INFORMATION PAPER

DefenseTravel Management Office

How to Determine a Public Key Intrastructure (PKI) Certificate Expiration Date

Introduction

PKI certificates allow the proper authorities to create, manage, distribute, use, store, and revoke digital certificates that are used to provide personal identification. PKI certificates are necessary when simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the party needing to access a computer system, document, etc.

**For this information paper, unless otherwise stated, "you" refers to a traveler or applies to anyone who will a PKI certificate to create documents for you (e.g., Non-DTS Entry Agent, travel clerk).*

Types of PKI Certificates

For most military members, as well as for most DoD civilian and contractor employees, your PKI certificate is located on your Common Access Card (CAC).

You may also receive training PKI certificates from other sources. These certificates will normally be sent via a secure email. You will open these certificates and install them in your computer's Certificate Store. For more information on opening and installing training certificates refer to the *EWTS Guide*.

All PKI certificates expire. Knowing how to check your PKI certificate expiration date ensures you can always access websites, documents, or other sources requiring a PKI certificate.

Determining the Expiration Date using a Browser

Open a browser window and activate the menu bar. Follow the below steps to determine the expiration date of the PKI certificates in your Certificate Store. The most commonly used browsers are Google Chrome, Mozilla Firefox, and Microsoft Edge. **Note**: Internet Explorer (IE) is scheduled to sunset as of 06/22 and will no longer be viable option for accessing certain applications such as EWTS or DTS. Recommend contacting your IT department for guidance on installing or using any new computer application.

For the purpose of this paper we will provide 2 examples; Firefox and Chrome. You can see additional examples in the *EWTS Guide*.

Use *Firefox* to locate a certificate and expiration date:

1. Open the browser. On the right side of the screen, select the **Options** (3 vertical lines) icon.
2. The window opens. Select **Settings**.
3. Select **Privacy and Security**.
4. Scroll down to the **Certificates** area and select **View Certificates** (Figure 1).

Determining the Expiration Date using a Browser

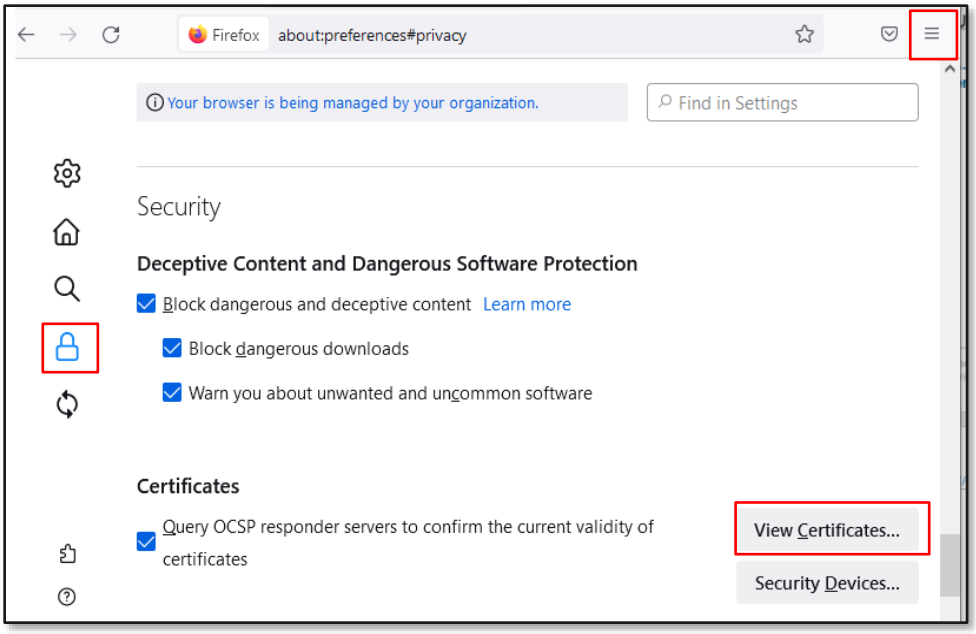

Figure 1: Certificates Option within Firefox Browser

a. The **Certificate Manager** screen opens (Figure 2). Select **Your Certificates** tab.

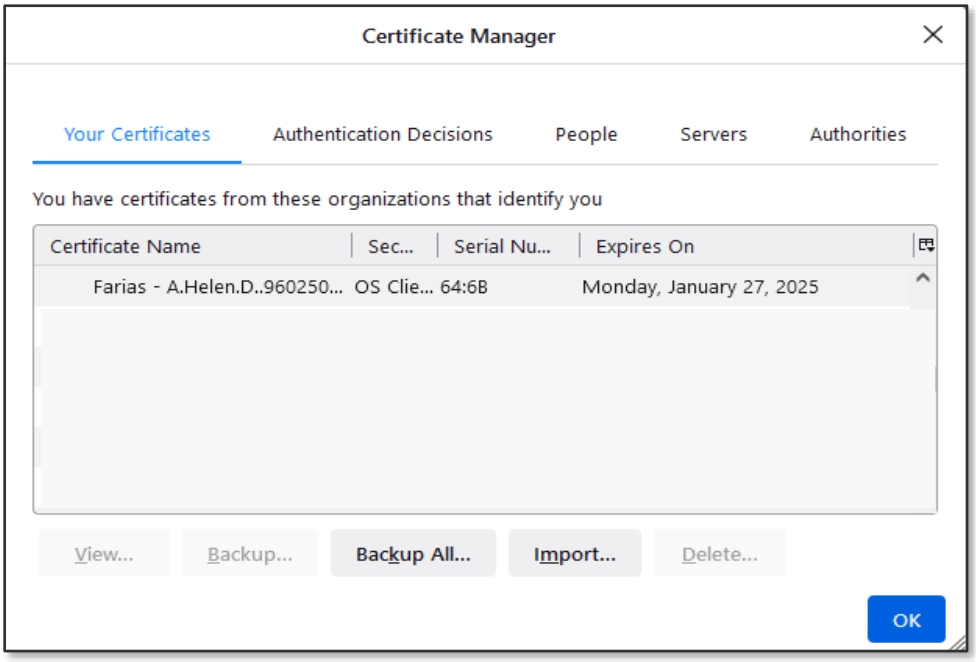

Figure 2: Certificate Manager Screen

Determining the Expiration Date using a Browser

b. The **Your Certificates** tab shows all installed certificates and their expiration dates (Figure 2).

If you cannot view the expiration date because it is hidden, select the cross-hairs between the columns and drag the column until you can readily view the information.

5. Once you confirm the certificate and expiration date select **OK** to exit.

Use *Chrome* to locate a certificate and expiration date:

1. Open the browser. On the right side of the screen, select the **Options** (3-dots vertical) icon and then choose **Settings**.
2. On the **Settings** page, scroll down and select **Privacy and Security**.
3. Select **Security**. Under the **Advanced** area, select **Manage certificates** (**Manage HTTPS/SSL certificates and settings**), (Figure 3).

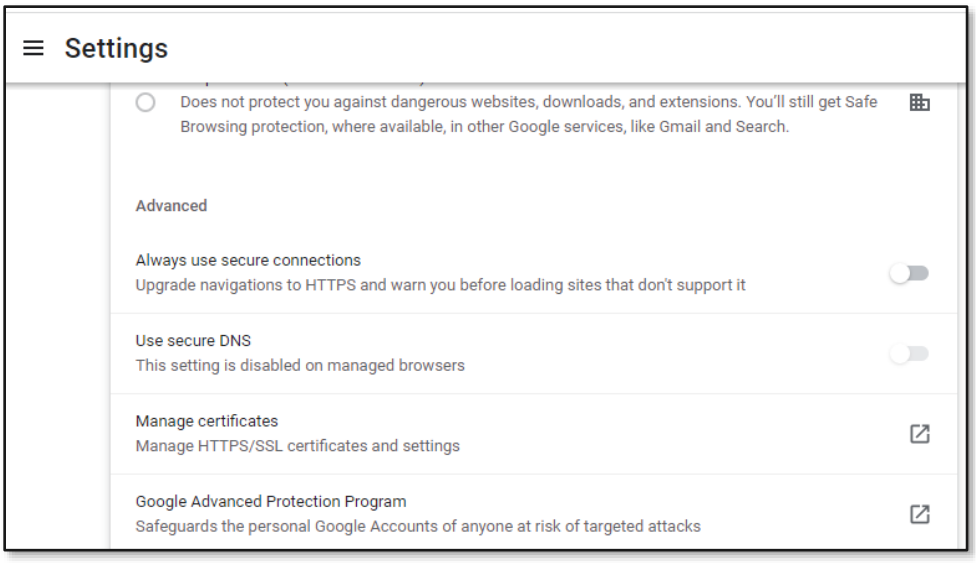

Figure 3: Manage Certificates in Chrome Browser

4. The **Certificates** window opens, displaying a list of imported certs (Figure 4).

Determining the Expiration Date using a Browser

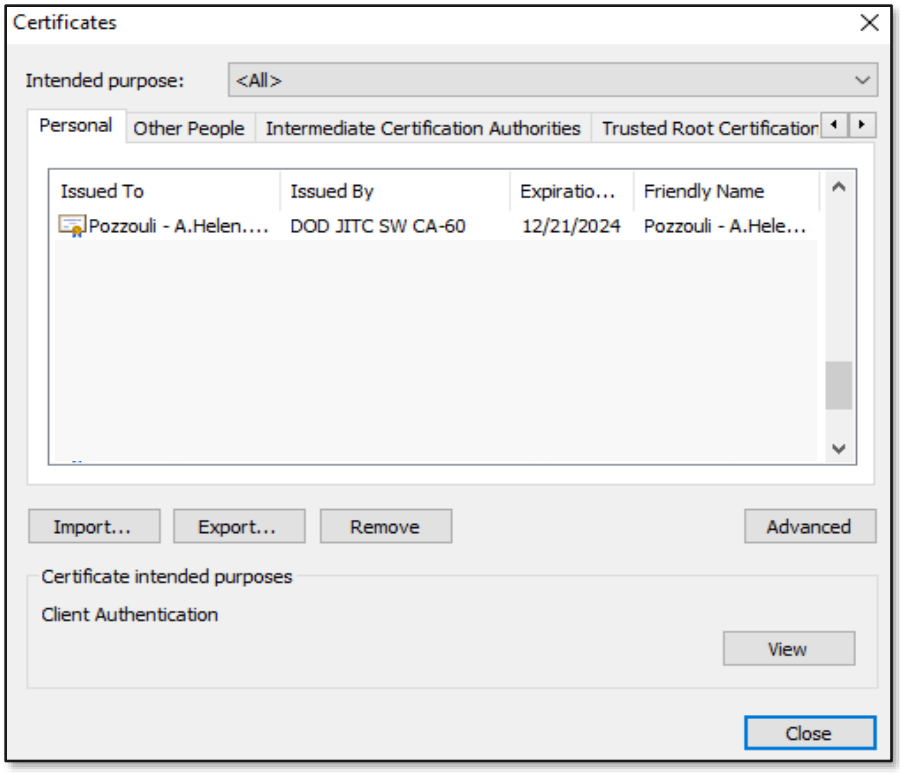

Figure 4: Certificates Widow

5. Once you verify the expiration date, select **Close** to exit.

Importing a Certificate into a Browser

Here are the steps to follow when you need to import a certificate into a browser:

1. Starting on the **Certificate Manager** screen, try to locate your certificate in the window, but if no certificate appears then either it is expired (browser wont display expired certs) or it was not imported from email or your stored location to the browser. **Note**: Follow IT guidance regarding PKI certificate retention.
2. From your email, locate the certificate you need to import into the browser (Figure 5).

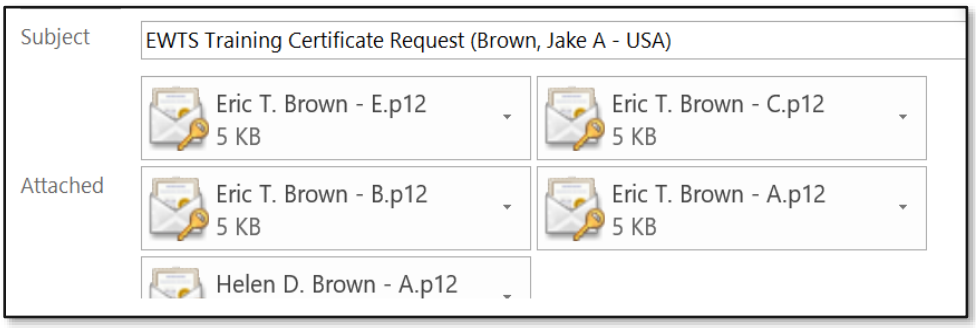

Figure 5: PKI Certificates

Importing a Certificate into a Browser *(continued)*

3. Double-click one certificate (.p12 file). An information message appears (Figure 6).

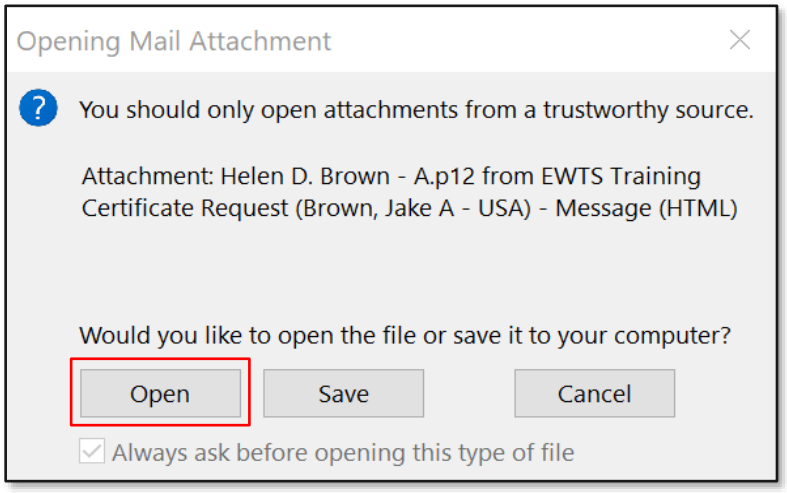

Figure 6: Opening Mail Attachments Screen

4. Select **Open** (Figure 6). The **Certificate Import Wizard** appears (Figure 7). The **Store Location** default is **Current User**. No need to change the setting.

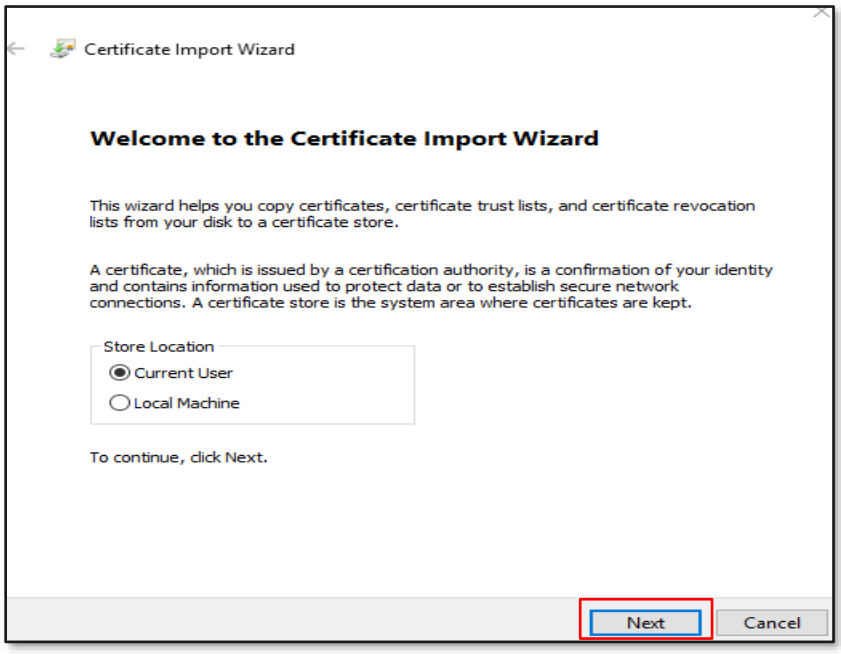

Figure 7: Welcome to the Certificate Import Wizard Window

5. Select **Next**, the **File to Import** screen opens (Figure 8). Do not change information in the **File Name** text box.

Importing a Certificate into a Browser *(continued)*

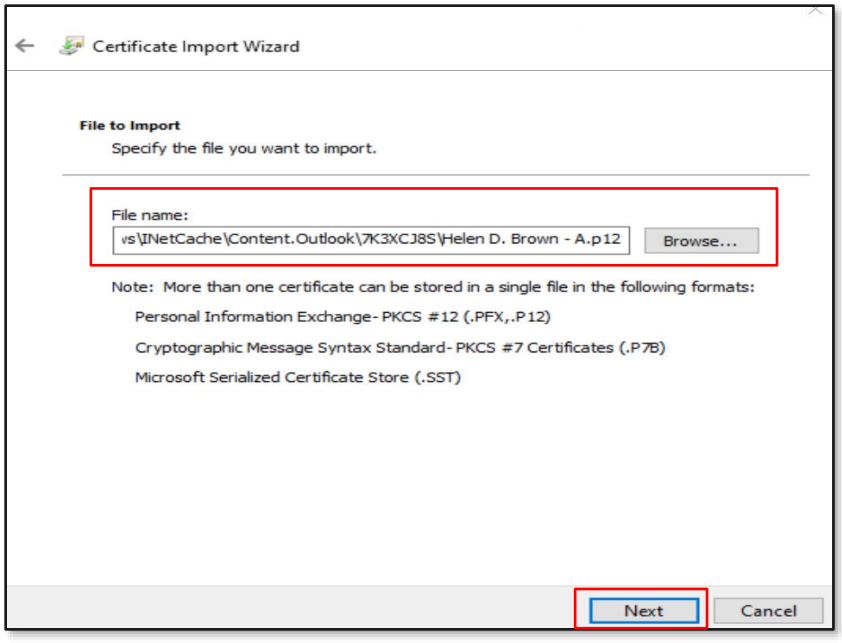

Figure 8: File to Import Screen

6. Select **Next**, the **Private key** protection screen opens (Figure 9). Type the password into the text box. **Note**: The password is case sensitive. The box **Include all extended properties** is checked. You should leave the other boxes unchecked.

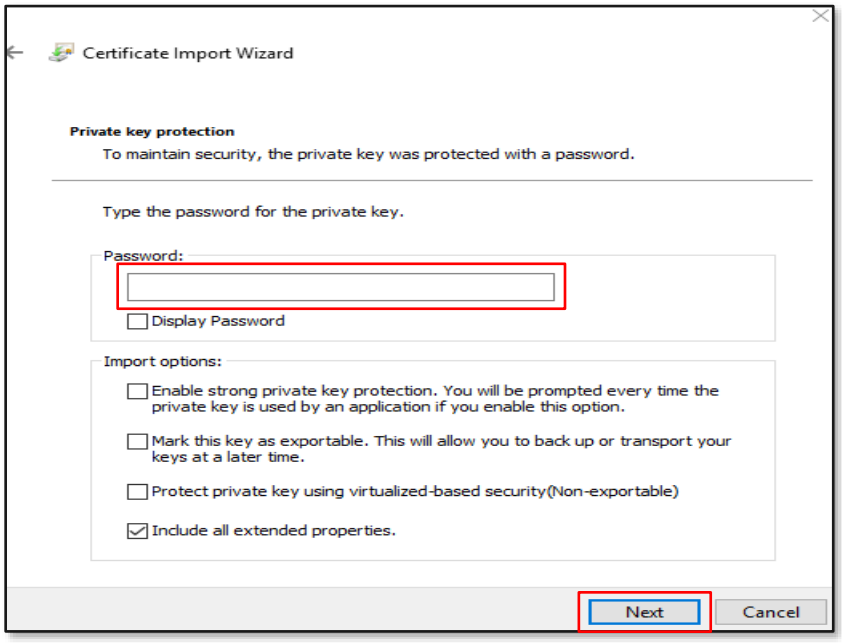

Figure 9: Private Key Protection Screen

Importing a Certificate into a Browser *(continued)*

7. Select **Next**, the **Certificate Store** screen opens (Figure 10). **Note**: The default is the first radio button and windows automatically selects a certificate store. *This paper only addresses the default option.

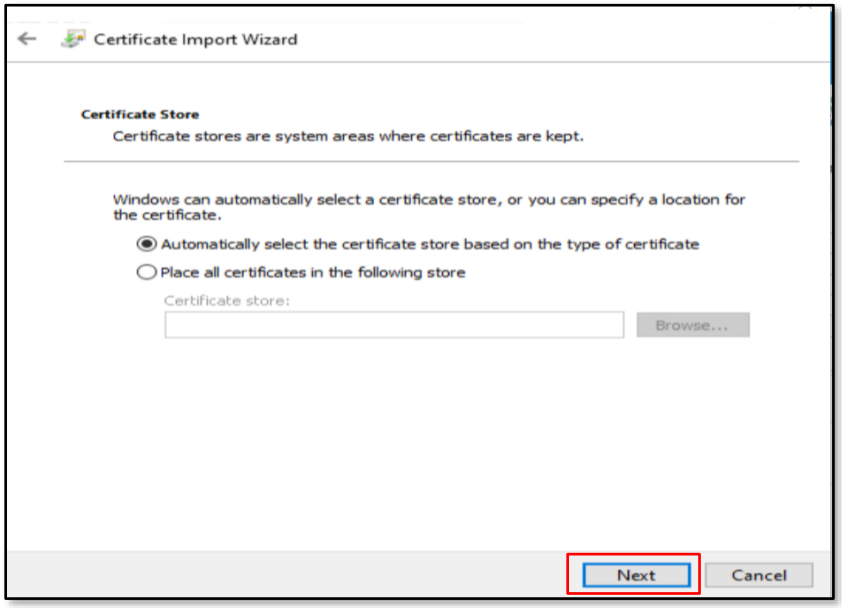

Figure 10: Certificate Store Screen

8. Select **Next**. The **Completing the Certificate Import Wizard** screen opens (Figure 11).

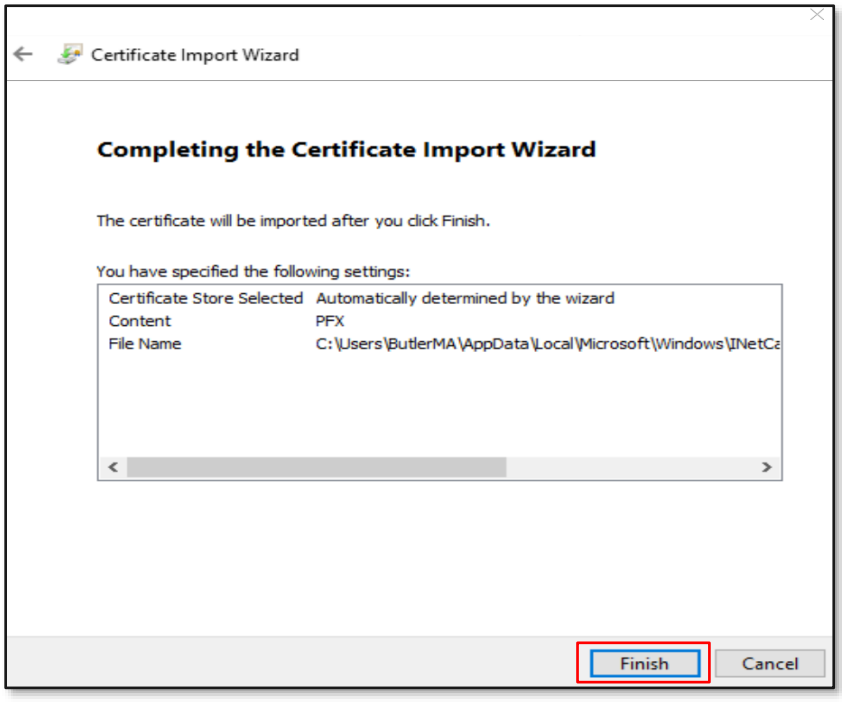

Figure 11: Completing the Certificate Import Wizard Screen

Importing a Certificate into a Browser *(continued)*

9. Select **Finish** (Figure 11). **The import was successful** message should appear (Figure 12).

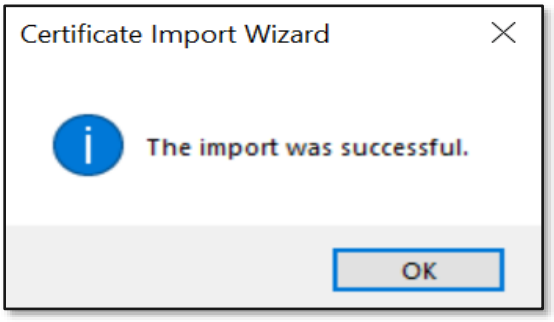

Figure 12: Success Message

10. Select **OK** to close the message.