THE FEDERAL RESERVE
Financial Services

FedLine Web®
Certificate Guide

June 2025

Table of Contents

Legal Notices

Limitations of This Guide

This guide provides confidential information to support your efforts to identify the FedLine Web configuration that best fits your organization's unique computing environment. All configuration options in this guide are provided on the basis of then-current industry practices for general security and configuration logic but may be superseded as time and circumstances change the security environment associated with your organization's configuration and/or the FedLine Web architecture. While the Federal Reserve Banks will endeavor to provide notice of changes to configuration options, as provided in OC 5, your organization is ultimately responsible for securing its own network and FedLine Web connection.

THIRD-PARTY INFORMATION REPRODUCED IN THIS GUIDE IS PROVIDED "AS IS." THE FEDERAL RESERVE BANKS PROVIDE SUCH INFORMATION ONLY AS A CONVENIENCE TO USERS AND DISCLAIM ALL REPRESENTATIONS AND WARRANTIES FOR SUCH INFORMATION, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES CONCERNING THE INFORMATION'S ACCURACY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT AND/OR USAGE. THE FEDERAL RESERVE BANKS SHALL NOT BE LIABLE FOR ANY LOSSES, DAMAGES OR EXPENSES ARISING OUT OF USE OF, INABILITY TO USE OR RELIANCE ON SUCH INFORMATION.

Trademarks

The Financial Services logo, “FedLine Web,” “FedLine” and “FRBservices.org” are service marks of the Federal Reserve Banks. A list of marks related to financial services that are offered to financial institutions by the Federal Reserve Banks is available at FRBservices.org®.

“Microsoft” and “Windows” are registered trademarks of Microsoft Corporation in the United States and other countries.

Overview

This guide provides step-by-step instructions to help you add and/or remove a Federal Reserve Banks digital certificate from your browser. It also provides information about certificate contingency procedures and practices. The certificate is issued to authenticate the Subscriber and to grant access to authorized FedLine® and Federal Reserve Bank services.

Browser-based access requires the user's personal computer (PC) to comply with basic hardware and software requirements. To download a Federal Reserve Banks certificate, your PC must meet the FedLine Web Hardware and Software Requirements.

If you are unsure if your PC meets the hardware and software requirements, FedLine customers should contact the Support Center at 833-FRS-SVCS (833-377-7827). Non-FedLine customers should contact support as directed during the enrollment process.

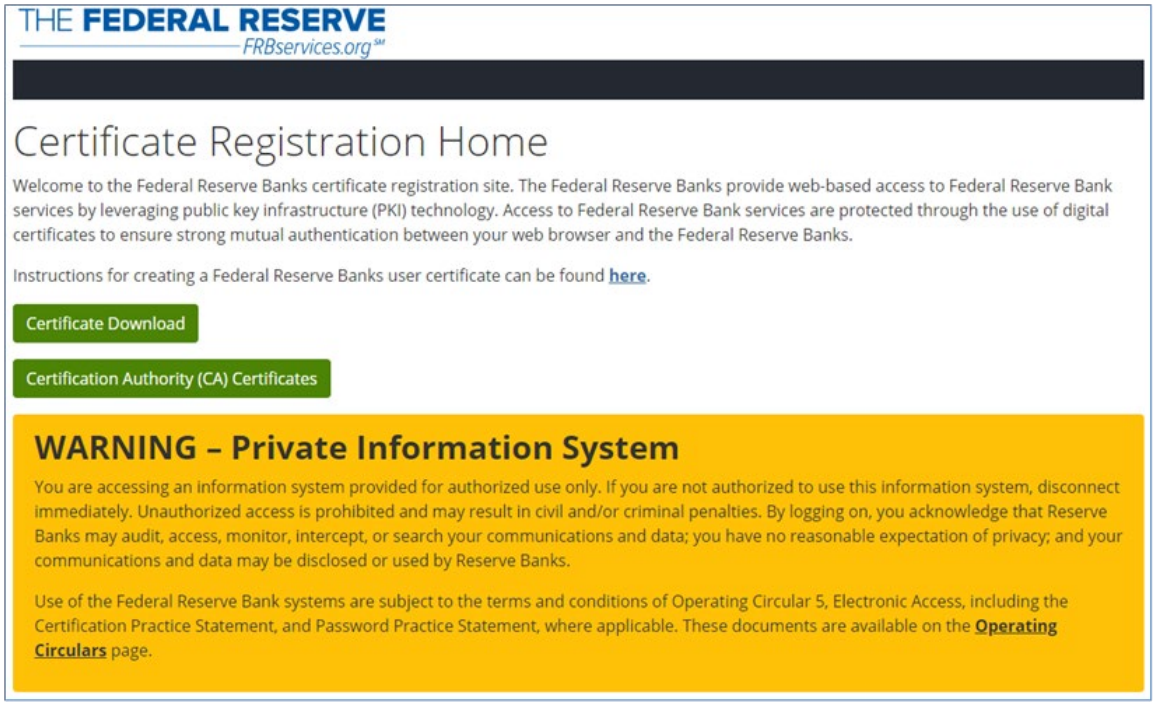
Before proceeding with the instructions provided in this guide, have both your Reference Number and Authorization Code available.

Certificate Retrieval Procedures

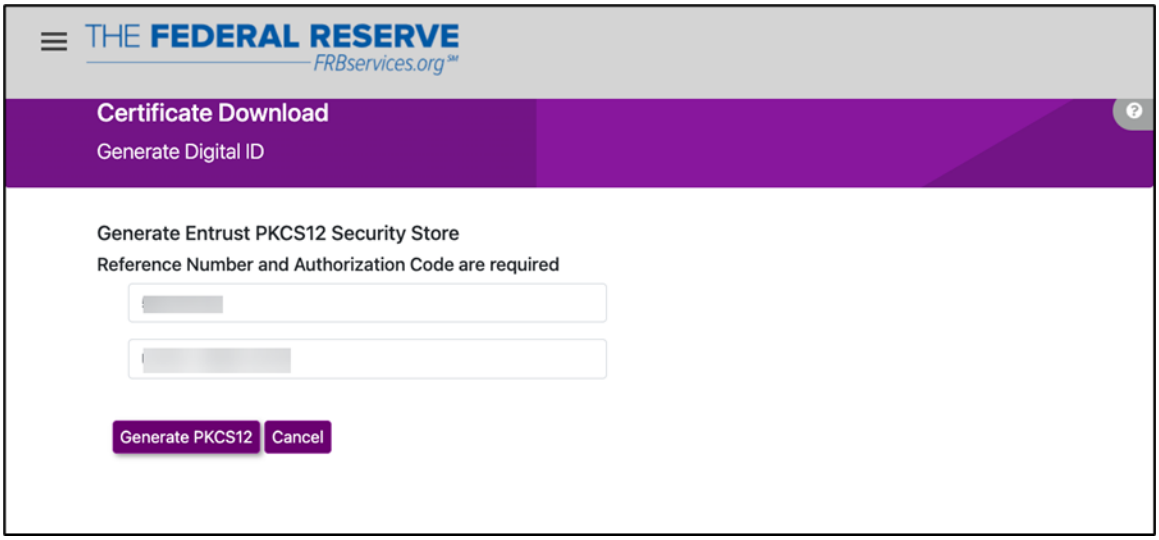
Certificate Creation

1. Using a supported browser, visit https://registration.federalreserve.org.

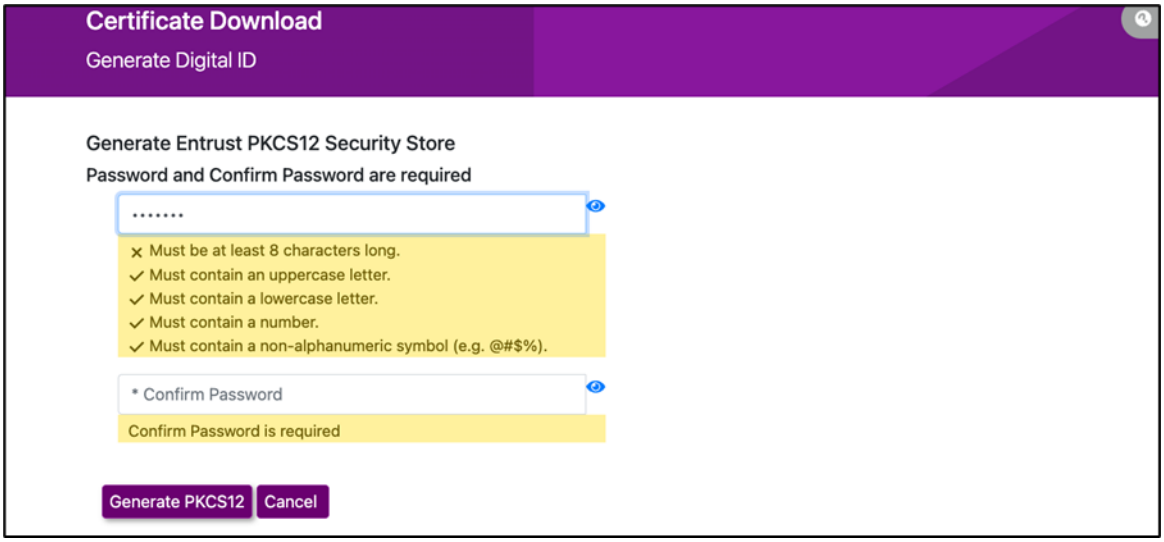
2. On the “Certificate Registration Home” page, click the **Certificate Download** button.



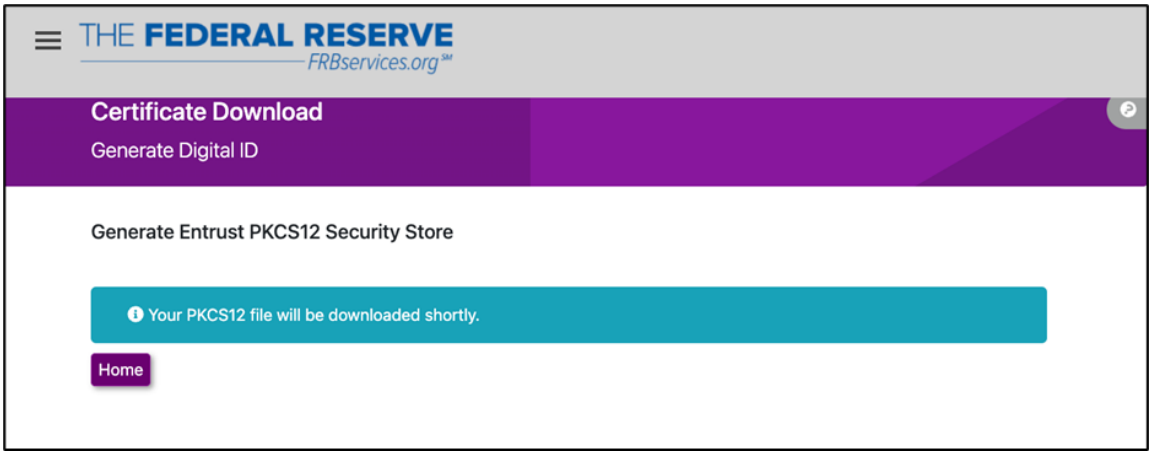
3. Enter your “Reference Number” and “Authorization Code” in the appropriate fields. Click the **Generate PKCS12** button.



4. Using the password rules that display when you begin to type, enter a password to protect the P12 certificate that you will download. Note this password, as you will need it to install your certificate. Click the **Generate PKCS12** button.

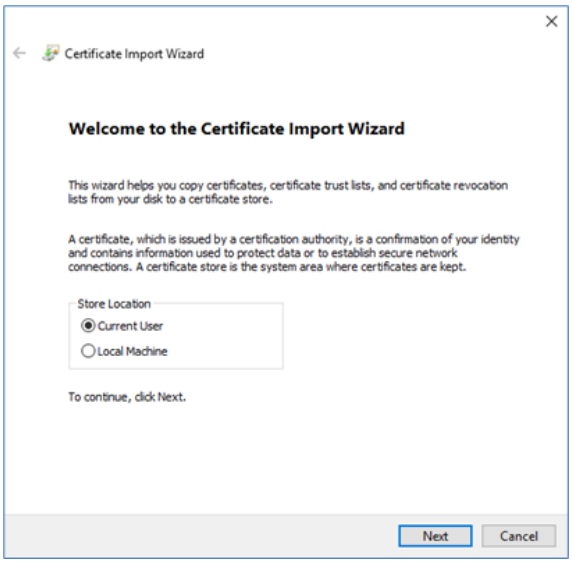


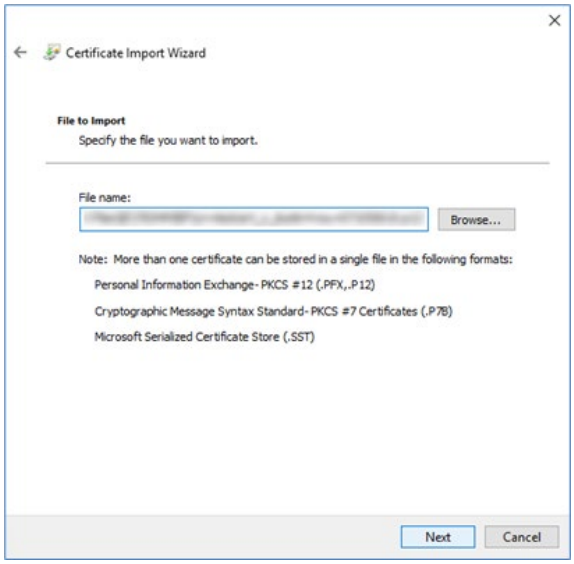
5. The following screen displays.



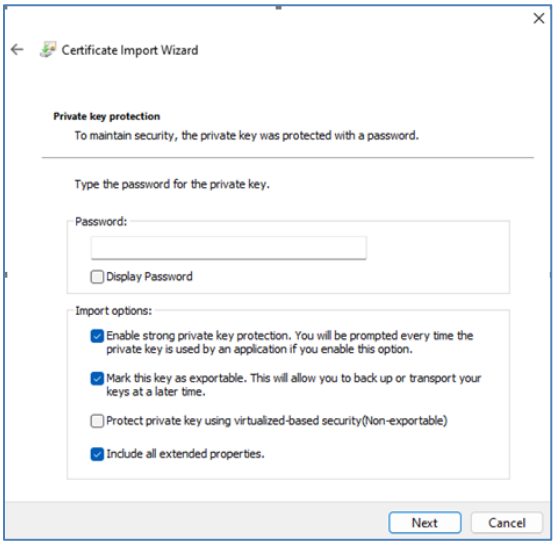
6. The certificate file will save to your Downloads directory unless you specify a different directory. Open the directory to which the file was saved and double-click the certificate file. This launches the Certificate Import Wizard.

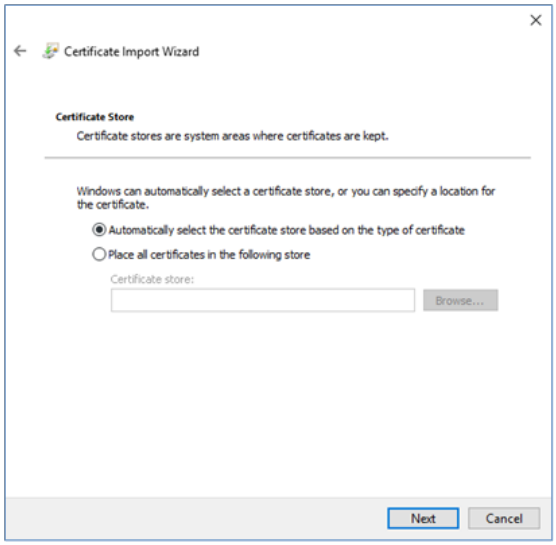
7. Select “Current User” and click the **Next** button, and then click the **Next** button on the following screen.



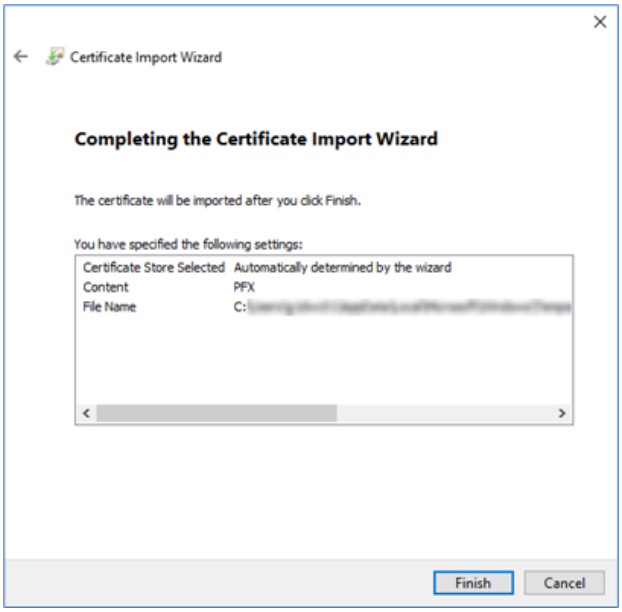


8. Enter the P12 password created in step 4, ensuring that the import options indicated below are selected. Click the **Next** button and then click the **Next** button on the following screen.

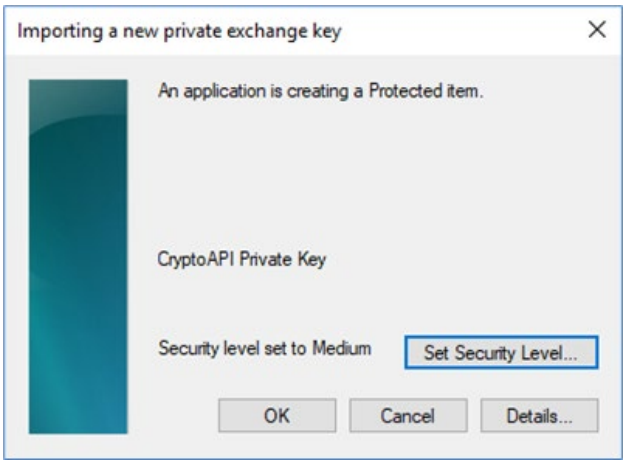




9. Click the **Finish** button.



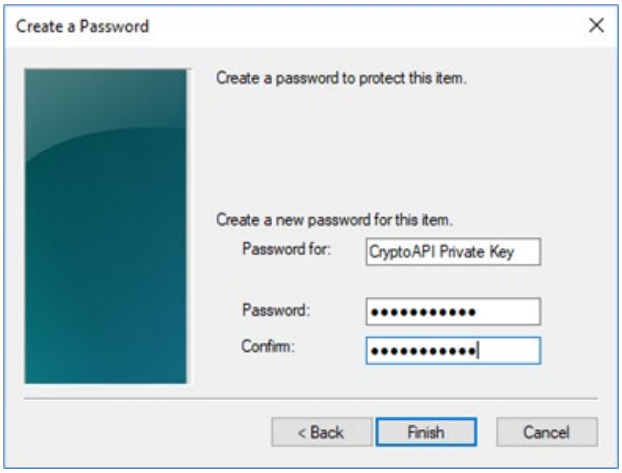
10. On the “Importing a new private exchange key” screen, click the **Set Security Level…** button.



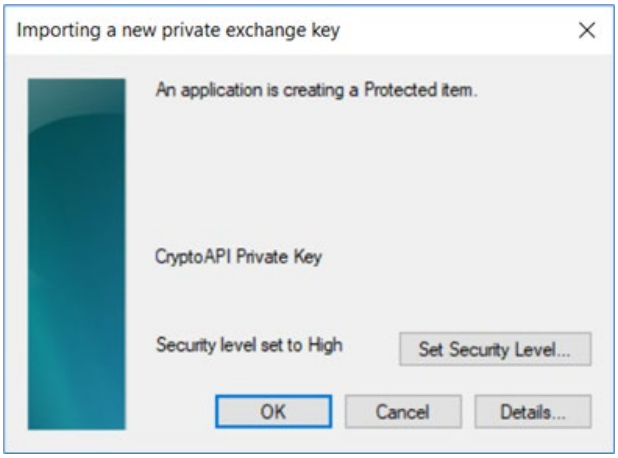
11. Select the “High” option and click the **Next** button.

12. Create a password to protect your private key. The password should follow your organization's password requirements. Click the **Finish** button.

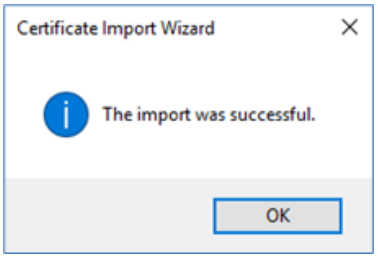
NOTE: This is a different password than the one created in step 4. Microsoft Windows will use this will be the password to protect your certificate. Remember this password, as any time you use your certificate in the future to connect to Federal Reserve Bank Services, your browser will prompt you for this password.



13. Verify that your security level is set to high, and then click the **OK** button.

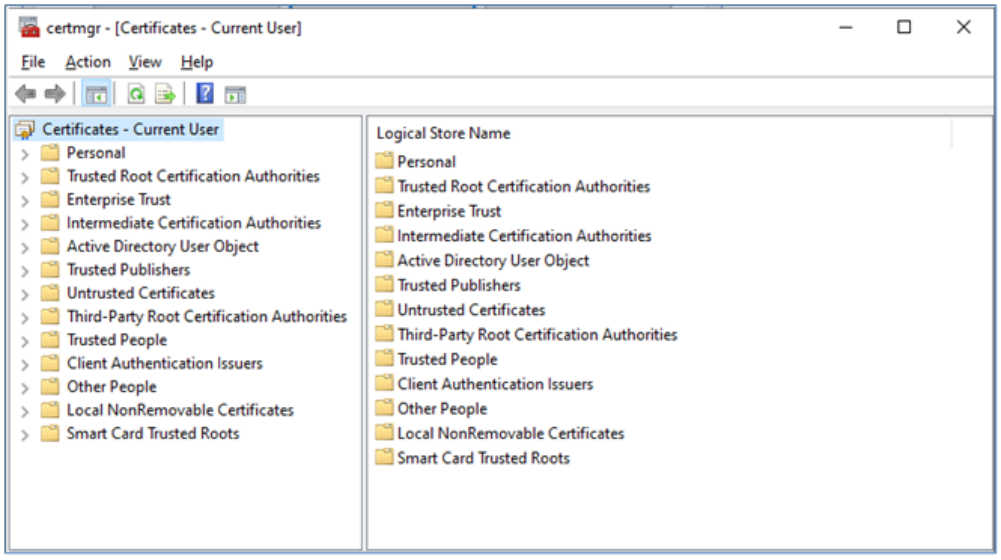


14. You have successfully downloaded and installed your certificate. Click the **OK** button. You may now close your browser.



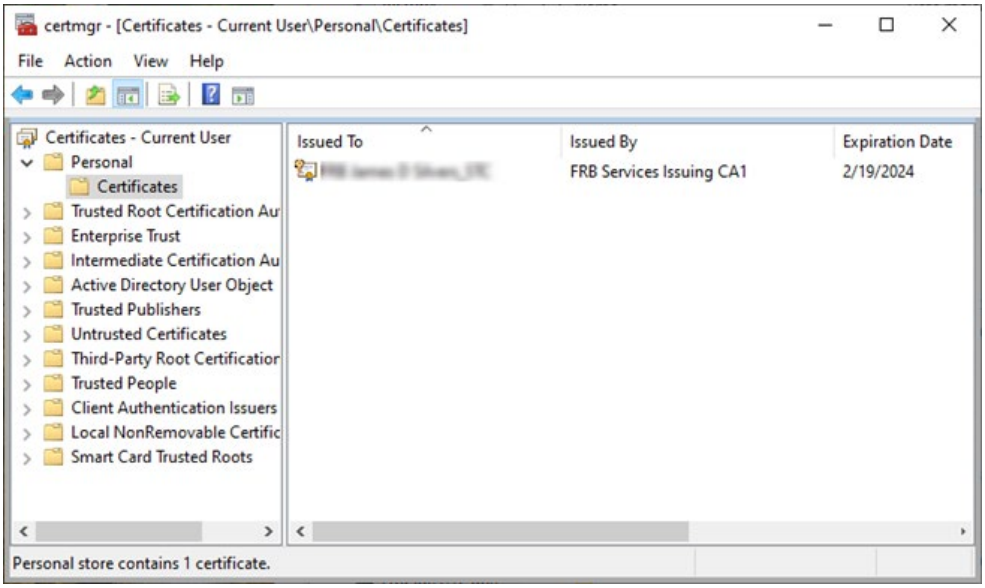
15. Locate the file that was downloaded in steps 5 and 6 and save it to a secure location (such as a network drive) for contingency purposes, in accordance with your organization's policies. Once saved to a secure contingency location, the file can be deleted from your PC's local drive. You should also save the password for the P12 file and the password for the private key to a secure location for contingency purposes, in accordance with your organization's policies.

16. Verify that you have correctly installed the certificate. In the Microsoft® Windows® search box in the lower-left corner of your screen, search for "Manage user certificates" and then press the **Enter** key or select "Open." The Windows Certificate Manager window will display.



17. In the left pane, expand the "Personal" folder and click the "Certificates" folder. You should see your newly downloaded certificate in this folder. If multiple Federal Reserve Bank credentials appear in the list, the newly downloaded certificate will typically have the latest expiration date. After verifying that your

certificate has imported, close the Certificate Manager window.



NOTE: You must safeguard the digital certificate and its associated private key. Make sure you:

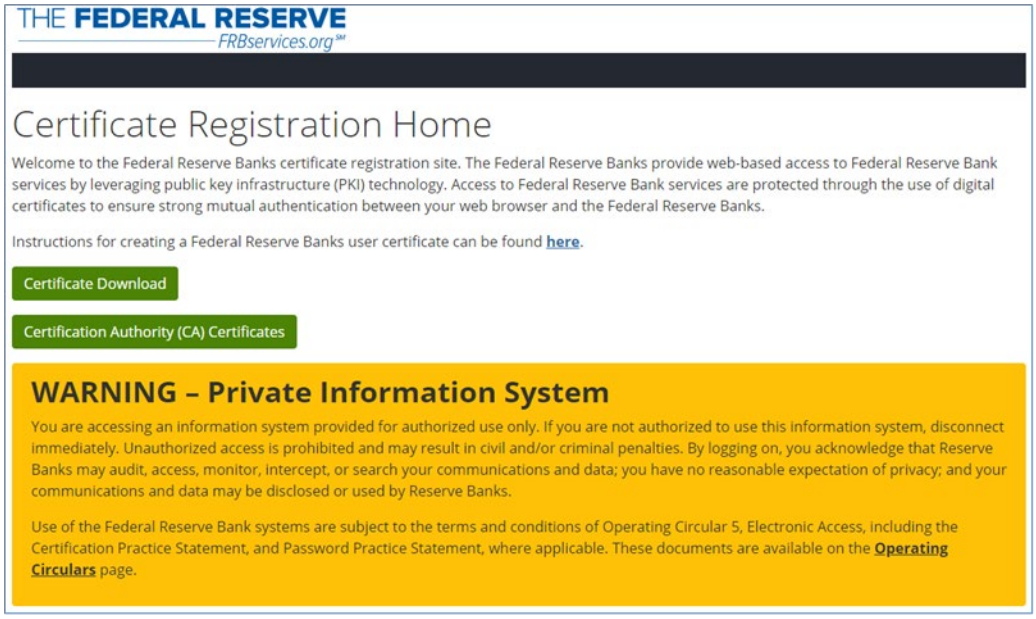
- Create a backup copy of the digital certificate file for business recovery purposes and store this copy in a safe location.
- Limit on a need-to-know or need-to-have basis all logical and physical access to the digital certificate. This includes access to the certificate repository that stores the certificate within your workstation or operating system.
- Limit on a need-to-know or need-to-have basis all logical and physical access to any backup copies of the digital certificate created through backup solutions.
- Remember the password for your certificate, as the Federal Reserve Banks cannot reset it. If you forget your password, a new certificate must be issued.

Installing the Federal Reserve Banks Certificate Authority Certificates

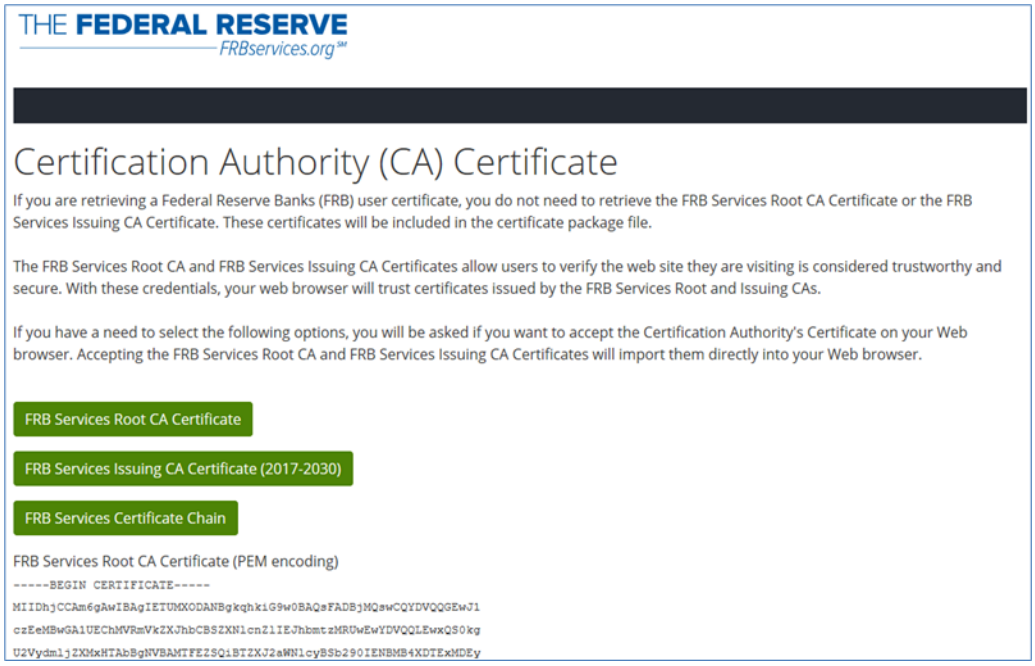
Some users may need to manually install the Federal Reserve Banks Certificate Authority (CA) certificates. Follow the procedures below to complete this activity on any computer that will be used to access Federal Reserve Bank Services.

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.

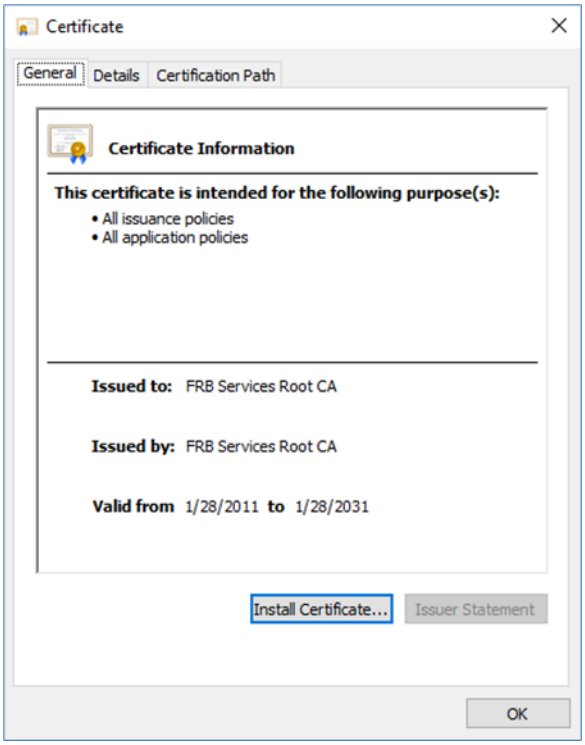


2. Click the **FRB Services Root CA Certificate** button.

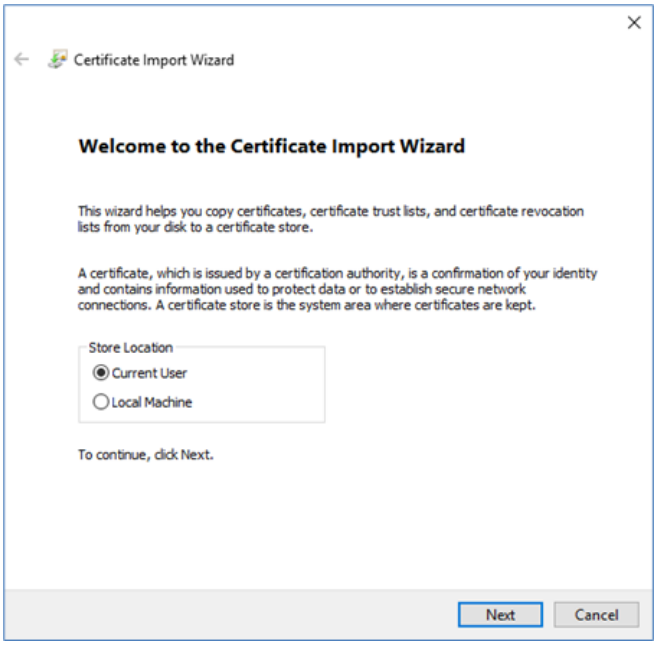


3. The certificate file will save to your Downloads directory unless you specify a different directory. Open the directory to which the file was saved and double-click the certificate file.

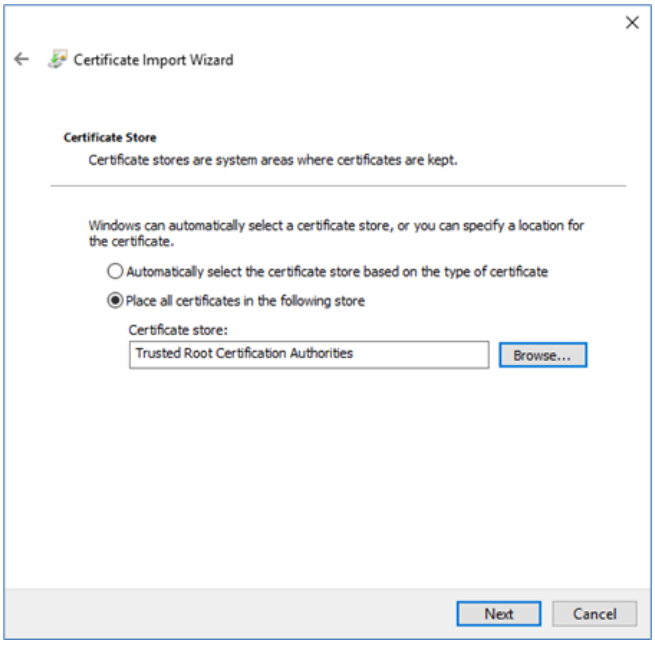
4. In the “Certificate Information” window, click the **Install Certificate…** button.



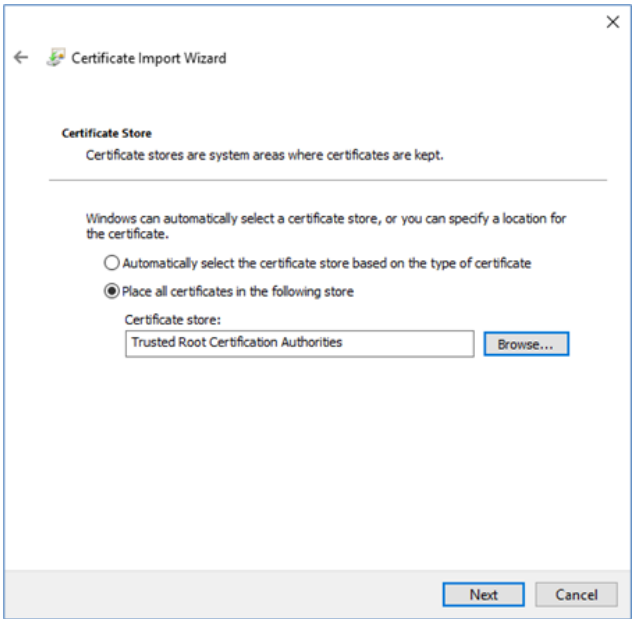
5. The “Certificate Import Wizard” initiates. Click the **Next** button.



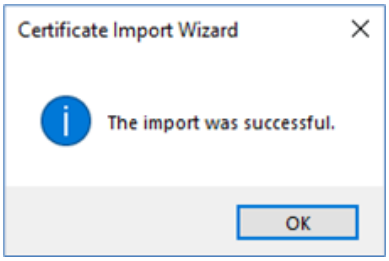
6. Select “Place all certificates in the following store” and click the **Browse** button. Browse to and select the “Trusted Root Certification Authorities” option and click the **OK** button. Click the **Next** button.



7. Click the **Finish** button.



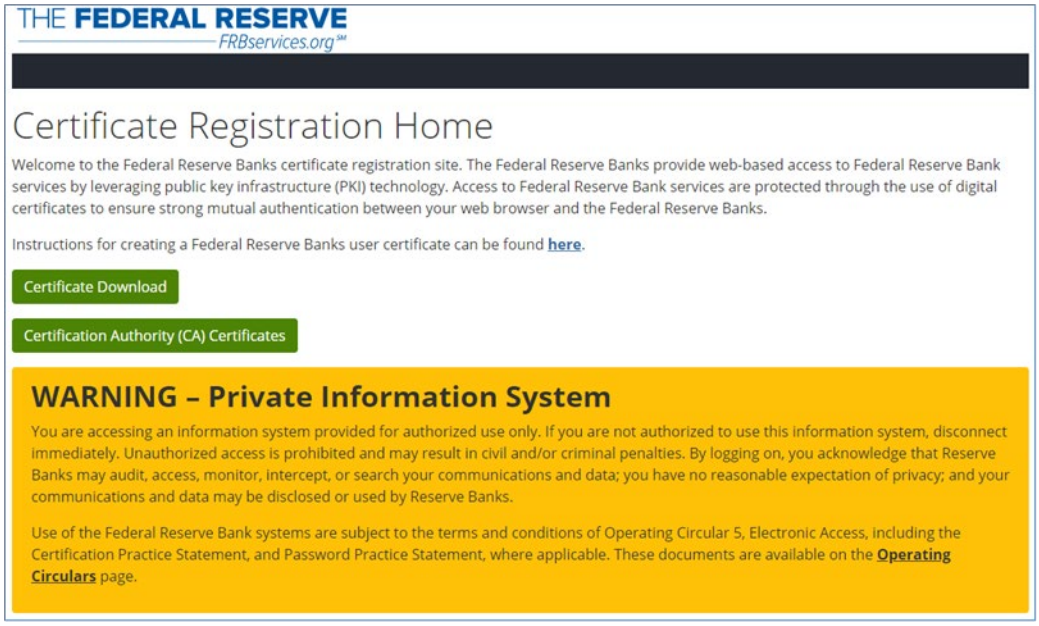
8. A confirmation window displays when the certificate has been installed successfully. Click the **OK** button.



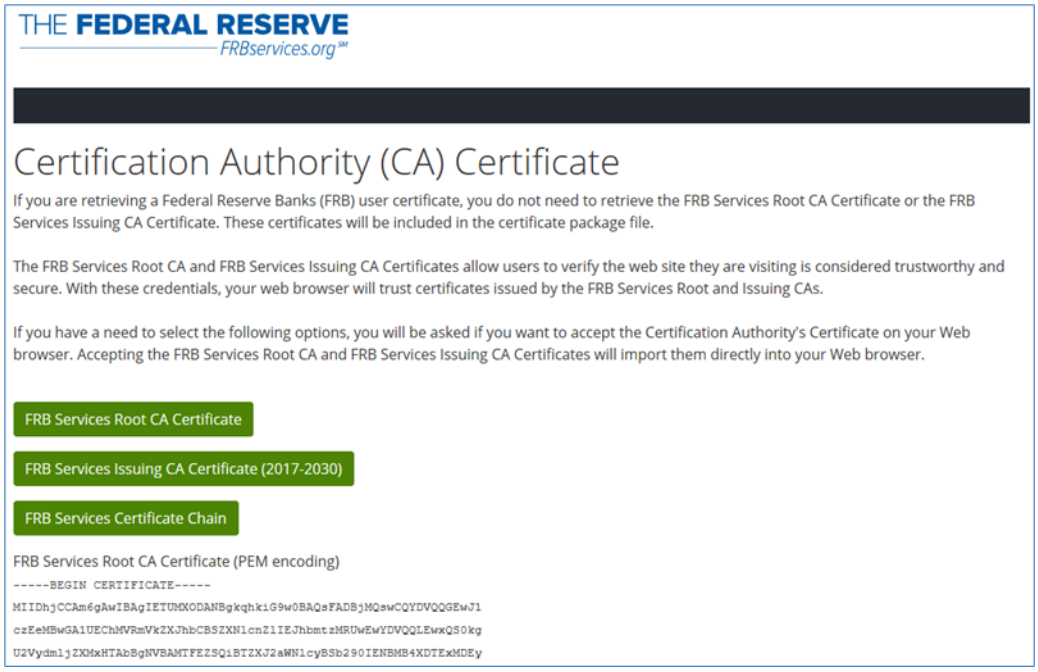
Federal Reserve Bank Services Issuing CA Certificate

To install the Federal Reserve Bank Services Issuing CA certificate:

1. Browse to the “Certificate Registration Home” page at https://registration.federalreserve.org and click the **Certification Authority (CA) Certificates** button.

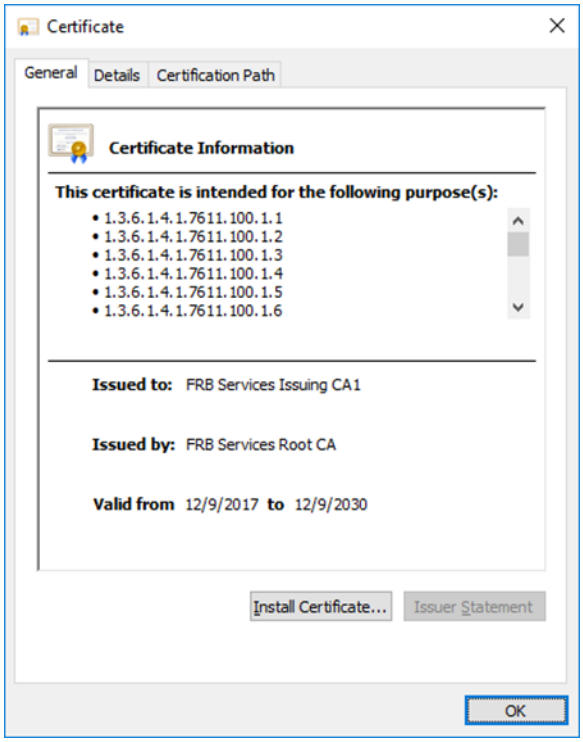


2. Click the **FRB Services Issuing CA Certificate (2017-2030)** button.

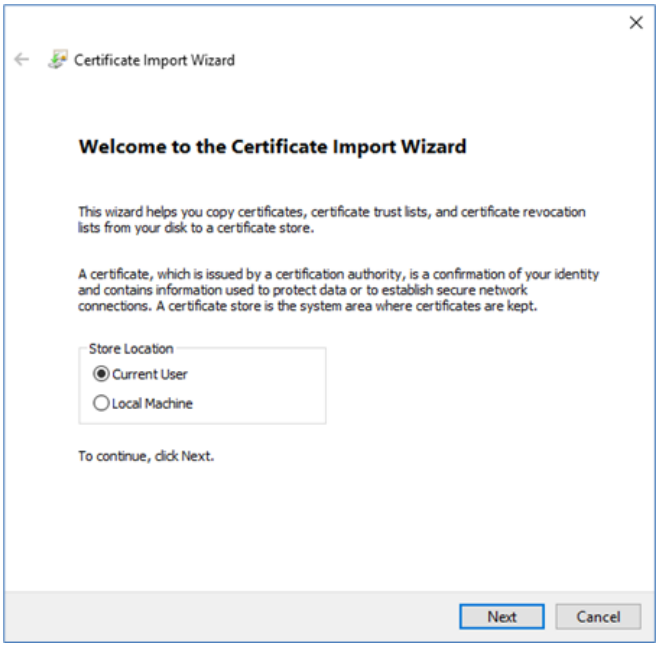


3. The certificate file downloads to your Downloads directory unless you specify a different directory. Open the directory to which the file was saved and double-click the certificate file.

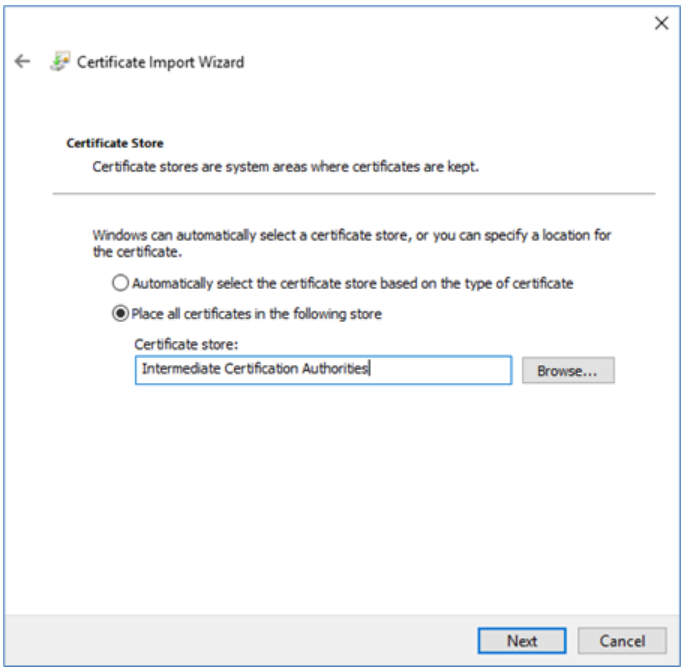
4. In the “Certificate Information” window, click the **Install Certificate…** button.



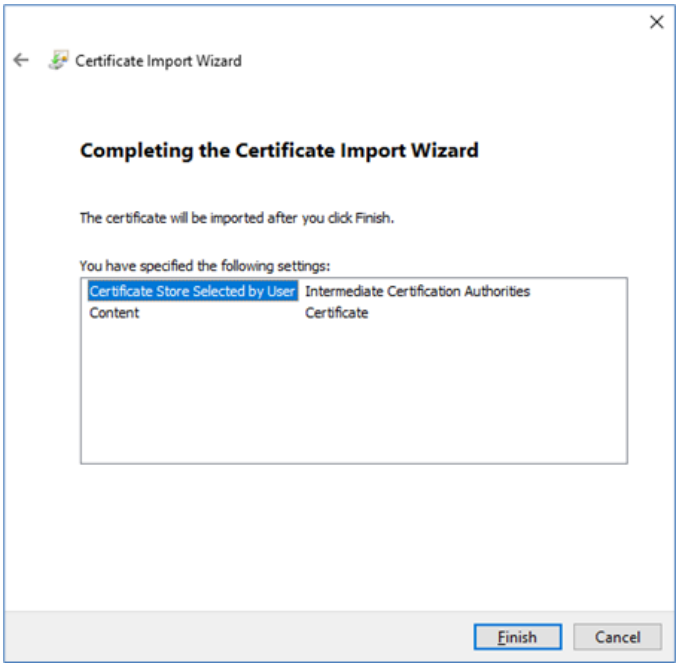
5. The “Certificate Import Wizard” initiates. Click the **Next** button.



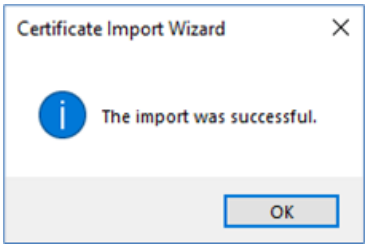
6. Select “Place all certificates in the following store” and click the **Browse…** button. Browse to and select the “Intermediate Certification Authorities” option and click the **OK** button. Click the **Next** button.



7. Click the **Finish** button.



8. A confirmation window displays when the certificate has been installed successfully. Click the **OK** button.



FedLine Web Certificate Removal Procedures

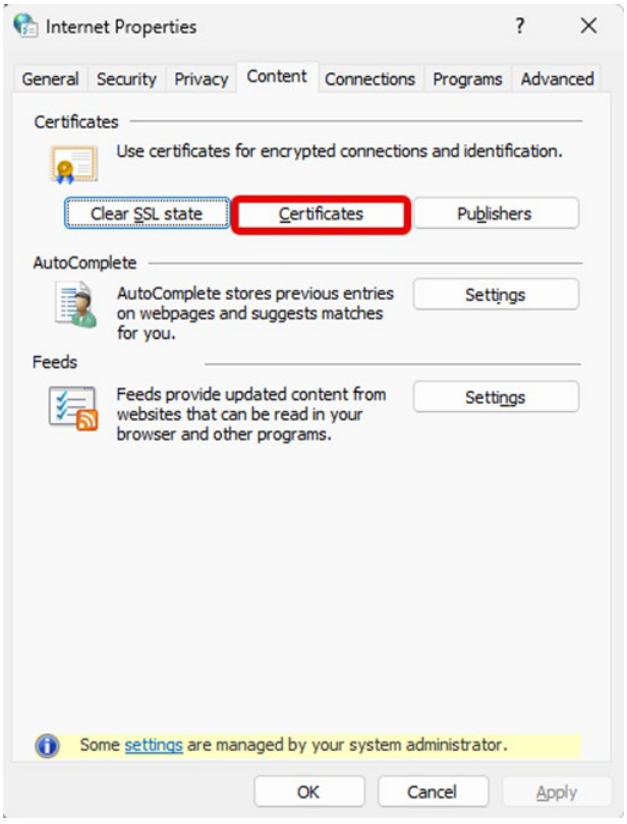
This section provides step-by-step instructions to help you remove a FedLine Web certificate. We recommend that you create a copy of your FedLine Web certificate using the contingency procedures before continuing with this guide.

Your screen images and language may vary slightly from the images in this section depending on your version of Windows and your browser. Review the FedLine Web Hardware and Software Requirements page on FRBservices.org for a list of supported platforms.

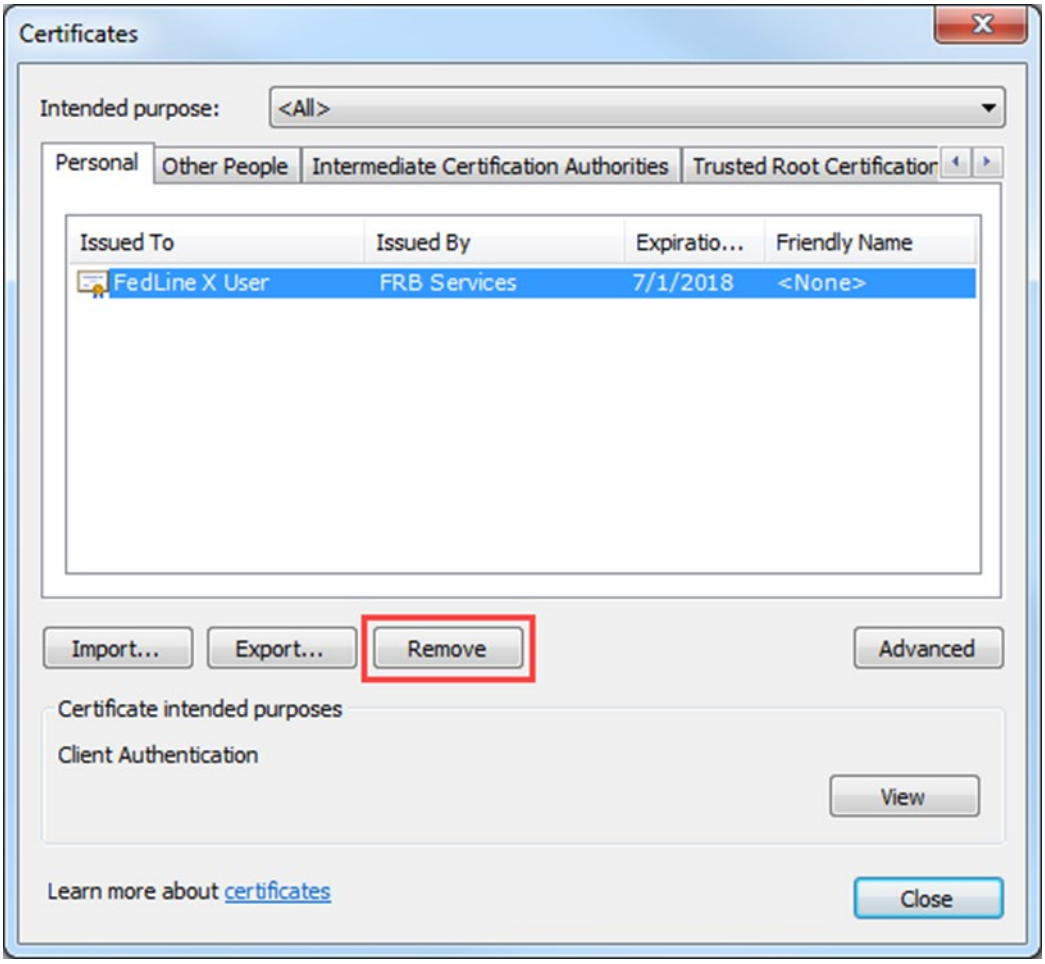
If you are unsure of how to proceed, call the Support Center at 833-FRS-SVCS (833-377-7827).

To remove a Federal Reserve Banks certificate:

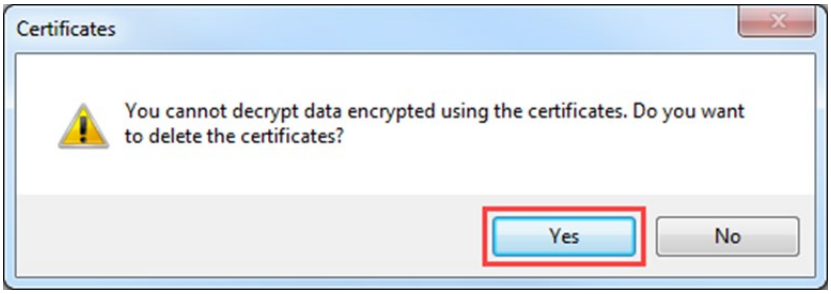
1. On your PC, search for and select “Internet Options” using the search bar on your taskbar. On the resulting “Internet Properties” window, select the “Content” tab. Click the **Certificates** button.



2. Select the certificate you want to delete and click the **Remove** button.



3. If you receive a message asking, “Do you want to delete the certificates?” click the **Yes** button.



4. Verify that you have successfully deleted the digital certificate by navigating back to the “Internet Properties” window, selecting the “Content” tab and clicking the **Certificates** button. Confirm that the deleted certificate is no longer displayed in the resulting “Certificates” window. When complete, click the **Close** button.

FedLine Web Certificate Contingency Procedures

This section provides instructions 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.

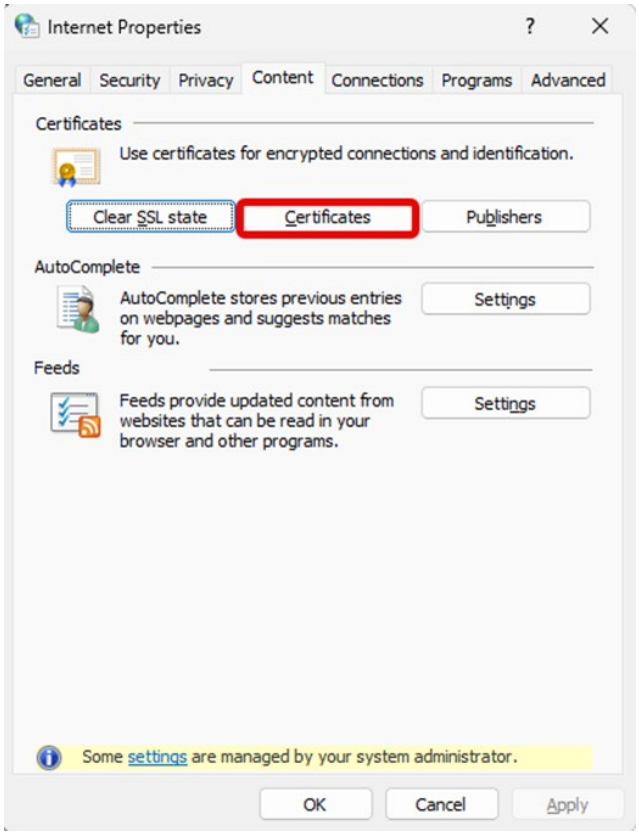
Your screen images and language may vary slightly from the images in this guide depending on the version of Windows you are using. Review the FedLine Web Hardware and Software Requirements page on FRBservices.org for a list of supported platforms.

If you need browser assistance, contact the Support Center at 833-FRS-SVCS (833-377-7827).

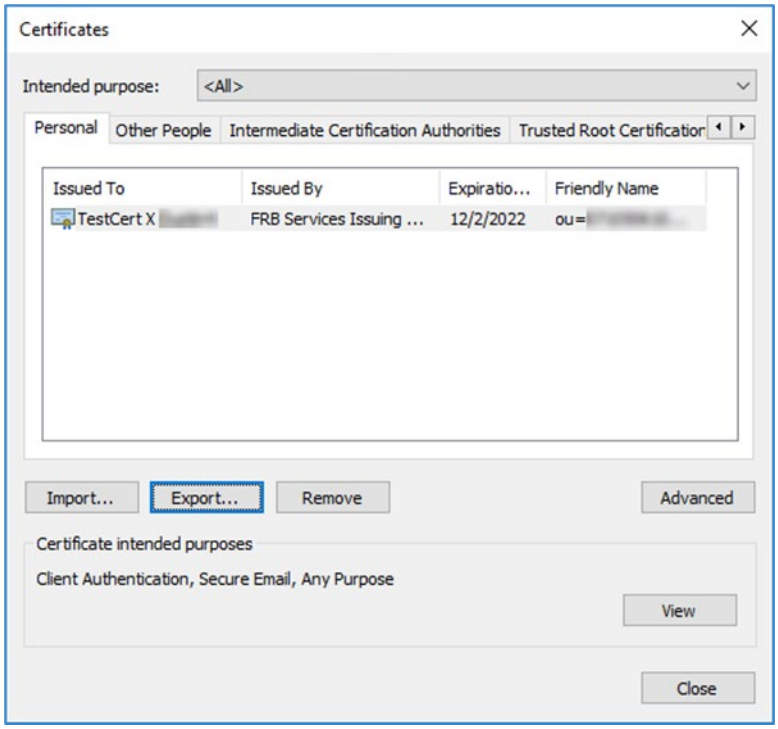
Certificate Export Procedures

To export a certificate:

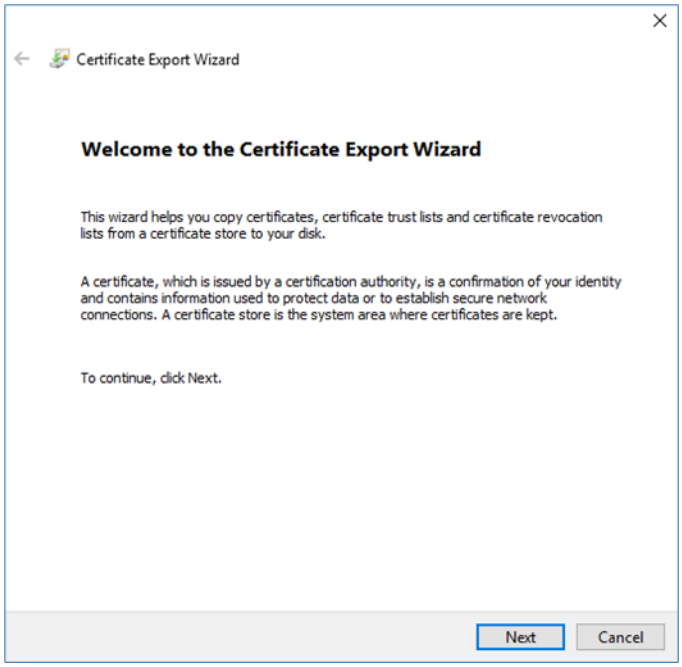
1. On your PC, search for and select “Internet Options” using the search bar on your taskbar. On the resulting “Internet Properties” window, select the “Content” tab. Click the **Certificates** button.



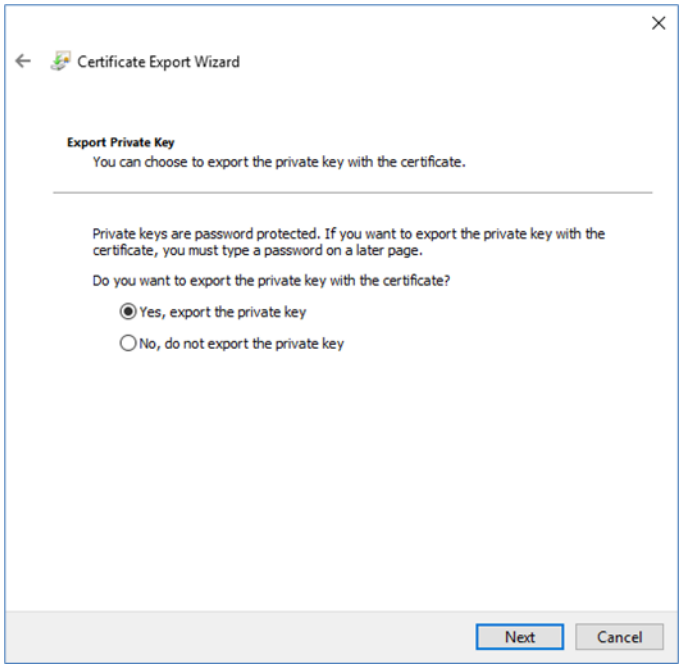
2. Highlight the certificate you want to export and click the **Export** button.



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

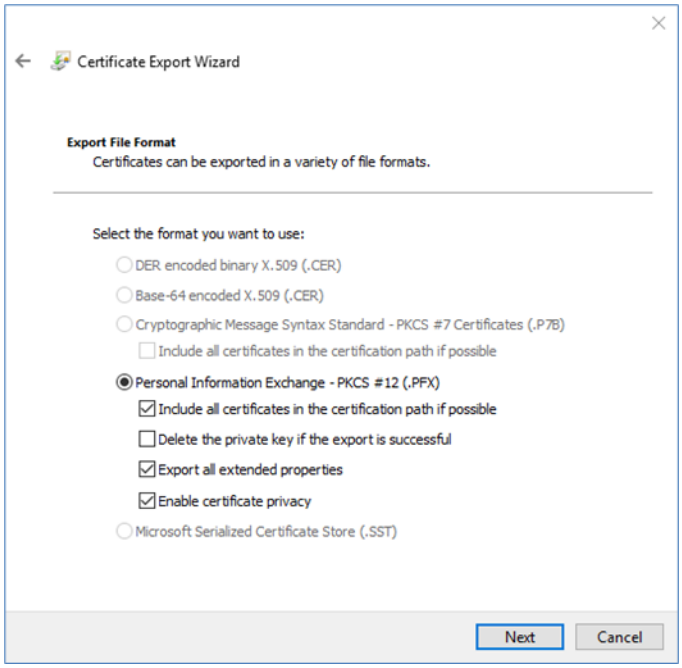


4. Select “Yes, export the private key” and click the **Next** button.

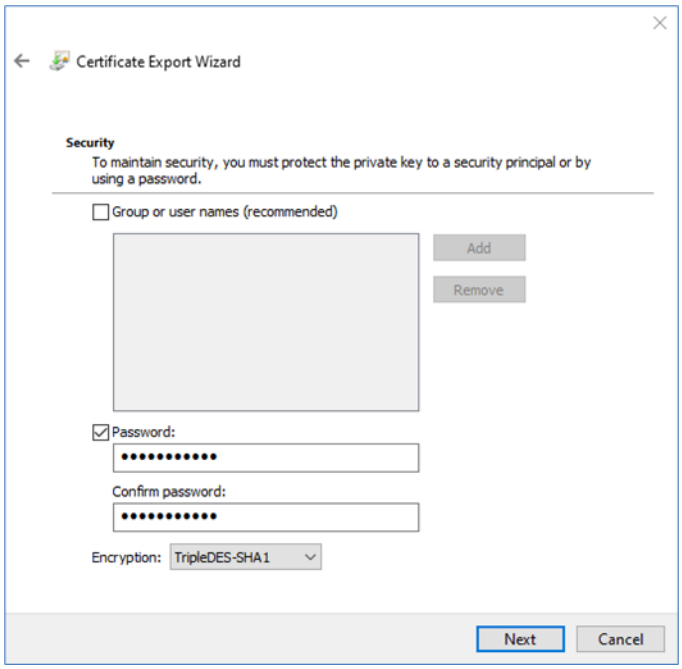


5. Select the settings indicated below, if available, and click the **Next** button.

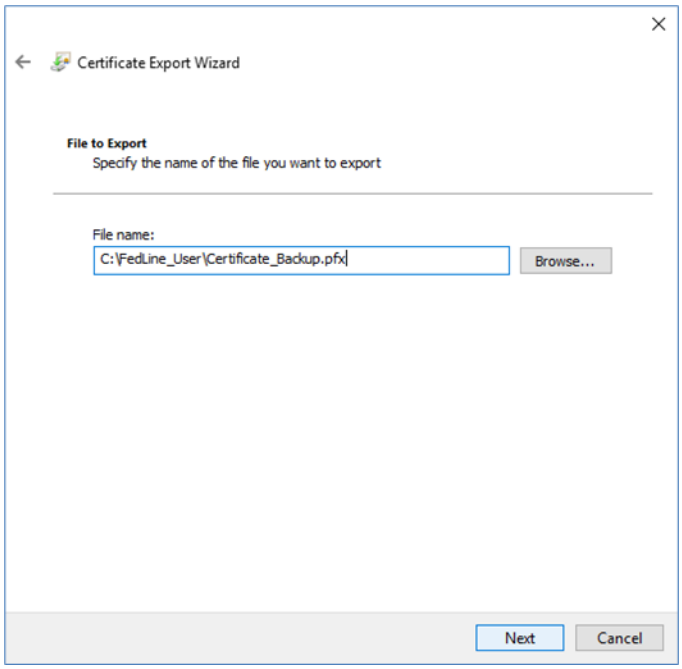
NOTE: Your options may differ from those shown in the screenshot below depending on your operating system.



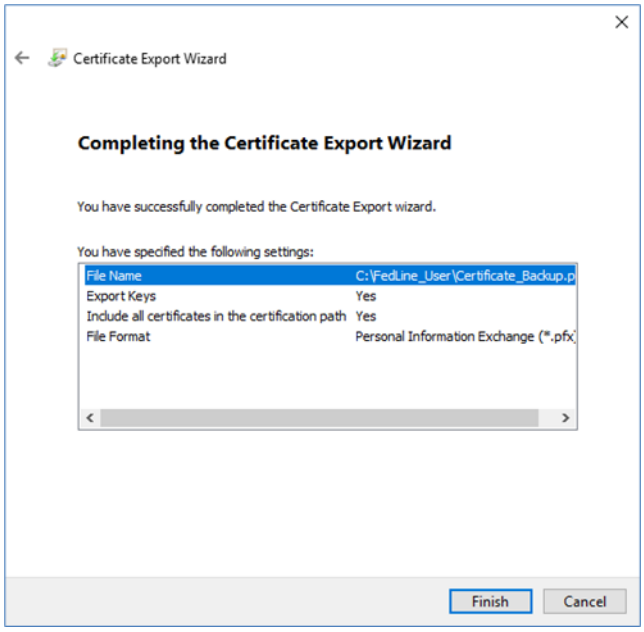
6. Enter a strong certificate password, as defined in the Federal Reserve Banks' *Password Practice Statement*. Ensure that "TripleDES-SHA1" is selected in the "Encryption" field. Click the **Next** button.



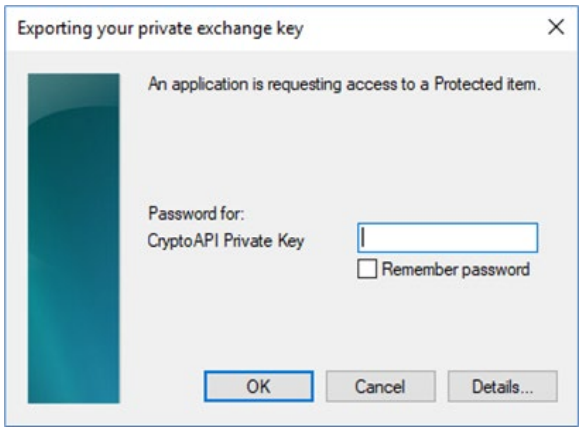
7. Specify the destination of the file. Click the **Next** button.



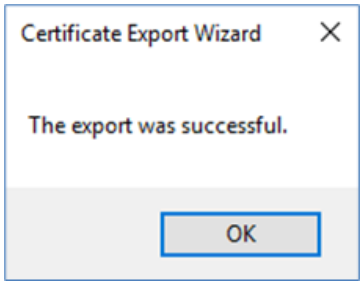
8. Click the **Finish** button.



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



10. The success message window displays. This completes the certificate export. Click the **OK** button.



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

To import the certificate on a contingency machine or contingency location, follow the certificate import procedures in the “Certificate Retrieval Procedures” section’s “Certificate Creation” subsection within this document. Certificate import procedures can be found in steps 6-14.