

Federal Aviation Administration (FAA)
Flight Standards Air Transport Division (AFS-200)
Web-Based Operations Safety System (WebOPSS) Program

eForm 337
Digital Certificate Installation



Version 3.1

**November
2016**

eForm 337 Digital Certificate Installation

The eForm 337 Digital Certificate installation consists of three processes to include:

- Prepare Adobe Reader
- Import Digital Signature
- Set the Default Signature



After receiving the .p12 or .pfx file, save a copy of the file to a safe and secure location as a backup file for future needs. Never import the signature from this file/location. In case the password is forgotten or a problem occurred with the file, copy the backup .p12 or .pfx to another location and import it again.

PREPARE THE ADOBE READER DC

1. Open Adobe Reader and/or Adobe Acrobat Professional.

NOTE: For optimal use, it is highly recommended that both Adobe Reader and Adobe Acrobat Professional are the same version.

2. From the main menu bar, click **Edit> Preferences**.

The Preferences pop-up window appears.

Preferences

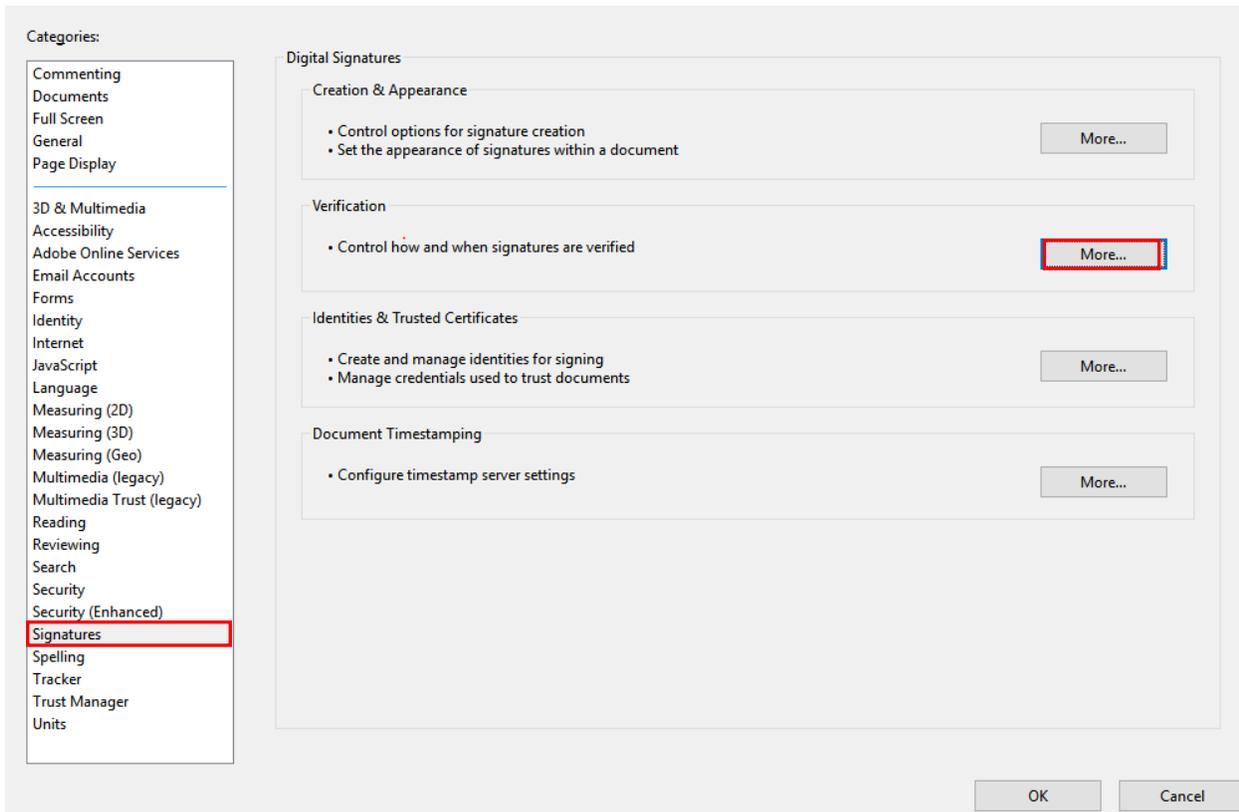


Figure 1. Preferences

3. If not already selected, select **Signatures** from the Categories listing (as shown in the previous figure).
4. Click the **More** button located next to the Verification header (as shown in the previous figure).

The Signature Verification Preferences pop-up window appears.

Signature Verification Preferences

Verify signatures when the document is opened

When document has valid but untrusted signatures, prompt to review and trust signers

Verification Behavior

When Verifying:

Use the document-specified method; prompt if unavailable

Use the document-specified method; if unavailable, use default method

Always use the default method: Adobe Default Security

Require certificate revocation checking to succeed whenever possible during signature verification

Use expired timestamps

Ignore document validation information

Verification Time

Verify Signatures Using:

Time at which the signature was created

Secure time (timestamp) embedded in the signature

Current time

Verification Information

Automatically add verification information when saving signed PDF:

Ask when verification information is too big

Always

Never

Windows Integration

Trust ALL root certificates in the Windows Certificate Store for:

Validating Signatures

Validating Certified Documents

Selecting either of these options may result in arbitrary material being treated as trusted content. Take care before enabling these features.

Help OK Cancel

Figure 2. Digital Signatures Advanced Preferences

5. Place a check mark next to **Verify signature when the document is opened**.
6. Select the **Use the document-specified method; if unavailable, use default** radio button.
7. Select the **Require certificate revocation checking to succeed whenever possible during signature verification** check box.

8. Under Windows Integration, place a check mark next to **Validating Signatures and Validating Certified Documents**.
9. Click the **OK** button. The Preferences pop-up window re-appears.
10. Click the **OK** button and close the Adobe application.

IMPORT DIGITAL SIGNATURE

1. Double-click your **.p12** or **.pfx** digital certificate file.
The Certificate Import Wizard pop-up window appears.

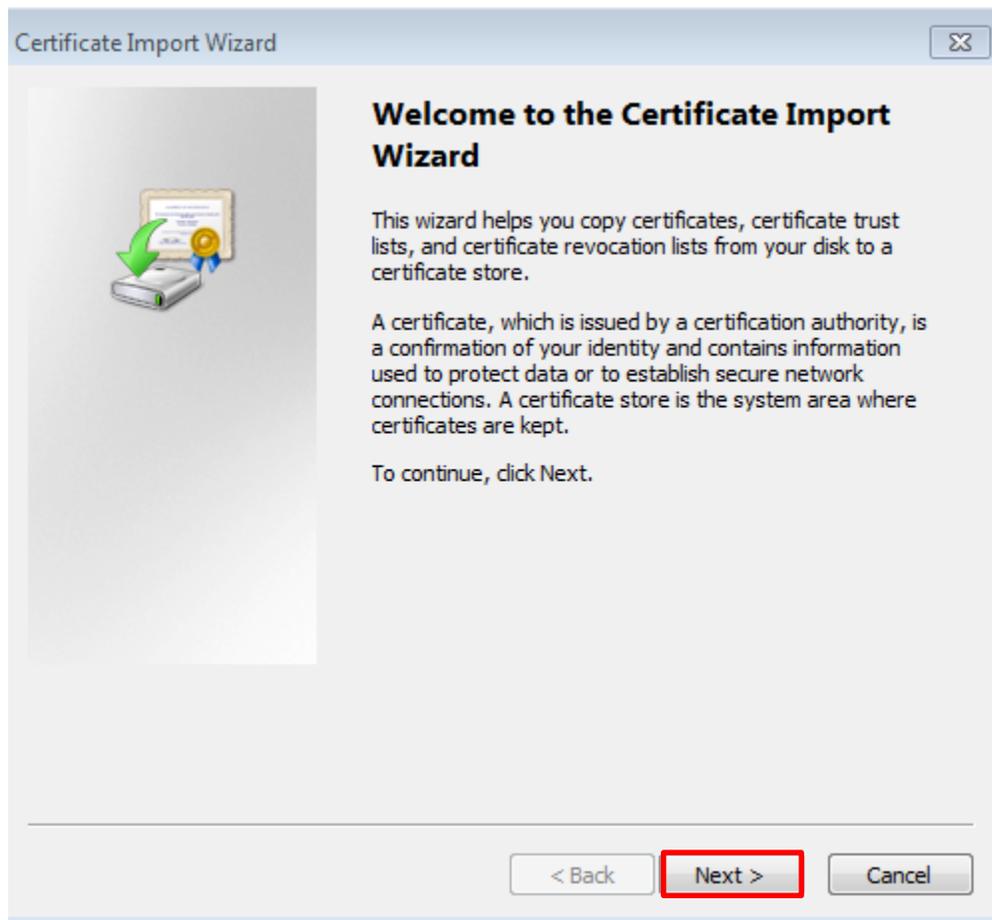


Figure 3. Welcome Certificate Import Wizard

2. Click the **Next** button.

The File to Import pop-up window appears.

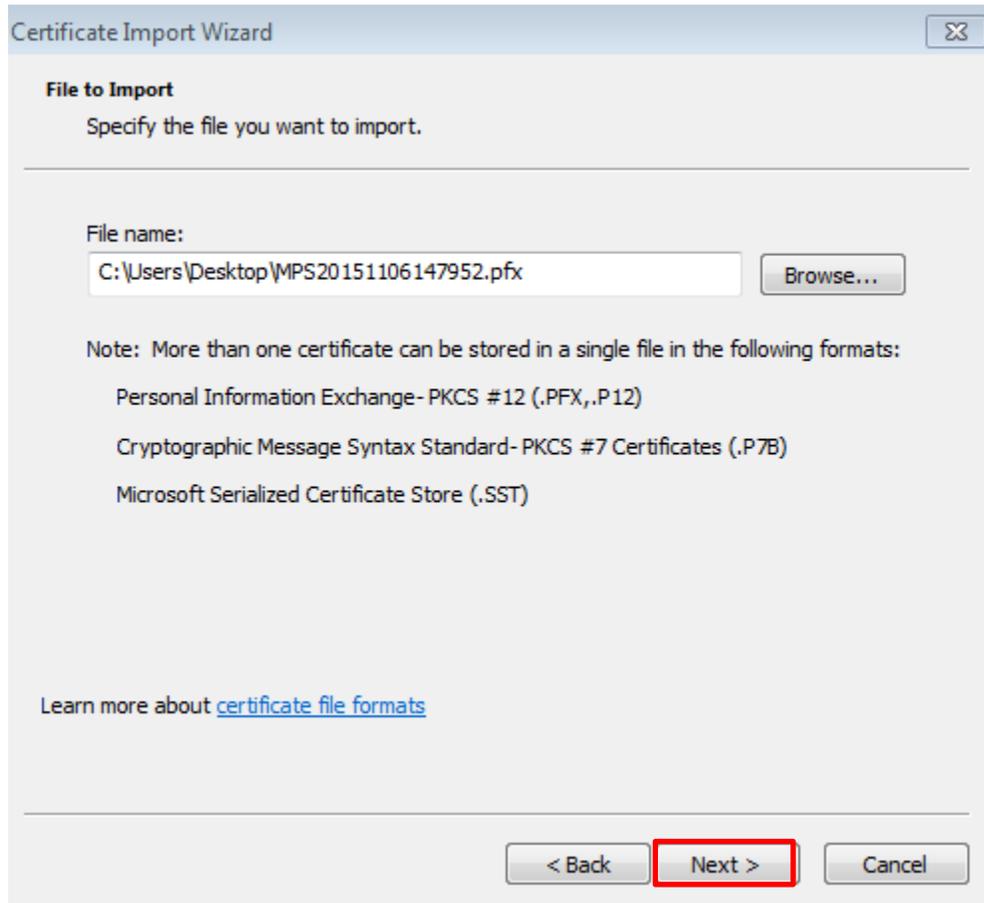
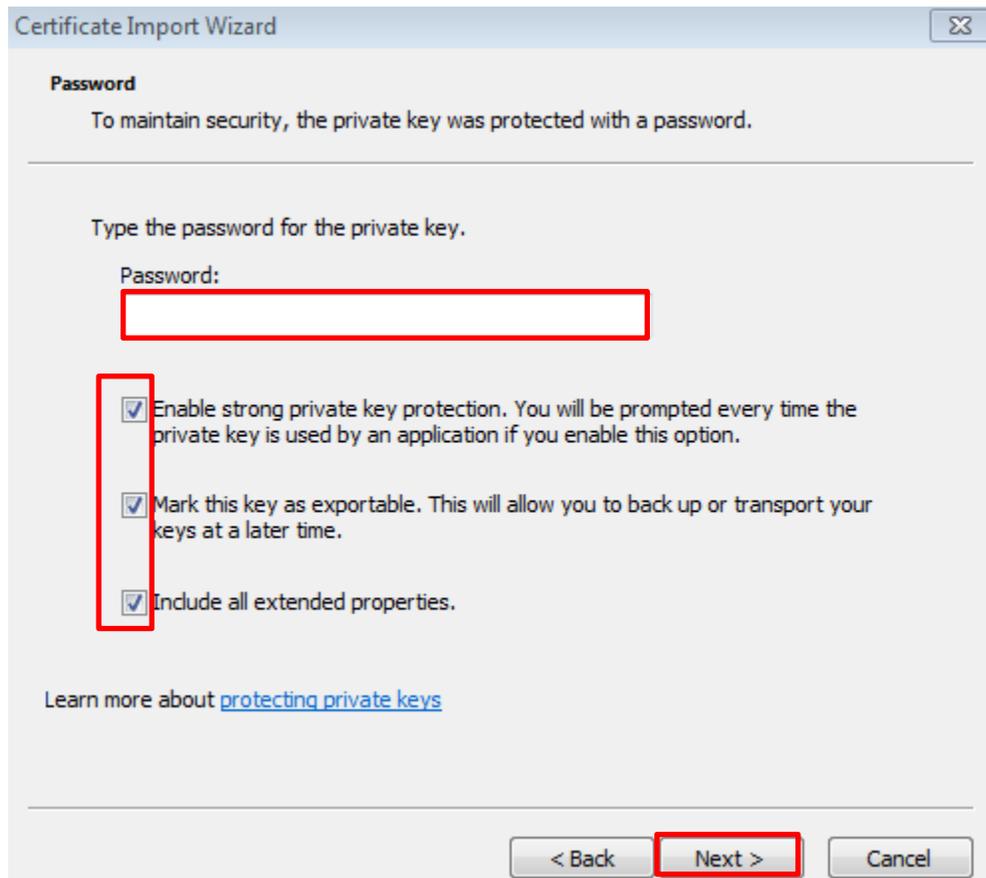


Figure 4. File to Import

The path to the digital certificate file is already entered in the File Name field.

3. Click the **Next** button.

The Password pop-up window appears.



The screenshot shows a dialog box titled "Certificate Import Wizard" with a close button in the top right corner. The main heading is "Password". Below it, a message states: "To maintain security, the private key was protected with a password." A horizontal line separates this from the next section, which says "Type the password for the private key." There is a "Password:" label followed by an empty text input field. Below the input field are three checked checkboxes, each with a red box around it: "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.", "Mark this key as exportable. This will allow you to back up or transport your keys at a later time.", and "Include all extended properties." At the bottom left, there is a link: "Learn more about [protecting private keys](#)". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a red box.

Figure 5. Password

4. Enter your password in the Password field.

NOTE: Use the same password you used to download the Digital Certificate

5. Select all check boxes.
6. Click the **Next** button.

The Certificate Store pop-up window appears.

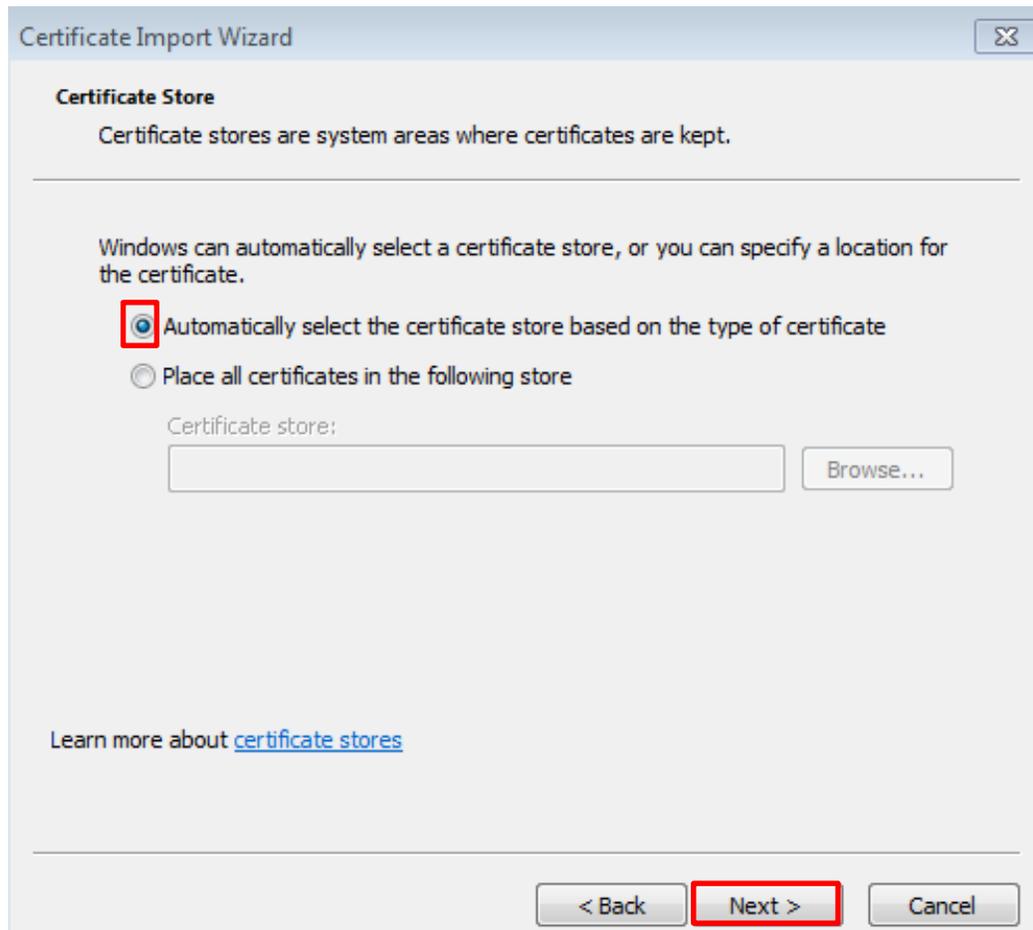


Figure 6. Certificate Store

7. Keep default selection
8. Click the **Next** button.

The Completing Certificate Import Wizard pop-up window appears.

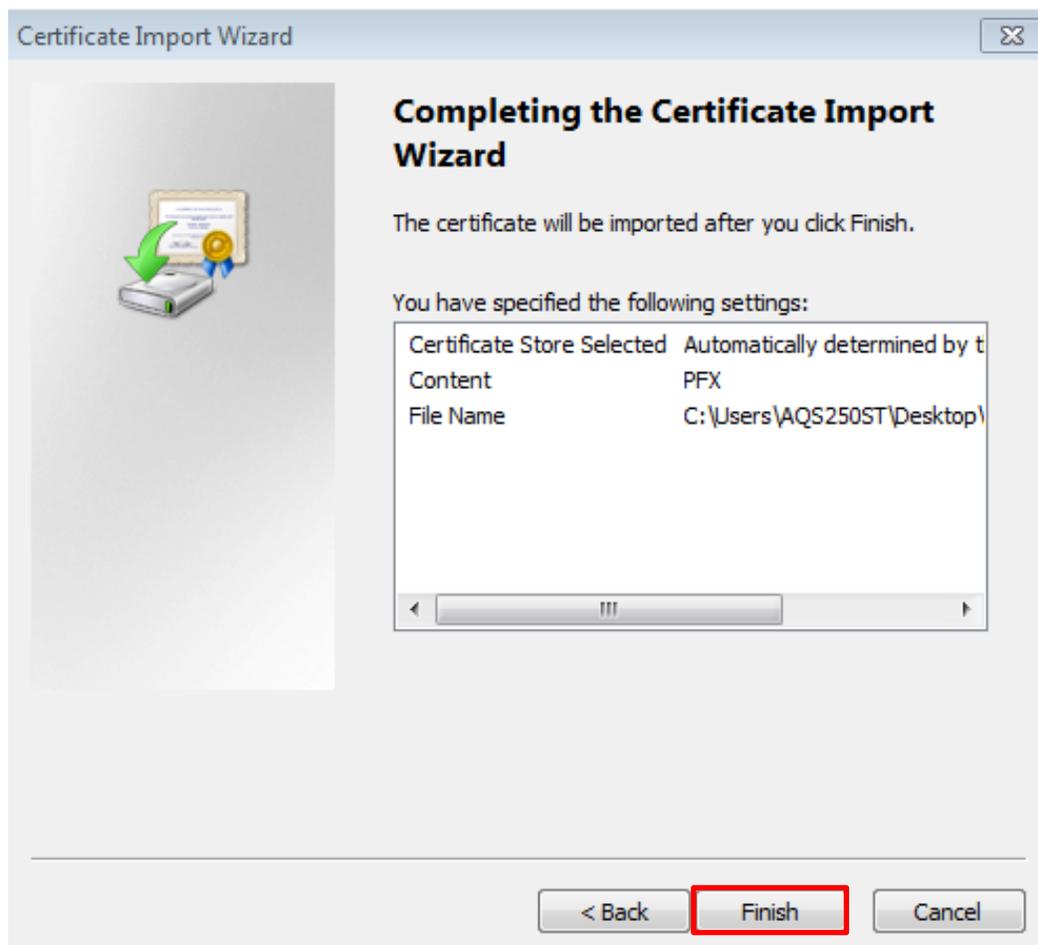


Figure 7. Completing Certificate Import Wizard

9. Click Finish

Set Security pop-up window appears.



Figure 8. Set Security

10. Click the **Set Security Level** button.

The Select Security Level pop-up window appears.



Figure 9. Select Security Level

11. Select the **High** radio button.
12. Click the **Next** button.

The Create Password pop-up window appears.

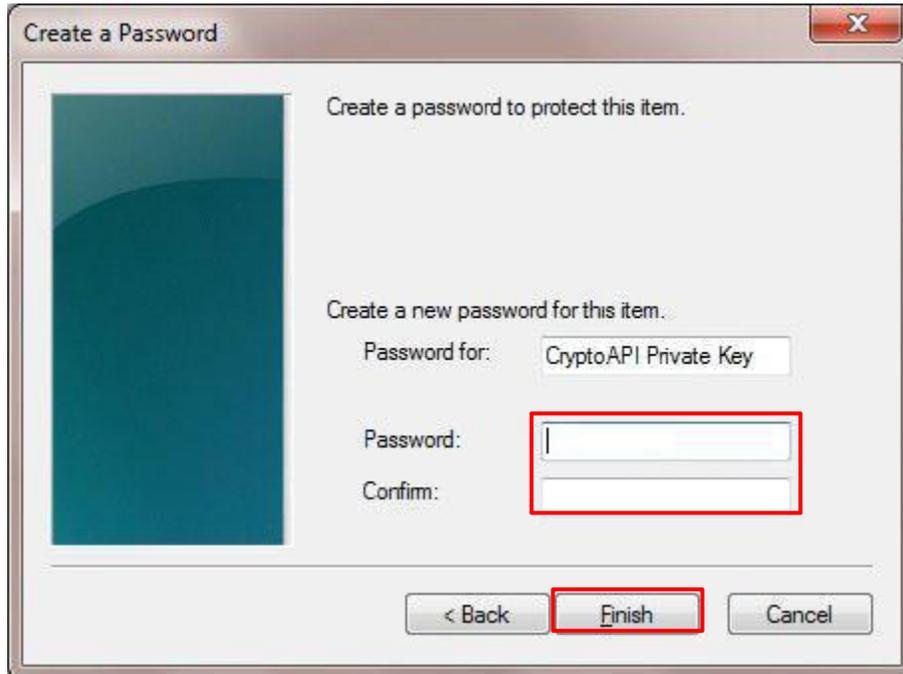


Figure 10 shows a "Create a Password" dialog box. The dialog has a title bar with a close button. The main content area contains the text "Create a password to protect this item." followed by "Create a new password for this item.". Below this, there are three input fields: "Password for:" with the value "CryptoAPI Private Key", "Password:", and "Confirm:". The "Password:" and "Confirm:" fields are highlighted with a red rectangle. At the bottom, there are three buttons: "< Back", "Finish", and "Cancel". The "Finish" button is also highlighted with a red rectangle.

Figure 10. Create Password

13. Enter your password in the Password field.

NOTE: Use the same password you used to download the Digital Certificate

14. Click the Finish button.

15. Click the OK button.

16. Click the OK button when prompted that the import was successful.

SET THE DEFAULT SIGNATURE

Open Adobe Reader > Go to Edit (from the menu bar) > Preferences

The Preferences pop-up window appears

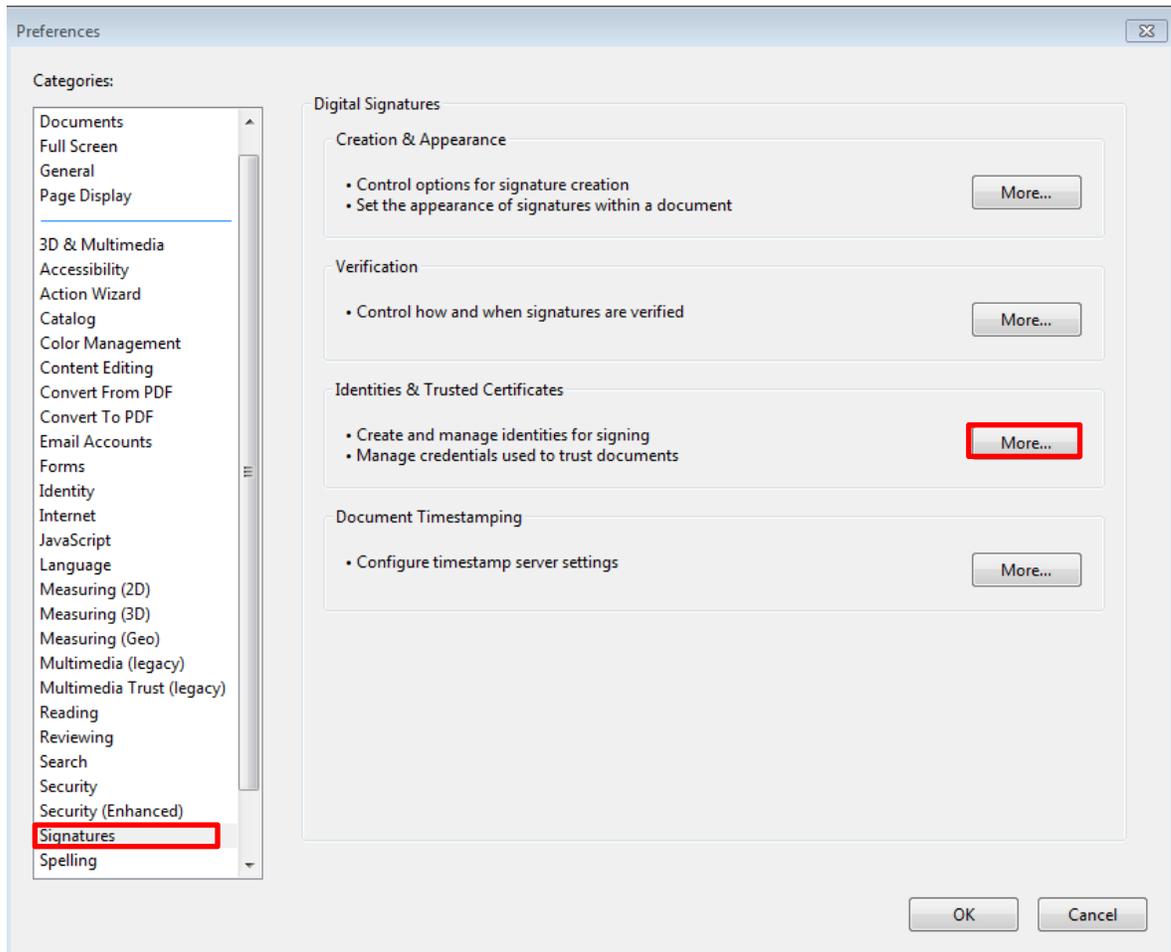


Figure 11. Preferences

1. If not already selected, select **Signatures** from the Categories listing (as shown in the previous figure).
2. Click the **More** button located next to the **Identities & Trusted Certificates** header (as shown in the previous figure).

The Digital ID and Trusted Certificate Settings window appears.

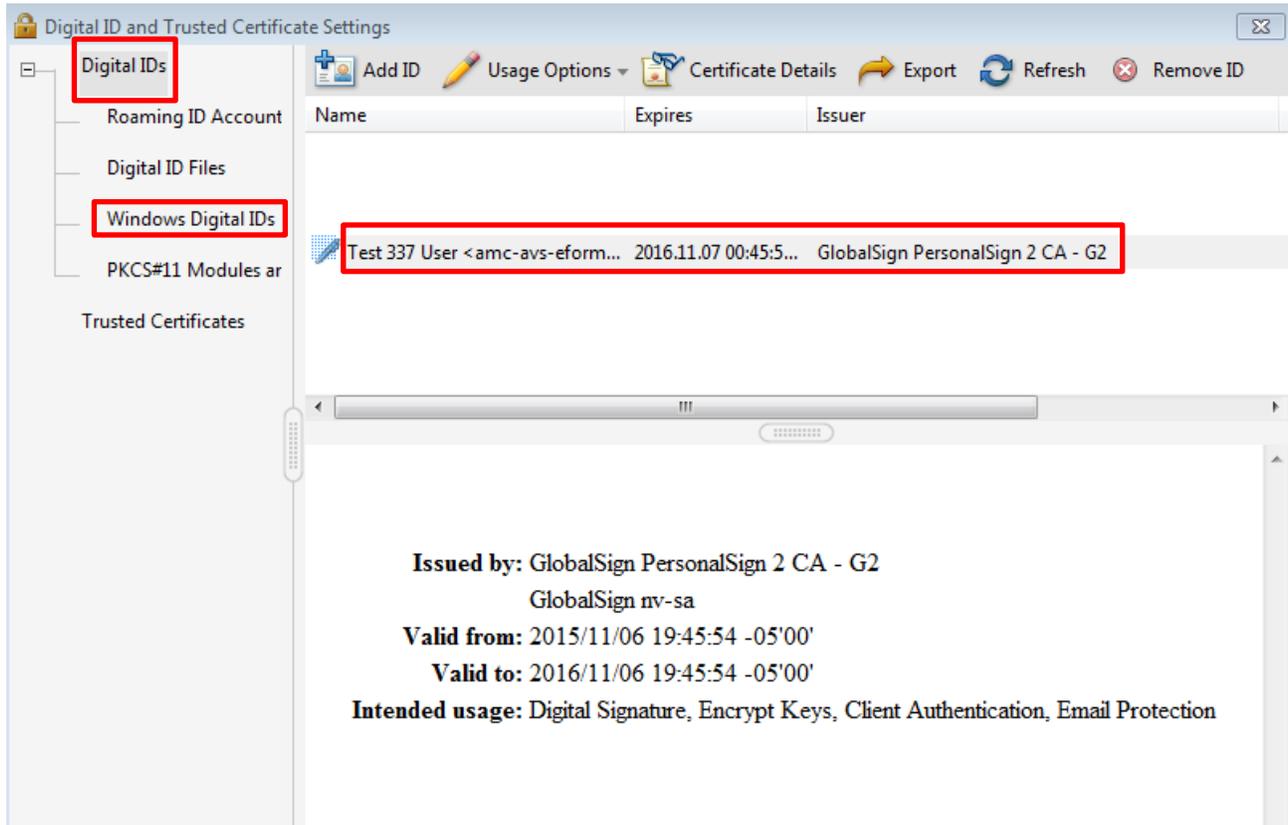


Figure 12. Digital ID's

3. Expand the Digital ID's section on the far left hand side of the window and select Windows Digital ID's (as shown in the previous figure).
4. In the list of Digital ID's, locate and highlight the Digital ID file that was just installed. Scroll to the far right to see the ID's expiration date. This will ensure you have chosen the newest ID.

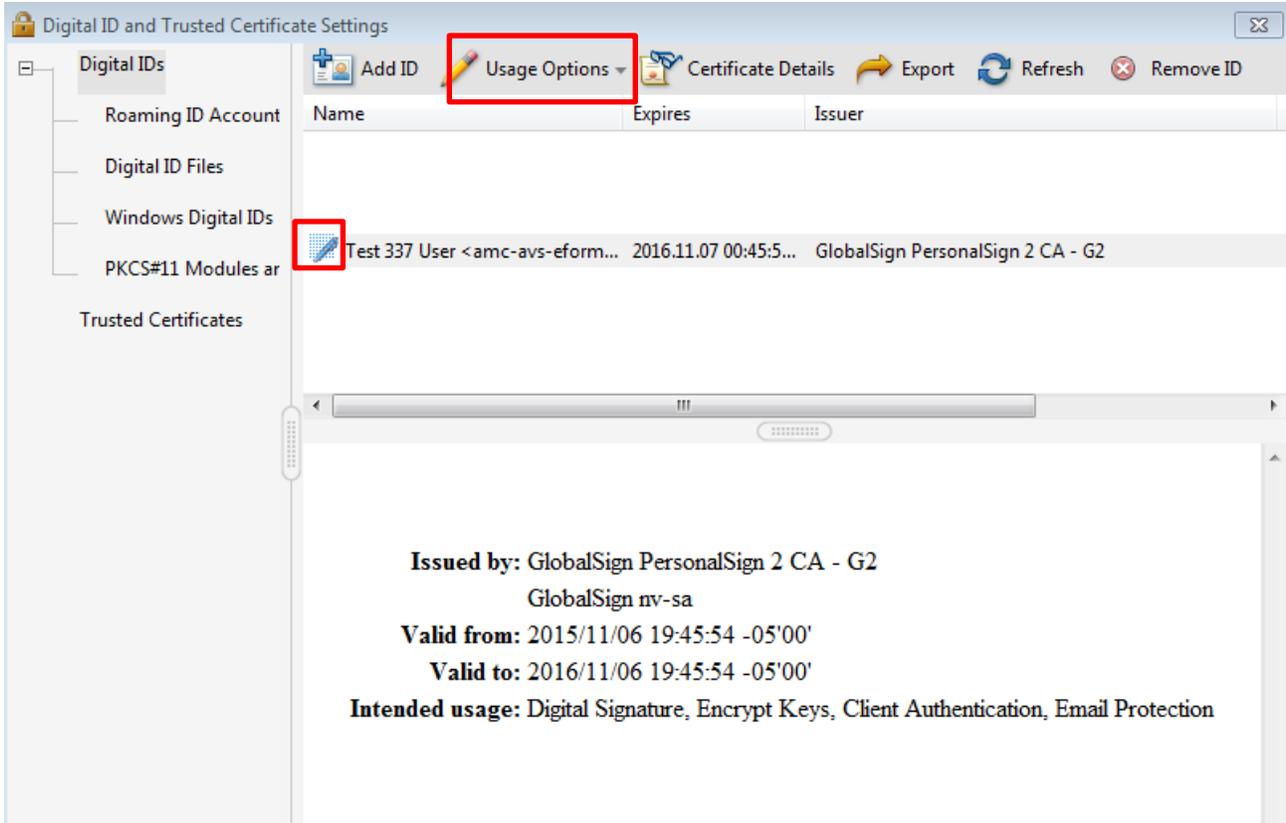


Figure 13. Digital ID's

5. Once the correct ID is selected, Click on: **Usage Options** and choose **Use For Signing** from the drop down menu (as shown in the previous figure).
6. The highlighted Digital ID is set as the default signature when the icon of a pen displays next to it (as shown in the previous figure).
7. Click the **X** in the top right corner of the window to exit.
8. Click OK at the Preferences window and close out of Adobe Reader.