Since Business Intelligence Extraction Service (BiXtractor) version 3.2, the BiXtractor has used certificates and requires you to have a valid DoD issued certificate installed on your machine. This document will provide you basic guidance on requesting a certificate and installing it onto your system.

The process of requesting and installing a certificate is summarized below:

1. Generate a Certificate Signing Request (CSR) from the system that needs the certificate.
    a. This requires you to know the Common Name (CN) and Subject Alternative Name (SAN) to be used in the certificate. The CN is the Fully Qualified Domain Name (FQDN) of the system. If the system is behind a proxy, the FQDN could be different from the public address of the system. In this case, the public address would be used.
    b. Your systems Common Name (CN) must be registered in the Defense Information Technology Portfolio Repository (DITPR).
2. Submit the request to a DoD Certification Authority (CA) and Registration Authority (RA) for processing and approval.
3. RA notifies requestor of approval.
4. Requestor retrieves their certificate from the CA website.
5. Requestor installs the certificate onto their system.

A certificate request and installation, can be performed by using the following tools:

- Windows **Certificates** MMC snap-in
- Certificate Authority website

Generate the Certificate Request

Log on to the server where the certificate is being installed.

Copy the saved certificate files to the server where the certificate is being installed.

Open an elevated Command Prompt, run as Administrator.

Open MMC and add the Certificates snap-in to manage certificates for the Computer account of the Local computer.

Expand the Certificates tree and right-click the Personal store.

Select Actions All Tasks > Request New Certificate. The Certificate Enrollment Wizard will open.

Submit the Certificate Request

Depending on your site's environment and procedures, the certificate request will either be sent to a local Trusted Agent for submission to a DoD Certification Authority (CA) for processing and approval, or the administrator will submit the request themselves. If submitting the request directly to a CA, refer to the CA website for instructions.

Retrieval of the Completed Certificate

After your certificate request has been approved, retrieve your certificate along with the CA certificate chain from the issuing CA.

Importing the Certificate

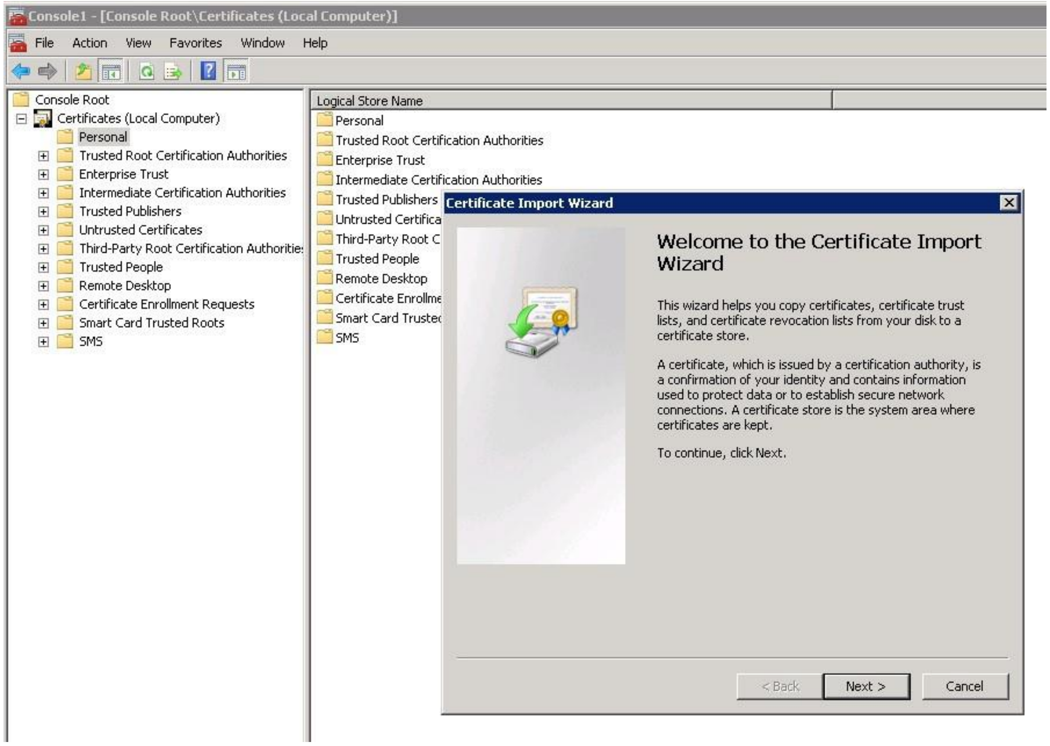
Log on to the server where the certificate is being installed.

Copy the saved certificate files to the server where the certificate is being installed. Open an elevated Command Prompt, run as Administrator.

Open MMC and add the **Certificates** snap-in to manage certificates for the Computer account of the Local computer.

Expand the **Certificates** tree and right-click the **Personal** store.

Select Actions **All Tasks** > **Import**. The **Certificate Import Wizard** will open.



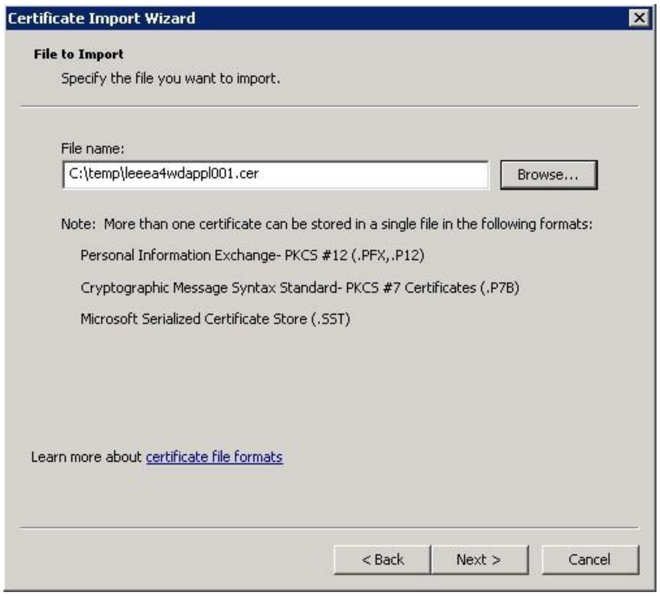
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Click **Next**. Browse to the saved certificate *.cer* file and select it. Click **Next**.


Certificate Import Wizard
Browse...
Learn more about certificate file formats
< Back
Next >
Cancel

File to Import

Specify the file you want to import.

File name: C:\temp\leeea4wdappl001.cer

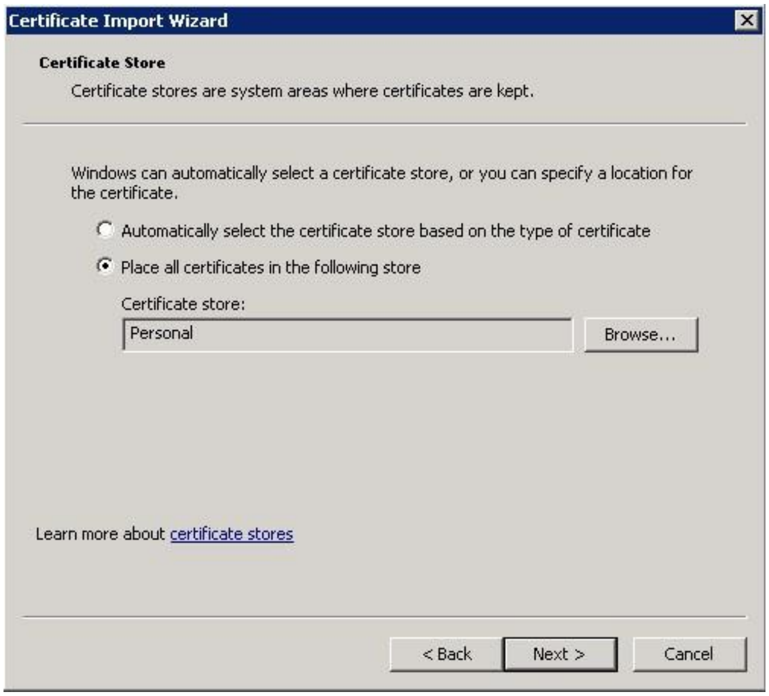
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

The wizard should have pre-selected **Place all certificates in the following store, Certificate store: Personal**


Certificate Import Wizard
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

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: Personal

Click **Next** and then Click **Finish**.

The import was successful should appear. Click **OK**.

A **Certificates** node should now be present under the **Personal** store in the **Certificates** snap-in. Browse to the **Certificates** node.

The server’s certificate should be present.

Importing the CA Certificate Chain

The CA Certificate Chain certificates may already be installed on your system. To check, select the **Trusted Root Certificate Authorities** node and then select the **Certificates** node. Look for the certificate for the CA that your request was submitted to. For example **DOD CA-27**.

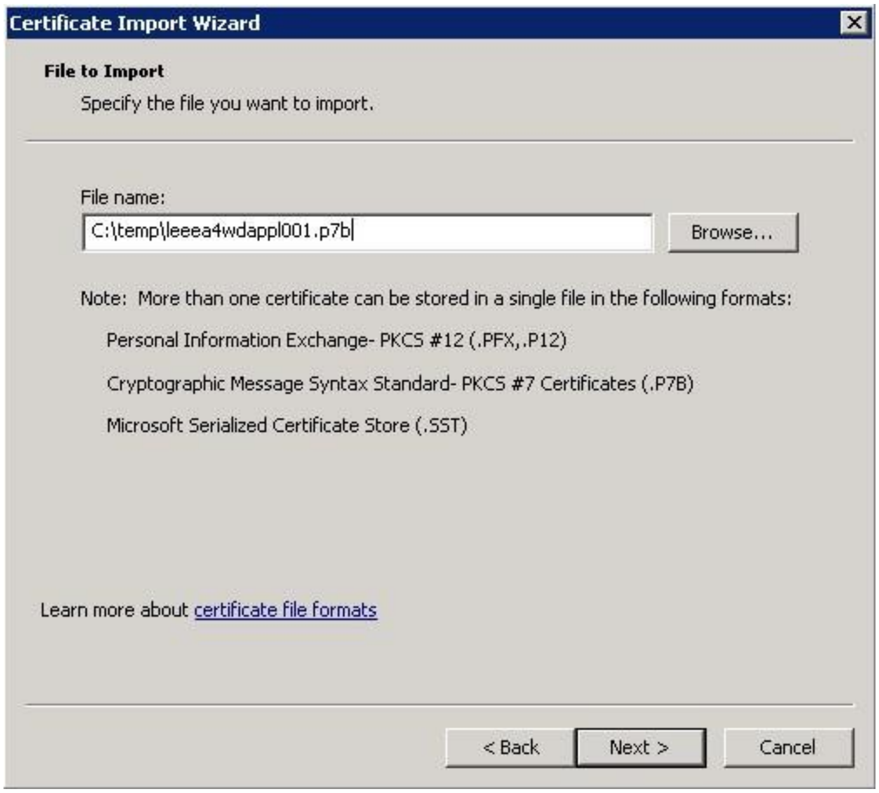
If the certificate does not exist, then import the CA Certificate Chain by right-clicking the **Certificates** node and select Actions **All Tasks > Import…**

The **Certificate Import Wizard** will open again.

Click **Next**.

Browse to the saved *.p7b* file and select it. The file type filter in the file open browser must be set to **PKCS #7 Certificates** or **All Files** before the *.p7b* file can be selected.

Click **Next**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:
C:\temp\leeea4wdappl001.p7b

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

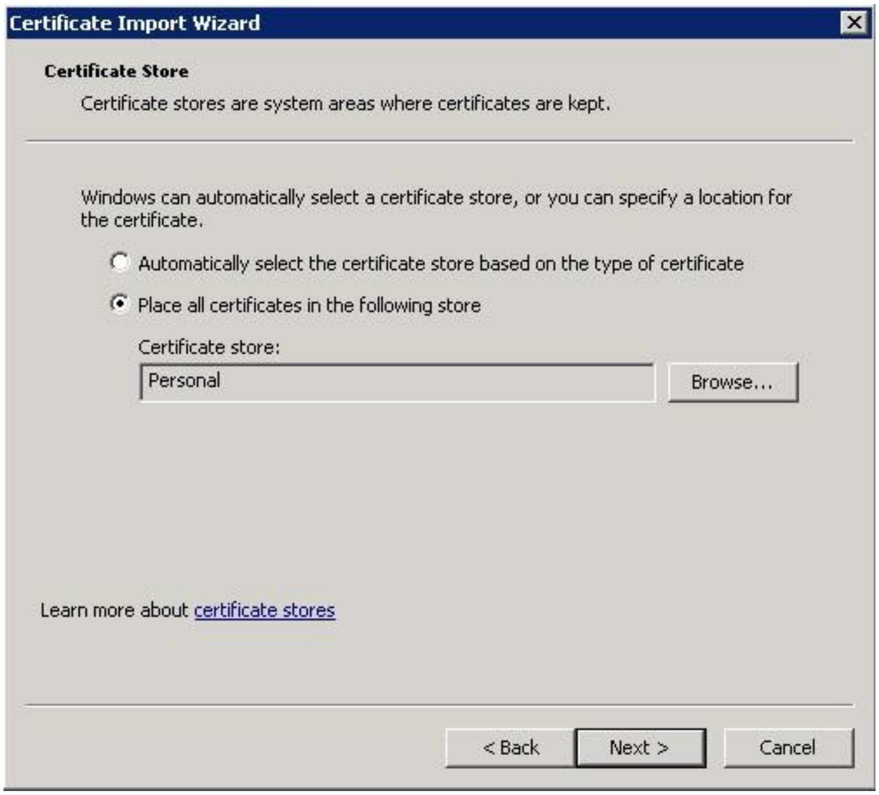
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

The wizard should have pre-selected **Place all certificates in the following store, Certificate store: Personal**

Click **Next**.



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: Personal

Learn more about certificate stores

Click **Finish**.

The import was successful window should appear.

Click **OK**.

The certificates for the issuing CA and the DoD Root CA 2 should now have been added to the **Certificates** store under the **Trusted Root Certificate Authorities** store of the **Certificates** snap-in.

Helpful DoD links:

Guidance to “Obtain and Install a Certificate for the System or Application” can be found at

http://iase.disa.mil/pki-pke/getting_started/Pages/administrators.aspx

https://ee-id-sw-ca-38.csd.disa.mil/ca/ee/ca/

https://ca-28.csd.disa.mil/ca/

http://iase.disa.mil/pki-pke

https://powhatan.iiie.disa.mil/pki-pke/landing_pages/downloads/unclass-fouo-rg_obtaining_pkicert_dodserver.pdf

Helpful Navy links:

https://infosec.navy.mil/PKI/server_cert_request_process01_11.pdf

https://infosec.navy.mil/PKI/lra.jsp