


Step by Step - Digital IDs in Adobe Acrobat & Reader versions XI and DC

Create a self-signed digital ID

1. In the upper left click **Edit**, choose **Preferences**, then **Signatures** on the left, under **Categories**.
2. In **Identities & Trusted Certificates**, click **More**.
3. Select **Digital IDs** on the left, and then click the **Add ID** button .
4. Select the option • **A New Digital ID I Want To Create Now**, and click **Next**.
5. Specify where to store the digital ID, and click **Next**.

- New PKCS#12 Digital ID File

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

-or-

- Windows Certificate Store (Windows only)

Stores the digital ID to a common location from where Microsoft Office programs can also retrieve it.

If you are on Mac OS, you won't see these options.

6. Type a name, email address, and other personal information for your digital ID. When you certify or sign a document, the name appears in the Signatures panel and in the Signature field.
7. Choose an option from the Key Algorithm menu. The 2048-bit RSA option offers more security than 1024-bit RSA, but 1024-bit RSA is more universally compatible.
8. From the **Use Digital ID For** menu, choose whether you want to use the digital ID for signatures, data encryption, or both.
9. Type a **password** for the digital ID file. For each keystroke, the password strength meter evaluates your password and indicates the password strength using color patterns. Reconfirm your password.

Note:

You may wish to make a backup copy of your digital ID file. If your digital ID file is lost or corrupted, or if you forget your password, you cannot use that profile to add signatures. Also, the file can be copied to all the computers you use to have the signature available on all of them.

In Windows 7 with Acrobat XI or Reader XI the path is:

Users*user profile*\AppData\Roaming\Adobe\Acrobat\11.01\Security*your name*.pfx

AppData is a hidden folder. Windows may need to be configured to show hidden folders on your computer before you will be able to navigate to the digital ID file. See more at the end of this document.

Self-signed digital IDs are good for 5 years. When yours expires, you will need to create a new ID.

Creating additional digital IDs on the same computer

If you have already created a digital signature on a computer and wish to create an additional signature, the process is simple. Click in a Signature Field in a PDF form.

This window should open. In the **Sign As:** drop-down menu, select **New ID...**

You will be led through the normal steps to create a digital signature. Make note of the name of the new signature that is created. You will need to select the new signature by that name in the future to sign documents with this new ID.

Sign Document

Sign As: My Name (My Name) 2021.12.06
My Name (My Name) 2021.12.06
Refresh ID List
New ID ...

Issued by: My Name

Appearance: Standard Text

My Name Digitally signed by My Name
Date: 2016.12.06 10:04:18 -06'00'

Click Review to see if document content may affect signing Review...

Enter certificate password and click the 'Sign' button

Help Sign Cancel

Create the appearance of a certificate-based signature

You determine the look of your certificate-based signature by selecting options in the Signatures panel of the Preferences dialog box. For example, you can include an image of your handwritten signature, a company logo, or a photograph. **You can also create different signatures for different purposes.** For some, you can provide a greater level of detail.

A signature can also include information that helps others verify your signature, such as reason for signing, contact information, and more.



Signature formats

A. Text signature B. Graphic signature

1. (Optional) If you want to include an image of your handwritten signature in the certificate-based signature, scan your signature, and save it as an image file. Place the image in a document by itself, and convert the document to PDF.
2. **Create an appearance** using the Signature preferences: (in Windows, within Acrobat or Reader) Edit > Preferences > Signatures or (in Mac OS) Acrobat > Preferences > Signatures.
3. From the **Appearance menu** in the Sign dialog box, select **Create New Appearance**.
4. In the **Configure Signature Appearance** dialog box, type a name for the signature you're creating. When you sign, you select the signature by this name. Therefore, use a short, descriptive title.
5. For **Configure Graphic**, choose an option:

No Graphic

Displays only the default icon and other information specified in the Configure Text section.

Imported Graphic

Displays an image with your certificate-based signature. For example, you could scan your signature and save it in PDF format, then select this option to include an image of your handwritten signature. To import the image file, click File, click Browse, and then select the image file. As seen above, in the example for Lisa Jones, you could import an attractive graphic as your signature.

Name

Displays only the default signature icon and your name as it appears in your digital ID file.

6. For **Configure Text**, select the options that you want to appear in the signature. **Distinguished Name** shows the user attributes defined in your digital ID, including your name, organization, and country.
7. For Text Properties, specify the writing direction and type of digits used, and then click OK.
8. (Optional) **If you wish the Sign Document dialog box to include the Additional Signature Information section, specify the reason for signing the document, the location, and your contact information**, these options are available only if you set them as your preferences in the Creation and Appearance Preferences dialog box (Edit > Preferences > Signatures > Creation & Appearance > More) in Windows or at Acrobat > Preferences (Mac OS).

Signing a PDF Document with your digital ID

With the PDF open, in the signature field, you should see a graphic such as:







Sign Here

Left click to **sign**, or **Right click** and choose to **sign** or **digitally certify the document**. Enter your **password** for the digital signature. In the Sign Document window, select the **APPEARANCE** you want applied to your signature. Then, click SIGN.

Specify the default digital ID

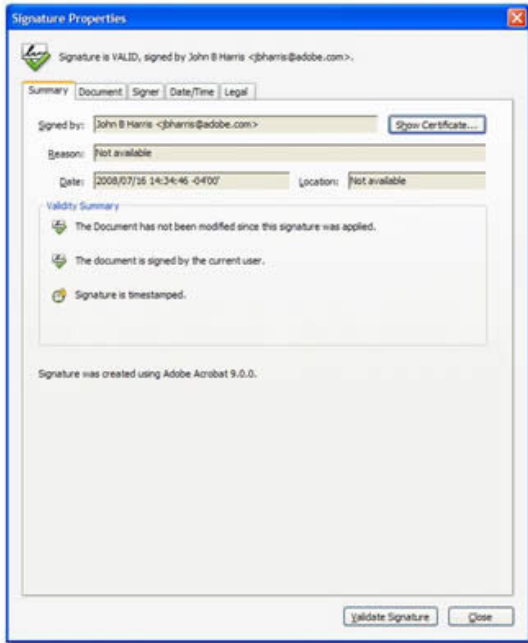
To avoid being prompted to select a digital ID each time you sign or certify a PDF, you can select a default digital ID.

1. Select Preferences > Signatures. In Identities & Trusted Certificates, and click More.
2. Click Digital IDs on the left, and then select the digital ID you want to use as the default.
3. Click the Usage Options button , and choose a task for which you want the digital ID as the default. To specify the digital ID as the default for two tasks, click the Usage Options button again and select a second option.

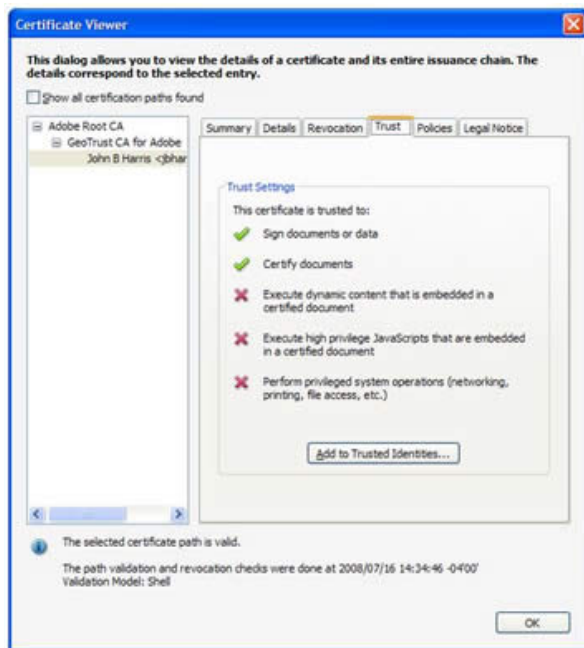
A check mark appears next to selected options. If you select only the signing option, the Sign icon  appears next to the digital ID. If you select only the encryption option, the Lock icon  appears. If you select only the certifying option, or if you select the signing and certifying options, the Blue Ribbon icon  appears.

To clear a default digital ID, repeat these steps, and deselect the usage options you selected.

Verifying the Identity of Self-Signed Certificates



This is the most straightforward method: if you receive a signed document from an individual who has not been previously trusted, open the document with Adobe Acrobat or Reader, right-click on the signature, choose **Show Signature Properties** and then **Show Certificate**.

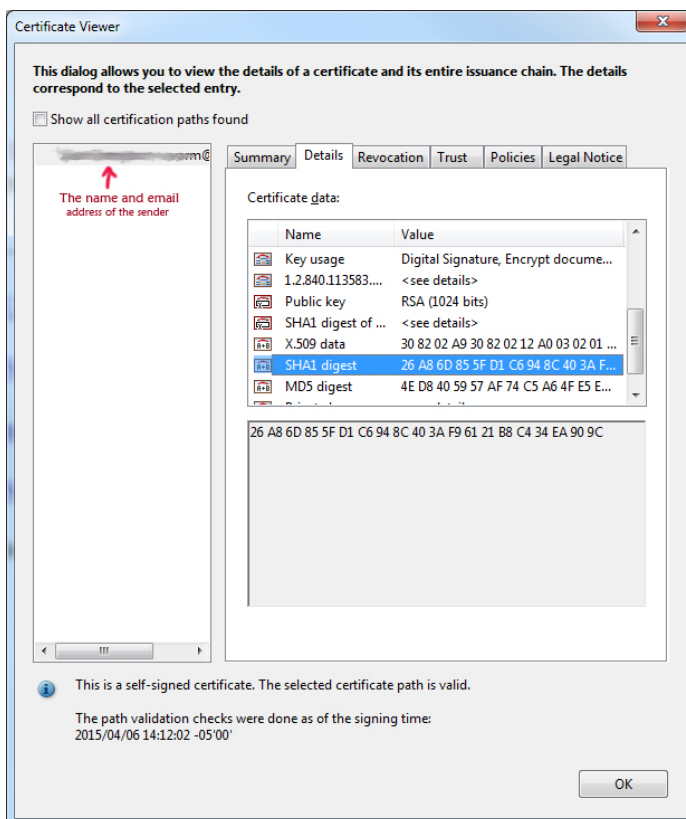


By clicking on the Trust tab within that dialog box, you can select Add to Trusted Identities to select whether the credential will be trusted for standard approval signatures and/or certification (publishing) signatures.

If you want an even highly certainty of the author of self-signed certificates, it is prudent to verify the certificate owner's identity before trusting the certificate.

To verify the origin of the certificate:

1. Display the certificate in the Certificate Viewer:
Right click on the signature, choose **Show Signature Properties**, display the Summary tab, and choose **Show Certificate**.
2. Display the **Details** tab.



3. In the Certificate data panel, scroll to **MD5-digest** and **SHA-1 digest**, and note the numbers.
4. **Contact the certificate's originator**, and verify the MD5-digest and SHA-1 numbers are correct. If you contact originators by phone, you can have them view the same digest numbers by following the above steps on their computers. Have them read the numbers to you. If the numbers match, you can be sure the digital signature is theirs.

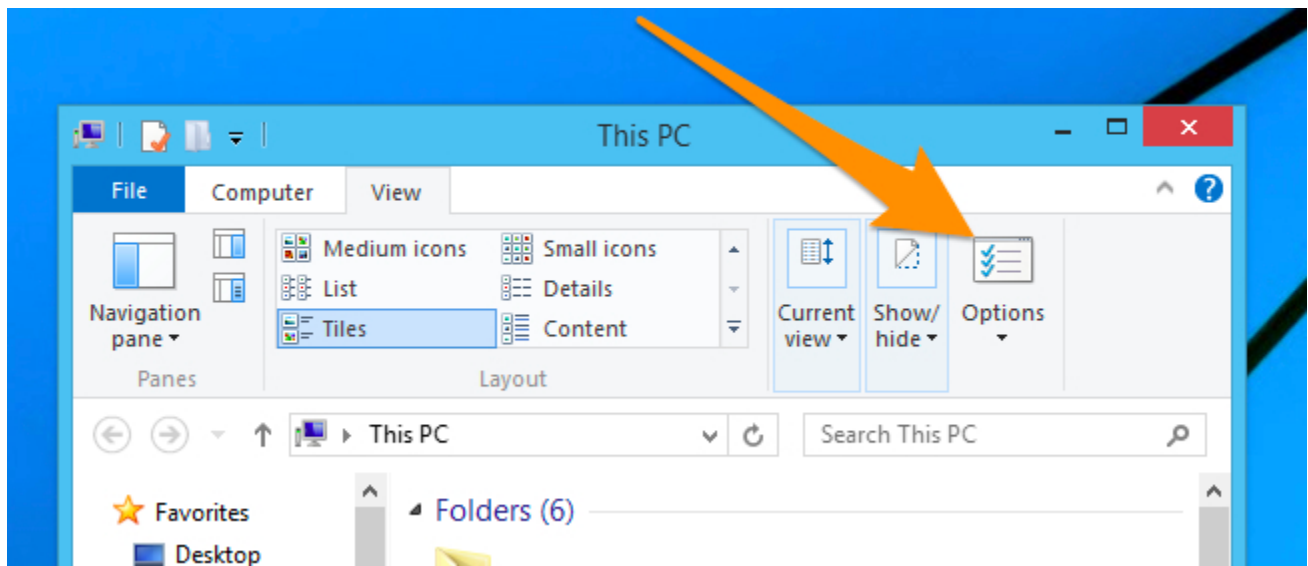
5. After the certificate is verified, display the Trust tab and add the certificate to the trusted identities list.
6. Specify certificate trust settings so that it can be used as a trusted root, to certify documents, and so on.

Show Hidden Files and Folders in Windows 7, 8.x, and 10

You will need Administrative rights to follow these directions.

On Windows 8.x and 10

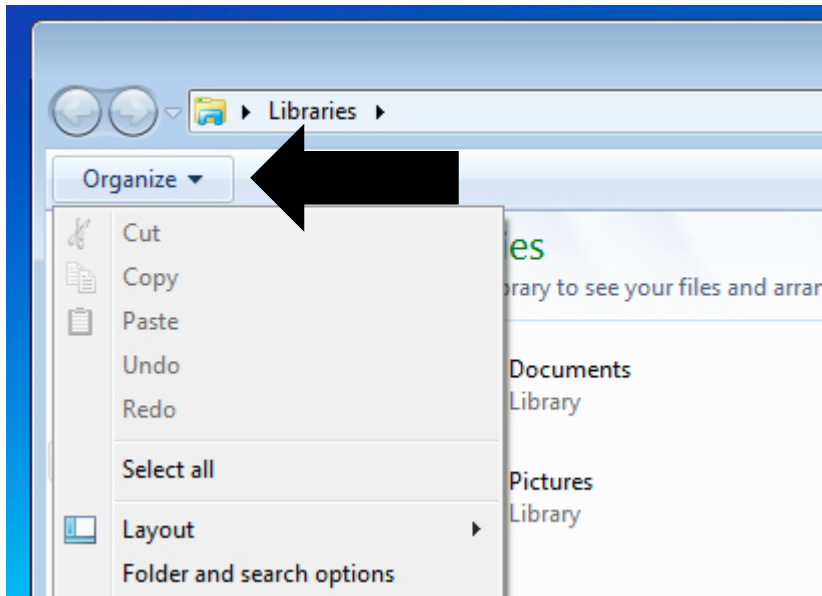
You can use this Ribbon in **File Explorer** on the **View** tab, to get to the **Folder Options** window:



On Windows 7 or Vista

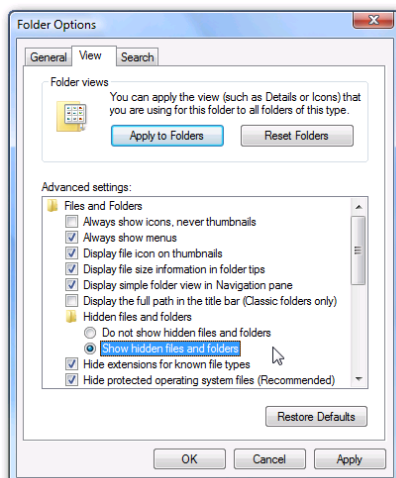
To show hidden files: within **File Explorer**, with **any folder selected**, click on the **Organize** button, and then select "**Folder and Search Options**" from the menu.

This will open the **Folder Options** window



NEXT: Toggling on Show Hidden Files and Folders

Click the **View** tab, and then you should select "**Show hidden files and folders**" in the list. If you are trying to get into the Windows directories, you might want to also remove the checkbox from "Hide protected operating system files" as well.



Once you are done, click OK.

Note: If you are missing this option entirely, you should [follow this guide to restore the option](#).