

Changing your password

You can change the password for your user profile at any time. Changing your password does not change your signature.

To change your password:

1 Log in to Acrobat Self-Sign Security as described in "Logging in to a profile" on page 201, and choose Tools > Self-Sign Security > User Settings**.**

2 In the User Setting dialog box, select Change Password in the left pane.

3 Enter your current password in the old password text box.

4 Enter your new password in the New Password and Confirm Password text boxes, and click Apply. Your password must contain at least six characters and may not contain the following characters: ! @ # $ % ^ & *, double quotation marks, and | \ ; < > _. You must enter the same password in both boxes.

5 Click Apply, and click OK in the alert that appears.

6 Click Close.

Changing your password time-out options

By default, your profile is preset to prompt for a password every time you sign a document. You can change it to prompt only after a certain period of time has elapsed or to never prompt for a password.

To change password time-out options:

1 Log in to Acrobat Self-Sign Security as described in "Logging in to a profile" on page 201, and choose Tools > Self-Sign Security > User Settings**.**

2 In the User Settings dialog box, select Password Timeout in the left pane.

To change when a password should be required, choose a value from the pop-up menu, and enter your password in the text box. Click Apply, and click OK in the alert that appears. The periods of time in the menu give the amount of time that has passed since you last entered a password while logged in to Acrobat Self-Sign Security in the current session.

Working with signatures

A document in Acrobat can be signed more than once and by more than one person. The first time a document is signed, it is saved in an *append-only* form of Adobe PDF that can be appended to but not altered. Every time the document is signed after that, the new signature and any changes made since the preceding version are appended to the file. When you view a document with more than one signature, you're viewing the most recent version, but you can open an earlier version in a separate file and compare the two versions to see changes between them.

In Acrobat 5.0, the digital signatures feature enables your signature handler to add digital signatures to PDF files, supports the Signature navigation pane, gives access to all the signatures in a document, and supports the Compare commands.

Important: *Because a document is saved in append-only form the first time it is signed, you can only append changes to the file (using Save As); you cannot do a full save (using Save). A full save will invalidate all signatures.*

Logging in to a profile

You need to be logged in to your profile before you can sign documents or verify signatures. If you sign a document using the digital signatures feature or the digital signature tool, you will be prompted to log in to your profile (if you have not already done so) before you can sign the document.

To log in to a profile:

1 Choose Tools > Self-Sign Security > Log In. (If you are already logged in to a profile, this command changes to Log In As Different User. If you have multiple profiles, use this command to log in to one of your other profiles.)

2 Choose a profile. The pop-up menu lists the most recently opened or created profiles. Or click Find Your Profile File, and browse to find a profile.

3 Enter your password, and click Log In.

4 If an alert appears confirming that you are logged in, click OK. Your Acrobat Self-Sign Security preference settings determine whether this alert appears.

To log out of a profile:

Choose Tools > Self-Sign Security > Log Out <*profile name*>.

About signature fields

When you sign a document, your signature and the related information are stored in a signature field embedded on the page. A signature field is an Acrobat form field.

You can add a signature field to a page as you sign, or you can use the form tool  to create an empty signature field that can be signed later. When you create a signature field with the form tool, you can have Acrobat execute a script or lock all fields in the document when it is signed. You can also customize the field in several other ways. For information on creating empty signature fields with the form tool, see "Creating signature fields" on page 150.

Note: *If you're signing an existing field, be aware that the document author may have put duplicates of the field on other document pages. For example, sometimes a field is copied to the same place on every page. You need to sign the field only once, and your signature will appear in all occurrences of the field. This is sometimes done to allow quick initialing of every page in a document.*

Adding signatures to a document

You can sign a document in several ways, both visibly and invisibly. Invisible signatures do not appear in the document, but they are visible in the Signatures palette. (In Acrobat 5.0, invisible signatures are added to the page of the document currently being viewed when the signature is added; in Acrobat 4.0, invisible signatures were added only to the first page of a document.)

Note: *If you delete a page that carries a signature, visible or invisible, the signature is deleted also.*

When you add a signature with Acrobat Self-Sign Security as your signature handler, your signature is verified automatically. Adding a signature does not affect the verification status of existing signatures in the document. For more information on the appearance or status of digital signatures in Acrobat Self-Sign Security, see "Verifying signatures" on page 203.

To sign a document:

1 If you are not already logged in to a profile, choose Tools > Self-Sign Security > Log In.

2 In the Log In dialog box, choose your profile from the pop-up menu, or click Find Your Profile File and use the browser to find a profile. Then enter your password for the profile, click Log Inn and click OK.

3 If you are logged in to a digital signatures profile, do one of the following:

- To fill in an existing signature field, click the unsigned field in the document pane, or select the unsigned field in the Signatures palette and choose Sign Signature Field from the Signatures palette menu.
- Right-click (Windows) or Control-click (Mac OS) the existing signature field in the palette or document, and choose Sign Signature Field from the context menu.
- Choose Tools > Digital Signatures > Sign Document, and click OK.
- To add a new signature field and sign at the same time, select the signature tool and drag to draw the field.
- To sign the document invisibly, choose Tools > Digital Signatures > Invisibly Sign Document.

4 In the Sign Document dialog box, enter your password in the Confirm Password text box. (You determine how often your password is required in the User Settings dialog box; the default is to require your password every time you sign.) Click Show Options to enter a reason for signing the document. You can either type a reason or choose one from the pop-up menu. Additionally, you can enter a location for the signature, such as your city, state, or country, or the hostname of your computer, and you can add contact information for validation purposes.

5 Choose a signature appearance. Standard Text displays the icon with the distinguished name defined in the profile, the date and time of the signing, and the reason for signing. If you have defined a personalized signature, choose it from the pop-up menu. To create a new signature appearance, click New and follow the steps in "Adding graphics to signatures" on page 198. To preview your signature before signing the document, click Preview.

6 Click Save. To save the file under a different name, click Save As, enter a filename, specify a location for the file, and click Save.

Note: *Except in your file system (Windows Explorer, for example) you will not have another opportunity to use Save As on the document (because Save As invalidates existing signatures), so you may want to use a name that is not based on a date or a particular version.*

The new signature appears as the last item in the Signatures palette.

Adding signatures to a document in a browser

Signing a document in a browser as opposed to in Acrobat is slightly different. When you sign a document in a browser, only the incremental portion of the file is saved to your hard drive. (You will notice that there is a Sign rather than a Save or Save As button when you sign the document.) To save a copy of the signed document, you must save the copy in the browser to your hard drive.

To sign a document in a browser:

1 Select the digital signature tool and drag to draw a rectangle on the document.

2 If you are not logged in to a profile, in the Log In dialog box, choose your profile, enter your password, and click Log In. For information on creating a new profile, see "Creating profiles" on page 197.

3 If you are already logged in to a profile, click Show Options to enter a reason for signing the document. You can either type a reason or choose one from the pop-up menu. Additionally, you can enter a location for the signature, such as your city, state, or country, or the hostname of your computer, and you can add contact information.

4 Click Sign, and click Save in the Save As dialog box.

5 To retain a copy of the signed document, click the Save a Copy of the File button on the toolbar, browse to select a location in which to save the file, and enter a name for the file. You must save the file in this way to retain a copy.

Verifying signatures

When you verify a signature that was added with Acrobat Self-Sign Security, Acrobat can confirm the authenticity of the signature in two ways:

- Acrobat checks to see that the document and the signature have not been altered since the signing.
- If you are logged in to a profile and have the signer's user certificate in your profile's list of trusted certificates, Acrobat compares information in the signature against the certificate to verify the identity of the signer.

You can view a signature's verification status on the document page and in the Signatures palette.

To verify a signature:

1 In an open document, do one of the following:

- Click the signature in the document pane. A dialog box indicates the status of the signature. Click Properties to access the Signature Properties dialog box. Click Verify Identity to check fingerprint information.
- Right-click (Windows) or Control-click (Mac OS) on the signature, and click Validate Signature. In the Validation Status dialog box, on Windows click Verify Identity (if you are logged in) or Log In (if you are not logged in, and follow the login process); on Mac OS click Properties and click Verify Identity in the Signature Properties dialog box.

2 In the Verify Identity dialog box, follow the on-screen instructions for verifying fingerprint information. Click Add to List when you are sure that this is a valid user certificate. (Click Details to see information about the signer.)

3 Click OK in the Alert dialog box, and click Close in the Validation Status dialog box to verify the signature.

Deleting signatures and clearing signature fields

You can remove a signature totally or you can clear a signature field (that is, delete the signature but leave the empty signature field). As with other edits you make to a signed document, this adds another version to the document without altering earlier versions. Another user can roll back to an earlier version to see the original signature.

To remove a signature or clear a signature field:

1 Do one of the following:

- To remove a signature, select the signature in the Signatures palette, and choose Delete Signature Field from the Signatures palette menu. (Shift-click to add more signatures to the selection.) Or right-click (Windows) or Control-click (Mac OS) the signature in the palette or document pane, and choose Delete Signature Field from the context menu. The signature is removed, and the Signatures palette notes that the document was modified.
- To remove a signature and leave the empty signature field, select the signature in the Signatures palette, and choose Clear Signature Field from the Signatures palette menu. (Shift-click to add more signatures to the selection.) Or right-click (Windows) or Control-click (Mac OS) the signature in the palette or document pane, and choose Clear Signature Field from the context menu.The signature is removed, and the Signatures palette notes that the document was altered after the last signing.The digital signature icon in the Signatures palette indicates the presence of the empty signature field.
- To clear all signature fields in a document, choose Tools > Digital Signatures > Clear All Signature Fields.

Tracking digital signatures in the Signatures palette

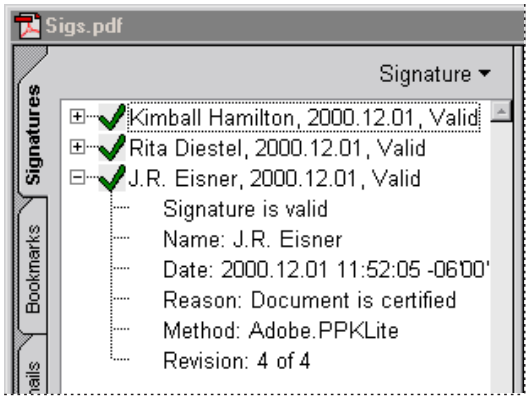
The Signatures palette lists all the signatures in the current document (with their status), in the order they were added. You can collapse a signature to see only a name, date, and status, or you can expand it to see more information.

To show the Signatures palette:

Choose Window > Signatures, or click the security key icon in the status bar and choose Show Signatures from the security key pop-up menu. The security key menu is available only when a document has signatures or other security properties.

To expand or collapse a signature in the palette:

Click the plus sign (Windows) or triangle (Mac OS) to the left of the signature to expand it. Click the minus sign (Windows) or the rotated triangle (Mac OS) to the left of the signature to collapse it.



Expanded signature

Each signature in the palette has an icon identifying its current verification status. For an explanation of these icons, see "Verifying signatures" on page 203.

If you edit a signed document, the question mark icon indicates that the document has been modified with the signature in the Signatures palette.

Getting information on signatures

You can open a dialog box to view an explanation of a signature's verification status, the document version the signature applies to, and information such as date and time of the signing. This dialog box is not editable, but you can copy text from it and click buttons to work with the signature.

To get information on a signature:

1 Select the signature in the Signatures palette, and choose Properties from the Signatures palette menu. Or right-click (Windows) or Control-click (Mac OS) the signature in the palette or document pane, and choose Properties from the context menu.

2 In the Signature Properties dialog box, do any of the following:

- To verify the signature, click Verify Signature. This also updates information in the dialog box.
- To view user attributes, verification parameters, and other information on the signature's certificate, click Show Certificate. (See "Getting information on certificates" on page 206.) This button is available only if the signature has been verified.

3 Click Close.

Viewing earlier versions of a signed document

If a document is signed more than once, Acrobat maintains all of the signed versions in a single Adobe PDF file. After the first time a document is signed, and each time the document is signed, a version is saved as append-only to ensure that it will not be altered. All signatures and the versions of the document corresponding to those signatures are listed in the Signatures palette.

To open an earlier signed version:

Select the signature in the Signatures palette, and choose View Signed Version from the Signatures palette menu. Or right-click (Windows) or Control-click (Mac OS) the signature in the palette or document pane, and choose View Signed Version from the context menu.

The earlier version opens in a new Adobe PDF file, with the version information and the name of the signer in the title bar.

To compare two versions of a signed document:

For information on comparing two versions of a signed document, see "Comparing two PDF documents" on page 123.

Managing user certificates

Your user certificate contains a public key that is used to verify your digital signature. Before other users can verify your signature on documents they receive, they must have access to your user certificate. You should build a list of user certificates that you use often.

Sharing your user certificate

You can share your user certificate with others by exporting your certificate (as an FDF file) to a key file or by e-mailing your certificate directly. Users can also import your user certificate from verified signatures in a document.

To share your user certificate:

1 Log in to Acrobat Self-Sign Security, and choose Tools > Self-Sign Security > User Settings**.**

2 In the User Settings dialog box, select User Information in the left pane to verify that your user information is correct.

3 Under Certificate, do one of the following:

- Click Details to verify the information for your user certificate.
- Click Export to File to save the user certificate in FDF or PKCS#7 format. Browse to specify a location for the key file, and click Save. In the Export Certificate dialog box, make a note of the fingerprint information, and click OK. (You can copy this fingerprint information out of the dialog box.) When other users import your certificate, they'll probably ask you to check this information against the information they receive with the certificate.
- Click EMail to launch your e-mail application and e-mail your user certificate to another user.

4 Click Backup to save a copy of your user certificate in another location.

5 Click Close (Windows) or Done (Mac OS) to exit the user profile setup.

Getting information on certificates

You can open a dialog box to view user attributes, verification parameters, and other information on a particular certificate. The dialog box is not editable, but you can copy text from it.

- The distinguished name (DN) is the name, organization, and country that the user provided when they created the profile. In Acrobat Self-Sign Security, the user DN and the certificate issuer DN are the same because a certificate is always issued by the user rather than by a third-party authority.
- The fingerprint information can be compared for two users when importing a certificate to make sure the certificate came from the user it represents. The serial number is a unique number that ensures no two certificates from the same DN can be identical.
- The validation period specifies a span of time in which the certificate is valid. It begins with the date and time the certificate was created.

To get information on a certificate:

1 Choose Tools > Self-Sign Security > User Settings. Or if you're not logged in, choose Tools > Self-Sign Security > Log In to log in, and then click User Settings in the alert.

2 Do one of the following:

- To get information on your own certificate, select User Information in the left pane of the User Settings dialog box. For Certificate, click Details.
- To get information on a certificate in your list of trusted certificates, select Trusted Certificates in the left pane of the User Settings dialog box, select the certificate in the list, and click Details.

3 Click Close to exit the dialog boxes.

Building a list of trusted certificates

You can keep a copy of other users' certificates in a list of trusted certificates so that you can verify the signatures of these users on any documents you receive. You add another user's certificate to your list of trusted certificates by importing the certificate from an Acrobat key file or from a PDF document signed by another Self-Sign user.

Important: *The format of the Acrobat key file is specific to Self-Sign Security; you cannot import user certificates from key files created by other applications.*

Acrobat Self-Sign Security provides unique fingerprint information for each certificate to help you ensure the certificate's authenticity when you import it.

To import a certificate from a key file:

1 Choose Tools > Self-Sign Security > User Settings. Or if you're not logged in, choose Tools > Self-Sign Security > Log In to log in, and then click User Settings.

2 In the User Settings dialog box, select Trusted Certificates in the left pane.

3 Click Import from File, use the browser to locate the Acrobat key file with the certificate, and click Open. A key file has the extension .apf or .p7c.

4 In the Import Certificate dialog box, note the MD5 Fingerprint and the SHA-1 Fingerprint numbers, and click OK. Confirm with the certificate's originator that the information is correct. If the strings are not correct, the certificate should not be trusted.

5 Click Close.

To import a certificate from a signature in a document:

1 Right-click (Windows) or Control-click (Mac OS) the signature in the Signatures palette or document pane, and choose Properties from the context menu.

2 If the signature is not valid, click Verify Signature. You can import a certificate only from a verified signature.

3 In the Signature Properties dialog box, click Verify Identity.

4 In the Verify Identity dialog box, note the MD5 Fingerprint and the SHA-1 Fingerprint numbers. Confirm with the certificate's originator that the strings are correct. If the strings are incorrect, the certificate should not be trusted. If the strings are correct, click Add to List.

5 Click Close.

To delete a certificate from the list of trusted certificates:

1 Log in to Acrobat Self-Sign Security, and choose Tools > Self-Sign Security > User Settings**.**

2 Select the certificate in the Trusted Certificates panel of the User Settings dialog box, and click Delete, and then click OK.

Setting Acrobat Self-Sign Security preferences

You can choose to encapsulate your signature in the standard PKCS#7 format for compatibility with other signature handlers.

To set Acrobat Self-Sign Security preferences:

1 Choose Edit > Preferences > General. Select Self-Sign Security in the left pane of the Preferences dialog box.

2 Select Use Certificate Message Syntax (PKCS#7 format) Signature to encapsulate signatures in the standard PKCS#7 format rather than leaving them as two separate entries in the PDF file. Select this option if interoperability with signature mechanisms other than Self-Sign Security (that support the PKCS#7 standard) are desired. Selecting this option is recommended.

3 Click OK.