IBM Business Consulting Services

FedTeDS.gov PKI Pilot Technical Solution
July 22, 2004

Using PKI Authentication with FedTeDS.gov

Public Key Infrastructure

Table of Contents

Section **Page**

1. What is PKI?

Public Key Infrastructure (PKI) based credentials offer considerable advantages for authentication. They are capable of higher assurance transactions and can be validated using only public information. The standards for PKI are also more mature and more widely used than the emerging standards for federated PIN/Password based identity management.

Public Key Infrastructure encompasses comprehensive security technologies and policies using cryptography and standards to provide fundamental computing infrastructure improvement. PKI features:

- User authentication stronger than traditional “passwords on servers” mechanisms,
- Digital signing of email and other documents proving the originator’s identity and faster, more efficient, paper free business processes, and
- Encryption to protect critical email and other data in user-focused manner.

Point solutions exist for each feature, but only PKI addresses them all well with standards and broad industry support. Robust services and commercial and open source tools provide a sound PKI foundation. Browsers, Web servers and services, email readers and list servers, database servers, PDF readers, VPN appliances, WPA wireless authentication, USB keys, and smart cards all have integrated PKI support. Because PKI is standards-based, these all can interoperate with each other.

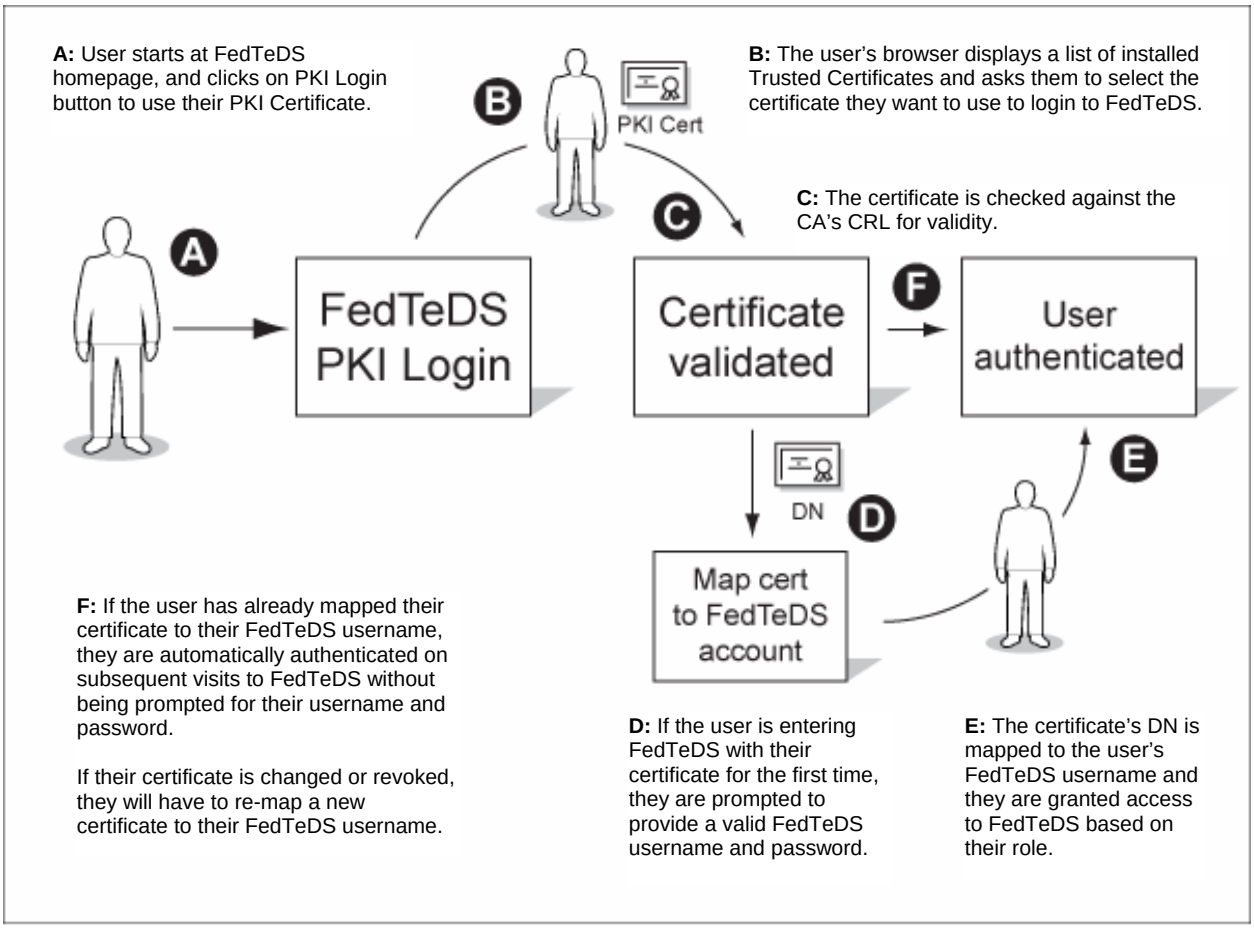
PKI uses asymmetric key pair encryption. One key of the pair is the only way to decrypt data encrypted with the other. Users and servers have industry standard certificates to associate their key pairs with their identity and information such as the authority that issued the certificate and designated uses for the certificate. Certificate Authorities (CAs) issue PKI certificates and attest to the validity of the identity specified by the certificate. Operating systems, applications, hardware add-ons, and servers use PKI certificates and keys for authentication, digital signing, authorization and encryption. PKI enables trust between two or more parties (possibly from different organizations or nations) without prior knowledge of each other.

The Federal PKI (FPKI) employs a Bridge Certificate Authority (BCA) to harmonize policies and procedures for Certificate Authorities (CAs). The eAuthentication initiative has deferred assessment and governance of PKI based credential services to the FPKI PA, the governing body for the BCA. Additional information on the FPKI is available at http://www.cio.gov/fpkipa/.

2. FedTeDS PKI Pilot Overview

The FedTeDS PKI Pilot will provide common authentication services and Single Sign-On (SSO) capability with other e-Gov applications. The goal is to provide common shared services that all Federal agencies can use to authenticate all users (both internal Federal and external private and public) for all applications that require authentication.

Figure 1.0: FedTeDS PKI Pilot approach overview



FedTeDS PKI Application Process Flow

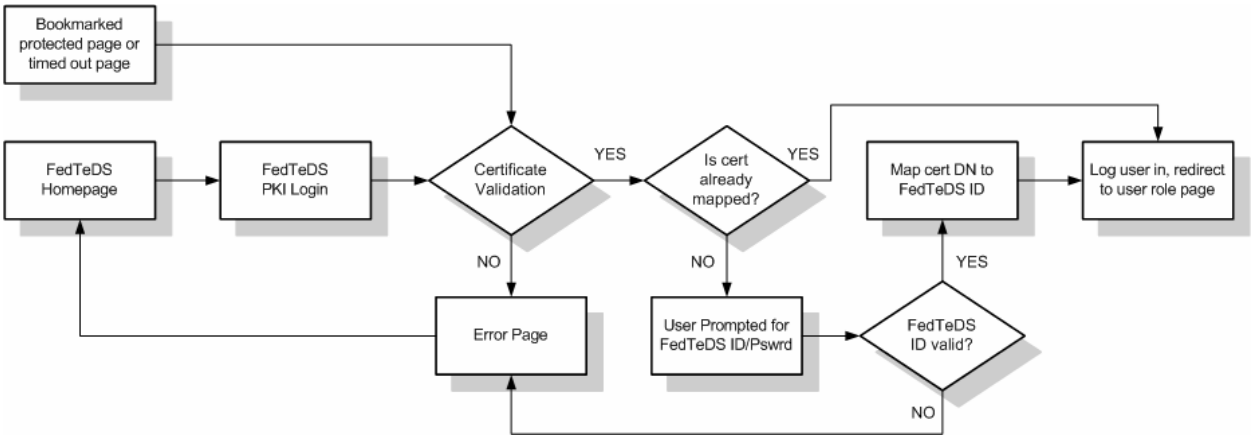
Users will come to FedTeDS via two primary entry points, the FedTeDS homepage and the FedTeDS Vendor login from either FedBizzOpps (FBO) or another solicitation-posting site that has a link directing users to data on FedTeDS.

The user will then click on the "PKI Login" button to authenticate using their PKI Certificate. FedTeDS will check the user's browser to see if they have any certificates installed that have been issued by Certificate Authorities (CAs) trusted by FedTeDS (see section 3 for more information on FedTeDS Trusted Certificate Authorities). If the user has one or more certificates that are trusted by FedTeDS they will be prompted to select the certificate that they wish to authenticate with via a selection pop-up window.

Once the user selects a certificate, FedTeDS performs a real-time certificate validation check against the public Certificate Revocation List (CRL) directory of the issuing CA. If the selected certificate cannot be validated for any reason, the user's browser is redirected to an error page where they are informed that the certificate they have selected cannot be validated.

If the selected certificate is valid, a check is performed against the existing FedTeDS registered user database to see if the certificate has been mapped to a user account. If the certificate cannot be identified as being mapped to an existing user, a page is displayed in the user's browser requesting them to provide their FedTeDS username and password. If the user enters a valid FedTeDS username and password and continues, their certificate is mapped to their existing account by means of the certificate's Distinguished Name (DN). They will be shown a confirmation page and redirected to the appropriate page in FedTeDS based on their role.

Figure 2.0: FedTeDS application PKI process flow



If the user does not have an existing FedTeDS username and password, they have the option to click on a link located on the certificate mapping page to register with FedTeDS using the existing registration process.

If the selected certificate is valid and has already been mapped to an existing FedTeDS account, the user is automatically authenticated and redirected to the appropriate page in FedTeDS based on their role.

The certificate mapping process is only necessary once. Once a valid certificate has been successfully mapped to an existing FedTeDS username and password, all subsequent logins via FedTeDS using that same certificate will occur automatically. If the mapped certificate changes or is revoked, the user will need to address these issues or acquire another valid certificate before being able to authenticate using

PKI. If the user acquires a new or different certificate, they will be required to map the new certificate to their existing FedTeDS username and password upon their first attempt to authenticate with it.

A user can have more than one valid certificate mapped to their FedTeDS username and password. A user cannot have a single valid certificate mapped to multiple FedTeDS usernames and passwords.

3. Types of PKI certificates accepted by FedTeDS

In accordance with the E-Authentication Initiative, FedTeDS will accept only PKI certificates that have been issued to you by a Certificate Authority (CA) that has been cross-certified with the Federal Bridge Certification Authority (FBCA) http://csrc.nist.gov/pki/fbca/welcome.html.

The following CAs are currently accepted:

For Government Users, Federal or State:

Typically these are issued to you by the Department or Agency that you work for.

- Department of Defense
- Department of Energy
- Department of Treasury
- NASA
- USDA/NFC
- State of Illinois

For Contractors and Vendors:

- Digital Signature Trust
  http://www.digsigtrust.com/federal/aces.html
  federal@trustdst.com
  301-921-5977

- ORC
  http://eca.orc.com
  pkihelp@orc.com
  1-800-386-6820

- Verisign
  https://dodeca.verisign.com
  ieca-support@verisign.com
  1-800-579-2848

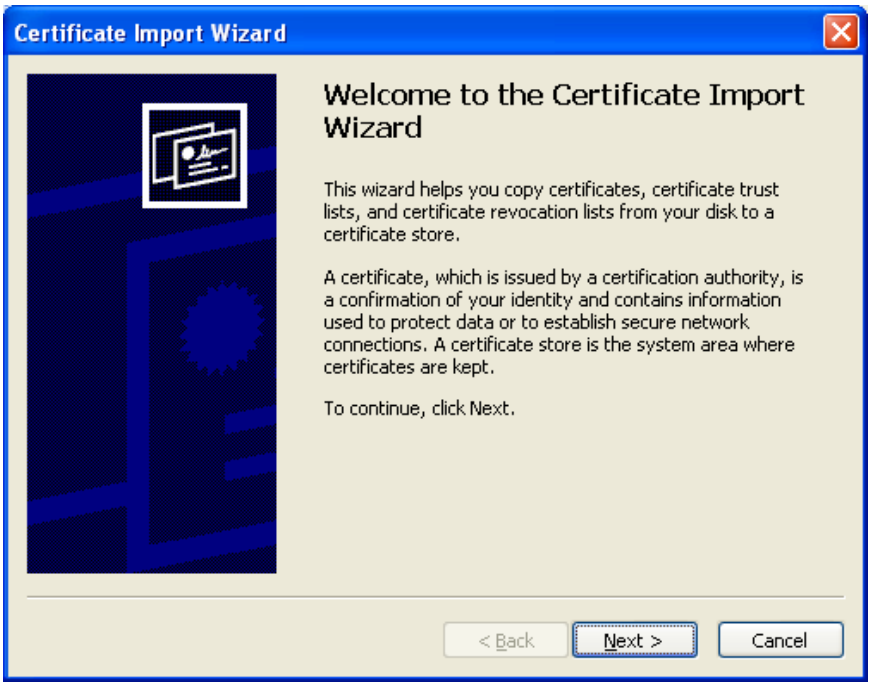
4. How to install a PKI certificate

The PKI application that runs on FedTeDS uses the standard Microsoft Windows Certificate Security Store to see what certificates you have installed. Regardless of which browser you use, your certificate must be correctly installed in the Microsoft Windows Security Store.

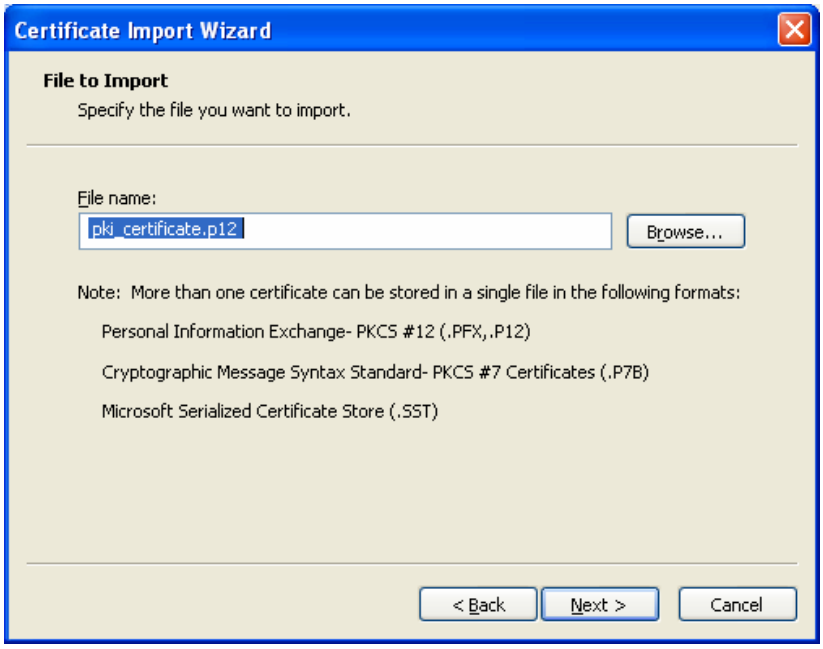
Using the Microsoft Certificate Import Wizard

1. Locate and double click your PKI certificate file. You can also open up Microsoft Internet Explorer, click on the "Tools" option from the top menu bar and then select "Internet Options." This will open your Microsoft Certificate Store and display currently installed certificates. To add a new certificate click on the "Import" button, this will activate the Certificate Import Wizard.

   The Microsoft Certificate Import Wizard pop-up box should appear.



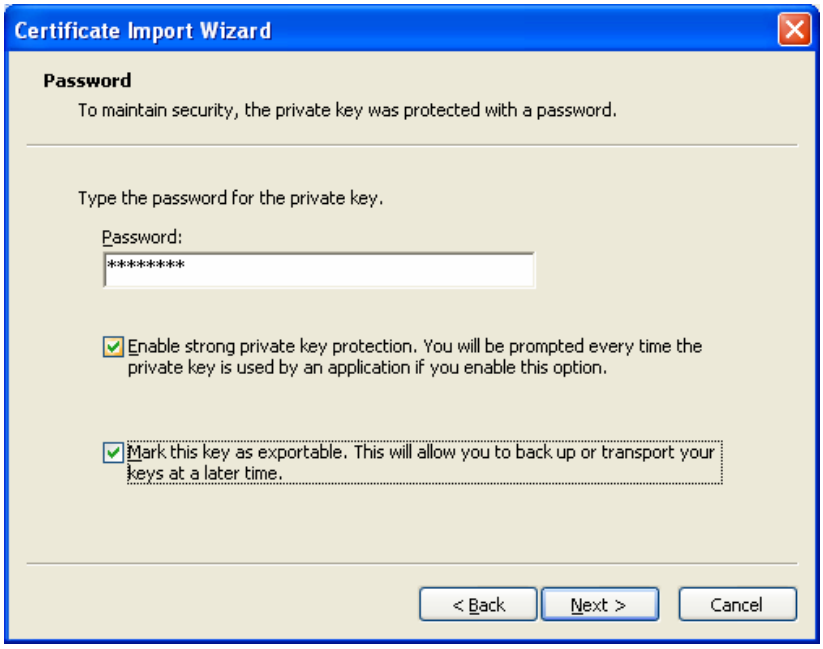
2. Click on the "Next" button to continue.



3. A new window will appear with the certificate file you selected highlighted. Make sure it is the correct file. If it is incorrect, or no file is selected, click on the "Browse" button to locate the correct file.

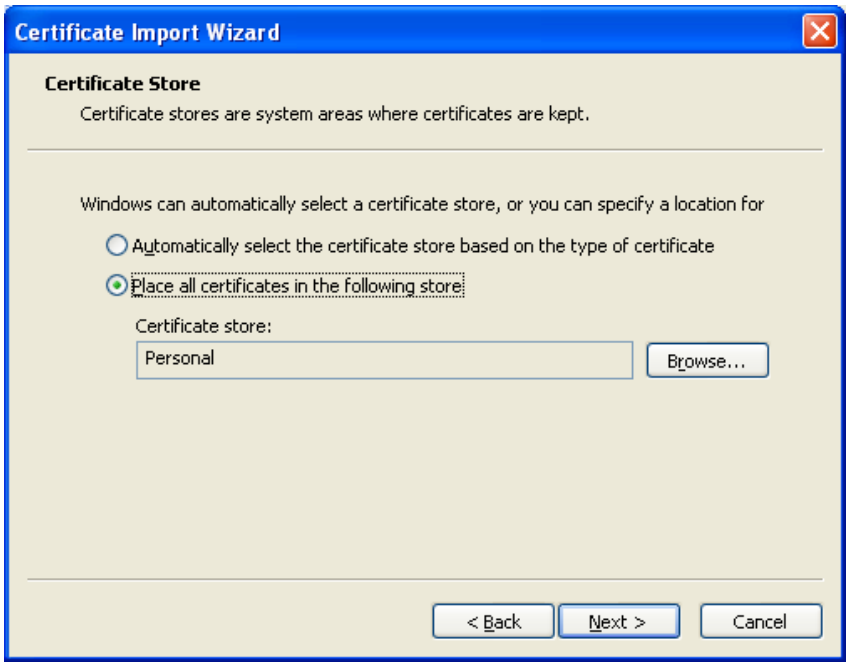
4. Click "Next" to continue.

5. You will be prompted to enter the password that is associated with your PKI certificate. Enter your password in the field provided. It is recommended that you select both of the options below the password field in order to maximize security and enable you to transfer or backup your keys (certificates) at a later time.



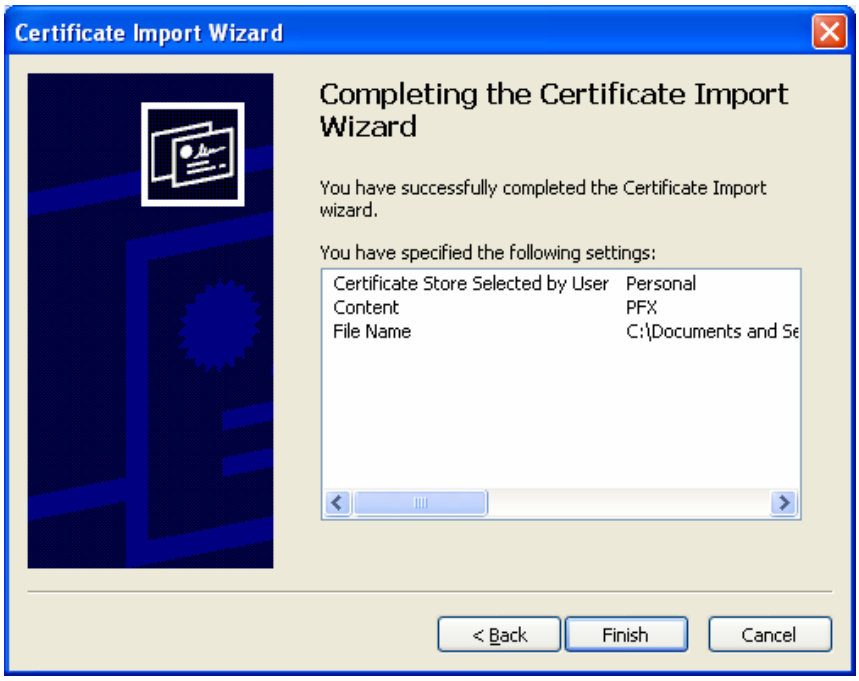
6. Click "Next" to continue.

7. A window will appear asking you where you want to store your certificate. By default the "Personal" store should be selected. If it is not, click on the "Browse" button and select "Personal" from the options.



8. Click "Next" to continue.

9. You will see the certificate completion window, showing details of the import process.



10. Click "Finish" when ready.

Setting the Certificate Security Level

11. You will then see a new window prompting you to set the security level of your PKI private key. By default the security level is set to "Medium". It is recommended that you change this to "High" by clicking on the "Set Security Level..." button.

Medium level means that you will not be prompted to enter your PKI certificate password when you attempt to use your certificate to authenticate with an application or to sign email.

High level means that you will be asked to enter your PKI certificate password every time you attempt to use your certificate to authenticate with an application or to sign email. This provides a much higher level of security and is the recommended level.

12. Click on the radio button next to "High" and then click on the "Next" button.

Entering your Certificate password

13. You will next be prompted to create a password for your private key. If you already have a password assigned to this key enter it here.

14. Click "Finish" to close this step.

15. You should now see that the security level has been set to **High**.

16. Click "OK" to complete the Certificate Import Wizard. After a few seconds you should see the Import Successful window.

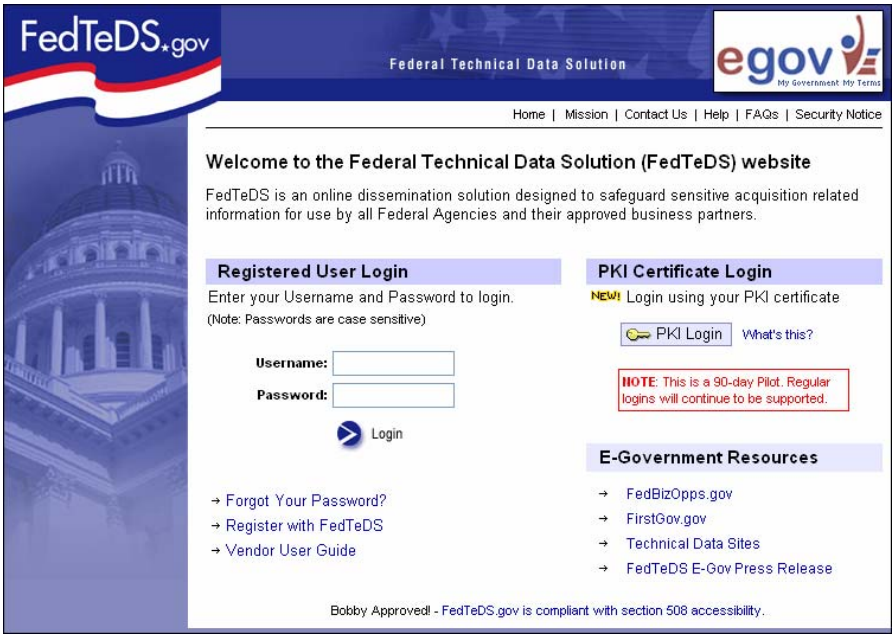
17. Click "OK" to close this window.

18. You have now successfully imported your PKI certificate into the Microsoft Certificate Security Store.

5. Using your PKI certificate with FedTeDS

Logging in with your PKI Certificate

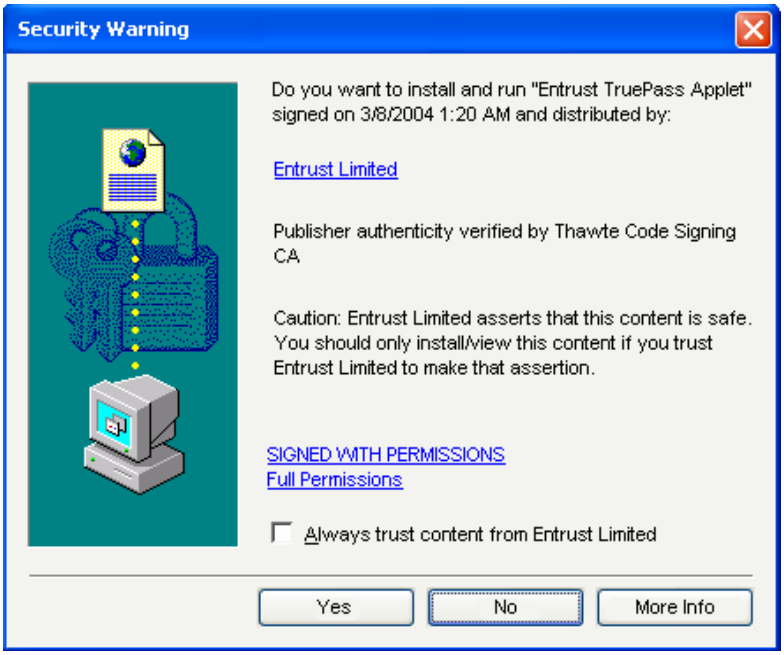
In your browser open up www.fedteds.gov.



Click on the “PKI Login” button located on the right-hand side of the homepage.

Accepting the TruePass PKI Applet

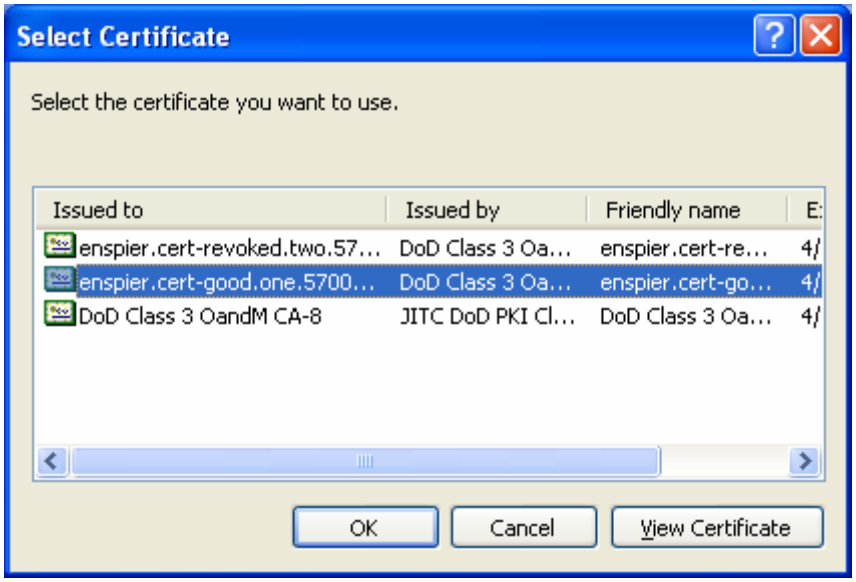
A security warning pop-up box will appear notifying you that your browser has been asked to install the Entrust TruePass Applet. This applet is required in order for TruePass to interact with your Microsoft Certificate Security Store which is where your PKI certificates have been installed. If you do not see this window, or if you get an error page, or if you do not have permission to install applets on your computer, please contact your IT department for assistance.



Click “Yes” to continue.

Selecting your PKI Certificate

The Microsoft Certificate Security Store selection dialog box will open, prompting you to select a certificate to authenticate with.

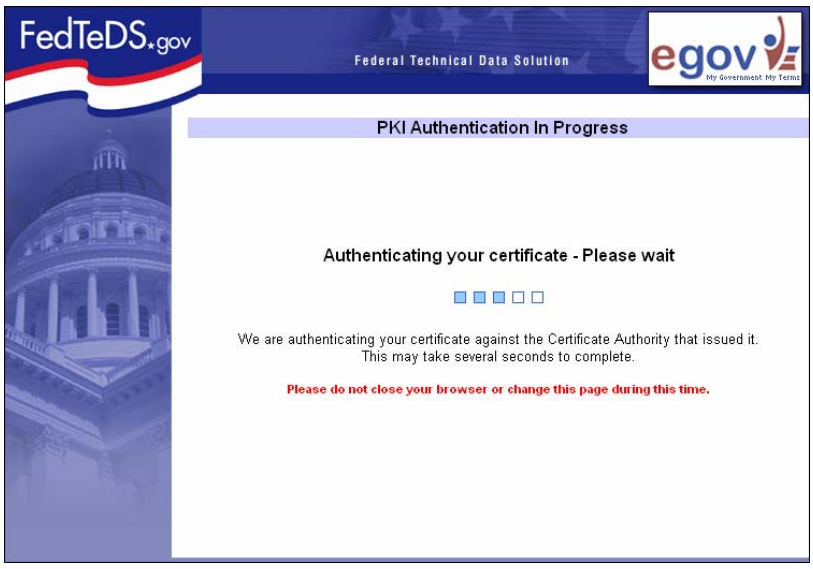


Select the certificate you want to use and click on the “OK” button to continue.

The Authentication Screen

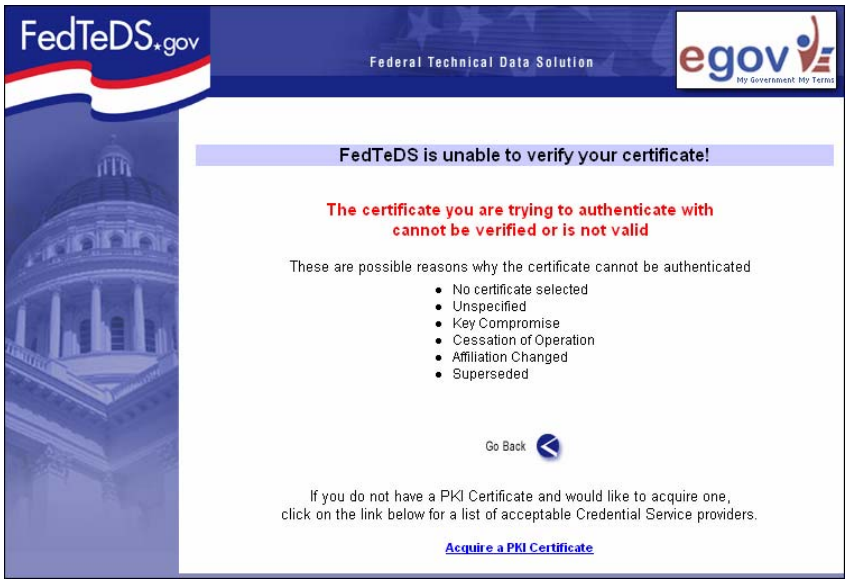
You will then see a page indicating that your certificate is being authenticated.

Important note: The certificate authentication process may take several seconds to perform while your certificate is checked against the revocation list of the Certificate Authority that issued it. **PLEASE DO NOT CLOSE YOUR BROWSER OR CHANGE THIS PAGE DURING THIS TIME.** It appears that the page is done, however the TruePass Applet is still working in the background.



Unable to Authenticate

If your certificate is invalid or cannot be authenticated against the Certificate Authority that issued it, you will see the “Unable to Authenticate your Certificate” page. If you are unable to authenticate but believe you should be able to, please contact the Certificate Authority that issued you your certificate for technical assistance.



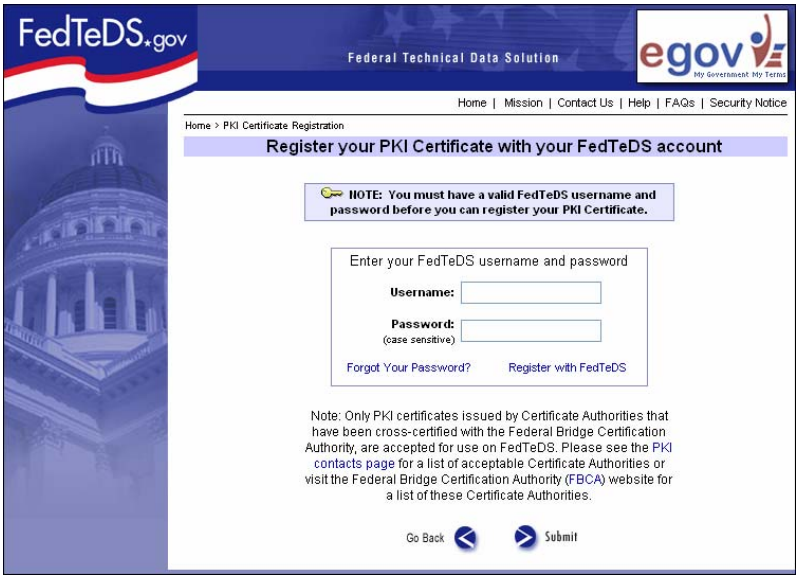
Entering your Certificate Password

If your certificate is successfully authenticated and you installed your PKI Certificate enabling the “High” level of security (recommended) you will be prompted to enter the password for the Private Key portion of your PKI Certificate. It is recommended that you do not check the “Remember password” box on this screen.

Click “OK” to continue.

Mapping your PKI certificate to your FedTeDS username

The first time you use your PKI certificate to authenticate with FedTeDS.gov, you will be asked to map your certificate to your FedTeDS username and password which was created when you registered with FedTeDS.

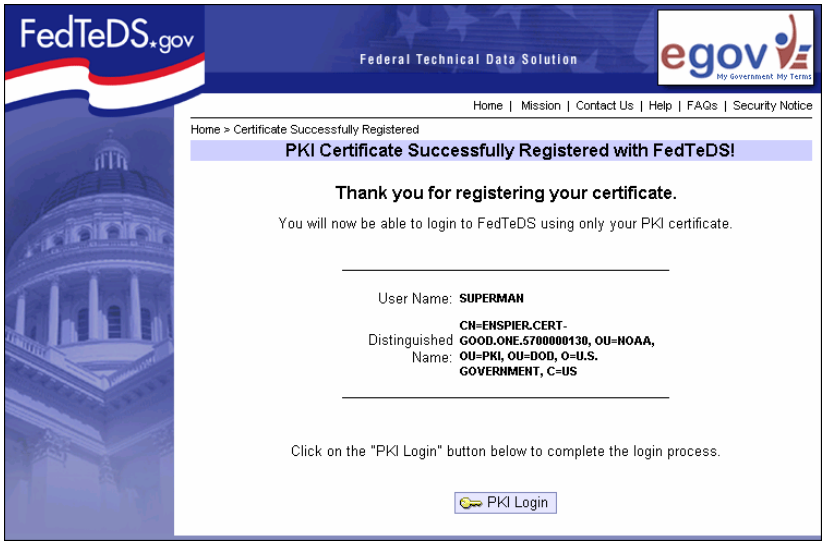


If you have not already registered with FedTeDS you can do so using the “Register with FedTeDS” link provided on the page. Note: You MUST have a valid FedTeDS username and password in order to use your PKI certificate. Your FedTeDS account is used to determine your permissions within the FedTeDS application based on your role.

Enter your username and password in the fields provided, and then click on the “Submit” button when done.

Confirmation of certificate mapping

You will then see a page displaying confirmation of your successful certificate mapping. Your FedTeDS username and the Distinguished Name (DN) unique identifying string from your certificate will be displayed in the center of the page.



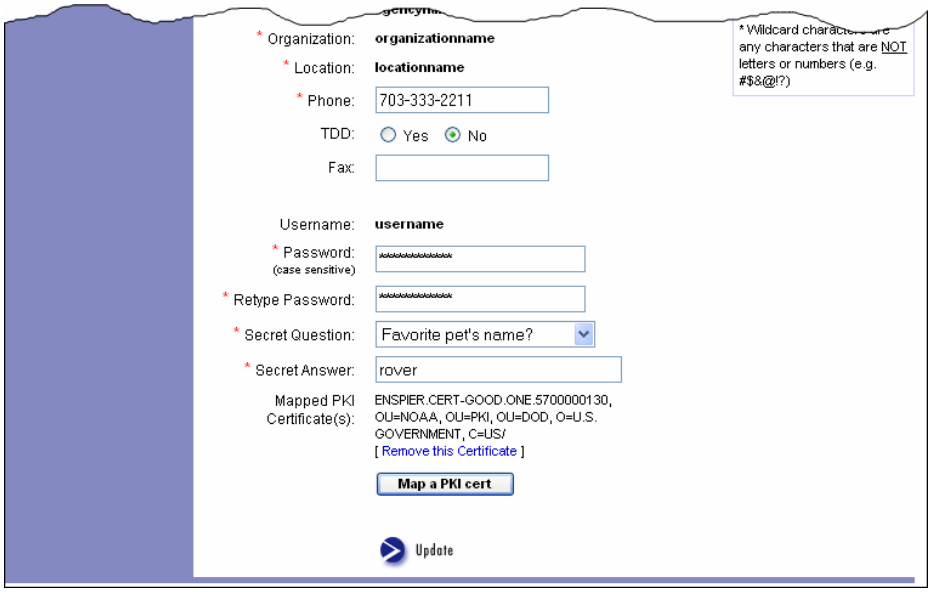
Click on the “PKI Login” button at the bottom of the page to complete the process.

You are now successfully authenticated with your PKI Certificate.

On all future PKI Logins using that same certificate, you will automatically be authenticated and logged in to the appropriate page for your login (based on your role), without the need to enter your FedTeDS username or password.

Editing, removing your PKI certificate

If for some reason you need to remove any PKI certificate that has been successfully mapped to your FedTeDS username, you can do so by clicking on the “Edit my Profile” link located on the left-hand navigation menu.



You can also add a new PKI certificate from your profile page by clicking on the “Map a PKI Cert” button and following the steps that were outlined above.

6. Assistance and Contact Information

Use the contact information if you are encountering problems specific to authenticating with your PKI certificate(s) and you would like to speak to a member of the FedTeDS Technical Team.

Brian Green
FedTeDS E-Authentication Team Lead
703-653-7217
bfgreen@us.ibm.com

Please note: Do not use the above contact information for general FedTeDS help inquiries. The general FedTeDS Help Desk contact number is: 703-653-7000, M-F, 8:30 am - 5:30 pm ET (help@fedteds.gov).