

FedLine Web[®] Customer Certificate Contingency Procedures

Version 2.0

Contents

- FedLine Web Certificate Contingency Procedures 2**
 - Certificate Export Procedures..... 2
 - Certificate Import Procedures..... 10
- Installing the Federal Reserve Banks Certificate Authority (CA) Certificates 21**
 - FRB Services Root CA Certificate..... 21
 - FRB Services Issuing CA Certificate 26

"FedLine Web" is a registered service mark of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at FRBservices.org.

"Internet Explorer" and "Windows" are registered trademarks of Microsoft Corporation.

FedLine Web® Certificate Contingency Procedures

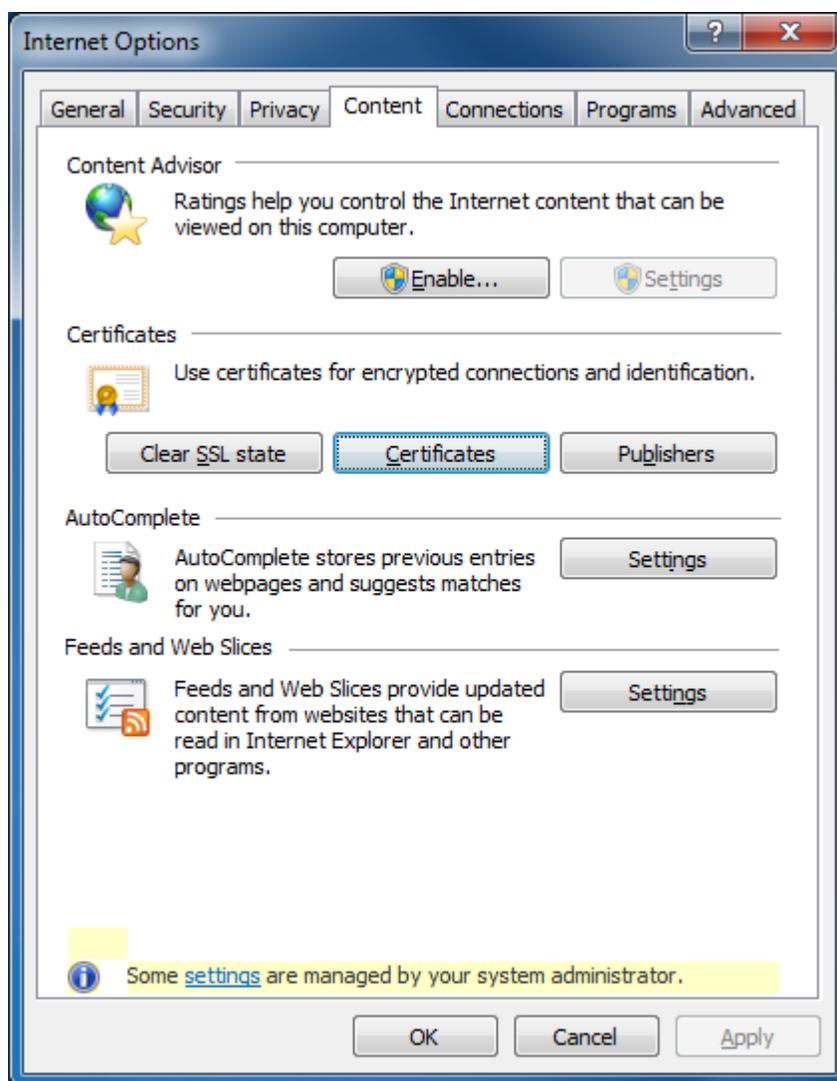
This guide provides step-by-step information to help you export a FedLine Web® certificate for your Internet Explorer® browser for contingency purposes. We recommend that you create a copy of your FedLine Web certificate in the event your stored certificate is corrupted or deleted.

Your screen images and language may vary slightly from the images in this guide depending on the versions of Windows and Internet Explorer you are using. Review the [FedLine Web Hardware and Software Requirements page](#) on FRBservices.org for a list of supported platforms.

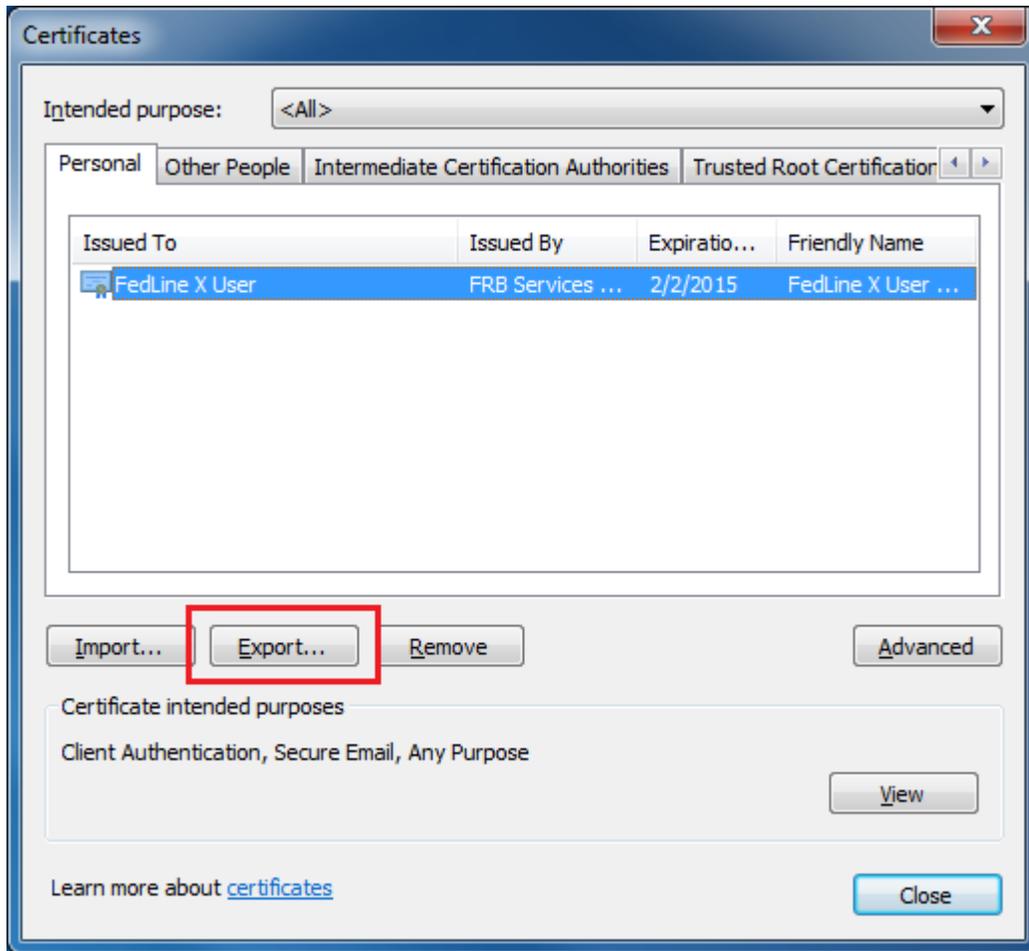
If you need browser assistance, please contact the Customer Contact Center at 1-888-333-7010.

Certificate Export Procedures

1. Open Internet Explorer. Click **Tools** → **Internet Options** → **Content**. Then click **Certificates**.



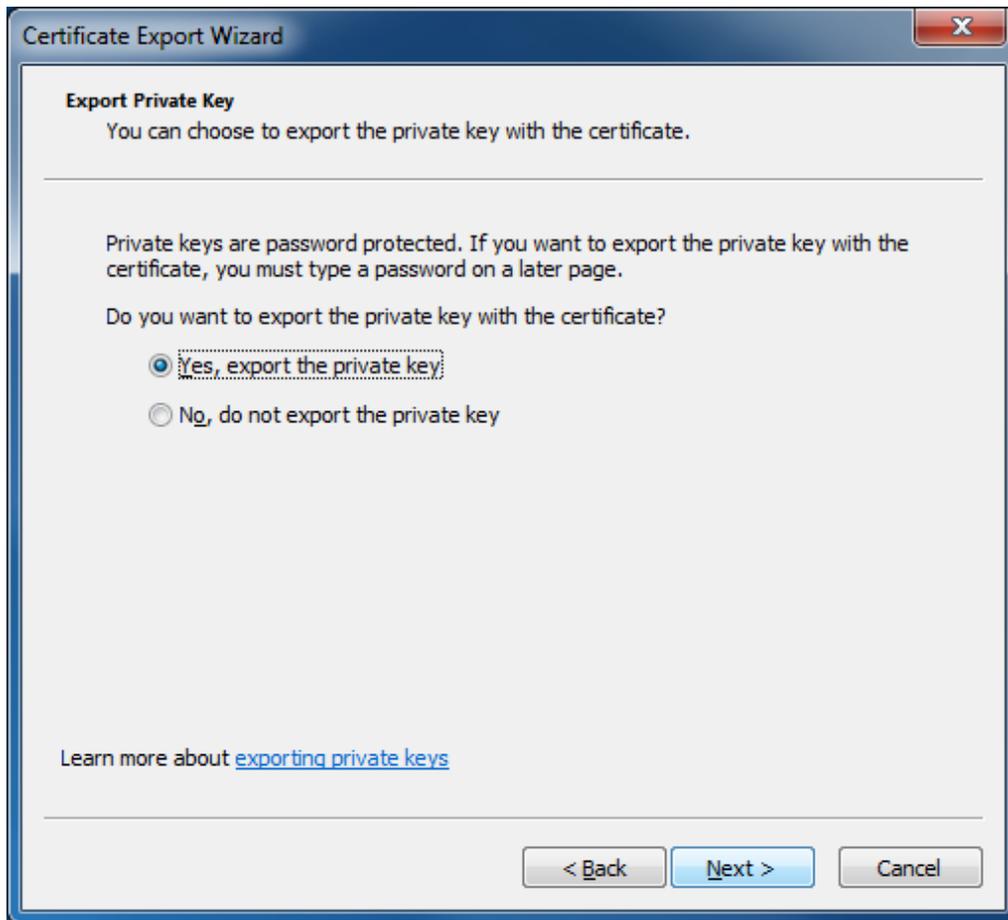
2. Highlight the certificate you want to export and click **Export**.



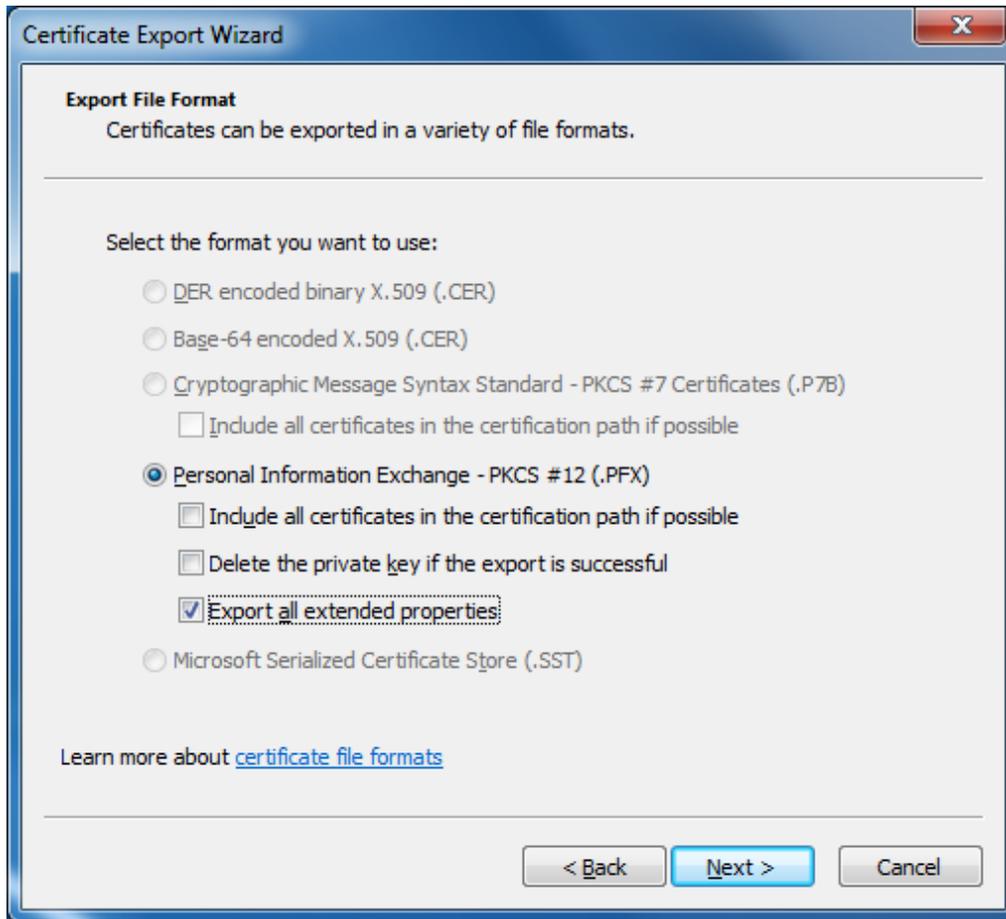
3. This opens the Certificate Export Wizard. Click **Next**.



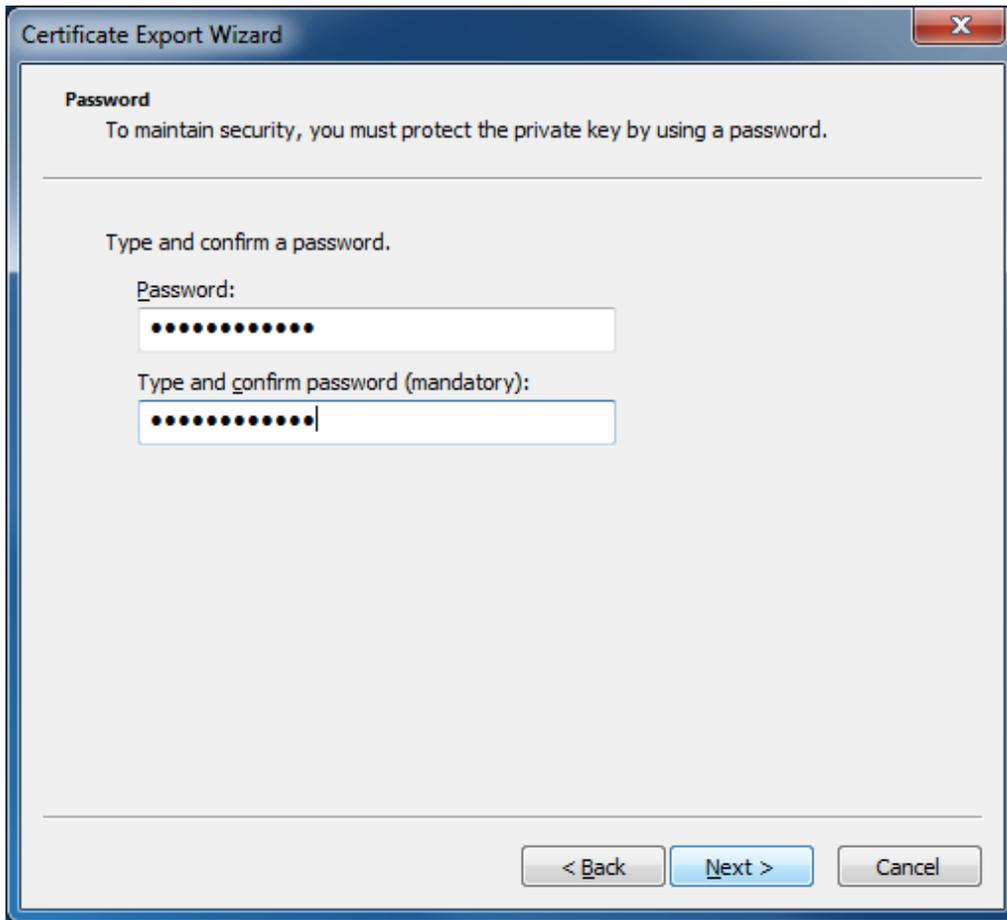
4. Ensure that **Yes, export the private key** is selected and click **Next**.



5. Choose the settings indicated below and click **Next**.

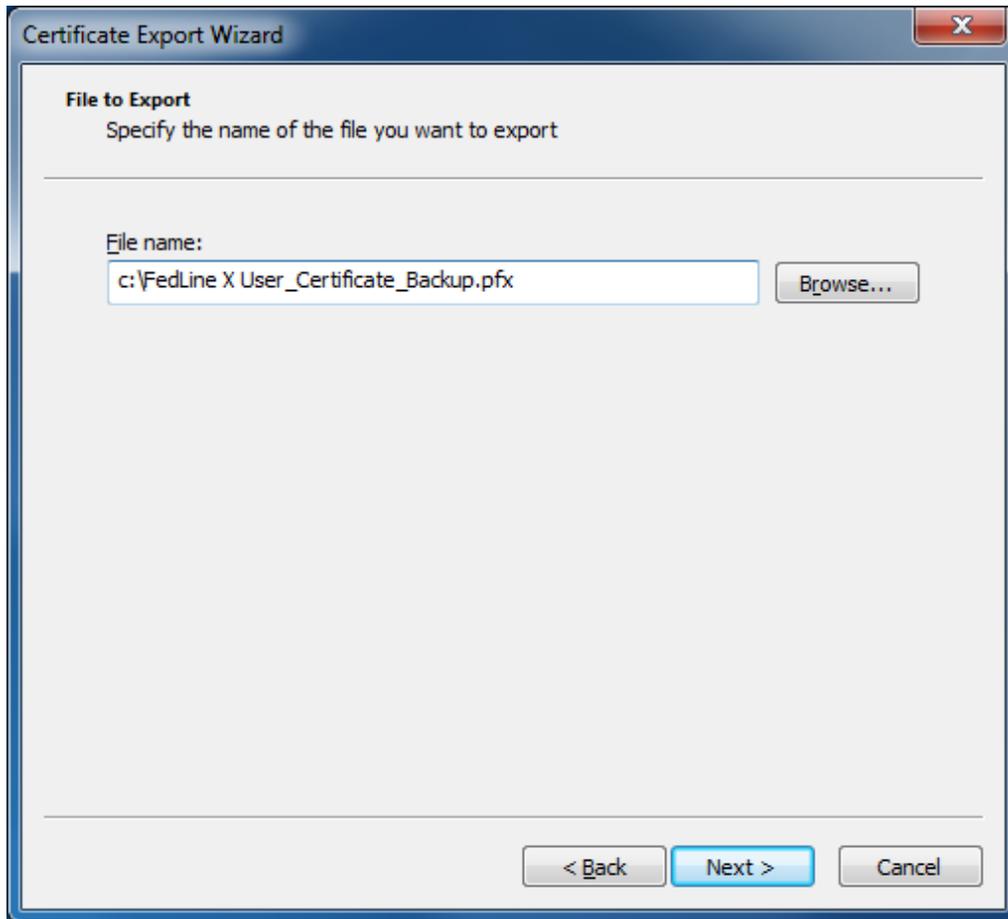


6. Enter a strong certificate password as explained in the [Federal Reserve Banks' Password Practice Statement](#). Click **Next**.

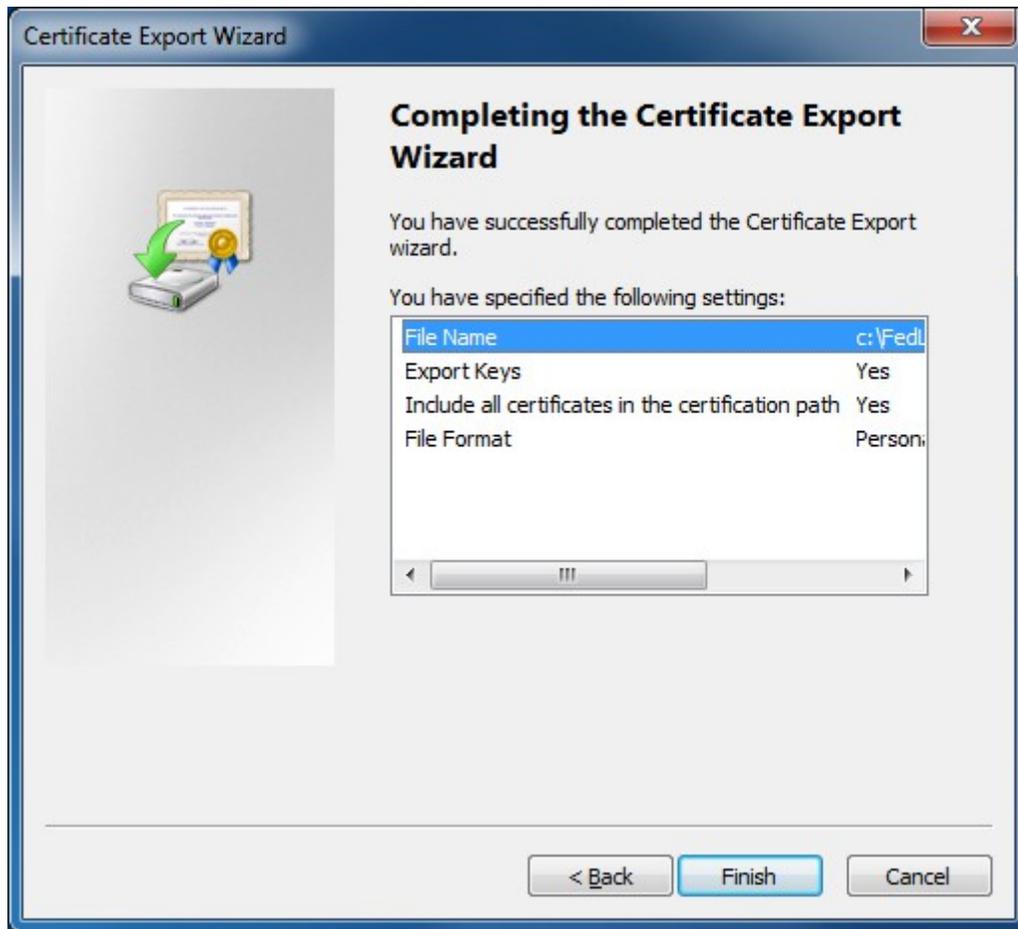


The image shows a Windows-style dialog box titled "Certificate Export Wizard". The window has a standard title bar with a close button (X) in the top right corner. The main content area is titled "Password" and contains the following text: "To maintain security, you must protect the private key by using a password." Below this is a horizontal line. The text "Type and confirm a password." is displayed. There are two input fields: the first is labeled "Password:" and contains ten black dots; the second is labeled "Type and confirm password (mandatory):" and also contains ten black dots. At the bottom of the dialog, there are three buttons: "< Back" (disabled), "Next >" (active/highlighted), and "Cancel" (disabled).

7. Specify the destination of the file. Click **Next**.



8. Click **Finish**.

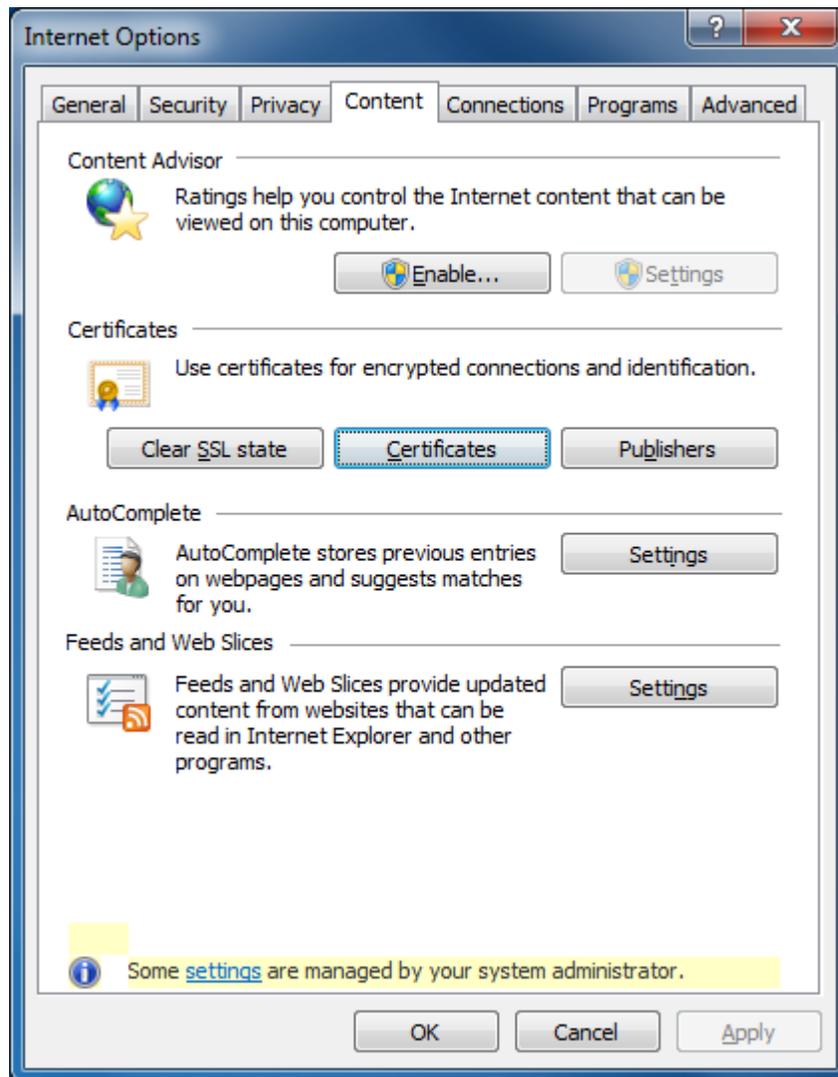


9. Ensure that you receive the following message. This completes the certificate export. Click **OK**.

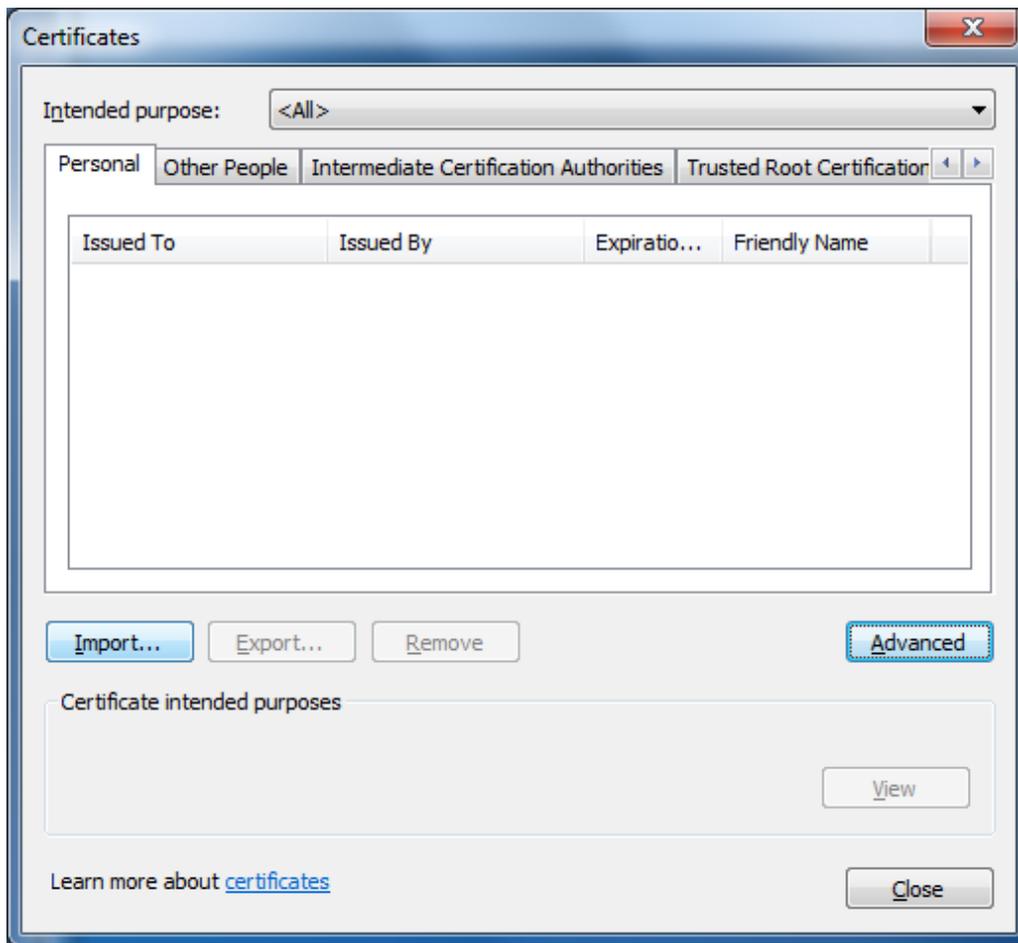


Certificate Import Procedures

1. Open Internet Explorer. Click **Tools** → **Internet Options** → **Content**. Click on **Certificates**.



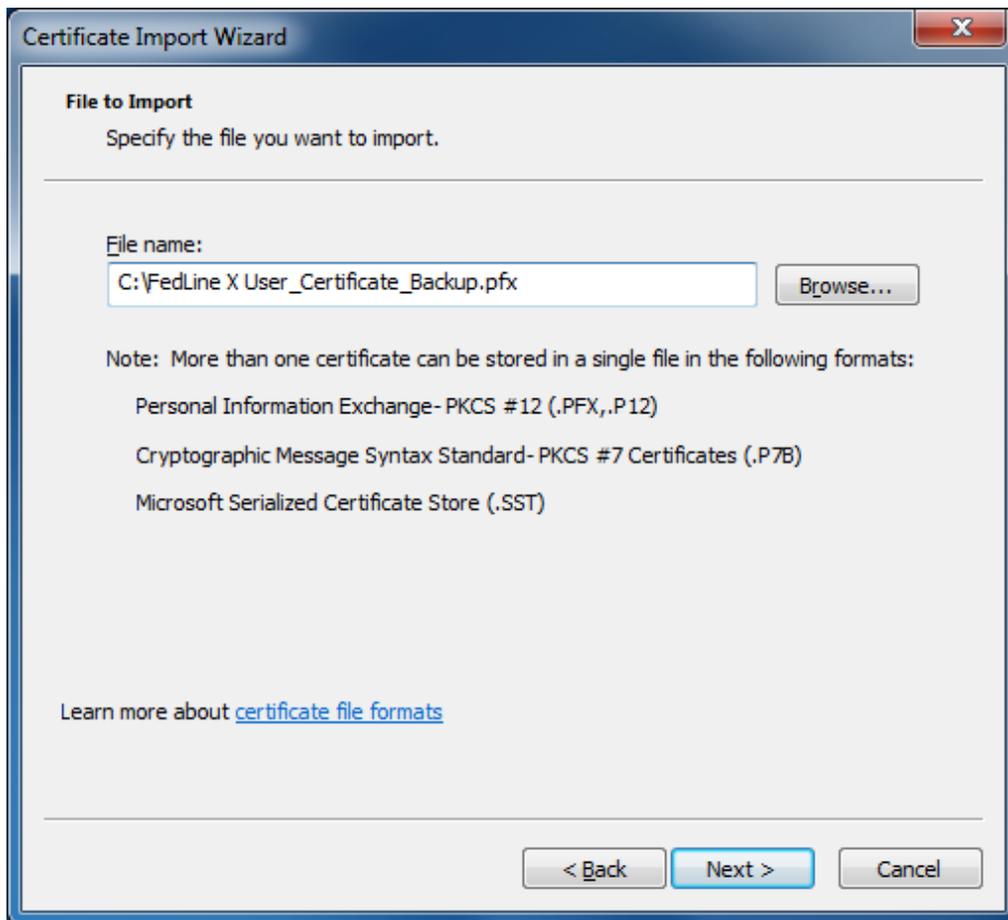
2. Click **Import**.



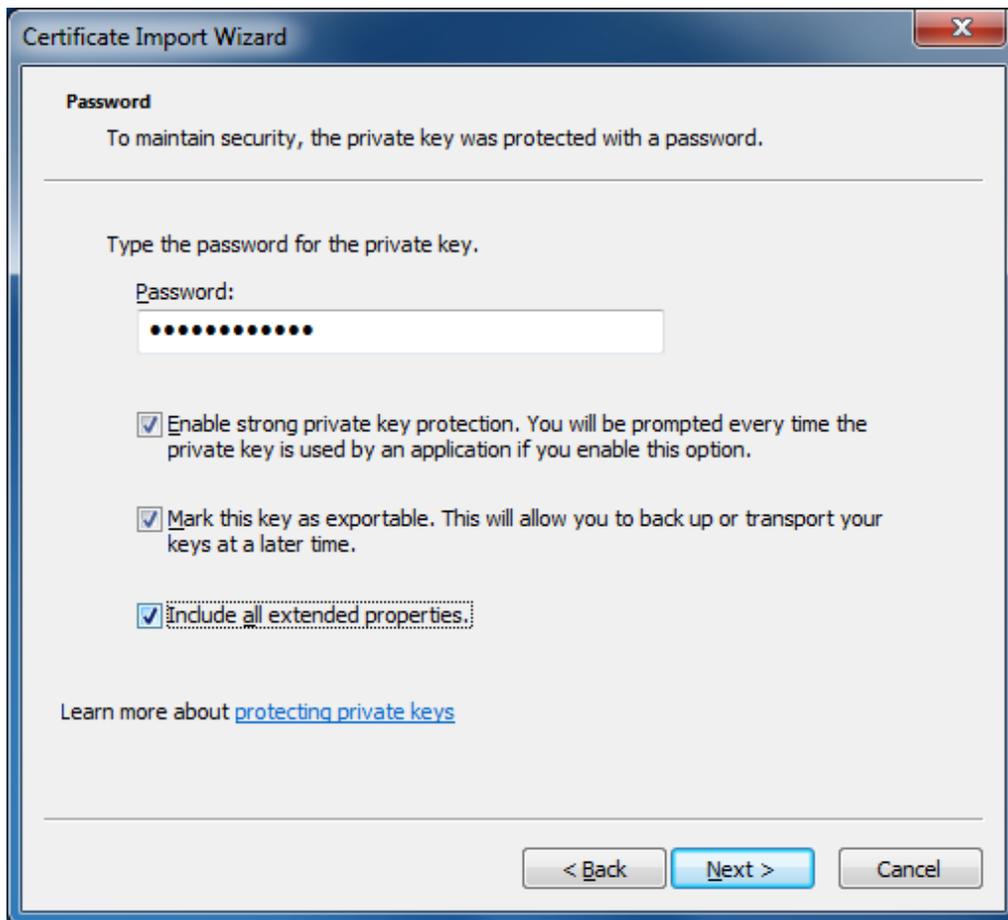
3. This opens the Certificate Import Wizard. Click **Next**.



4. Browse to the certificate file that you would like to Import. Click **Next**.

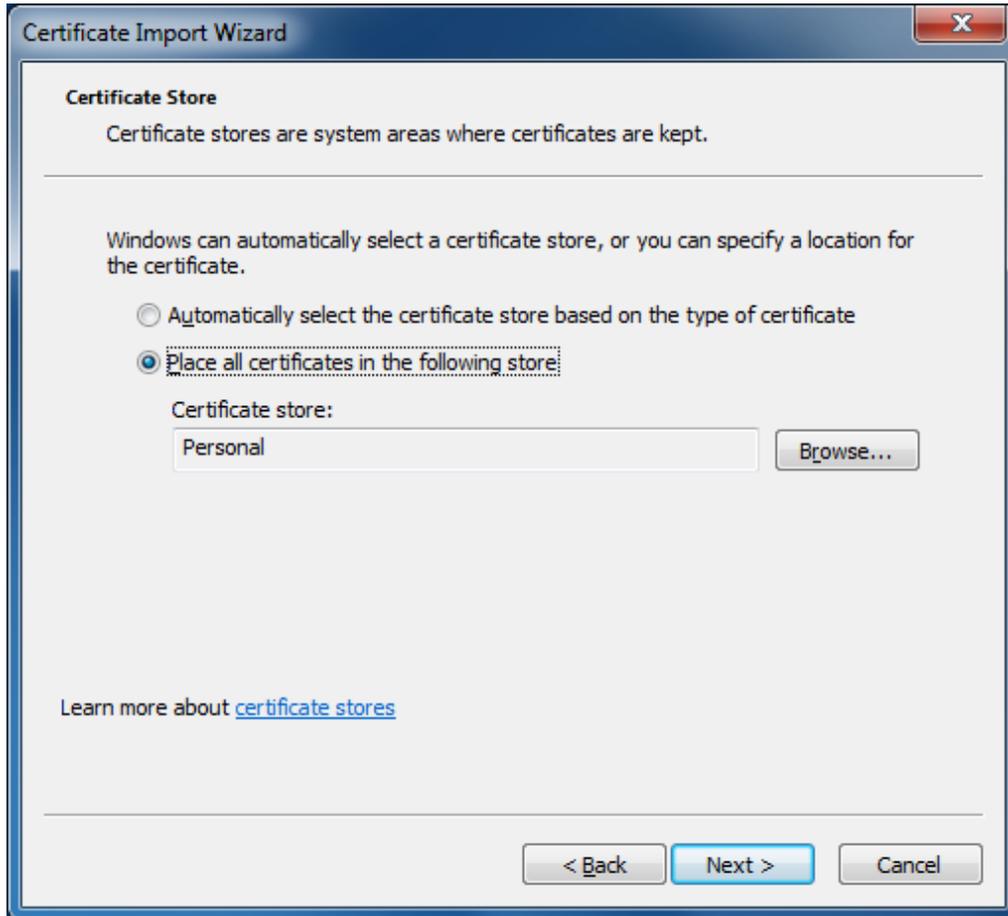


5. Enter the password for the private key and ensure that the settings below are selected. Click **Next**.

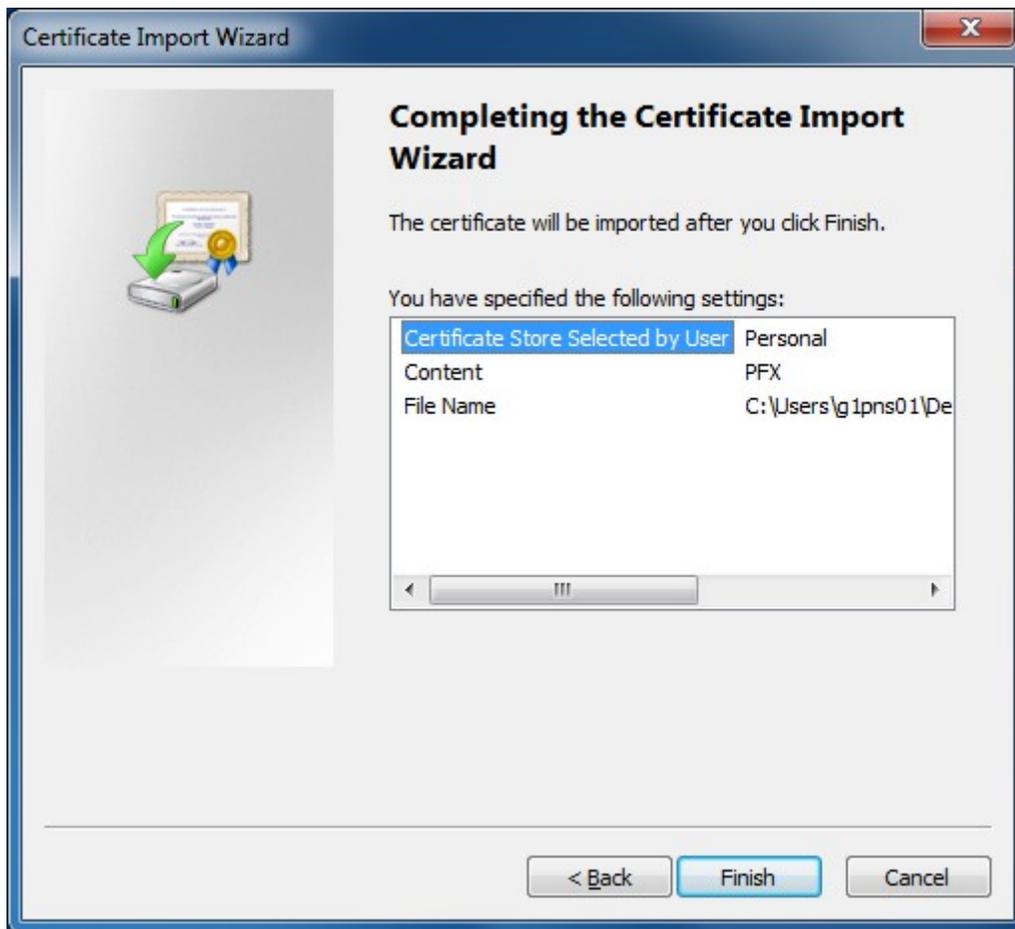


The image shows a Windows-style dialog box titled "Certificate Import Wizard". The window has a standard title bar with a close button (X) in the top right corner. The main content area is titled "Password" and contains the following text: "To maintain security, the private key was protected with a password." Below this is a horizontal line, followed by the instruction "Type the password for the private key." There is a text input field labeled "Password:" containing ten black dots. Below the input field are three checked checkboxes with the following descriptions: "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 of the main area is a blue hyperlink that says "Learn more about protecting private keys". At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted in blue), and "Cancel".

6. Ensure that the settings below are selected. **Place all certificates in the following store:** **Personal** will be selected automatically. Click **Next**.



7. Click **Finish**.



8. Once **Finish** is selected, you will see the following screen. Click **Set Security Level**.



9. Select **High**. Click **Next**.



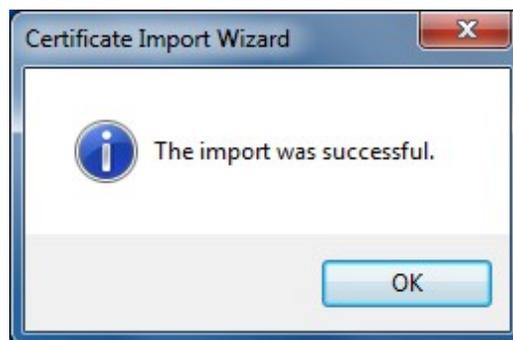
10. Specify a strong password for the certificate password as explained in the [Federal Reserve Banks' Password Practice Statement](#). Click **Finish**.



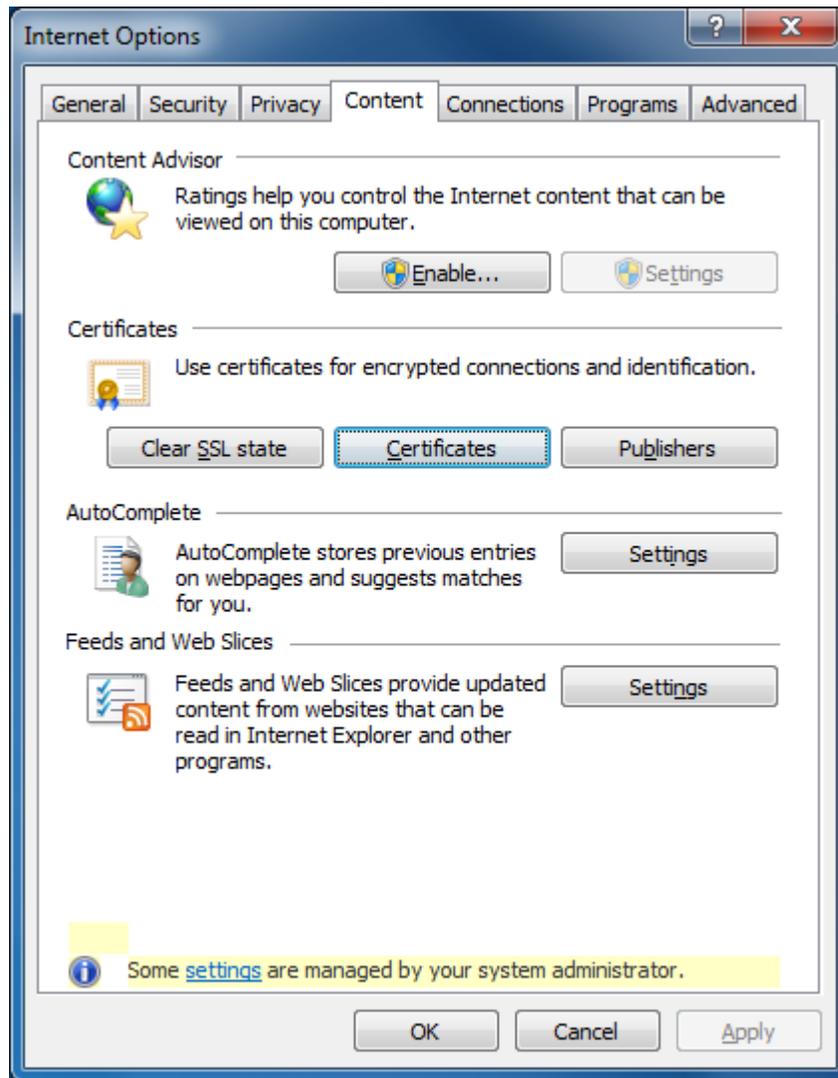
11. Note the Security level is now set to High. Click **OK**.



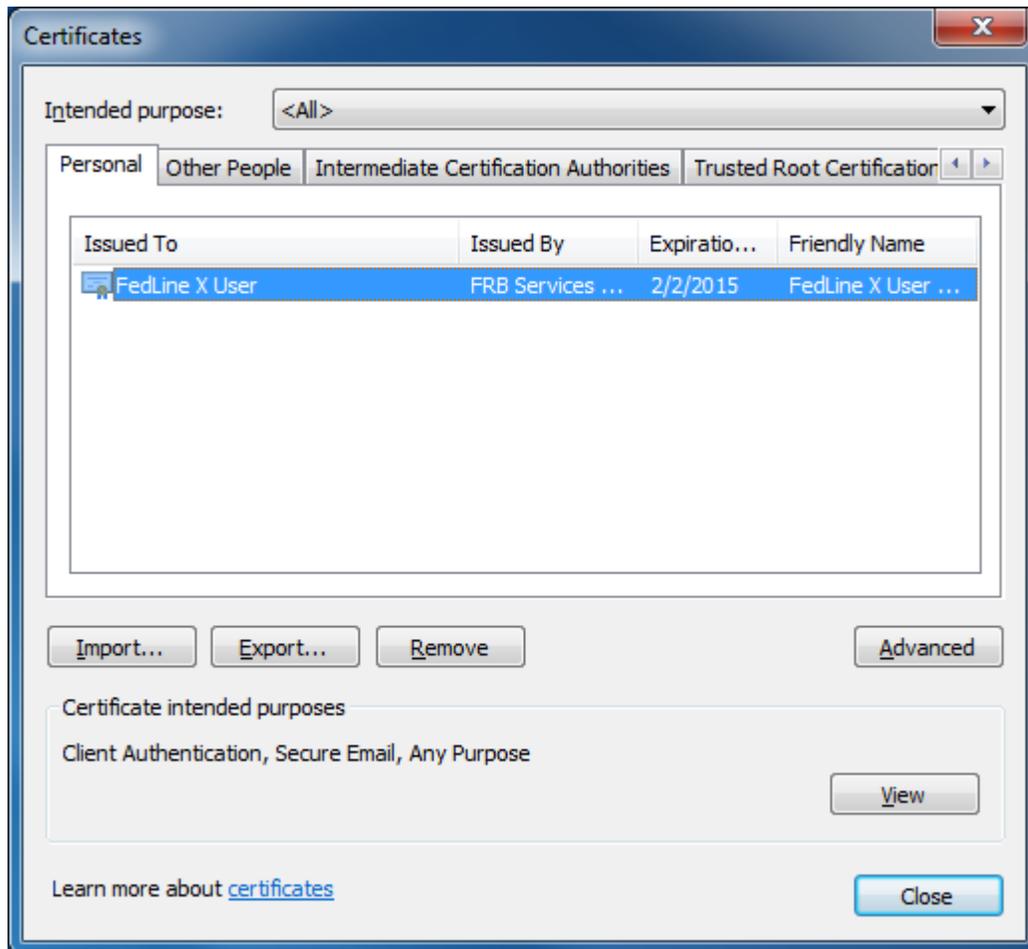
12. Ensure that you receive the following message. This completes the certificate import. Click **OK**.



13. Verify that your import was completed successfully. Open Internet Explorer and click **Tools** → **Internet Options** → **Content**. Click **Certificates**.



14. The newly imported certificate should appear in the Certificates section at this time.



Installing the Federal Reserve Banks Certificate Authority (CA) Certificates

Some users may need to manually install the Federal Reserve Bank CA Certificates. Follow the procedures below to complete this activity on any new computer that will be used to access Federal Reserve Bank Services.

FRB Services Root CA Certificate

1. To install the Federal Reserve Banks CA certificates on a PC that will be used to access Federal Reserve Bank Services, browse to the following URL:

https://registration.federalreserve.org/UserRegistration2/en_US/cacert.jsp

2. Two links to the separate certificates are listed. Click on **FRB Services Root CA Certificate**.

FEDERAL RESERVE BANK SERVICES

- [Certificate Registration Home](#)
- [Create Certificate](#)
- [Certification Authority Certificate](#)
- [Certification Practice Statement](#)

Federal Reserve Banks Certification Authority (CA) Certificate

If you are retrieving a Federal Reserve Banks (FRB) digital certificate you do not need to retrieve the FRB Services Root CA Certificate or the FRB Services Issuing CA Certificate. These certificates are automatically imported into your Web browser when you retrieve a FRB Digital Certificate.

The FRB Services Root CA and FRB Services Issuing CA Certificates allow users to verify that the Web site they are visiting is considered trustworthy and secure. With these credentials, your Web browser will automatically trust all Certificates assigned by the FRB Services Root and Issuing CAs.

If you have a need to select the following options, you will be asked if you want to accept the Certification Authority's Certificate on your Web browser. Accepting the FRB Services Root CA and FRB Services Issuing CA Certificates will import them directly into your Web browser.

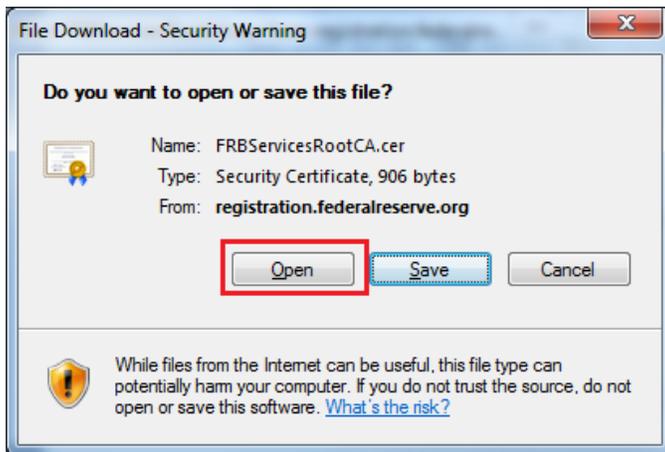
[FRB Services Root CA Certificate](#)

[FRB Services Issuing CA Certificate](#)

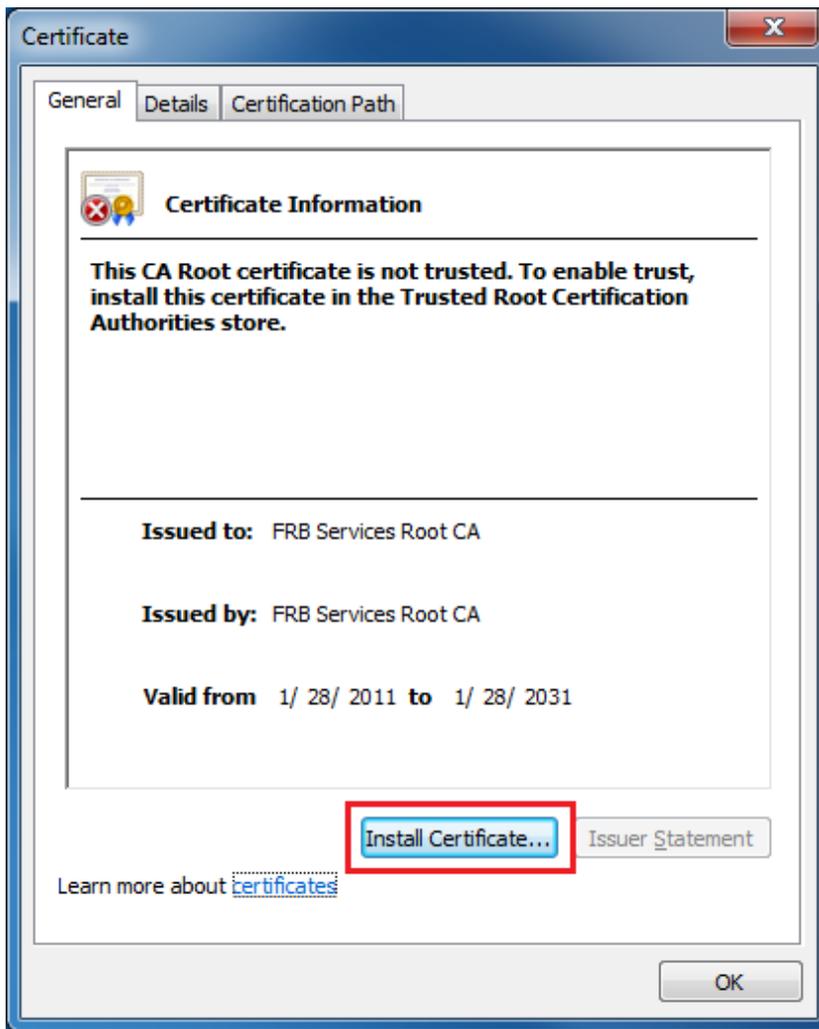
FRB Services Root CA Certificate (PEM encoding)

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIETUMXODANBgkqhkiG9w0BAQsFADBJMQswCQYDVQQGEwJ1
czEeMBwGA1UEChMVRmVrZXJhbCBSZSZNcnZlIEJhbmtzMRUwEwYDVoQLEwxs0kg
U2VydmljZXMxHTAbBgNVBAMTFEZZSQ1BTZXU2aWNlcyBSb290IENBMB4XDTEy
ODE4NTE1NFoXDTMxMDEyODE5MjE1NFowYzELMAkGA1UEBhMCdXMxHjAcBgNVBAoT
FUZlZGVyYWwgUmVzZXJ2ZSBCYW5rczEVMGMGA1UECzMMUUEtJIFN1cnZpY2VzMR0w
```

3. In the **File Download** prompt, click on the **Open** button.



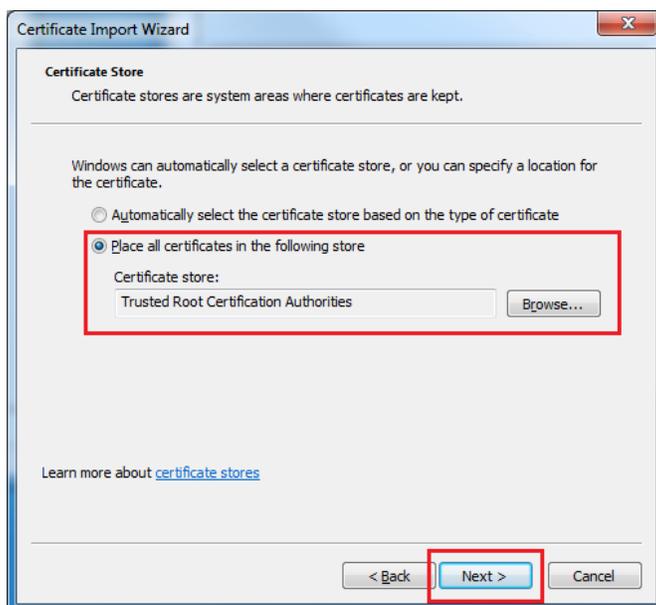
4. In the **Certificate Information** window, click on the **Install Certificate** button.



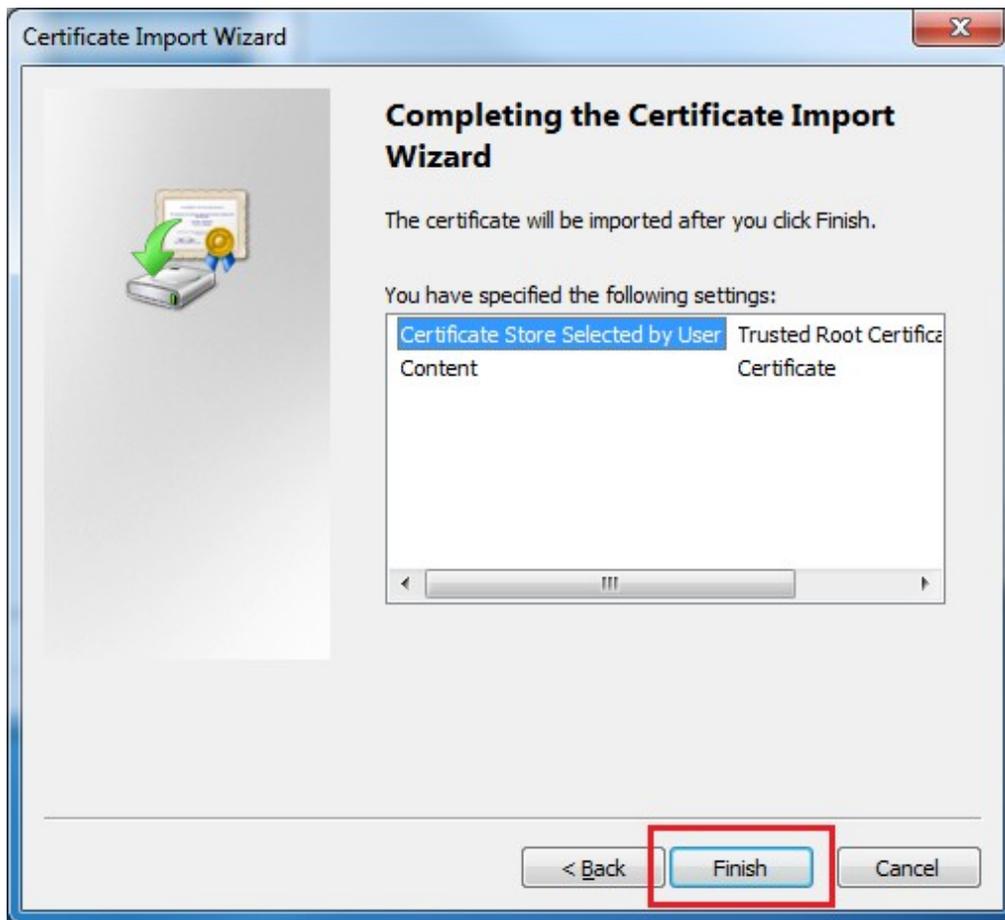
5. The Certificate Import Wizard will be initiated. Click on the **Next** button.



6. Select **Place all certificates in the following store** and click **Browse**. Select the **Trusted Root Certification Authorities** option and click **OK**. Verify the selection and click on the **Next** button.

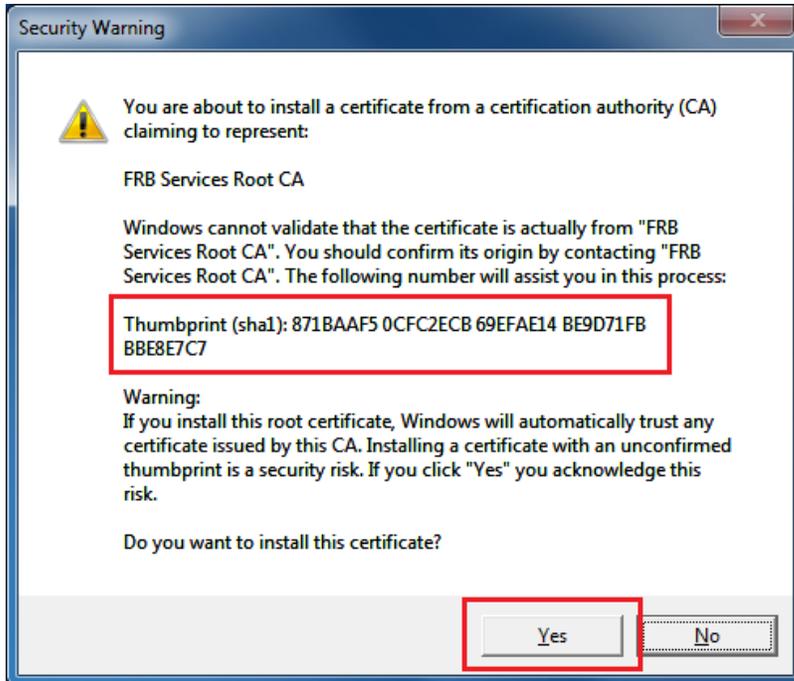


7. Click **Finish**.



8. A Security Warning prompt will be displayed containing the Thumbprint information for the **FRB Services Root CA Certificate**. (This will not be displayed for the FRB Services Issuing CA Certificate.) Verify the Thumbprint and click on the **Yes** button to install the certificate.

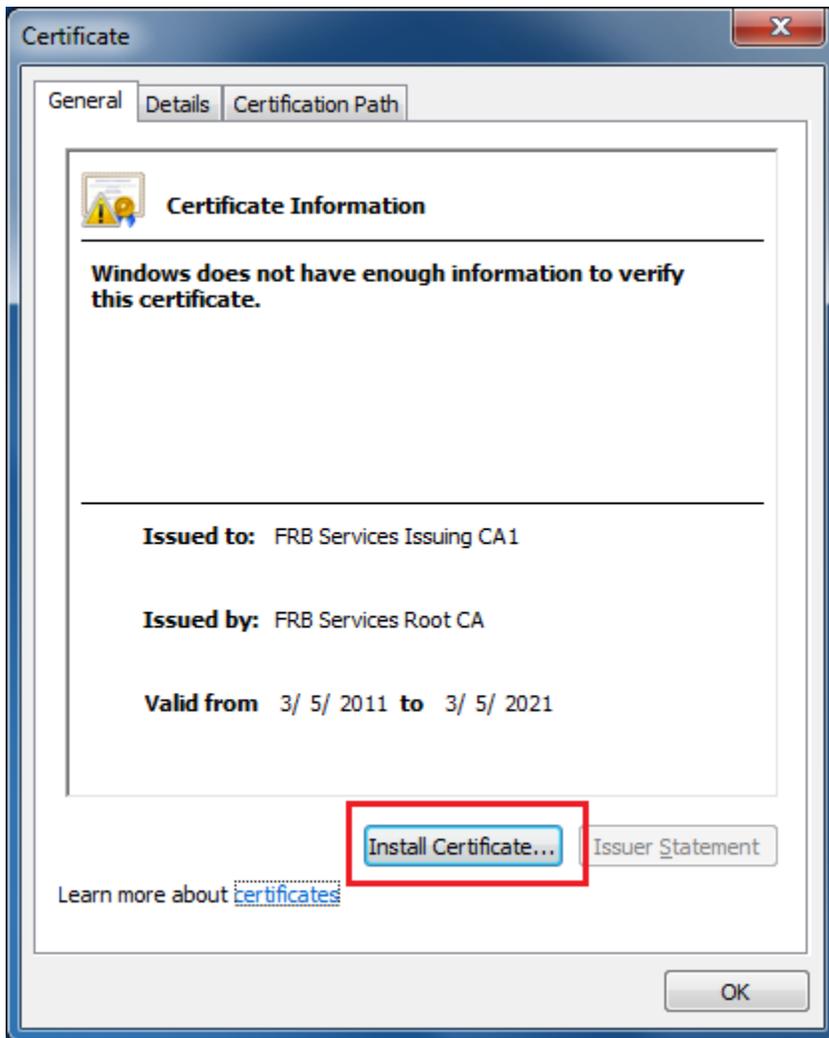
Thumbprint (sha1): 871BAAF5 0CFC2ECB 69EFAE14 BE9D71FB BBE8E7C7



9. A confirmation prompt will be displayed when the certificate has been installed successfully. Click on the **OK** button to complete the FRB Services Root CA Certificate installation.



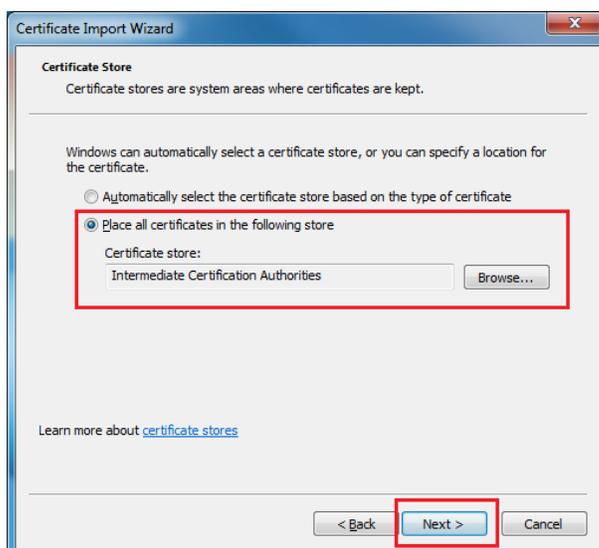
4. In the Certificate Information window, click on the **Install Certificate** button.



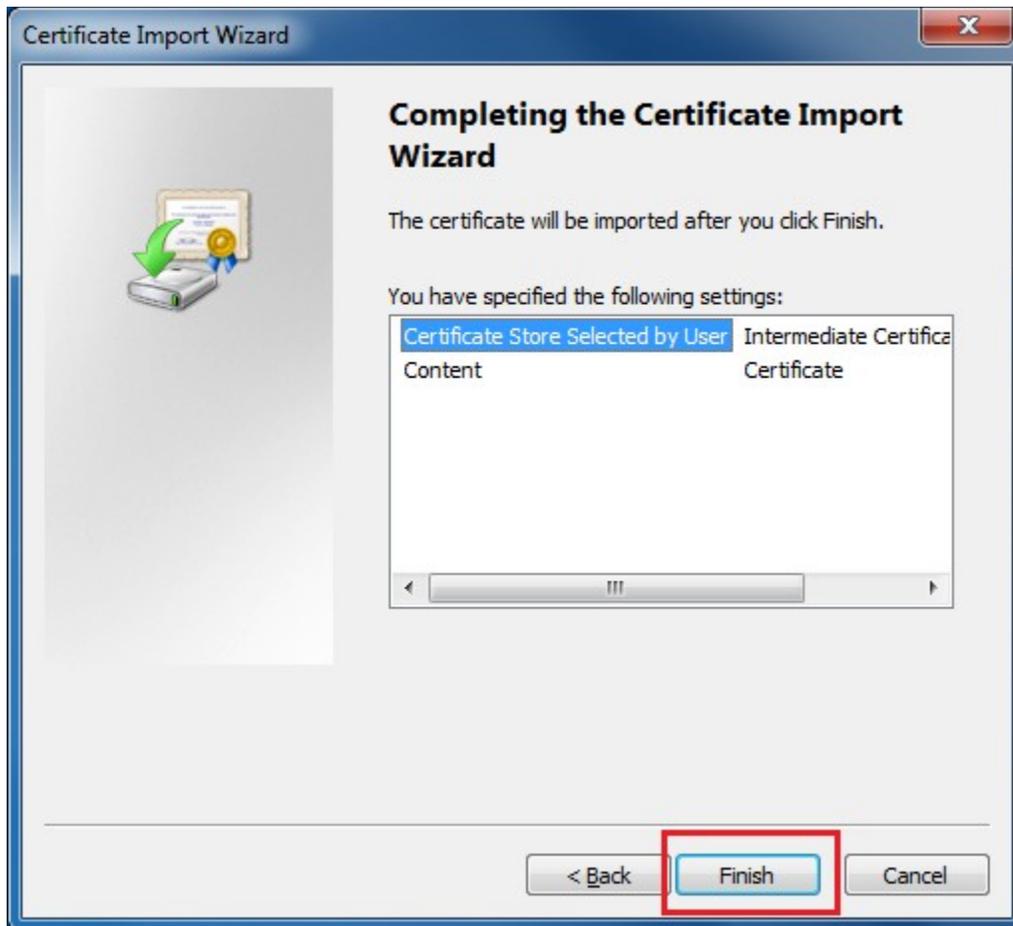
5. The Certificate Import Wizard will be initiated. Click on the **Next** button.



6. Select **Place all certificates in the following store** and click **Browse**. Select the **Intermediate Certification Authorities** option and click **OK**. Verify the selection and click on the **Next** button.



7. Click **Finish**.



8. A confirmation prompt will be displayed when the certificate has been installed successfully. Click on the **OK** button to complete the FRB Services Issuing CA Certificate installation.

