

User Certificate Retrieval Procedures

Version 3.1

Contents

Federal Reserve Banks User Certificate Retrieval Overview and Preparation Procedures.....	2
User Certificate Creation Procedures.....	2
Installing the Federal Reserve Banks Certificate Authority (CA) Certificates	8
FRB Services Root CA Certificate.....	8
FRB Services Issuing CA Certificate.....	12

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

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

Federal Reserve Banks User Certificate Retrieval Overview and Preparation Procedures

This guide provides step-by-step information to help you download a Federal Reserve Banks digital certificate (certificate) for your Internet Explorer® browser. 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 be in compliance with basic hardware and software requirements. In order 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 Customer Contact Center at (888) 333-7010. Non-FedLine customers should contact support as directed during the enrollment process.

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

User Certificate Creation Procedures

1. In Internet Explorer, go to the URL provided in the documents you received containing your Authorization Code and Reference Number. For security purposes, you should validate that the address begins with <https://registration.federalreserve.org>.
2. You will be presented with the page shown below. Click the **User Certificate Download** button.

THE **FEDERAL RESERVE**
FRBservices.orgSM

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](#).

User Certificate Download

Server 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.

3. Enter your **Reference Number** and **Authorization Code** in the appropriate fields. Click the **Generate Security Store** button.

THE **FEDERAL RESERVE**
FRBservices.orgSM

User Certificate Download

Generate Digital ID
Generate PKCS12 Security Store.

To generate your PKCS12 security store, please enter the required information in the form below.

* Reference Number (for example: 27600839)
12345678

* Authorization Code (for example: 6JIG-4LOV-OXLQ)
12AB-34CD-56EF

Generate Security Store Cancel Clear Form

4. In the next screen, enter a password to protect your P12 user certificate that you will download (Note: Follow the Password Rules on the right side of the screen). Make note of this password as you will need it to install your user certificate. Click the **Generate Security Store** button.

THE **FEDERAL RESERVE**
FRBservices.orgSM

User Certificate Download

Generate Digital ID
Generate PKCS12 Security Store.

To generate your PKCS12 security store, please enter the required information in the form below.

* Password
●●●●●●●●

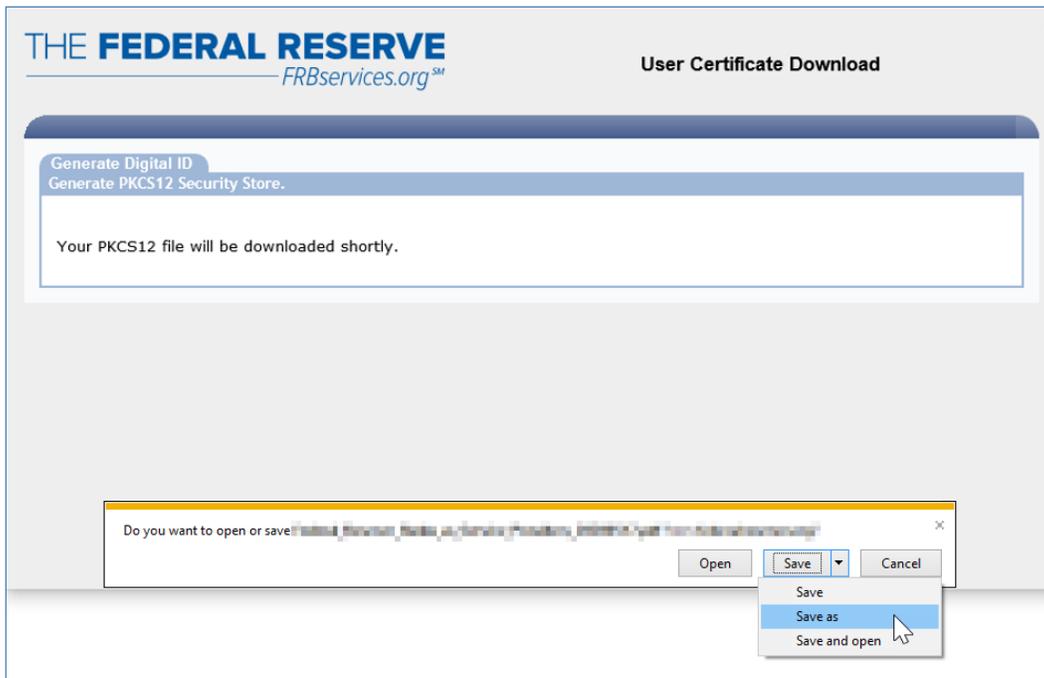
* Confirm Password
●●●●●●●●

Generate Security Store Cancel Clear Form

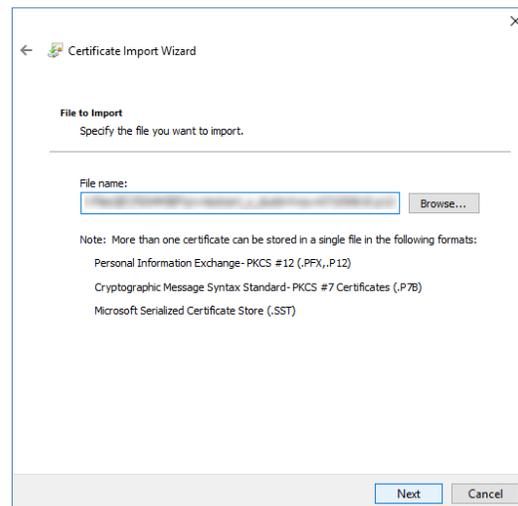
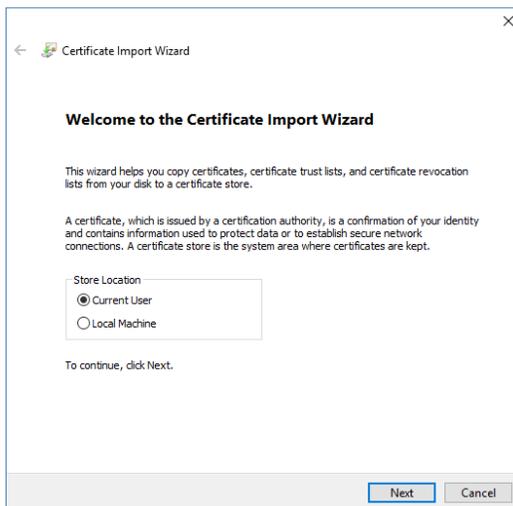
Password Rules

- ✓ must be at least 8 characters long
- ✓ must contain an uppercase character
- ✓ must contain a lowercase character
- ✓ must contain a numeric character
- ✓ must contain a non alpha or numeric character
- ✓ password and confirm password must match

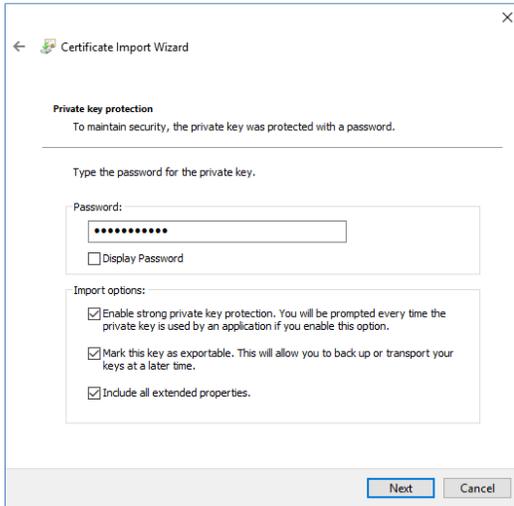
- The following screen will appear. Wait until you see the prompt at the bottom of the screen to save or open your certificate. Click **Save As**. If your browser does not permit you to Save As, please contact your local IT support group.



- Save the file to your desktop or other location of your choosing.
- Open the folder the file was saved to and double-click on the file.
- Select **Current User** and click **Next**, then click **Next** on the following screen.



9. Enter the P12 password saved from earlier, ensuring that the import options indicated below are selected, click **Next**, and then click **Next** on the following screen.



Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

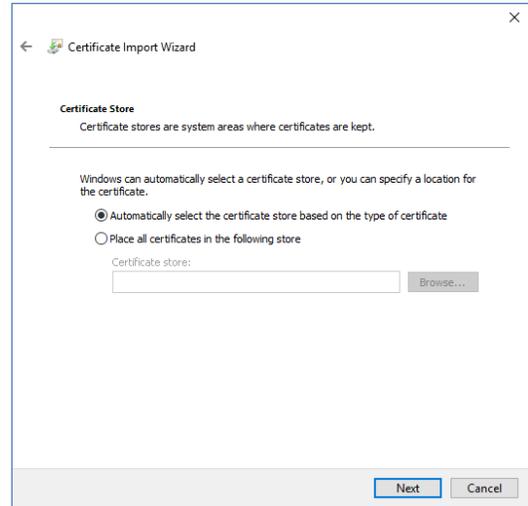
Password:

Display Password

Import options:

- 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.
- Include all extended properties.

Next Cancel



Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

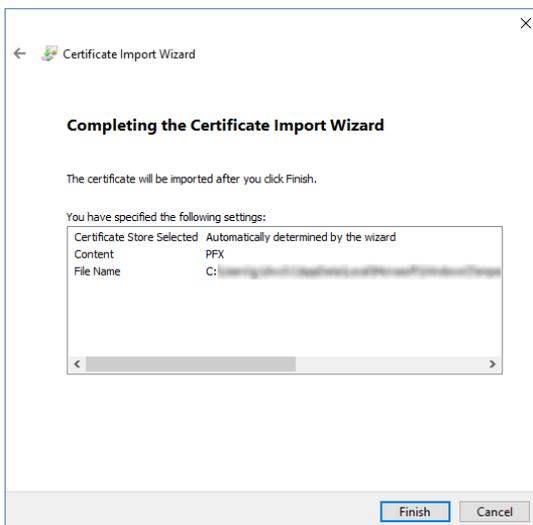
Automatically select the certificate store based on the type of certificate

Place all certificates in the following store

Certificate store: Browse...

Next Cancel

10. Click **Finish**.



Certificate Import Wizard

Completing the Certificate Import Wizard

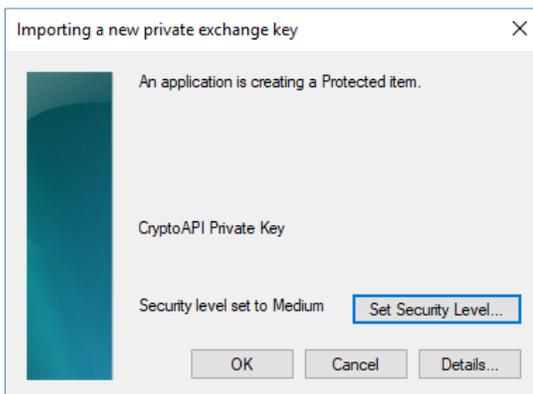
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\[unclear]

Finish Cancel

11. On the **Importing a new private exchange key** screen click on the **Set Security Level** button.



Importing a new private exchange key

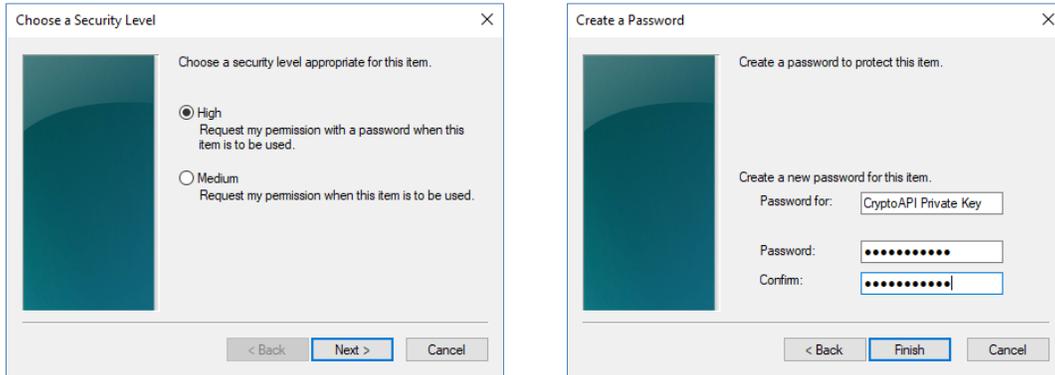
An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

OK Cancel Details...

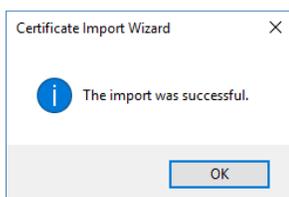
12. Select the **High** option and click **Next**. Enter a password to protect your Private Key. It is important that you remember this password. This will be the password used by Windows to protect your certificate. Any time you use your certificate in the future to connect to Federal Reserve Bank Services your browser will prompt you for this password. Click **Finish**.



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



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



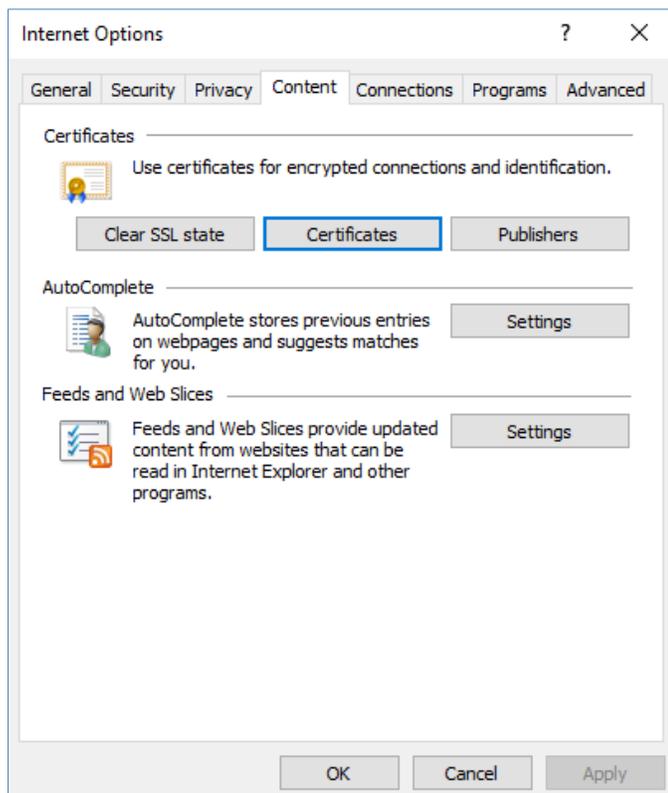
15. Locate the file that was downloaded in Steps 5 and 6 and save it to a secure location (such as a network drive) for contingency purposes, in accordance with your organization's policies. Once saved to a contingency location, the file can be deleted from your PC. You should also save the password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

IMPORTANT: You must safeguard the digital certificate and its associated private key.

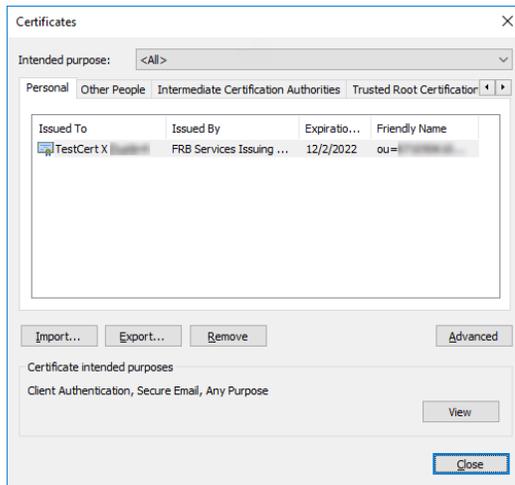
Key considerations include:

- Create a physical 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.
- It is important to 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.
- Do not share your password with anyone.

16. Verify that you have correctly installed the certificate. In Internet Explorer, click **Tools** → **Internet Options** → **Content**, then click **Certificates**.



17. You should see your newly downloaded certificate in the **Personal** tab. If multiple Federal Reserve Bank credentials appear in the list, the newly downloaded certificate will typically have the farthest expiration date. Click **Close**.

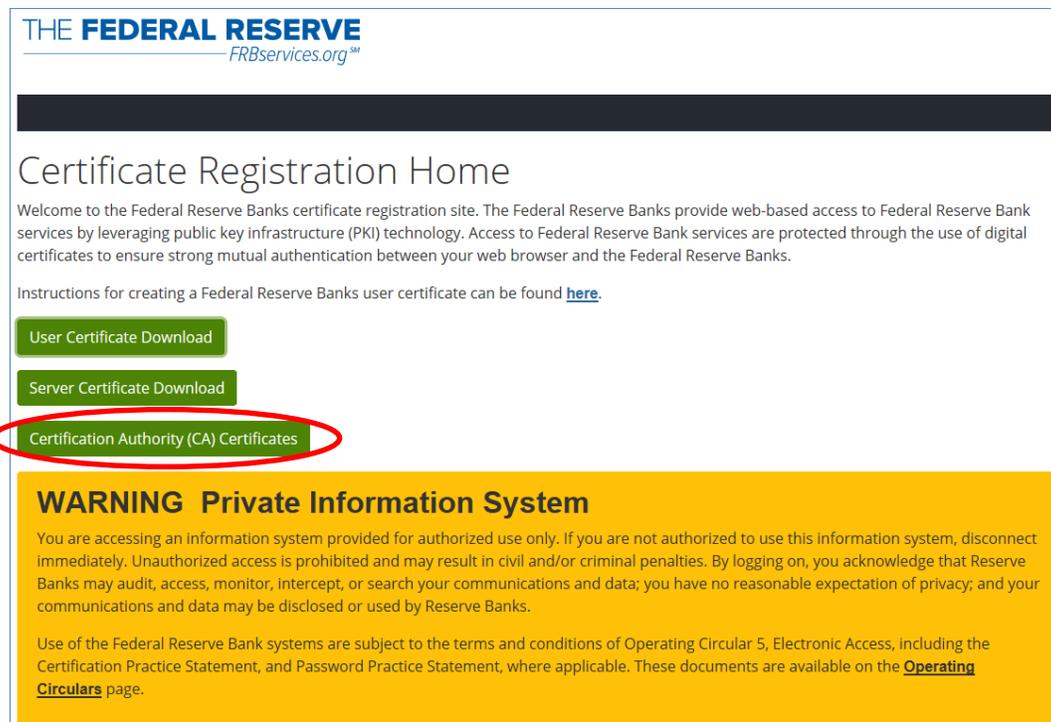


Installing the Federal Reserve Banks Certificate Authority (CA) Certificates

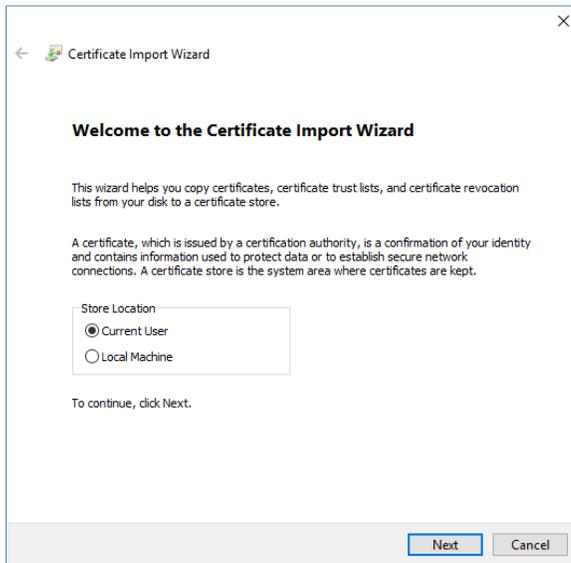
Some users may need to manually install the Federal Reserve Banks CA Certificates. Follow the procedures below to complete this activity on any new computer that will be used to access Federal Reserve Bank Services.

FRB Services Root CA Certificate

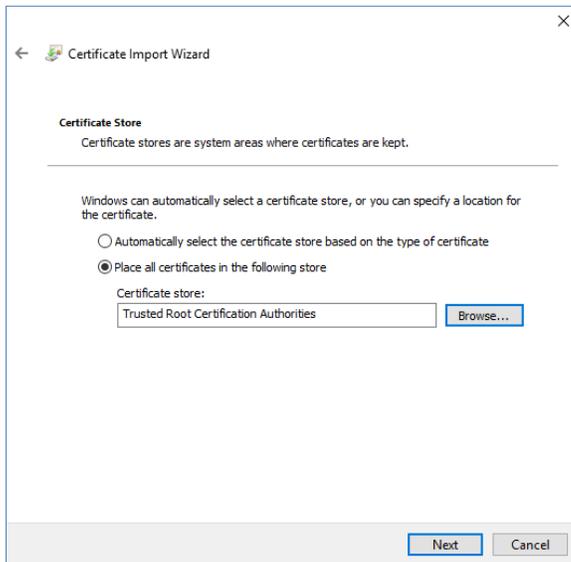
1. Browse to the Certificate Registration Home page at <https://registration.federalreserve.org> and click the **Certification Authority (CA) Certificates** button.



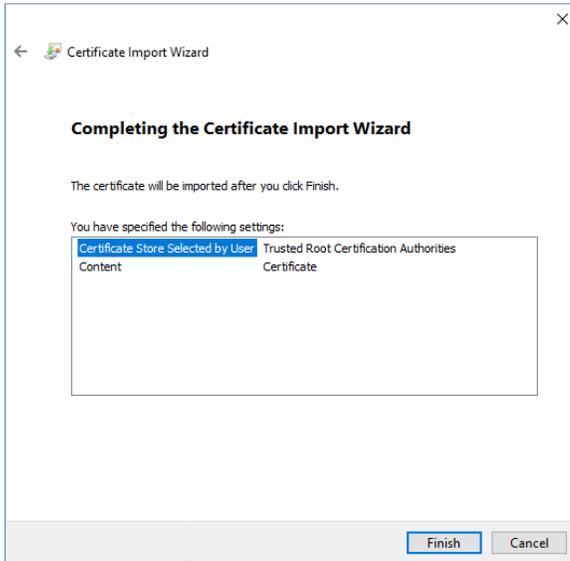
5. The **Certificate Import Wizard** will be initiated. Click **Next**.



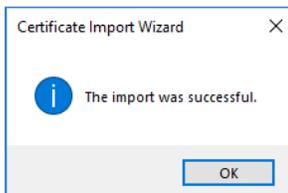
6. Select **Place all certificates in the following store** and click **Browse**. Select the **Trusted Root Certification Authorities** option and click **OK**. Verify the selection and click **Next**.



7. Click **Finish**.



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



FRB Services Issuing CA Certificate

1. Browse to the Certificate Registration Home page at <https://registration.federalreserve.org> and click the **Certification Authority (CA) Certificate** link in the left-hand navigation menu.

THE **FEDERAL RESERVE**
FRBservices.orgSM

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](#).

User Certificate Download

Server 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 Issuing CA Certificate (2017-2030)**.

THE **FEDERAL RESERVE**
FRBservices.orgSM

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

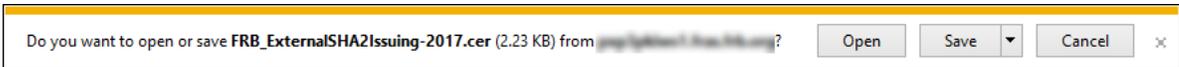
FRB Services Issuing CA Certificate (2017-2030)

FRB Services Certificate Chain

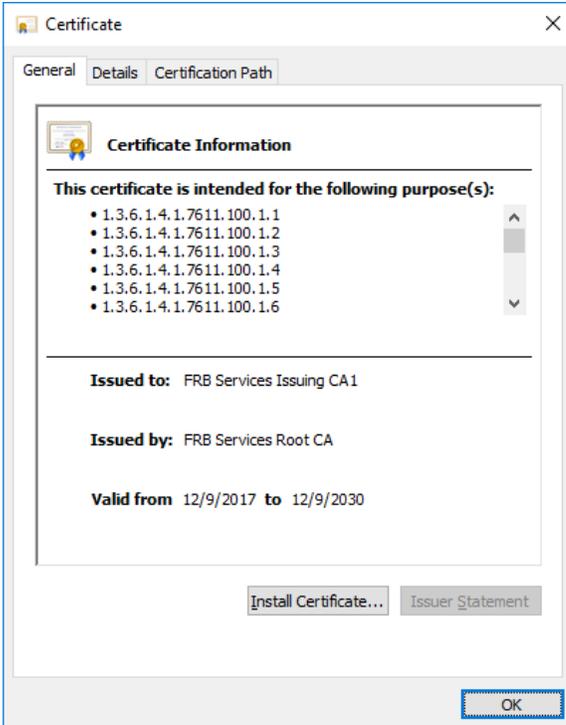
FRB Services Root CA Certificate (PEM encoding)

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIETUNXODANBgkqhkiG9w0BAQsFADBJMQswCQYDVQQGEwJ1
czEeMBwGA1UEChMVRmVhcnRmVzZXJhbCBSZXN1cnZ1IEJhbmtzMRUwEwYDVQQLExQ0kg
U2VydmljZXNkHTAbBgNVBAMTFEZZSQ1BTZKJ2aWN1cyBSb290IENBMmB4XDEyMDEy
ODE4NTE1NFoXDTMxMDEyODEyMDEyMDEyMDEyMDEyMDEyMDEyMDEyMDEyMDEyMDEy
FUZlZGVyYWwvVzZXJ2ZSB0YXN0cmVudC51UECkMMUEtJlF1cnZlY2VzMR0w
GwYDVQDEExRGUkIjU2VydmljZXNkHTAbBgNVBAMTFEZZSQ1BTZKJ2aWN1cyBSb290
ggEFAADCAQoCggEBAKwP7+9CRkfkIKV/5j2+1V9sefzSxZ11NI6MtpgqHvwSPWuFO
```

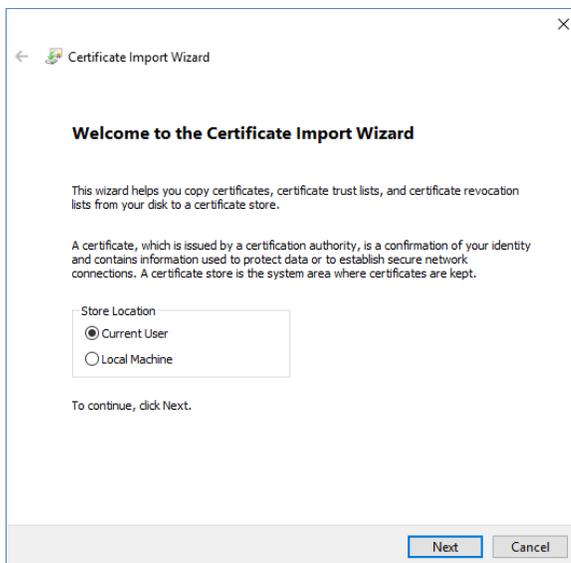
3. At the prompt at the bottom of the window, click **Open**.



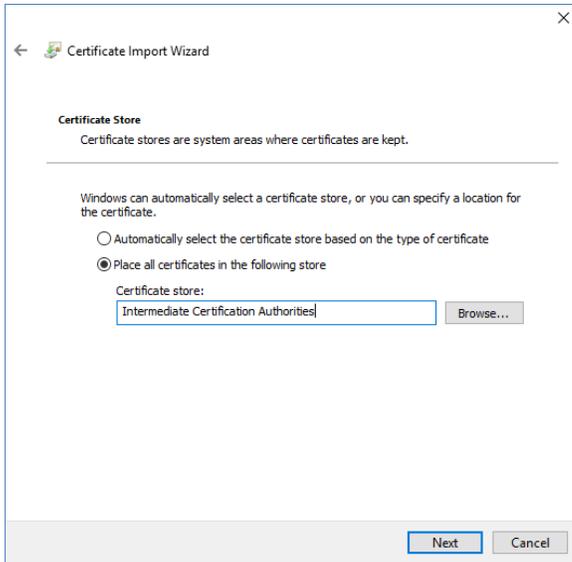
4. In the **Certificate Information** window, click **Install Certificate**.



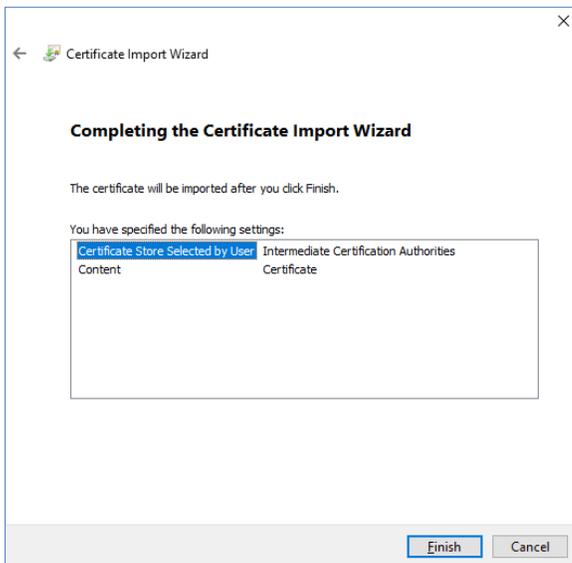
5. The **Certificate Import Wizard** will be initiated. Click **Next**.



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**.

