

FedLine Web[®] Certificate Contingency Procedures

Version 3.1

Contents

FedLine Web® Certificate Contingency Procedures	2
Certificate Export Procedures	2
Certificate Import Procedures	7
Installing the Federal Reserve Banks Certificate Authority (CA) Certificates	13
FRB Services Root CA Certificate	13
FRB Services Issuing CA Certificate.....	16

"FedLine" and "FedLine Web" are service marks of the Federal Reserve Banks. A list of marks related to financial services products that are offered by the Federal Reserve Banks is available at www.FRBservices.org.

"Windows" is a registered trademark of Microsoft Corporation.

FedLine Web® Certificate Contingency Procedures

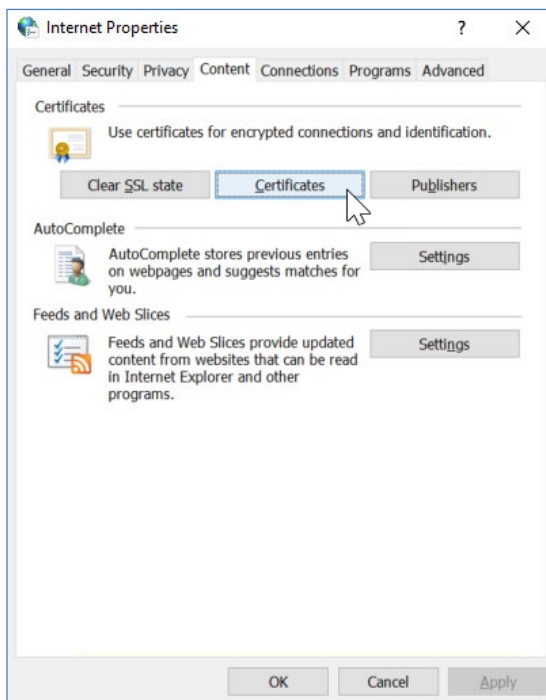
This guide provides step-by-step information to help you export a FedLine Web® certificate for your browser for contingency purposes. We recommend that you create a copy of your FedLine Web certificate in the event your stored certificate is corrupted or deleted.

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

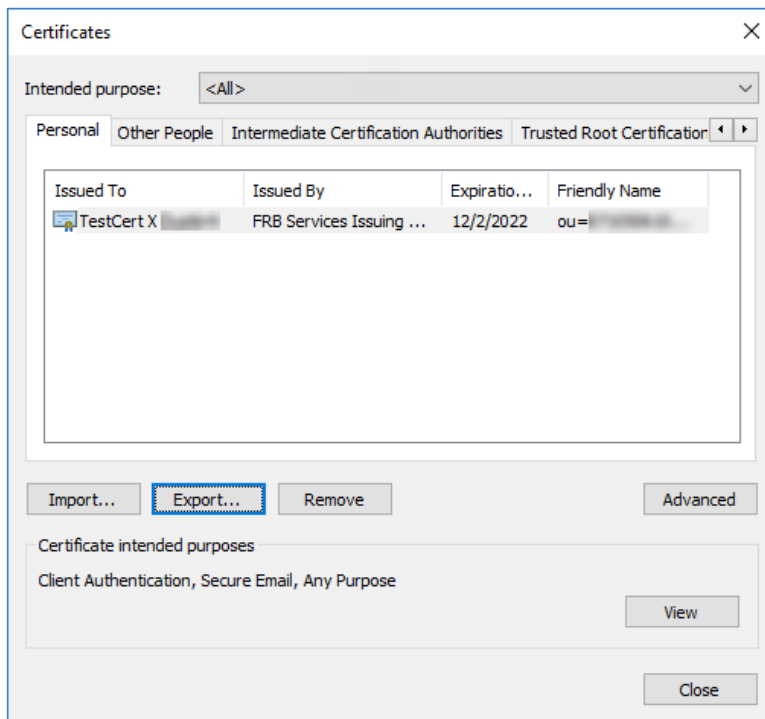
If you need browser assistance, please contact the Customer Contact Center at (888)333-7010.

Certificate Export Procedures

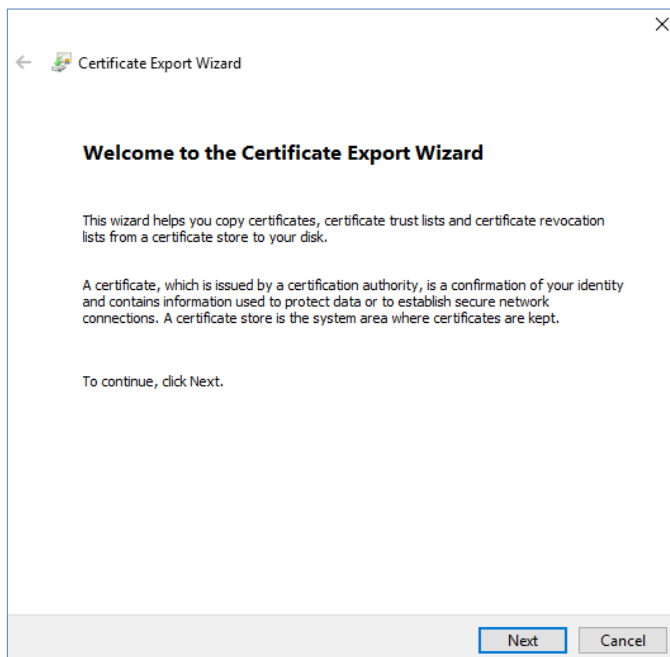
1. In the Windows search bar, search for and select **Internet Options**. The **Internet Properties** window will open. Select the **Content** tab, then click **Certificates**.



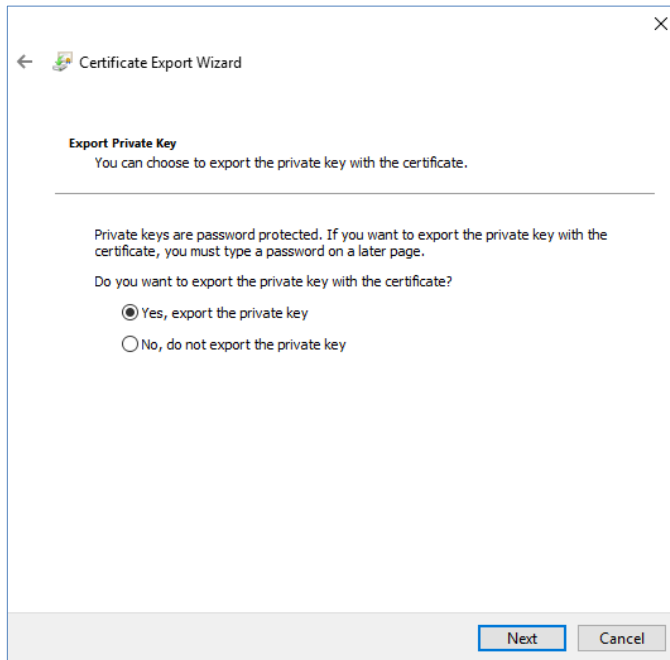
2. Highlight the certificate you want to export and click **Export**.



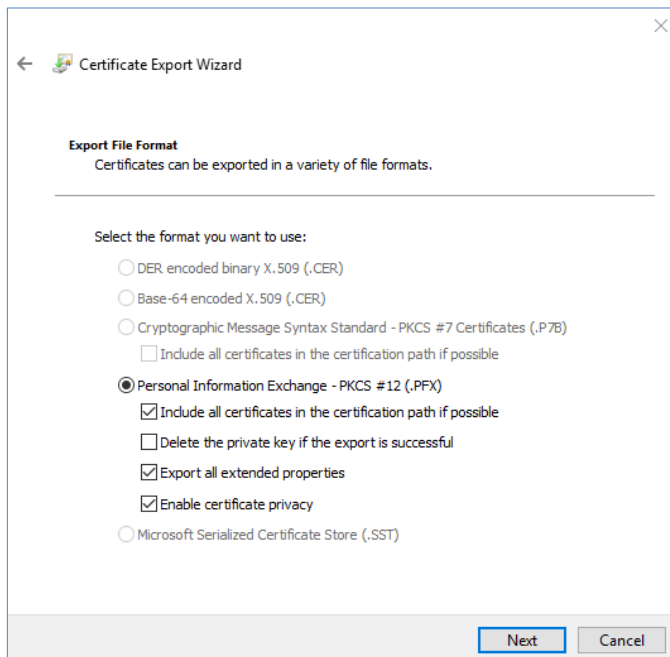
3. This opens the **Certificate Export Wizard**. Click **Next**.



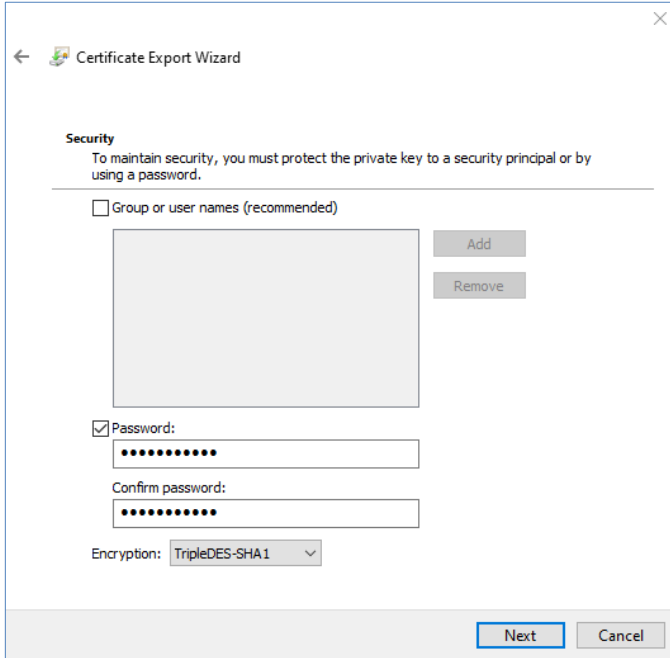
4. Ensure that **Yes, export the private key** is selected and click **Next**.



5. Select the settings indicated below if available and click **Next**. **Note:** your options may differ from those shown below depending on your operating system.

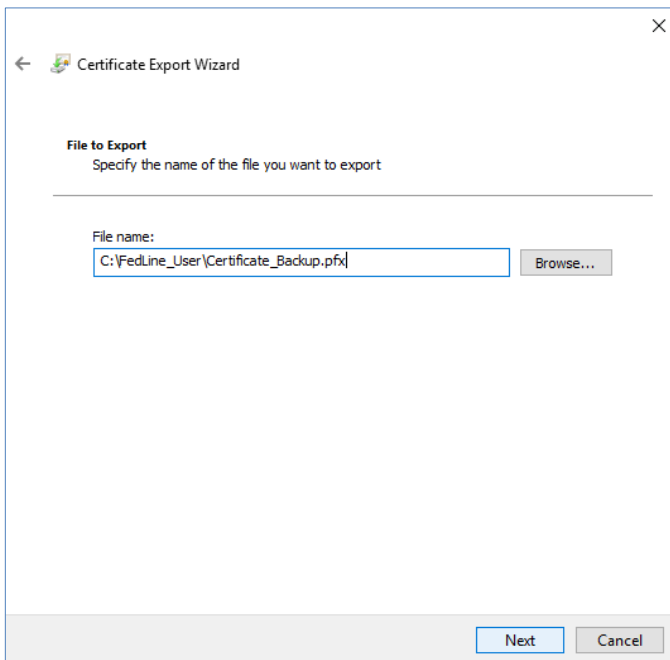


6. Enter a strong certificate password as explained in the [Federal Reserve Banks' Password Practice Statement](#) and ensure that **TripleDES-SHA1** is selected in the Encryption field. Click **Next**.



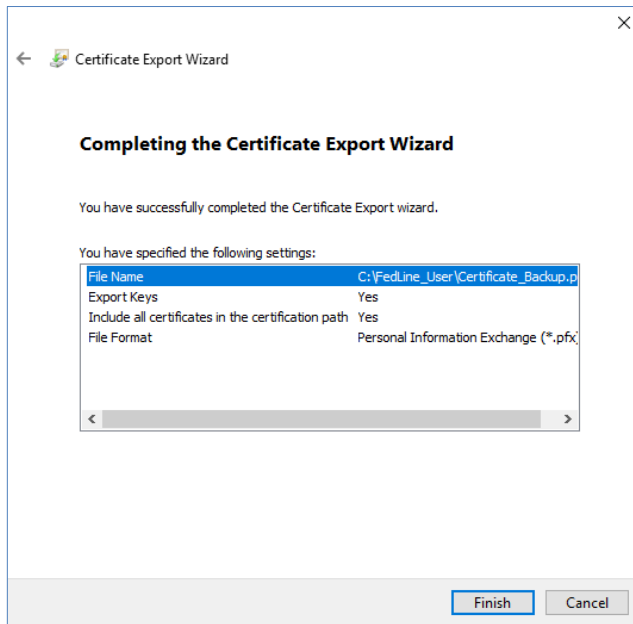
The screenshot shows the 'Certificate Export Wizard' dialog box at the 'Security' step. The title bar reads 'Certificate Export Wizard'. Below the title bar, there is a back arrow icon and the text 'Certificate Export Wizard'. The main content area is titled 'Security' and contains the following elements: a sub-header 'Security' followed by the text 'To maintain security, you must protect the private key to a security principal or by using a password.'; a checkbox labeled 'Group or user names (recommended)' which is currently unchecked; a large empty rectangular box for listing security principals; two buttons labeled 'Add' and 'Remove' to the right of the box; a checked checkbox labeled 'Password:' followed by two password input fields, both containing ten black dots; and a dropdown menu labeled 'Encryption:' with 'TripleDES-SHA1' selected. At the bottom right, there are 'Next' and 'Cancel' buttons.

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

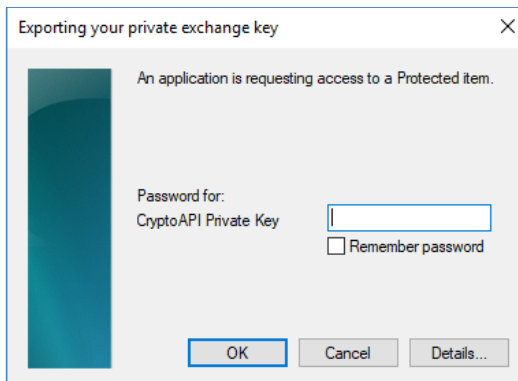


The screenshot shows the 'Certificate Export Wizard' dialog box at the 'File to Export' step. The title bar reads 'Certificate Export Wizard'. Below the title bar, there is a back arrow icon and the text 'Certificate Export Wizard'. The main content area is titled 'File to Export' and contains the following elements: a sub-header 'File to Export' followed by the text 'Specify the name of the file you want to export'; a 'File name:' label followed by a text input field containing the path 'C:\Fedline_User\Certificate_Backup.pfx'; a 'Browse...' button to the right of the input field; and 'Next' and 'Cancel' buttons at the bottom right.

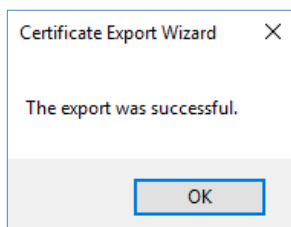
8. Click **Finish**.



9. You will be prompted to enter your certificate password. Enter your password and click **OK**.



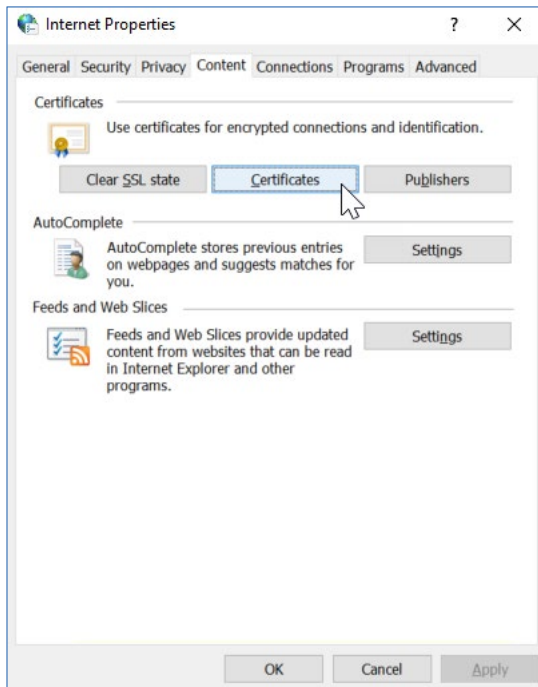
10. Ensure that you receive the following message. This completes the certificate export. Click **OK**.



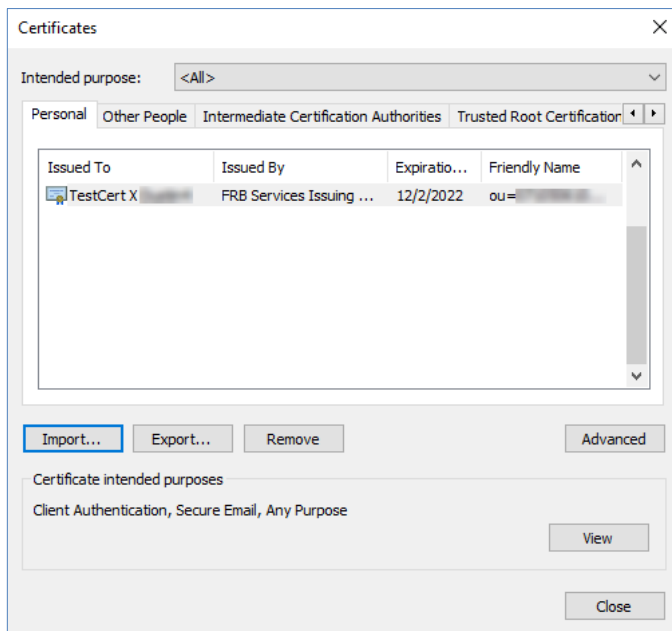
If you no longer require the certificate on the PC after it has been exported, please make sure to delete the certificate.

Certificate Import Procedures

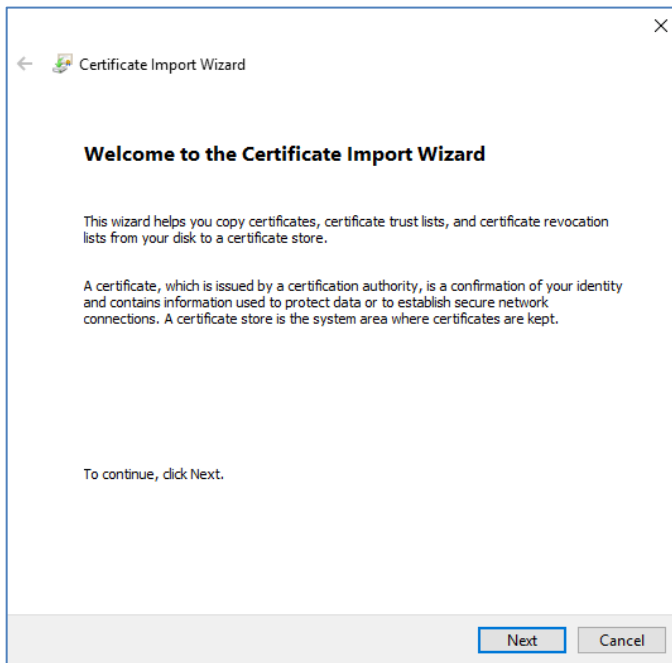
1. In the Windows search bar, search for and select **Internet Options**. The **Internet Properties** window will open. Select the **Content** tab, then click **Certificates**.



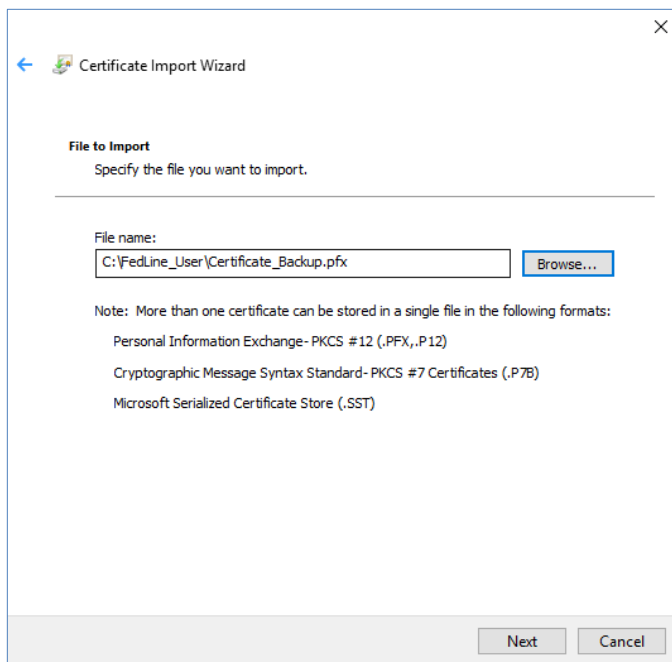
2. Click **Import**.



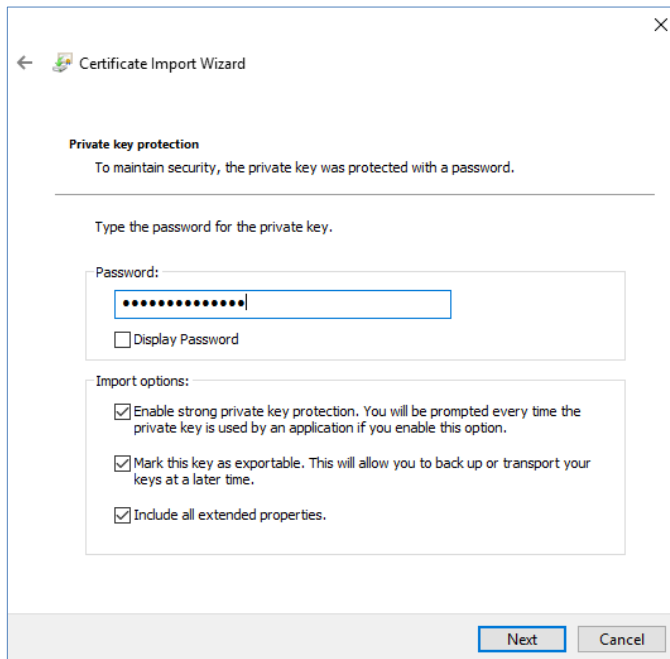
3. This opens the Certificate Import Wizard. Click **Next**.



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

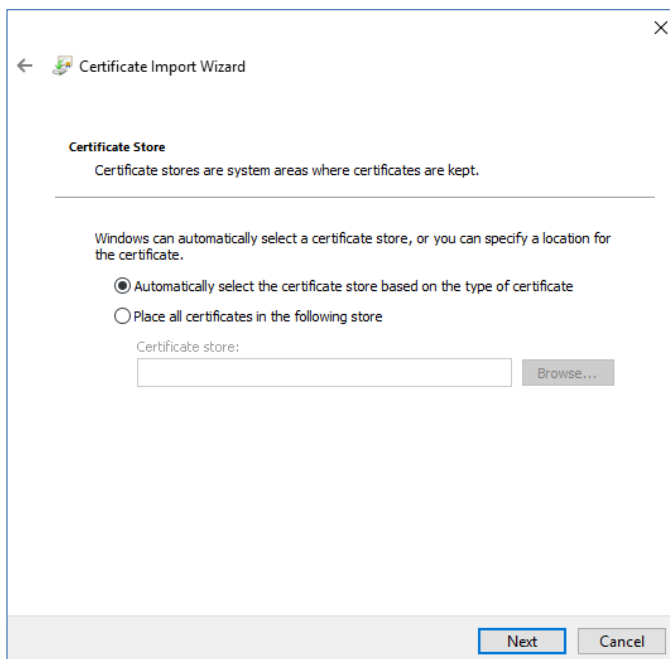


5. Enter the password for the private key and ensure that the import options indicated below are selected. Click **Next**.



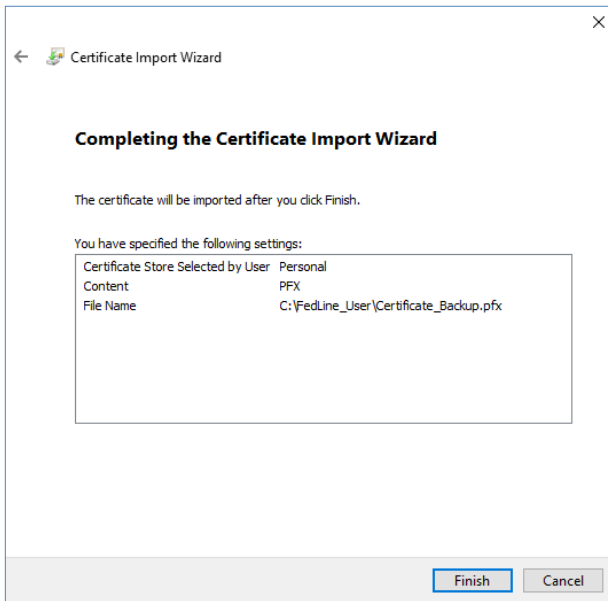
The screenshot shows the 'Certificate Import Wizard' window. The title bar includes a back arrow, a folder icon, and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the following text: 'To maintain security, the private key was protected with a password.' Below this is a horizontal line and the instruction 'Type the password for the private key.' There is a 'Password:' label followed by a text input field containing ten black dots. Below the input field is a checkbox labeled 'Display Password'. Underneath is the 'Import options:' section, which contains three checked checkboxes with their respective 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 of the window, there are two buttons: 'Next' and 'Cancel'.

6. Select **Place all certificates in the following store**. The Certificate store **Personal** will be selected automatically. Click **Next**.

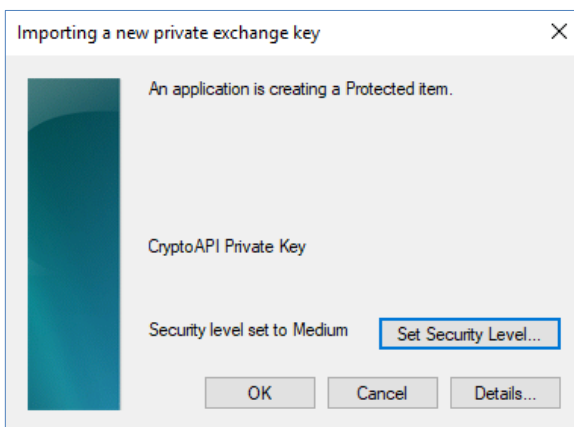


The screenshot shows the 'Certificate Import Wizard' window. The title bar includes a back arrow, a folder icon, and the text 'Certificate Import Wizard'. The main content area is titled 'Certificate Store' and contains the following text: 'Certificate stores are system areas where certificates are kept.' Below this is a horizontal line and the instruction 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is selected) and 'Place all certificates in the following store'. Below the second option is a 'Certificate store:' label followed by a text input field and a 'Browse...' button. At the bottom of the window, there are two buttons: 'Next' and 'Cancel'.

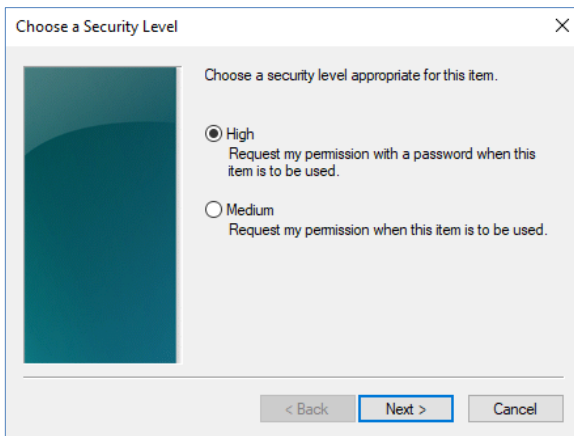
7. Click **Finish**.



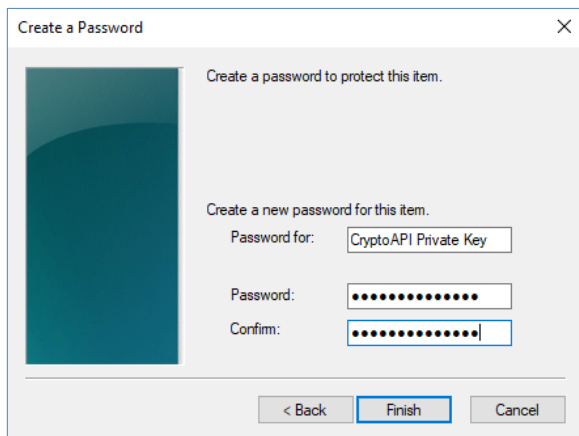
8. Once **Finish** is selected, you will see the following screen. Click **Set Security Level**.



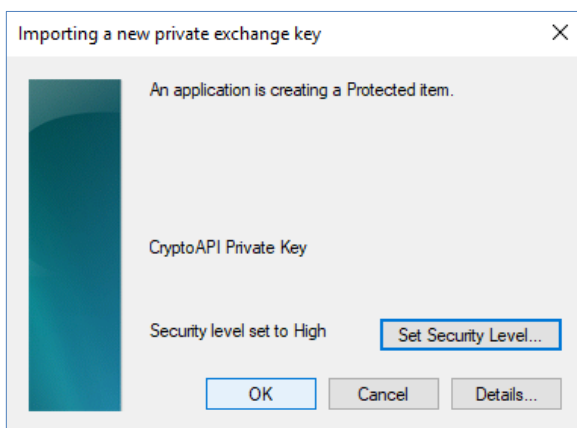
9. Select **High**. Click **Next**.



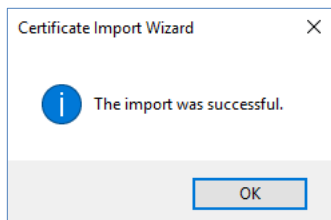
10. Specify a strong password for the certificate password as explained in the [Federal Reserve Banks' Password Practice Statement](#). Click **Finish**.



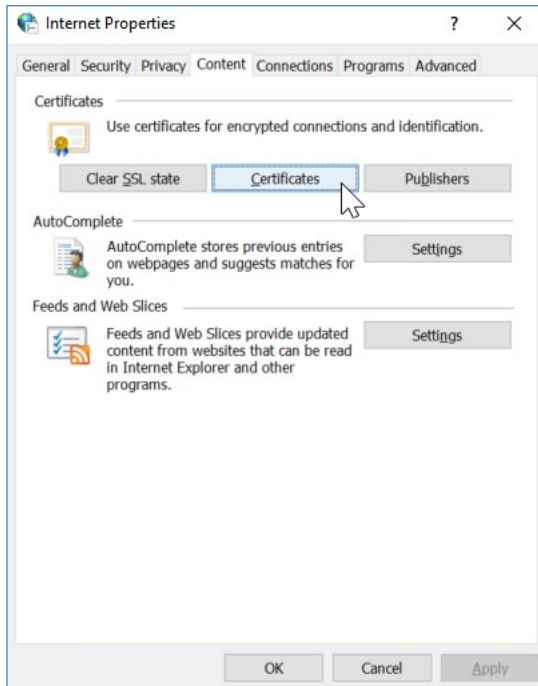
11. Verify that your security level is set to **High**, then click the **OK**.



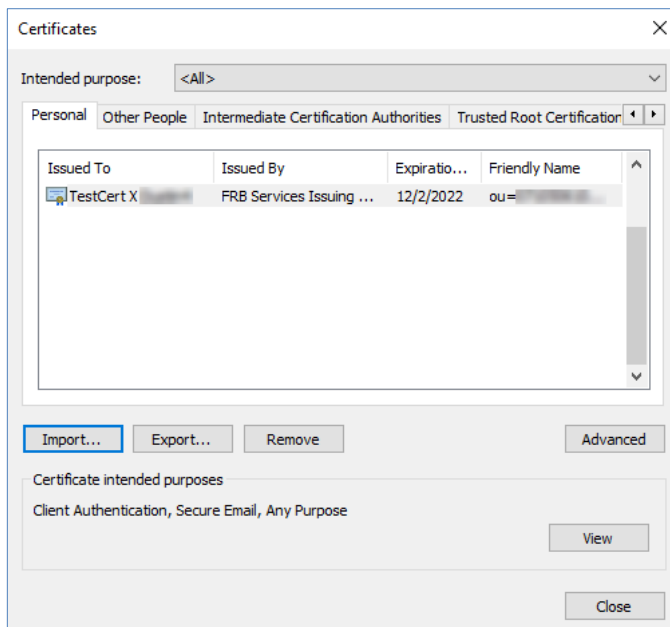
12. Ensure that you receive the following message. This completes the certificate import. Click **OK**.



13. Verify that your import was completed successfully. In the Windows search bar, search for and select **Internet Options**. The **Internet Properties** window will open. Select the **Content** tab, then click **Certificates**.



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

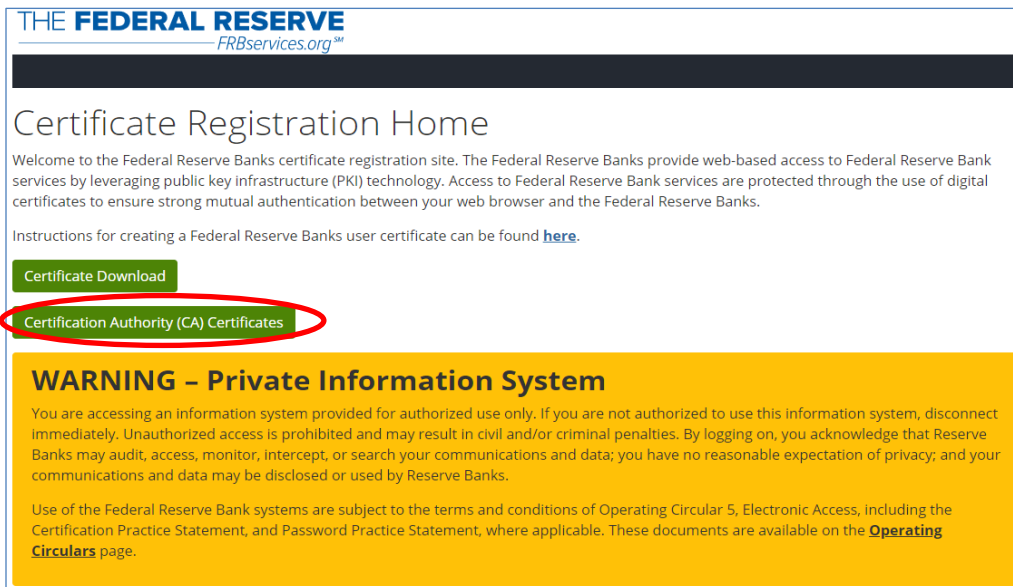


Installing the Federal Reserve Banks Certificate Authority (CA) Certificates

Some users may need to manually install the Federal Reserve Banks 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. Browse to the Certificate Registration Home page at <https://registration.federalreserve.org> and click the **Certification Authority (CA) Certificates** button.



THE **FEDERAL RESERVE**
FRBservices.org™

Certificate Registration Home

Welcome to the Federal Reserve Banks certificate registration site. The Federal Reserve Banks provide web-based access to Federal Reserve Bank services by leveraging public key infrastructure (PKI) technology. Access to Federal Reserve Bank services are protected through the use of digital certificates to ensure strong mutual authentication between your web browser and the Federal Reserve Banks.

Instructions for creating a Federal Reserve Banks user certificate can be found [here](#).

[Certificate Download](#)

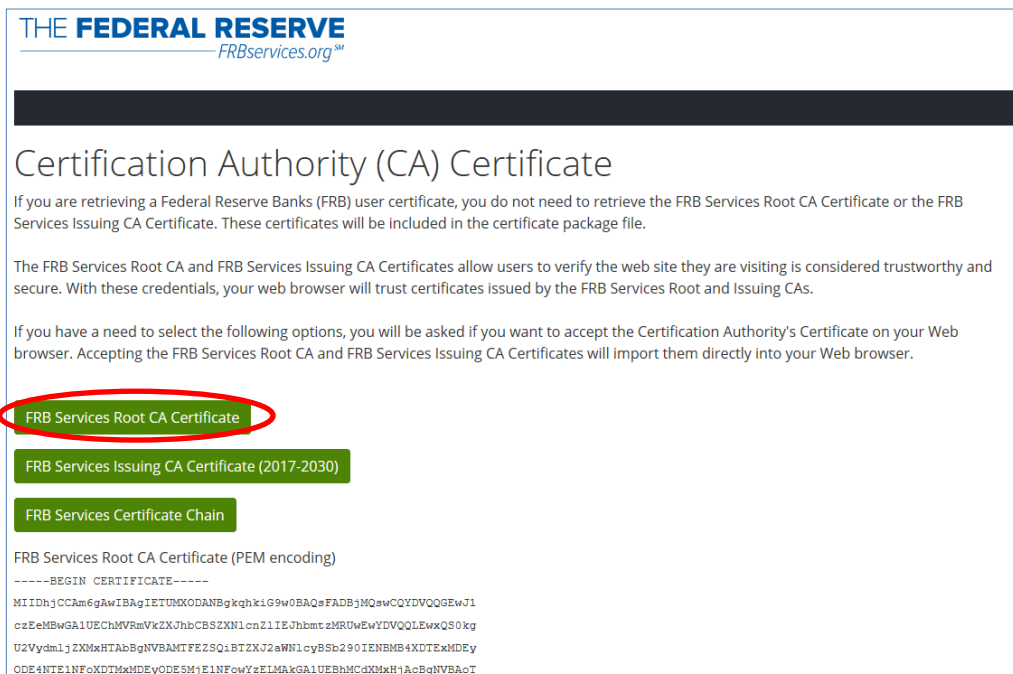
[Certification Authority \(CA\) Certificates](#)

WARNING - Private Information System

You are accessing an information system provided for authorized use only. If you are not authorized to use this information system, disconnect immediately. Unauthorized access is prohibited and may result in civil and/or criminal penalties. By logging on, you acknowledge that Reserve Banks may audit, access, monitor, intercept, or search your communications and data; you have no reasonable expectation of privacy; and your communications and data may be disclosed or used by Reserve Banks.

Use of the Federal Reserve Bank systems are subject to the terms and conditions of Operating Circular 5, Electronic Access, including the Certification Practice Statement, and Password Practice Statement, where applicable. These documents are available on the [Operating Circulars](#) page.

2. Click on **FRB Services Root CA Certificate**.



THE **FEDERAL RESERVE**
FRBservices.org™

Certification Authority (CA) Certificate

If you are retrieving a Federal Reserve Banks (FRB) user certificate, you do not need to retrieve the FRB Services Root CA Certificate or the FRB Services Issuing CA Certificate. These certificates will be included in the certificate package file.

The FRB Services Root CA and FRB Services Issuing CA Certificates allow users to verify the web site they are visiting is considered trustworthy and secure. With these credentials, your web browser will trust certificates issued 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](#)

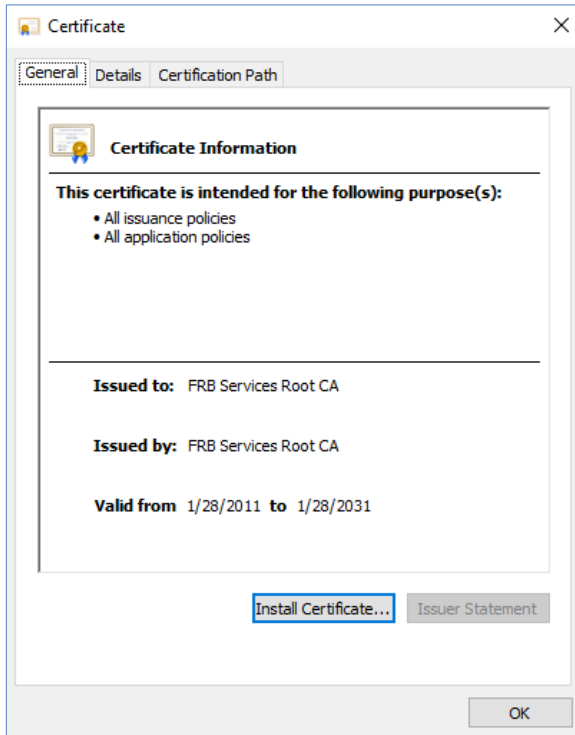
[FRB Services Issuing CA Certificate \(2017-2030\)](#)

[FRB Services Certificate Chain](#)

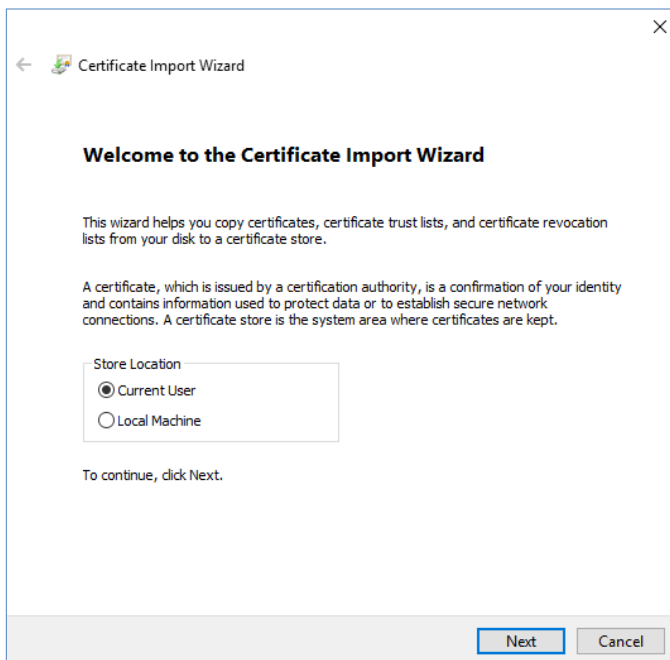
FRB Services Root CA Certificate (PEM encoding)

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIETUMXODANBgkqhkiG9w0BAQsFADBjMQswCQYDVQQGEwJ1
czEeHBwGAlUEChMVRmVrZXJhbnRlbnR1eWVlbnR1eWVlbnR1eWVlbnR1eWVlbnR1
U2VydmljZXNkHTAbBgNVBAMTFEzS0iBTXJ2aW11cyBSb290IENBMB4XDTEyMD
ODE4NTE1NFoXDTEyMDMDEyODESMjE1NFoWYzE1LMAkGA1UEBHMdXkxhZjAcBgNVBAoT
```

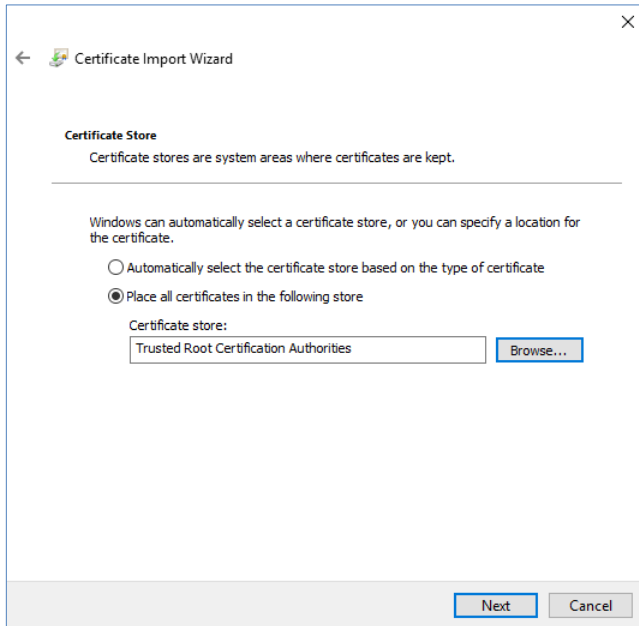
3. The certificate file will be saved to your Downloads directory unless another directory is specified. Open the directory the file was saved to and double-click on the certificate file.
4. In the **Certificate Information** window, click **Install Certificate**.



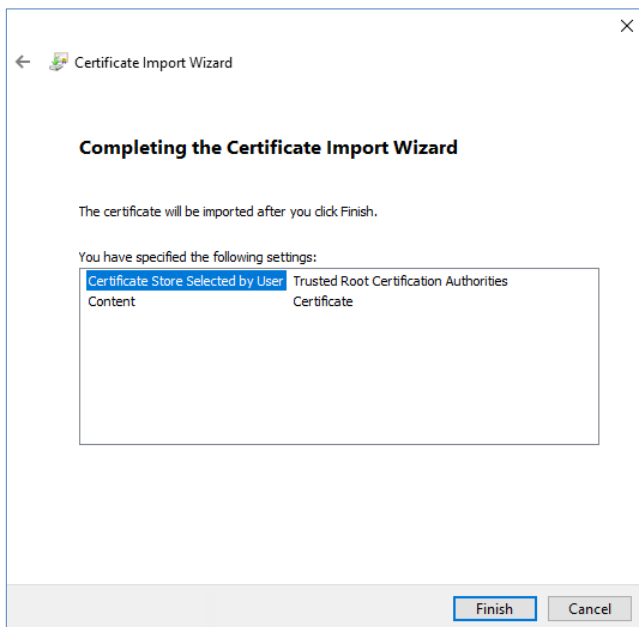
5. The **Certificate Import Wizard** will be initiated. Click **Next**.



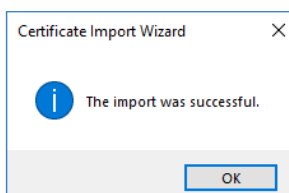
6. Select **Place all certificates in the following store** and click **Browse**. Select the **Trusted Root Certification Authorities** option and click **OK**. Verify the selection and click **Next**.



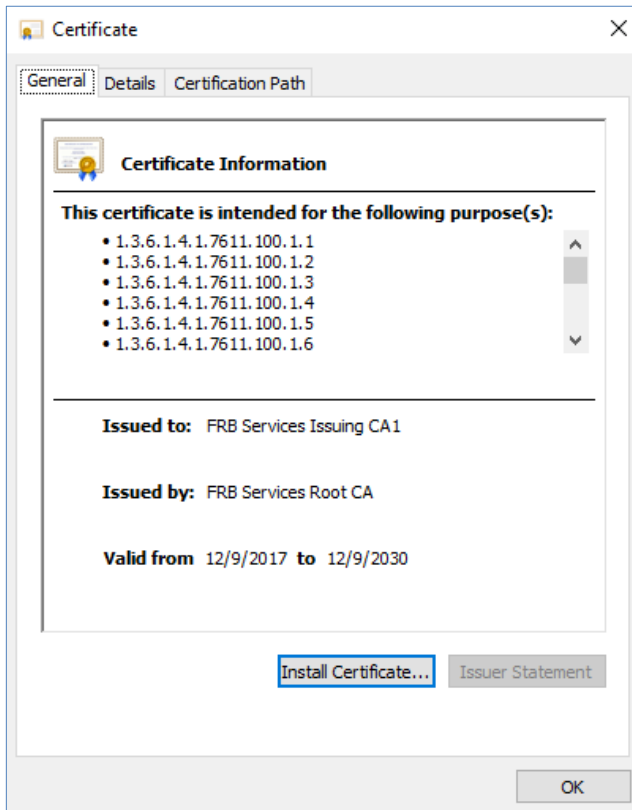
7. Click **Finish**.



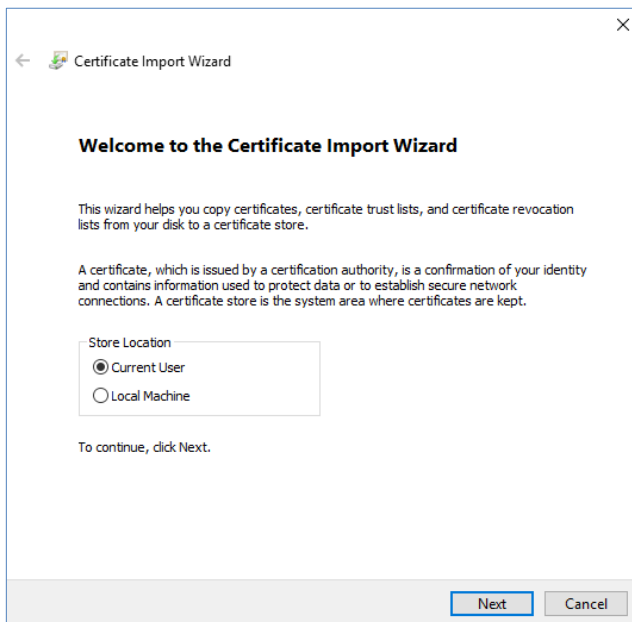
8. A confirmation prompt will be displayed when the certificate has been installed successfully. Click **OK**.



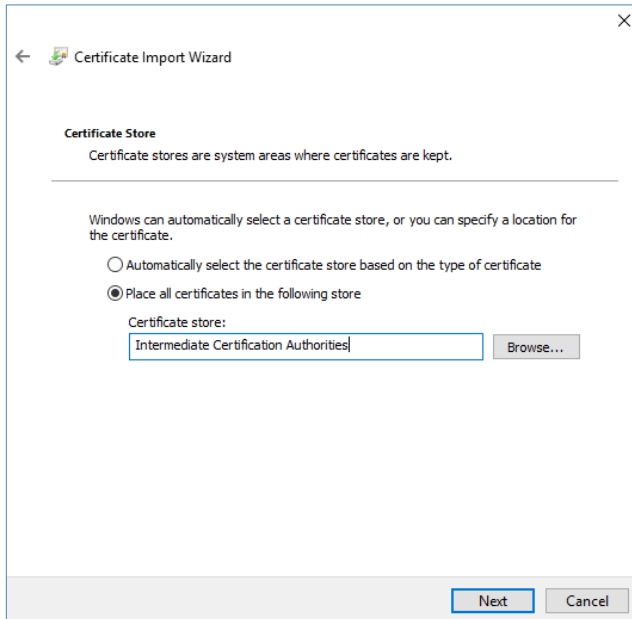
4. In the **Certificate Information** window, click **Install Certificate**.



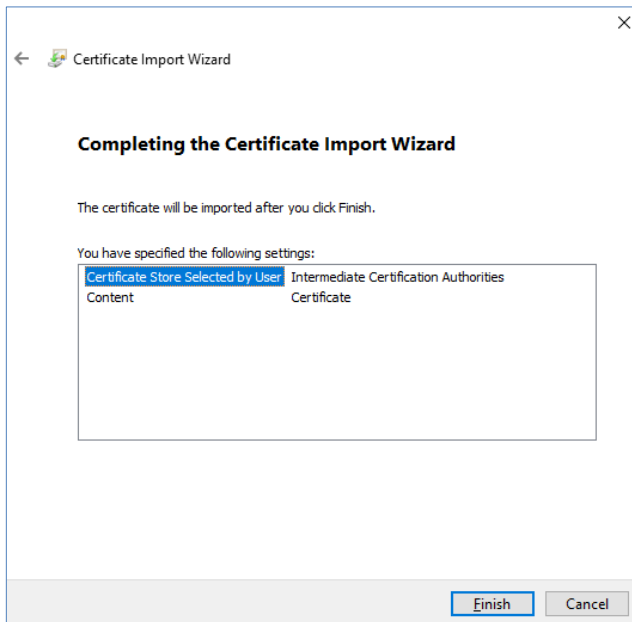
5. The **Certificate Import Wizard** will be initiated. Click **Next**.



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 **Next**.



7. Click **Finish**.



8. A confirmation prompt will be displayed when the certificate has been installed successfully. Click **OK**.

