Importing a Certificate onto an eToken

The following certificate types are supported:

- .pfx
- .p12
- .cer

If a PFX file is selected, the private key and corresponding certificate will be imported to the eToken. You will be asked if CA certificates should be imported to the eToken, and you will be asked to enter the password (if it exists) protecting the PFX file.

When downloading a certificate to the computer and then importing the certificate to the eToken, remove the certificate from the local store and reinsert the eToken before using the certificate to sign and encrypt mail. This ensures you are using the certificate and keys stored on the eToken.

To import a certificate:

1. To open eToken PKI Client Properties do one of the following:
    - Right-click or double-click the eToken tray icon and select Open eToken Properties from the menu.
    - From desktop select Start > Programs > eToken > eToken Properties.

The eToken PKI Client Properties window opens.

2. Click the Advanced View icon 

The Advanced View window opens.

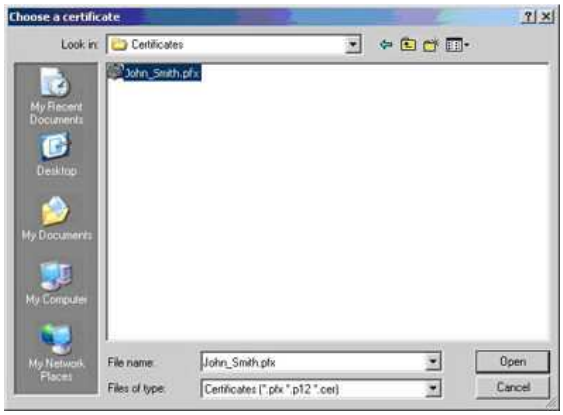
3. Do one of the following:
    1. On the left side of the Advanced View window, select the required eToken and click the Import Certificate icon 

    2. On the left side of the Advanced View window, right click the required eToken Right-click and select Import Certificate from the shortcut menu

The Import Certificate window opens.

1. Select Import a certificate from a file

If you select Import a certificate from a file, the Choose a certificate window opens.

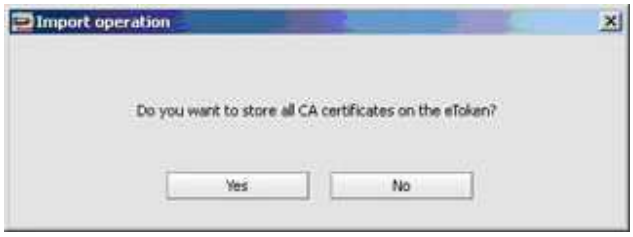


6. Select the certificate to import and click Open.

If the certificate requires a password, the Password window opens.

7. Enter the certificate password.

The Import Operation window opens asking if you want to store the CA certificates on the eToken.



8. Select Yes or No.

All requested certificates are imported, and a confirmation message opens.

Source: Alladin eToken PKI Client User guide.