Creating a Certificate-Based Signature in Adobe

This method uses public and private keys to authenticate the signer's identity. This method is preferred when signing documents that need to meet compliance regulations. To use a certificate-based signature, the signer needs to have an Adobe Digital ID.

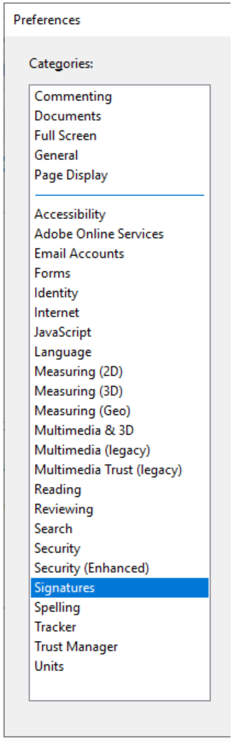
More information about certificate-based signatures may be found at:

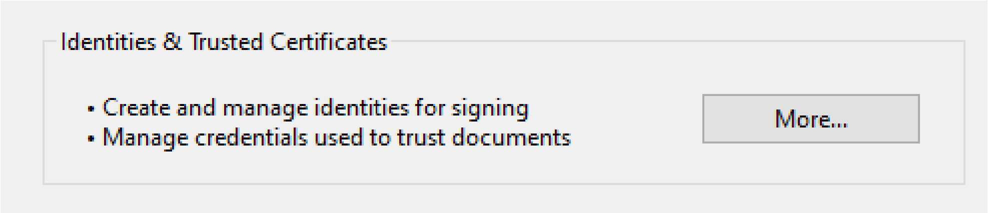
- https://helpx.adobe.com/acrobat/using/certificate-based-signatures.html
- https://helpx.adobe.com/acrobat/using/digital-ids.html

Create an Adobe Digital ID

1. In Adobe Acrobat or Adobe Professional, click on the **Edit > Preferences** menu.

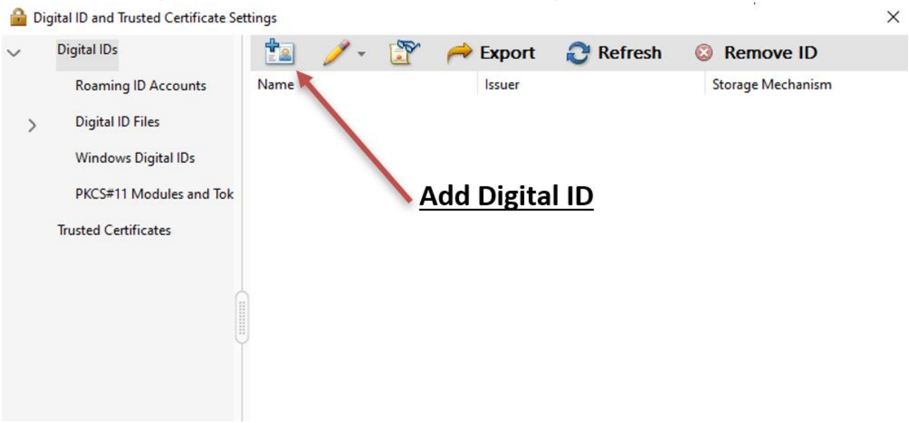
2. Under Categories: Choose **Signatures**, then click on **More** under Identities & Trusted Certificates.





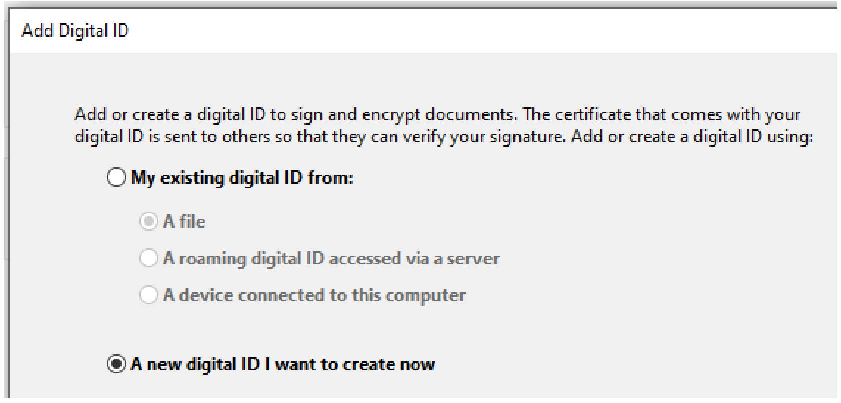
- Create and manage identities for signing
- Manage credentials used to trust documents

3. Click on **Digital IDs**, then click on the **add Digital ID** button.



Add Digital ID

4. Select the option **A new digital ID I want to create now**.



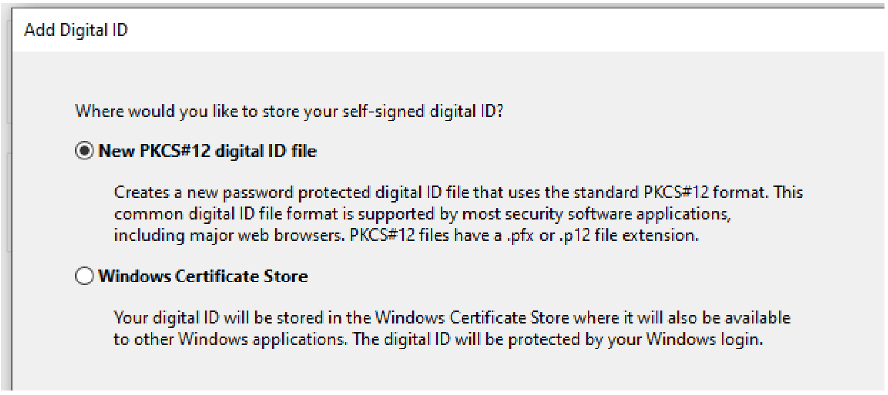
Add or create a digital ID to sign and encrypt documents. The certificate that comes with your digital ID is sent to others so that they can verify your signature. Add or create a digital ID using:

○ **My existing digital ID from:**

- ● **A file**
- ○ **A roaming digital ID accessed via a server**
- ○ **A device connected to this computer**

● **A new digital ID I want to create now**

5. Select the option **New PKCS#12 digital ID file** and click **Next**.



Where would you like to store your self-signed digital ID?

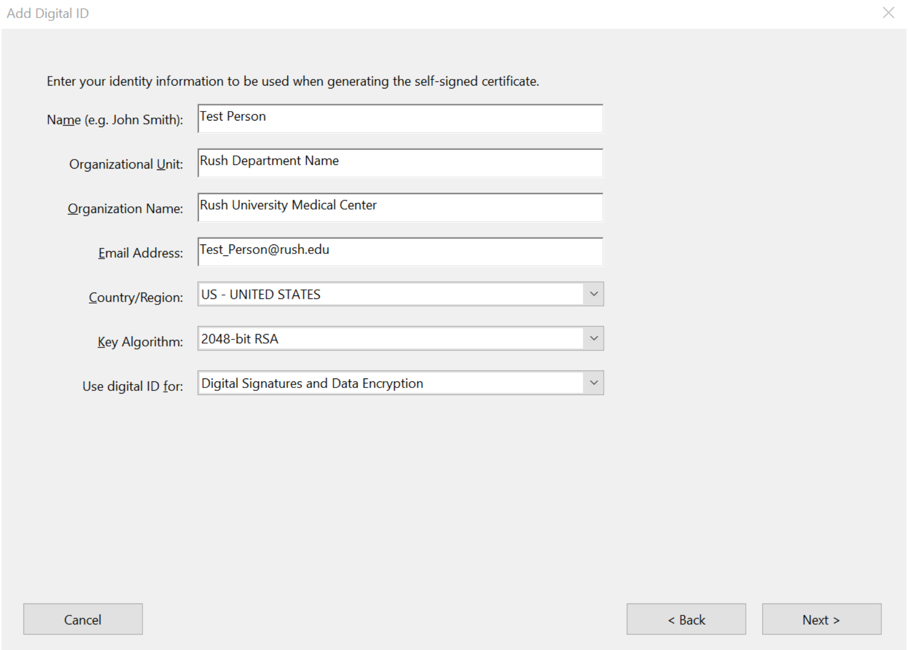
● **New PKCS#12 digital ID file**

Creates a new password protected digital ID file that uses the standard PKCS#12 format. This common digital ID file format is supported by most security software applications, including major web browsers. PKCS#12 files have a .pfx or .p12 file extension.

○ **Windows Certificate Store**

Your digital ID will be stored in the Windows Certificate Store where it will also be available to other Windows applications. The digital ID will be protected by your Windows login.

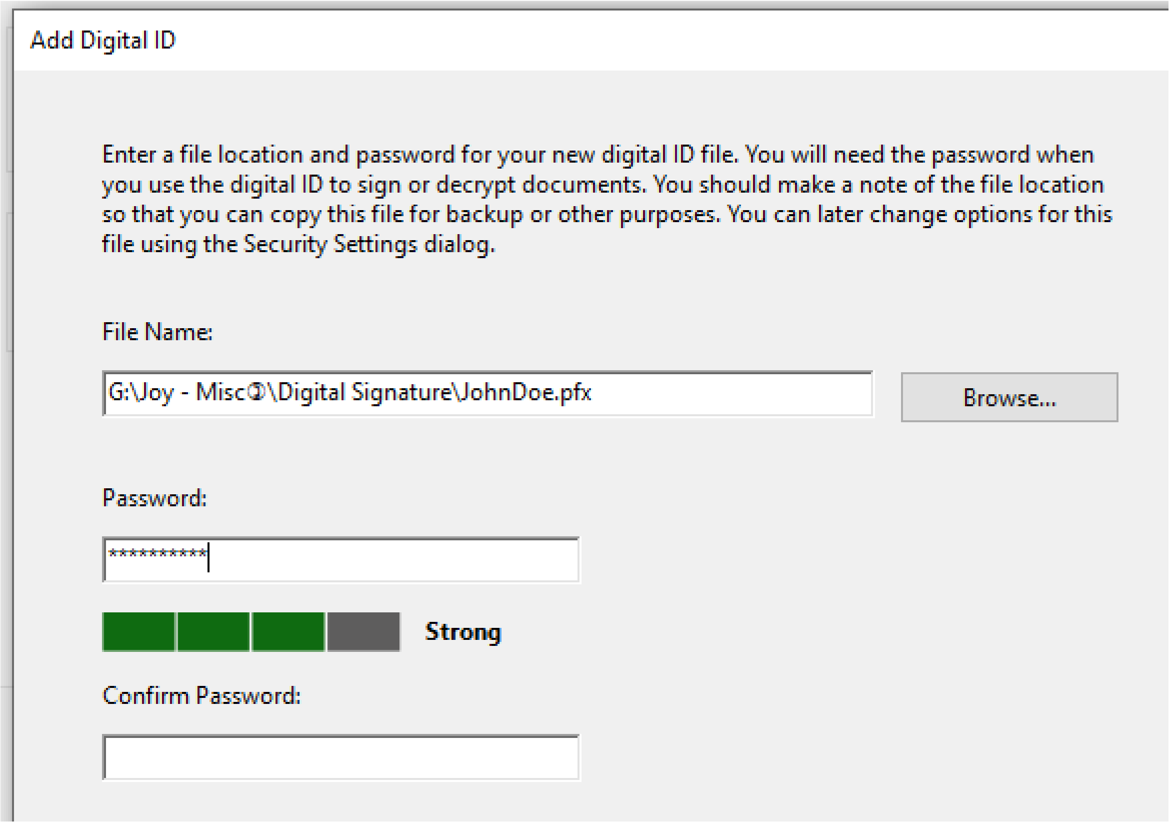
6. On the next screen enter the information you want included in your digital certificate. Your e-mail address is required.



Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):	Test Person
Organizational Unit:	Rush Department Name
Organization Name:	Rush University Medical Center
Email Address:	Test_Person@rush.edu
Country/Region:	US - UNITED STATES
Key Algorithm:	2048-bit RSA
Use digital ID for:	Digital Signatures and Data Encryption

7. Click **Browse** to choose a location to save the file if other than the default location. Type a password for the digital ID file.



Add Digital ID

Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

File Name:

G:\Joy - Misc①\Digital Signature\JohnDoe.pfx

Password:

****

Strong

Confirm Password:

8. Click **Finish**.

Add a Certificate-Based Signature to a blank PDF form

1. Open the PDF form that you want to sign.

2. Open the **Certificates** tool from the **Tools** page.

3. Choose **Digitally Sign** from the Certificates tool bar.

4. Follow the instructions in the pop-up window to create a digital signature box where you want your signature located on the document.

5. Choose the signature you want to use and click **Continue** in the Sign with a Digital ID box.

IMPORTANT! The Sign as [*your signature text*] box has a checkbox giving you the option to lock the document after signing. If any more changes need to be made to the document, do not check this box.

6. Enter your password and click **Sign**. You will be prompted to save the file. After saving the file, your certificate-based digital signature will appear in the document.

Troubleshooting

Certificate-based signatures need to be validated by the receiver. When you right click on a digital signature a signature validation status may appear indicating that the signature is not validated.

1. Click on **Signature Properties**.

2. In the Signature Properties box, click on **Show Signer's Certificate**.

3. In the Certificate Viewer box, choose the **Trust** tab.

4. An Acrobat Security notice appears, click OK.

5. The Certificate Details appear, click **OK**, then close the Signature Properties box.

6. Open the digital signatures verification icon on the left of the screen. Right click the signature that needs validated and click on **Validate Signature**.

7. The digital signature is now validated. This step will not need to be repeated when a form with that same digital signature is received at your computer again.