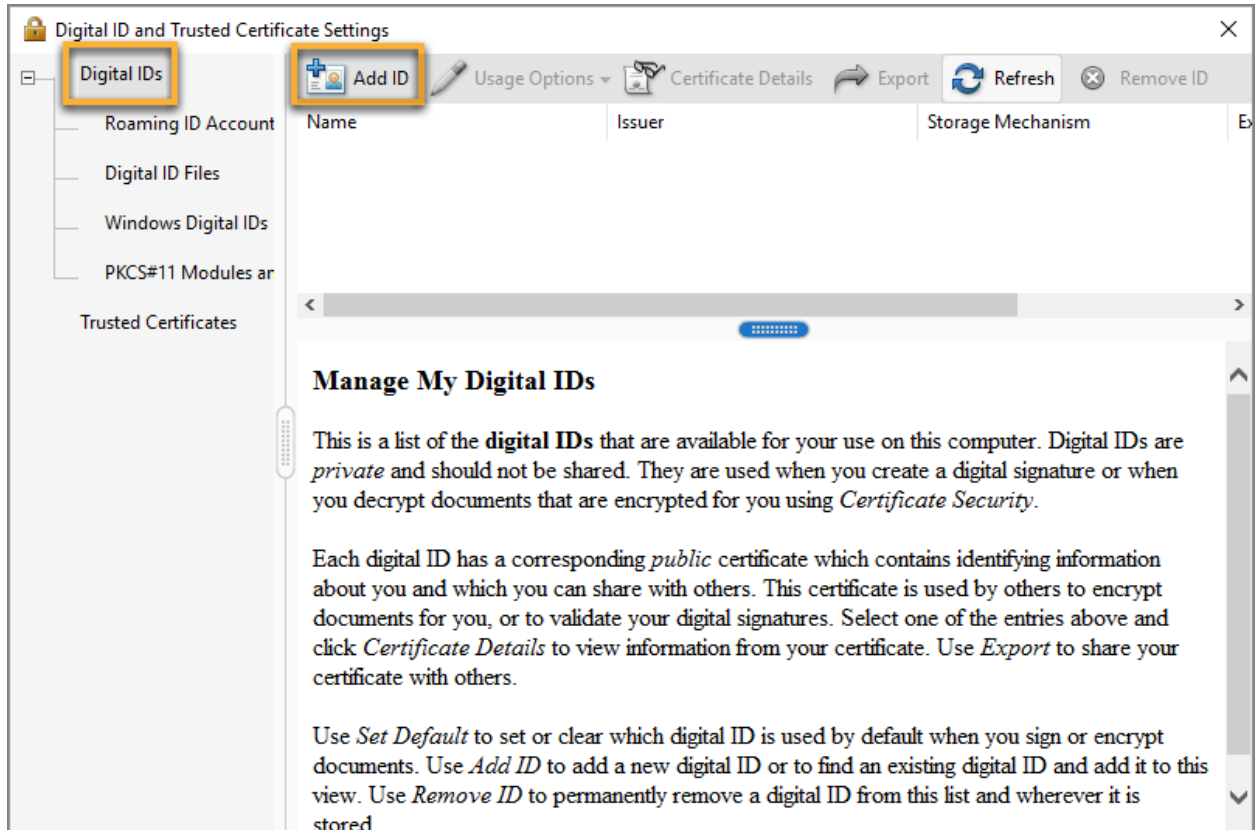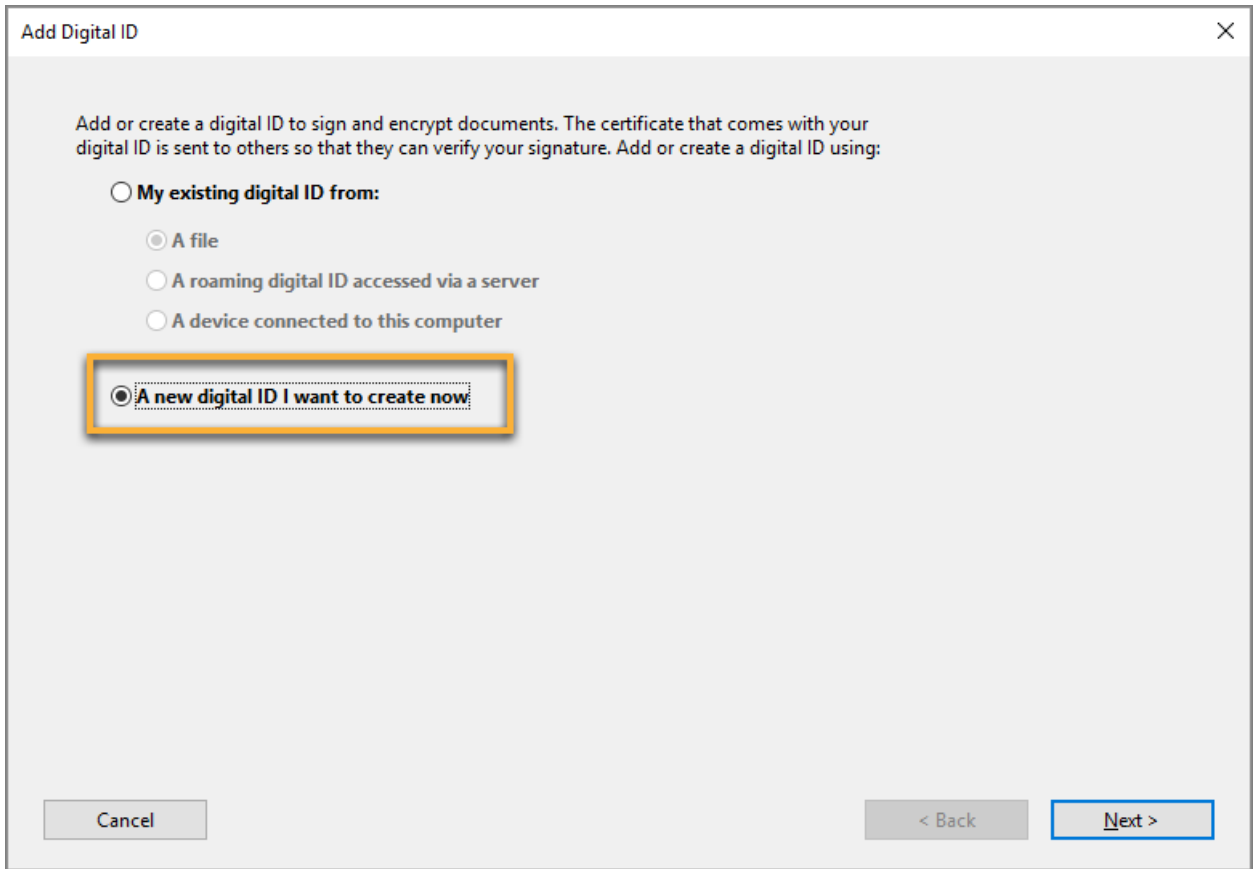# Create a self-signed digital ID

Sensitive transactions between businesses generally require an ID from a certificate authority rather than a self-signed one.

1. In Acrobat, click the **Edit** menu and choose **Preferences** > **Signatures**.
2. On the right, click **More** for **Identities & Trusted Certificates**.
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.

Add Digital ID

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**

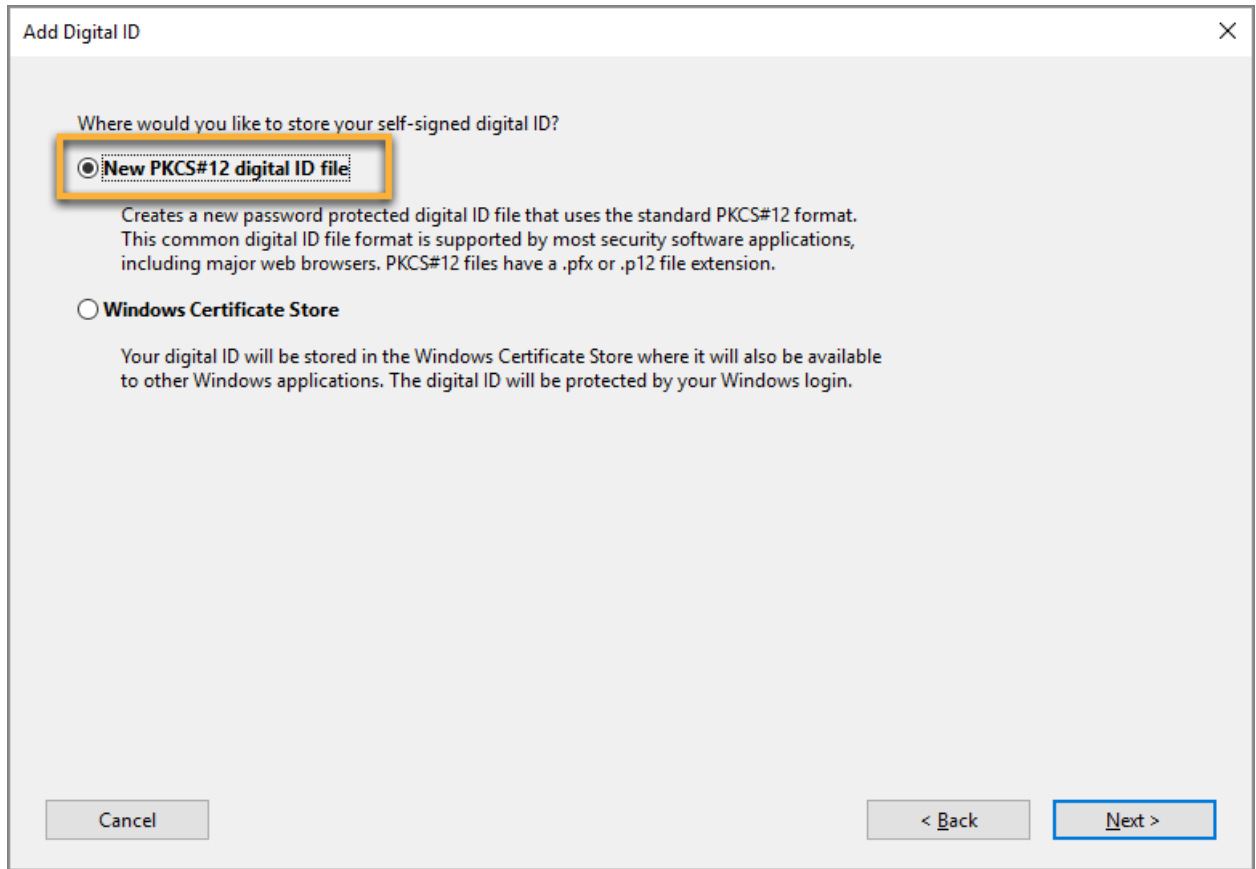Cancel   < Back   Next >

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.

Windows Certificate Store (Windows only)

Stores the digital ID to a common location from where other Windows applications can also retrieve it.

Add Digital ID

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.

Cancel   < Back   Next >

6. Do the following:
    1. 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.
    2. 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.
    3. From the **Use Digital ID For** menu, choose whether you want to use the digital ID for signatures, data encryption, or both.
    4. Click **Next**.

7. Do the following:
   1. 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.
   2. The digital ID file is stored at the default location as shown in the **File Name** field. If you want to save it somewhere else, click **Browse** and choose the location.
   3. Click **Finish**.

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.
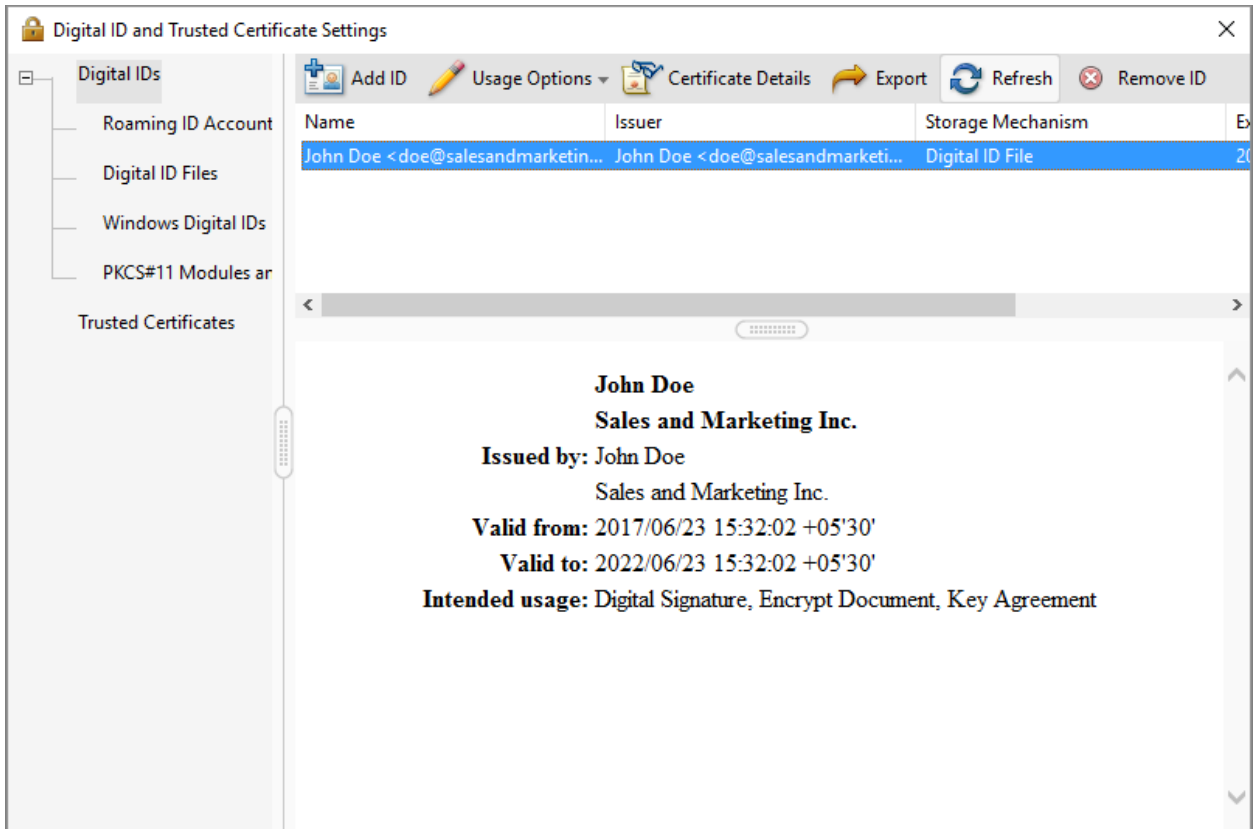
File Name:

ers_____\AppData\Roaming\Adobe\Acrobat\DC\Security\JohnDoe.pfx   Browse...

Password:

****

Strong

Confirm Password:

****

Cancel   < Back   Finish

If a digital ID file with the same name exists, you're prompted to replace it. Click **OK** to replace, or browse and select a different location to store the file.

8. The ID is created. You can export and send your certificate file to contacts who can use it to validate your signature.

Note:

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.