



## Over the Counter Channel Application (OTCnet)

### Development Treasury Root Certificate Installation

There are three primary tasks required in order to install the development Treasury root certificate onto a workstation:

1. Obtain the root certificate container files from the Treasury website. Two container files must be obtained, one for production and one for QA (i.e. Treasury Development).
2. Export the Treasury root certificates from the certificate container files.
3. Import the Treasury root certificates into the local computer certificate/trust store.

This document details the steps involved with each of these tasks and assumes that the tasks will be performed while logged into the workstation as a workstation administrator. This document is applicable for a Windows Vista or Windows 7 workstation. Please refer to the "RootCertificateInstall-XP.docx" document for performing the tasks on a Windows XP workstation.

Note that the two root certificate container files obtained from the Treasury website both contain multiple certificates, but OTCnet only requires the root certificates to be imported. Since task 3 (certificate import) only allows the import of *all* certificates from a container file, task 2 (certificate export) is necessary in order to create container files containing only the required certificates.

## Task 1: Obtain the root certificate container files from the Treasury website

First, download the Treasury **production** root certificate container file onto the workstation from the following URL:

[https://pki.treas.gov/root\\_sia.p7b](https://pki.treas.gov/root_sia.p7b)

Click “yes” if prompted with a security alert. If a browser instance launches and displays a certificate error page, click “Continue to this website...”. Note that the security alert prompt and certificate error page is normal. These merely indicate that you have not yet installed the Production Treasury Root Certificates into your Trusted Root Certificate store. Note that as of December 2010, this URL points to a file that contains the SHA-1 keyed Production Treasury Root Certificates. The URL and/or certificates contained within are subject to change.

Next, download the Treasury **development** root certificate container file onto the workstation from the following URL:

[http://devpki.treas.gov/devroot\\_sia.p7b](http://devpki.treas.gov/devroot_sia.p7b)

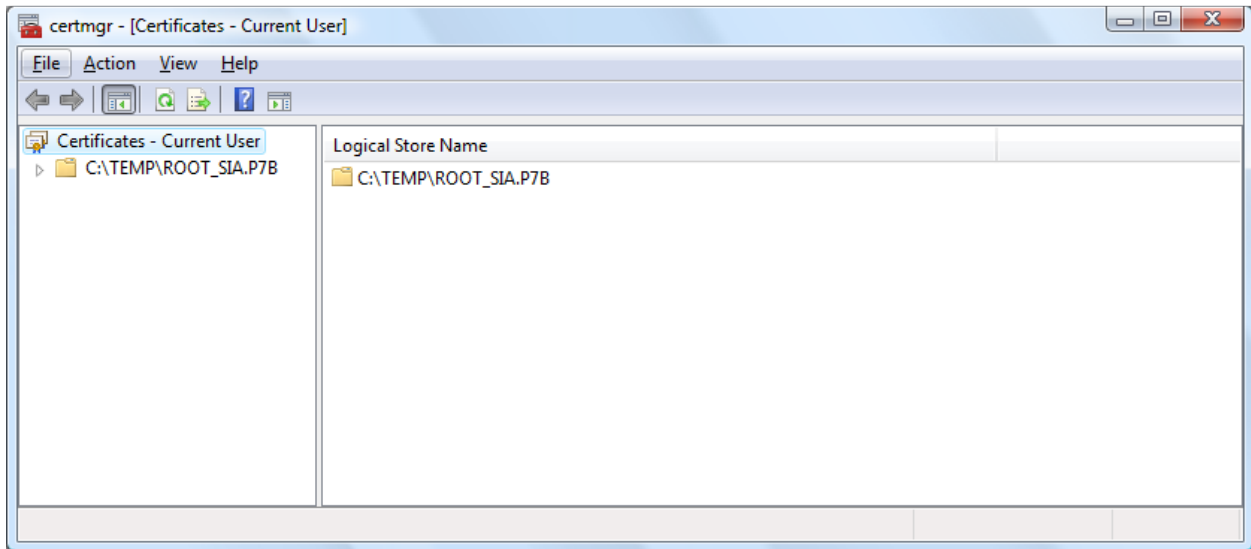
Note that as of December 2010, this URL points to a file that contains the SHA-1 keyed Development Treasury Root Certificate. The URL and/or certificates contained within are subject to change.

## Task 2: Export the Treasury root certificate from the certificate container file

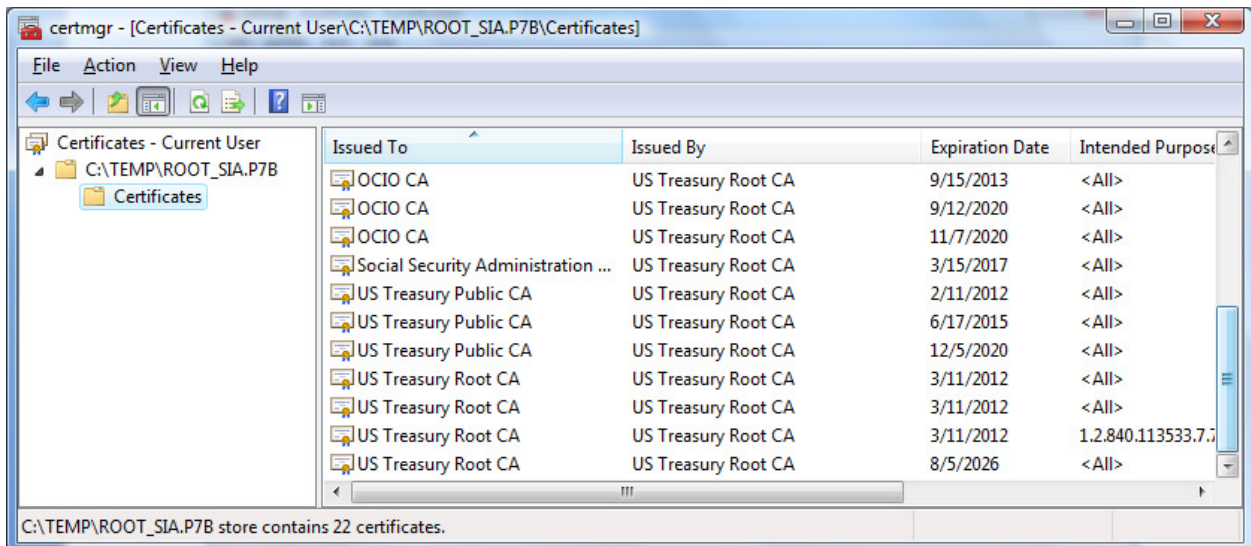
### Export the Production Treasury Root Certificates

Double-click on the downloaded production certificate container file, **root\_sia.p7b**.

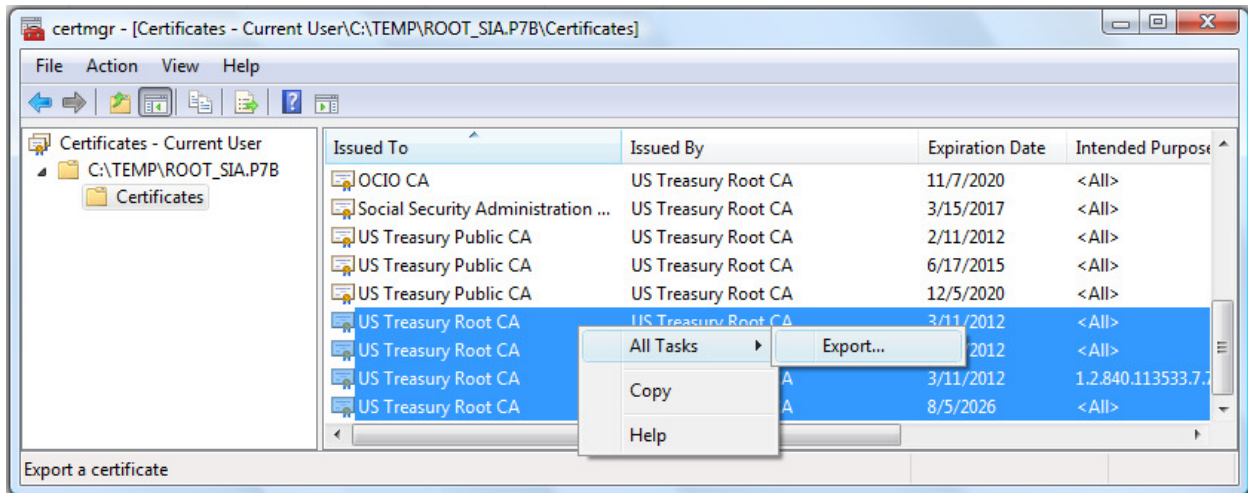
Click the **“Continue”** button if prompted with a User Account Control message indicating that **“Windows needs your permission to continue”**. The following screen appears.



Navigate to **“Certificates”**



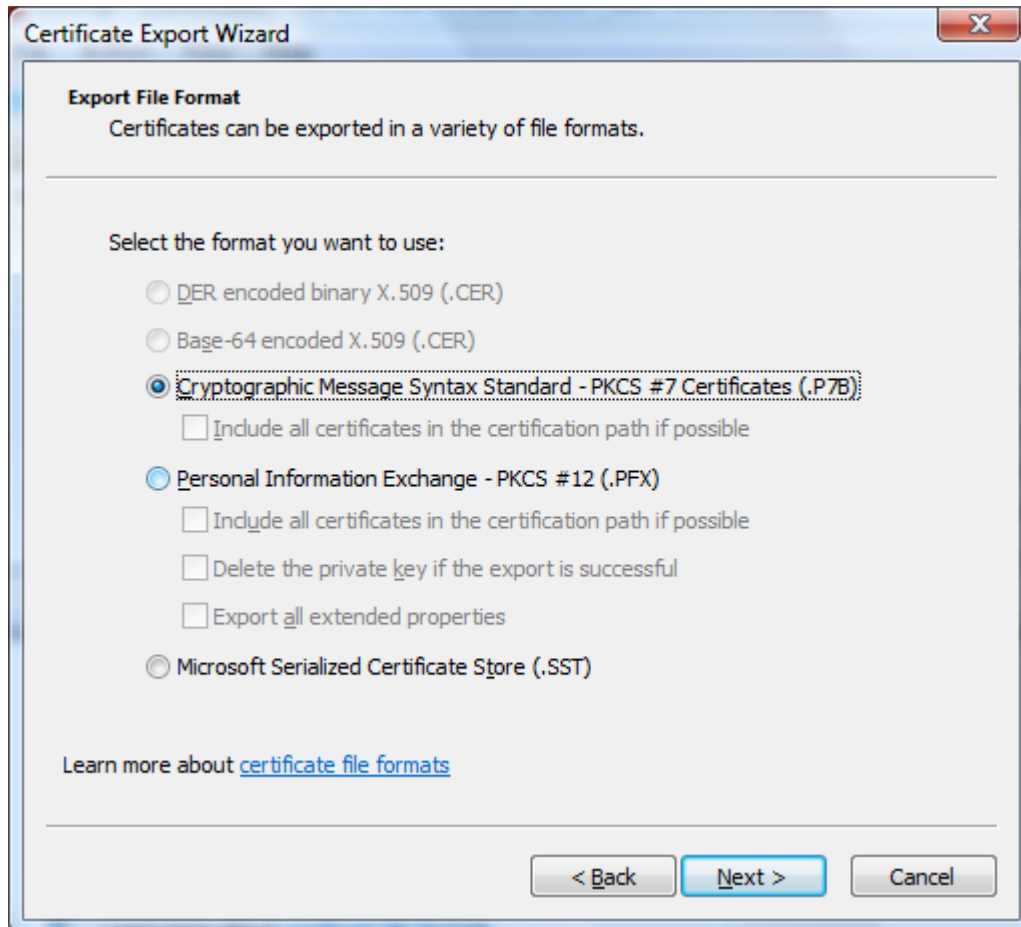
Scroll to the bottom of the list of certificates in the right pane, hold down the Ctrl key and select all four of the “US Treasury Root CA” items. Right-mouse click on the selected items and click “All Tasks -> Export...”



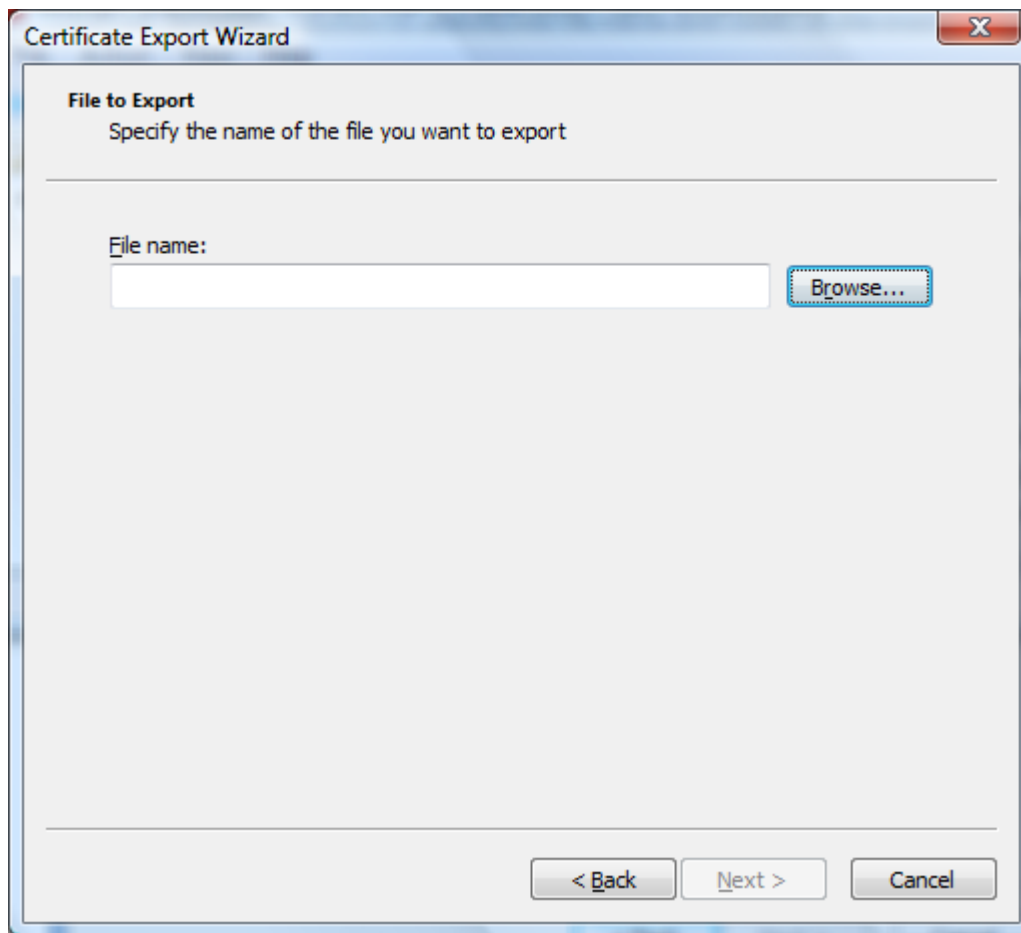
The Certificate Export Wizard displays. Click the “Next” button



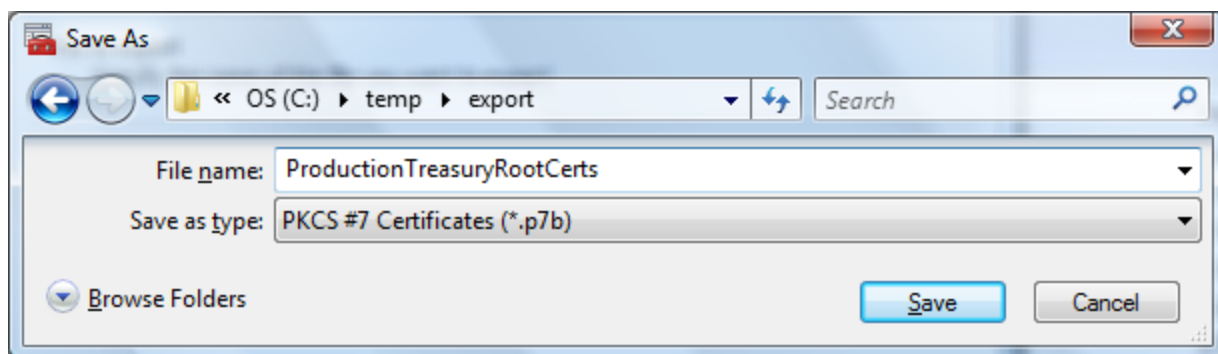
Select “**Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**” and click the “**Next**” button



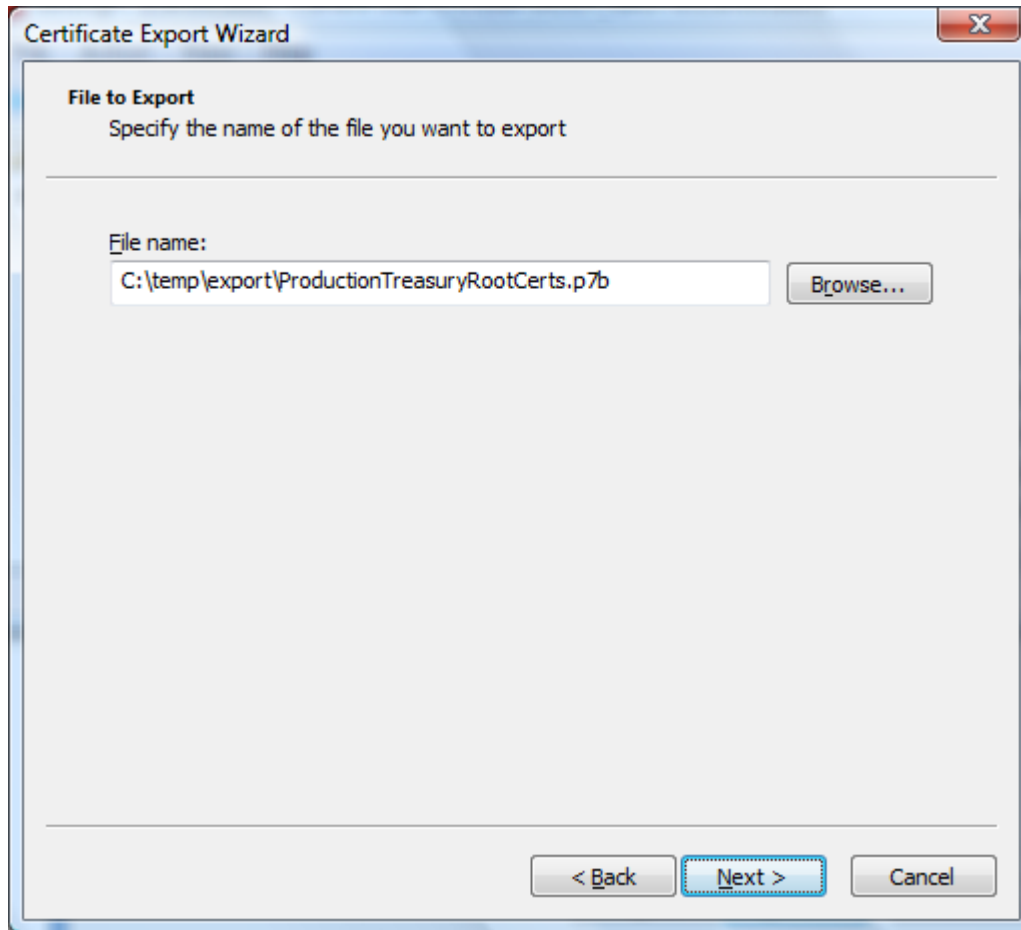
Click the “**Browse...**” button to specify the file name and folder of the export file



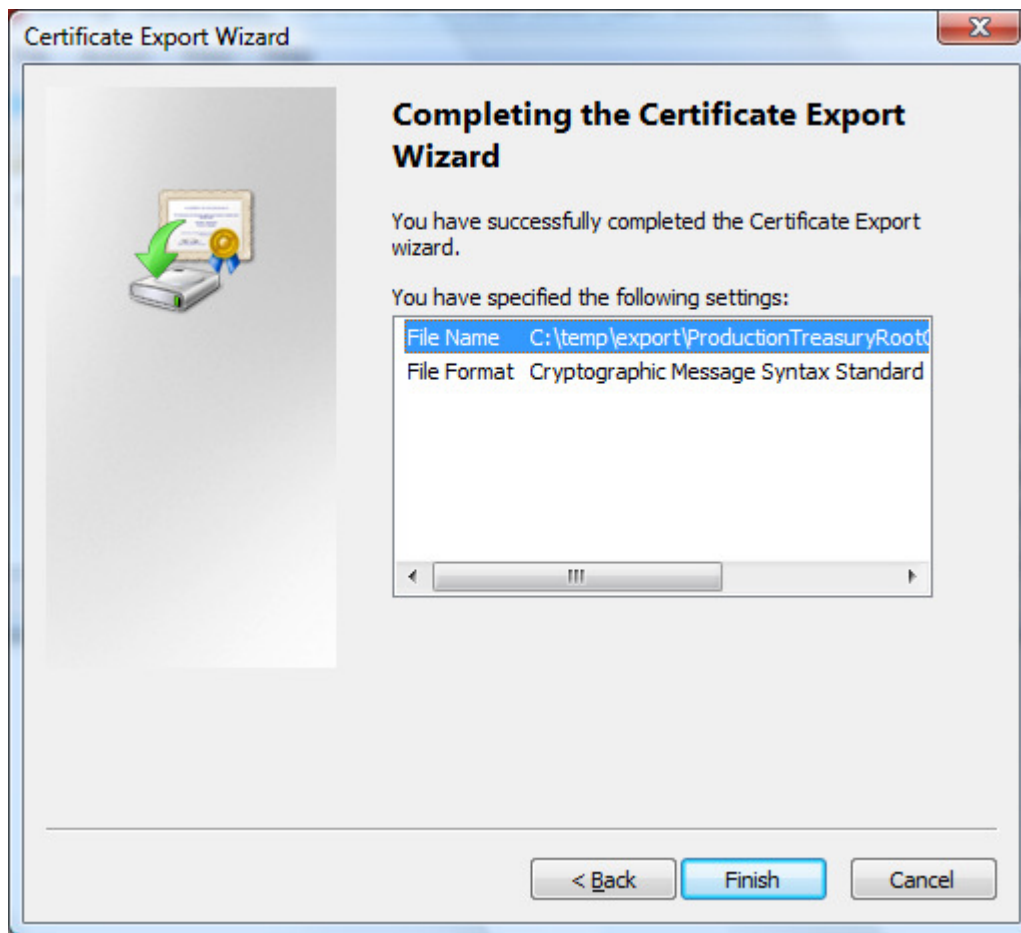
Type in file name and click the “**Save**” button



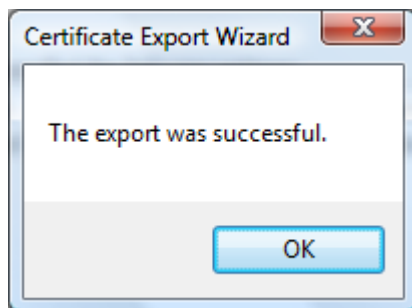
Confirm file name and click the “**Next**” button



Click the **“Finish”** button



You will see the following message if the export was successful.



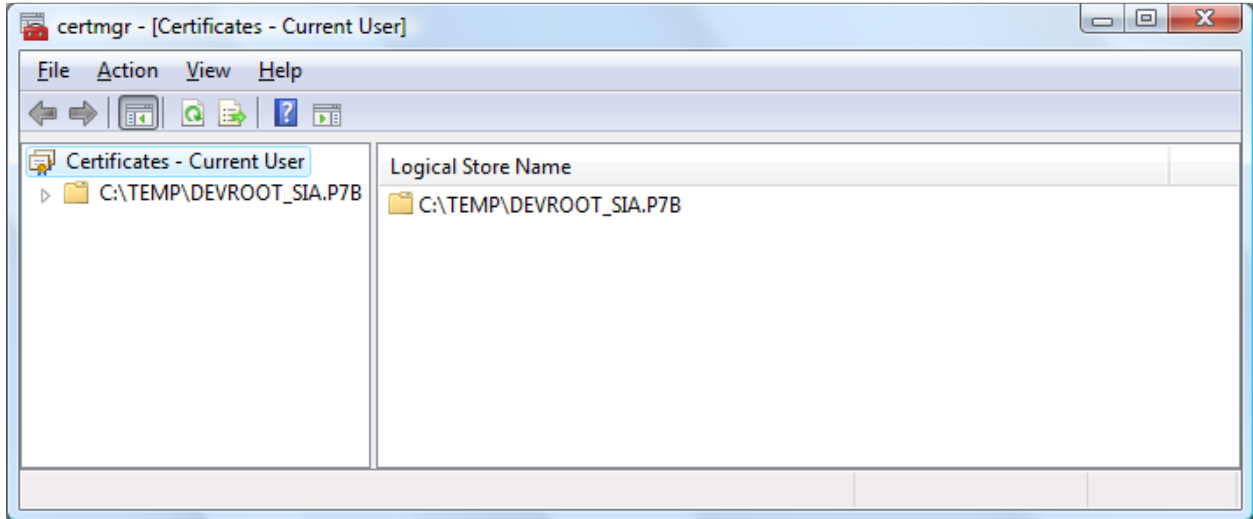
Close the **“certmgr”** application.



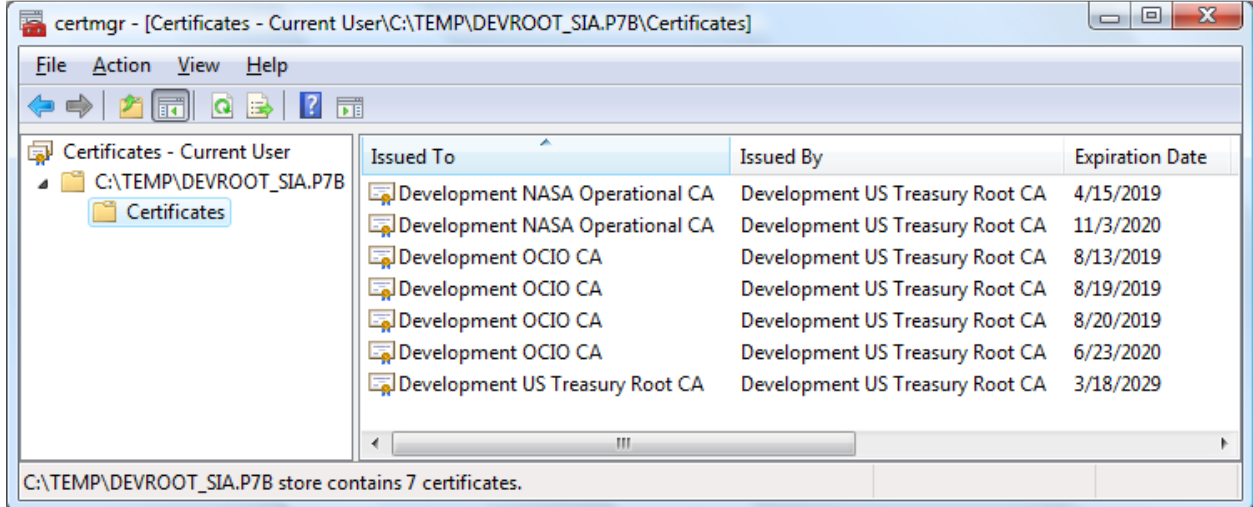
## Export the Development Treasury Root Certificate

Double-click on the downloaded development certificate container file, **devroot\_sia.p7b**.

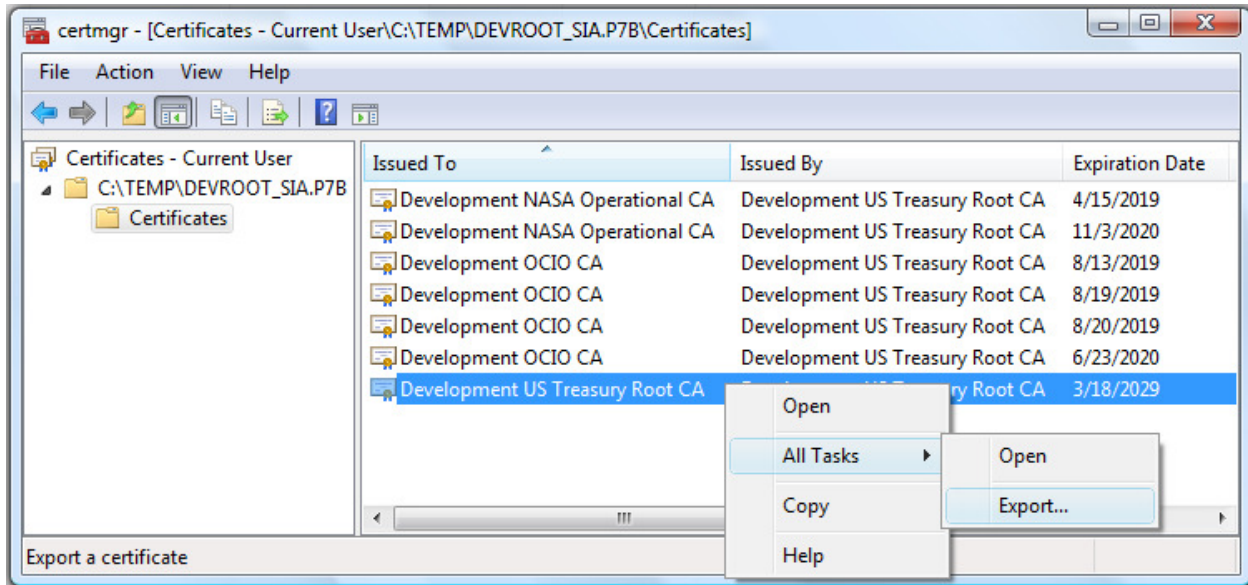
Click the “**Continue**” button if prompted with a User Account Control message indicating that “**Windows needs your permission to continue**”. The following screen appears.



Navigate to “**Certificates**”



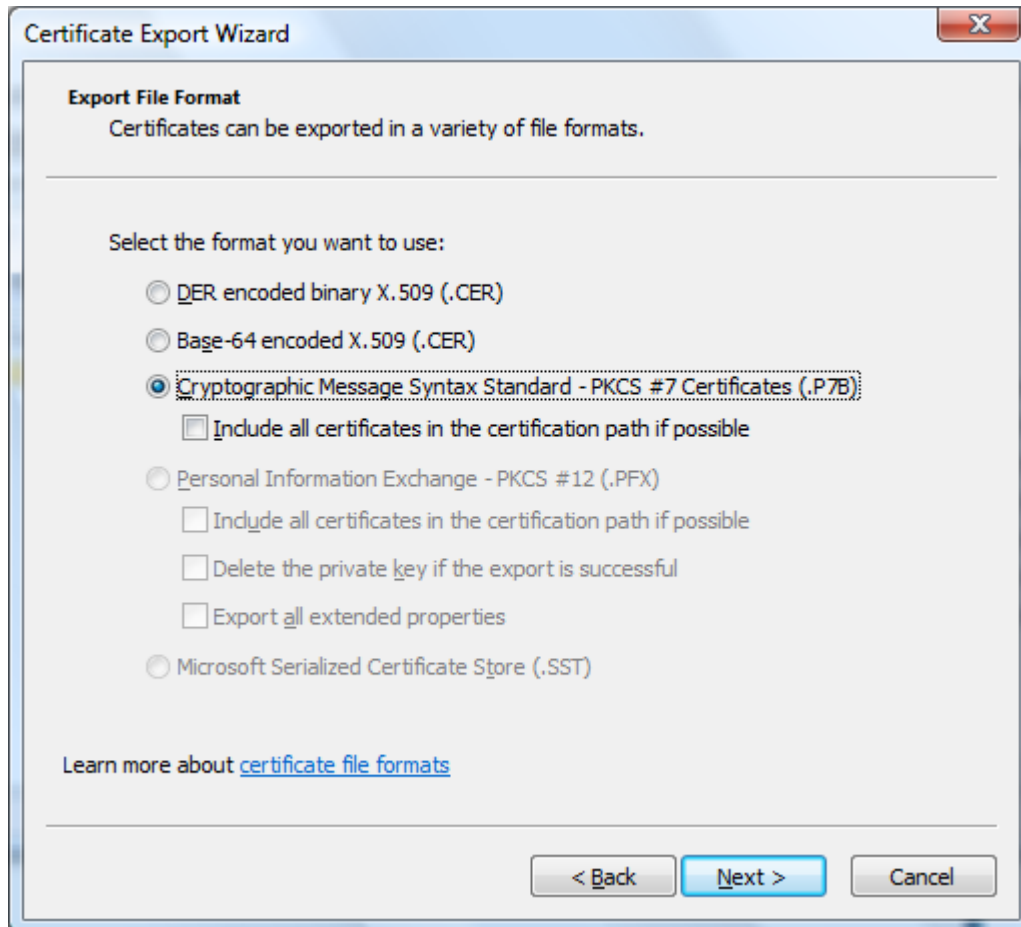
Select “**Development US Treasury Root CA**”, right-mouse click, select “**All Tasks -> Export...**”



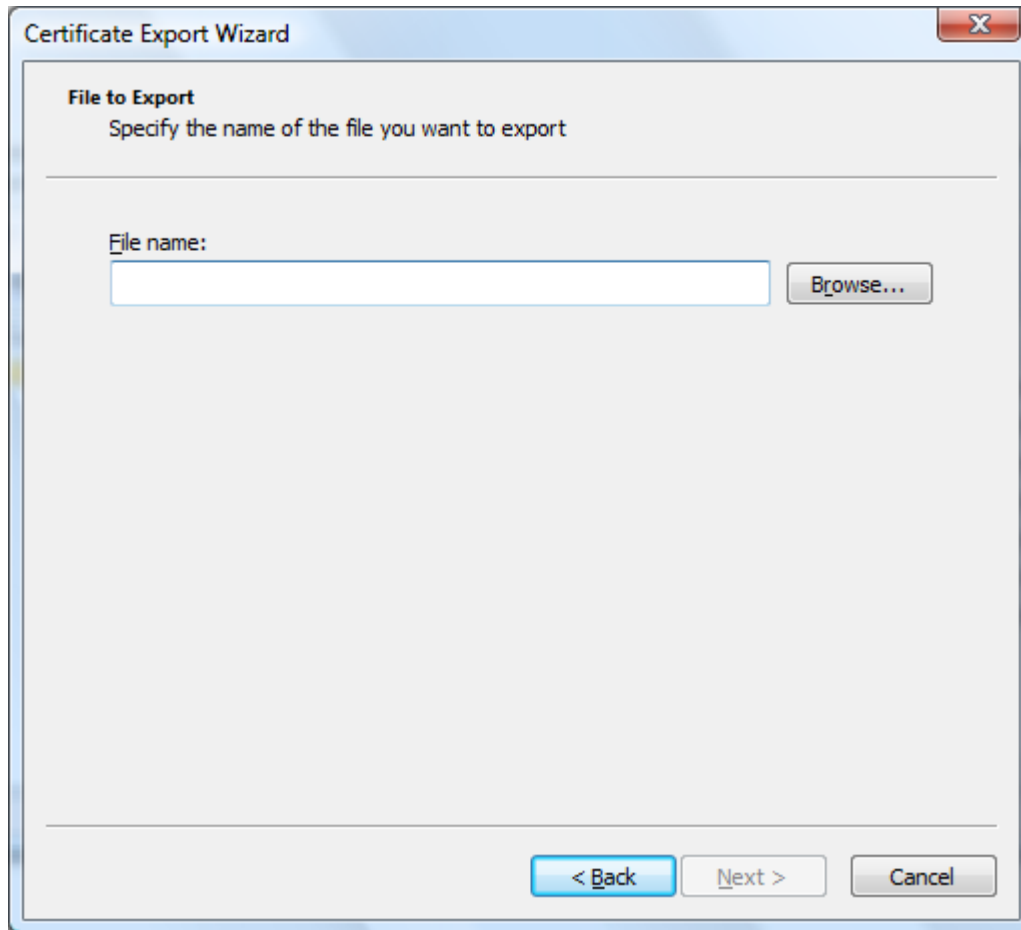
The Certificate Export Wizard displays. Click the “**Next**” button



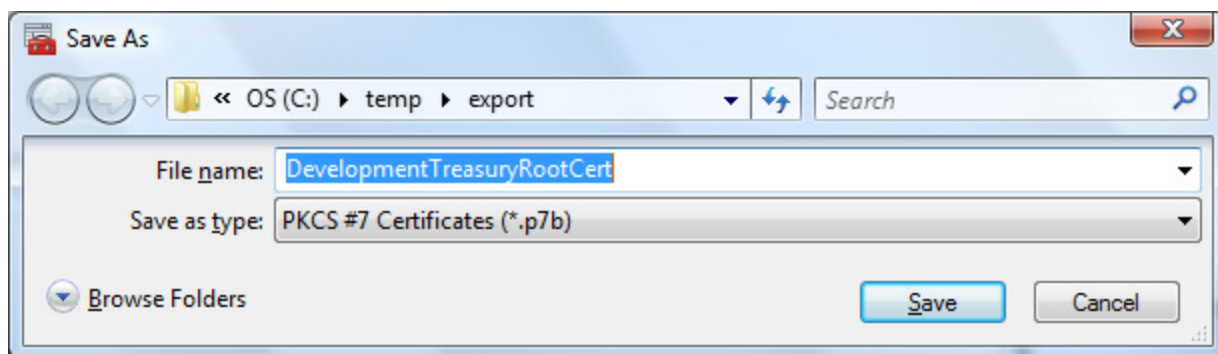
Select “**Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**” and click the “**Next**” button



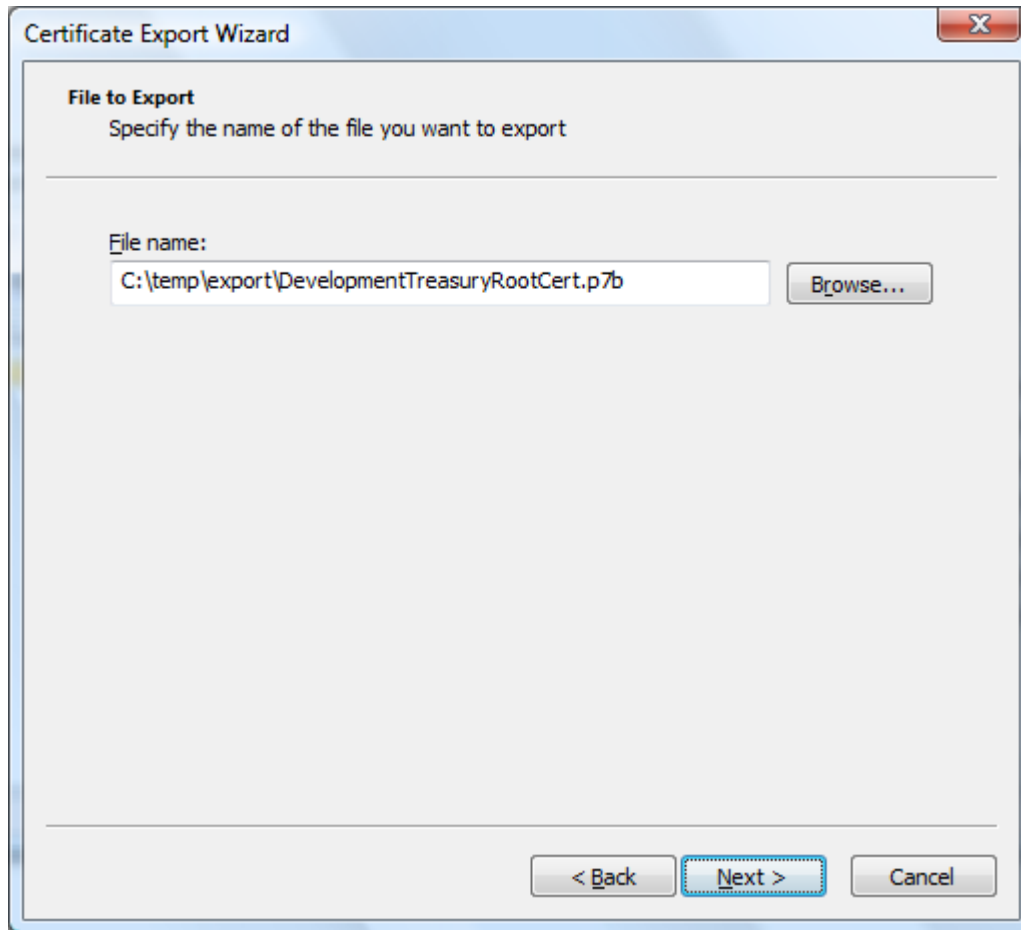
Click the “**Browse...**” button to specify the file name and folder of the export file



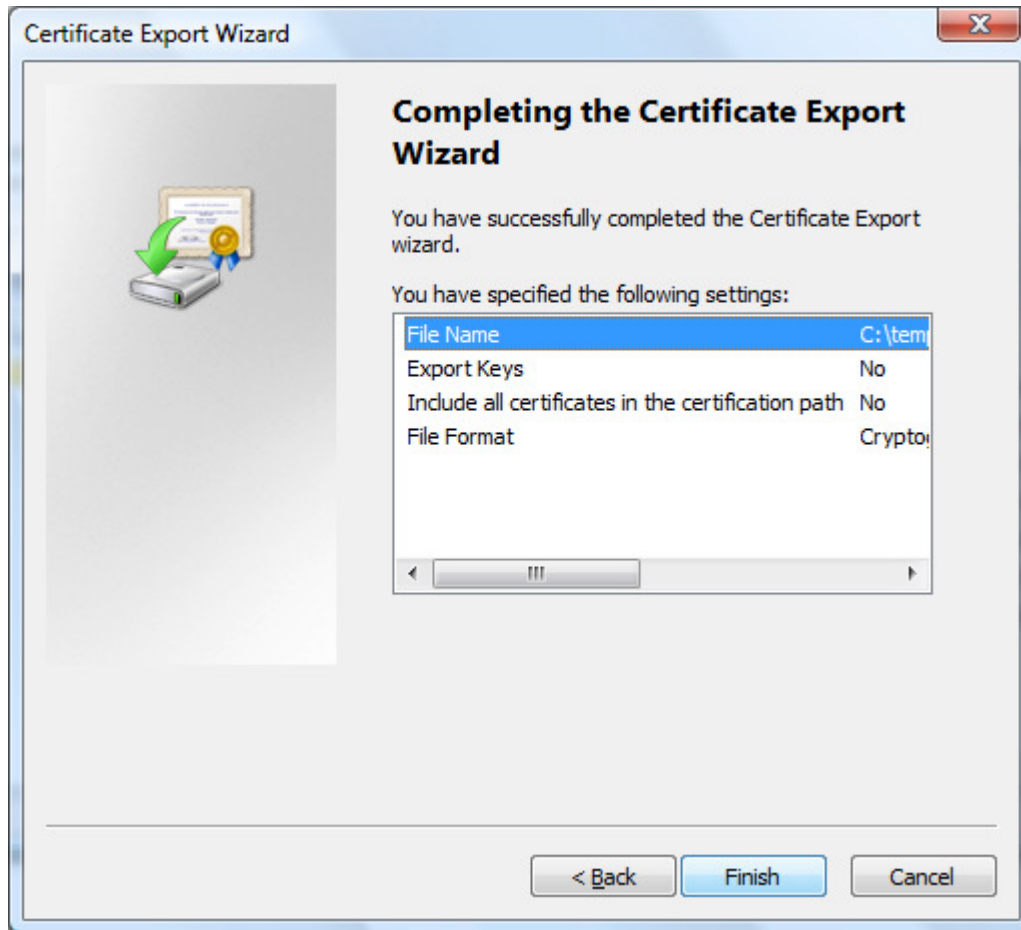
Type in file name and click the “**Save**” button



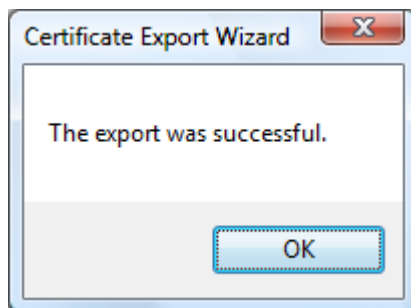
Confirm file name and click the “**Next**” button



Click the “**Finish**” button



You will see the following message if the export was successful.

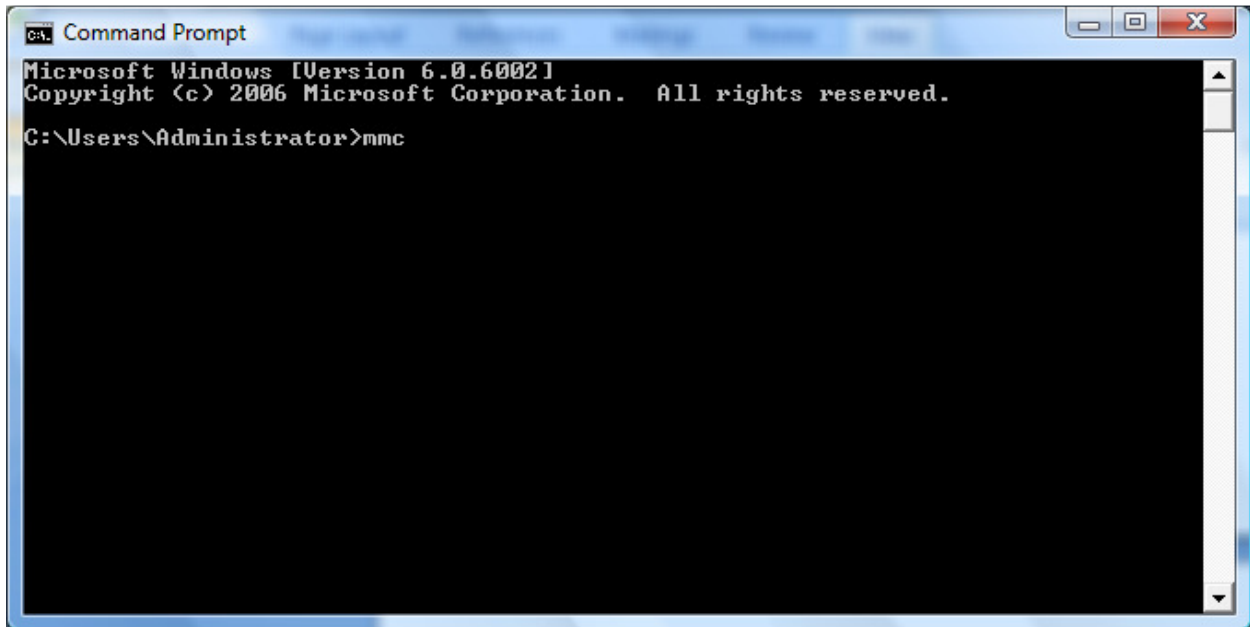


Close the “**certmgr**” application.

### Task 3: Import the Treasury root certificate into the local computer trust store

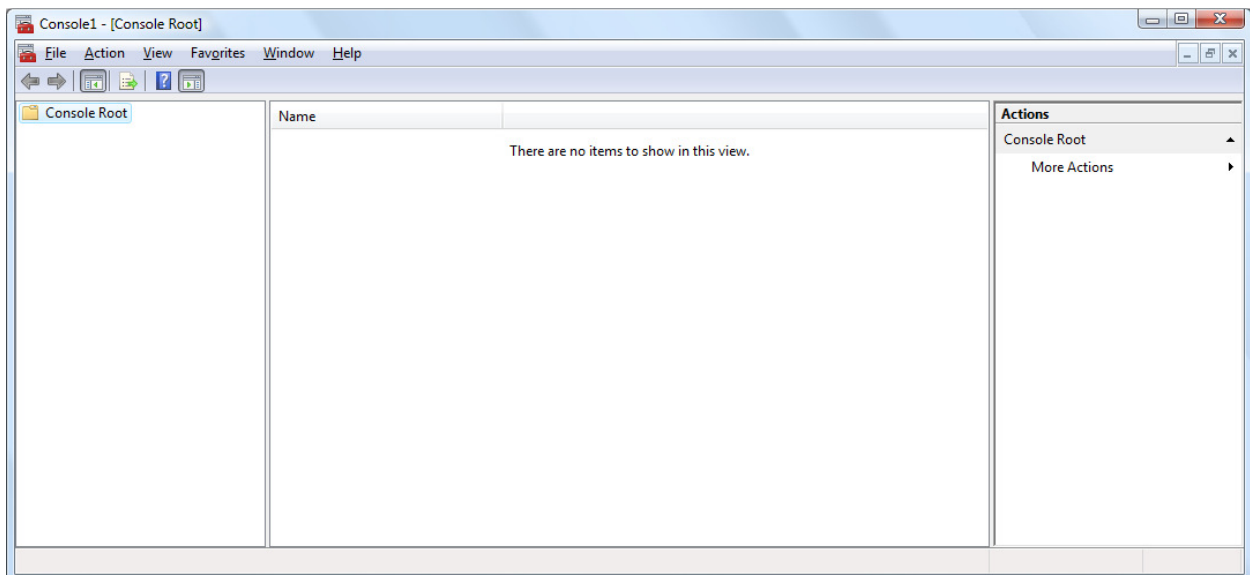
#### Import the Production Treasury Root Certificates

Open Command Prompt window, type “mmc” and hit “Enter” on keyboard

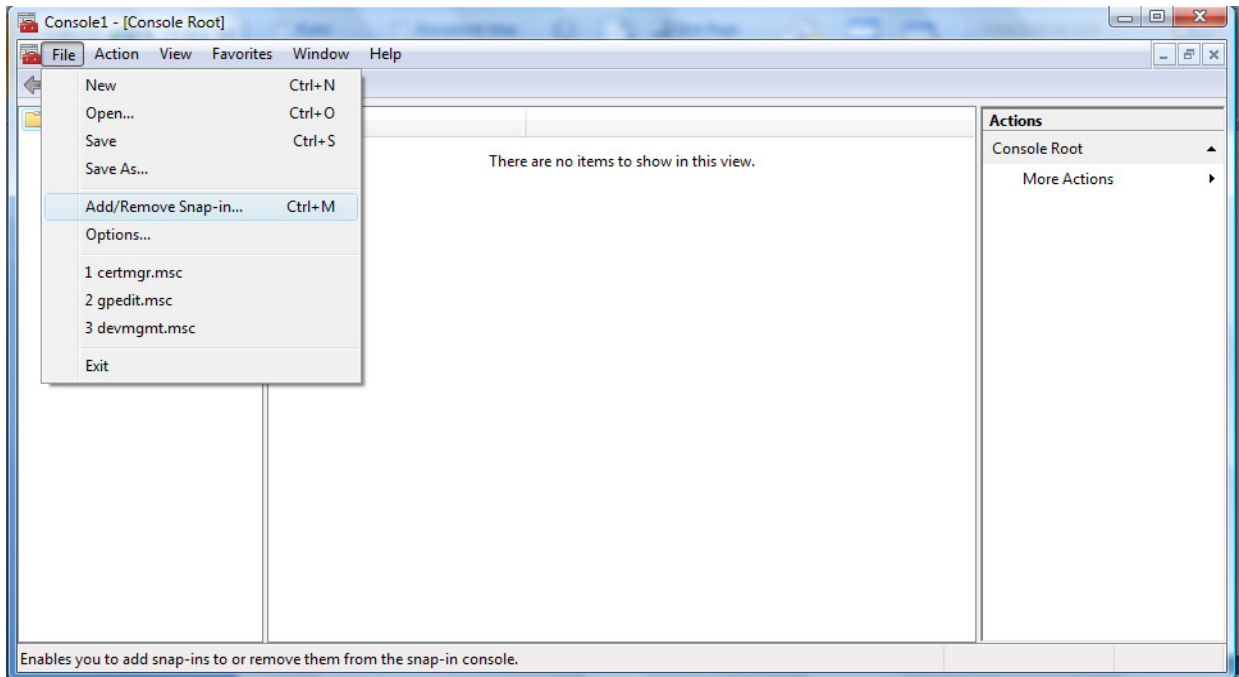


Click the “Continue” button if prompted with a User Account Control message indicating that “Windows needs your permission to continue”

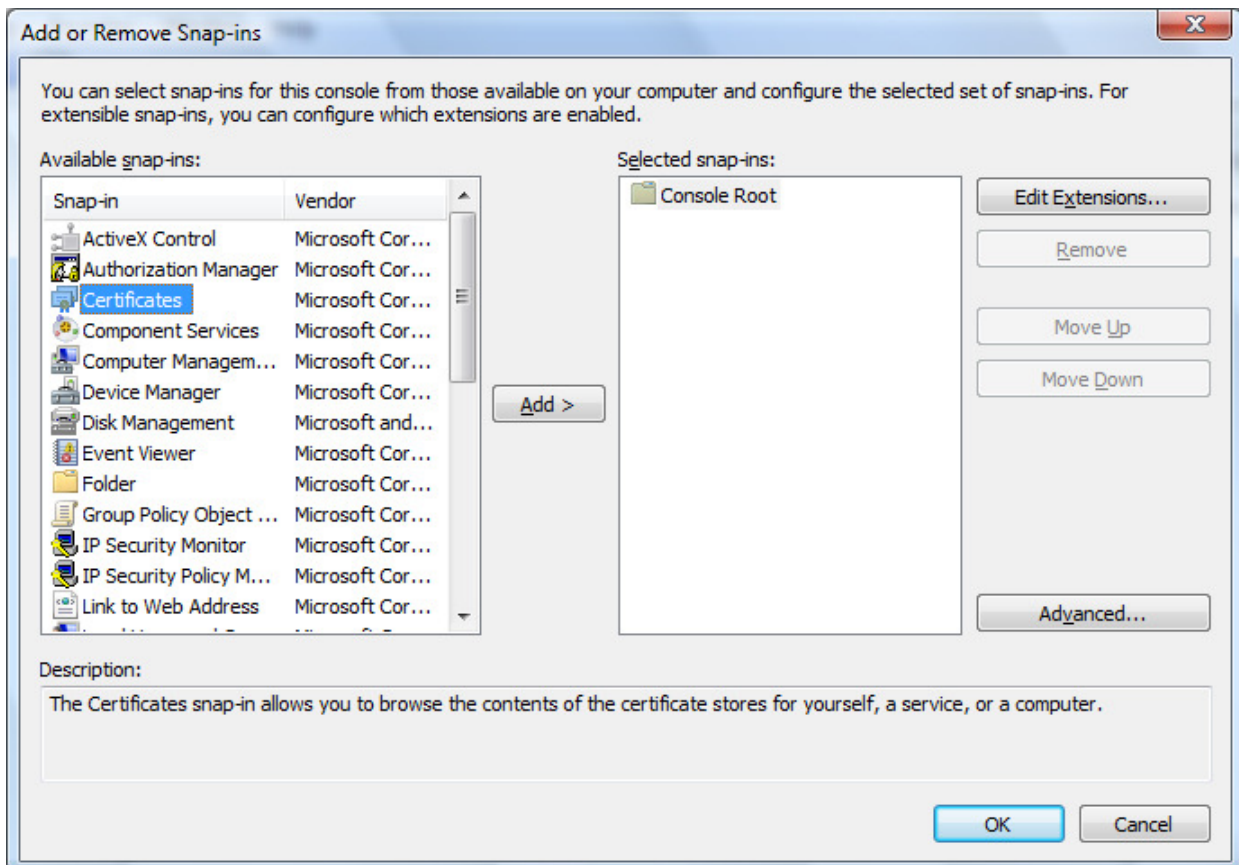
The following screen appears:



Select **"File -> Add/Remove Snap-in..."**

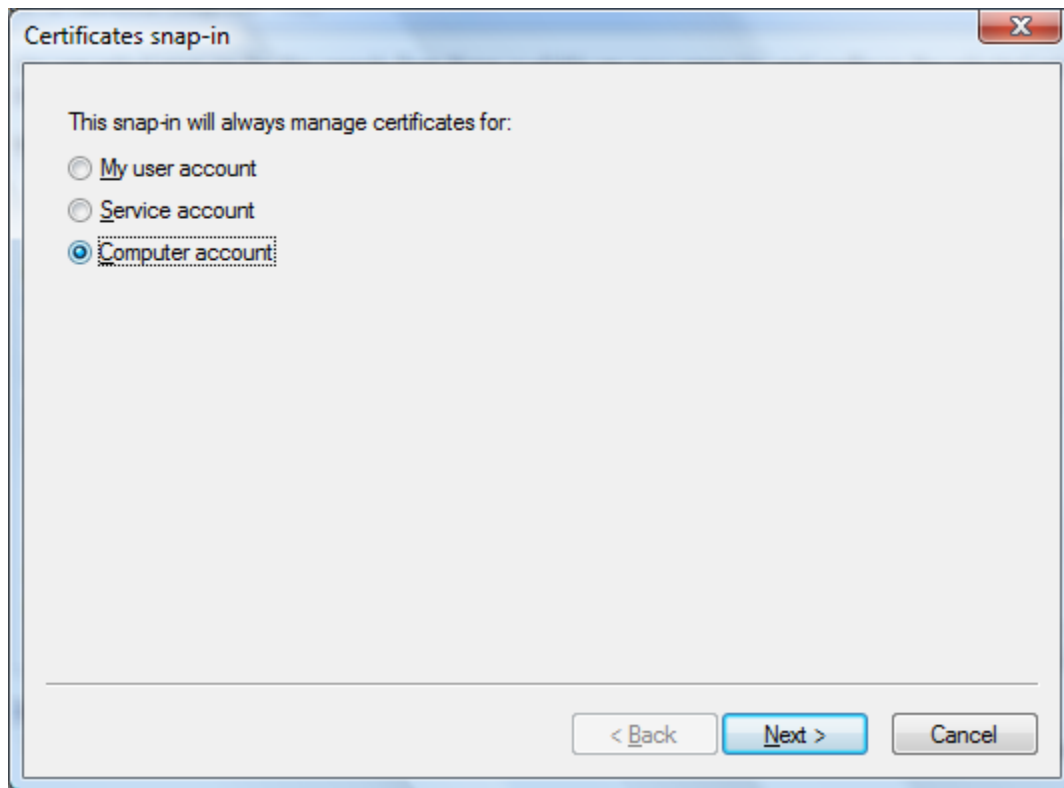


The following screen appears. Select **"Certificates"** on the left pane and click the **"Add"** button.

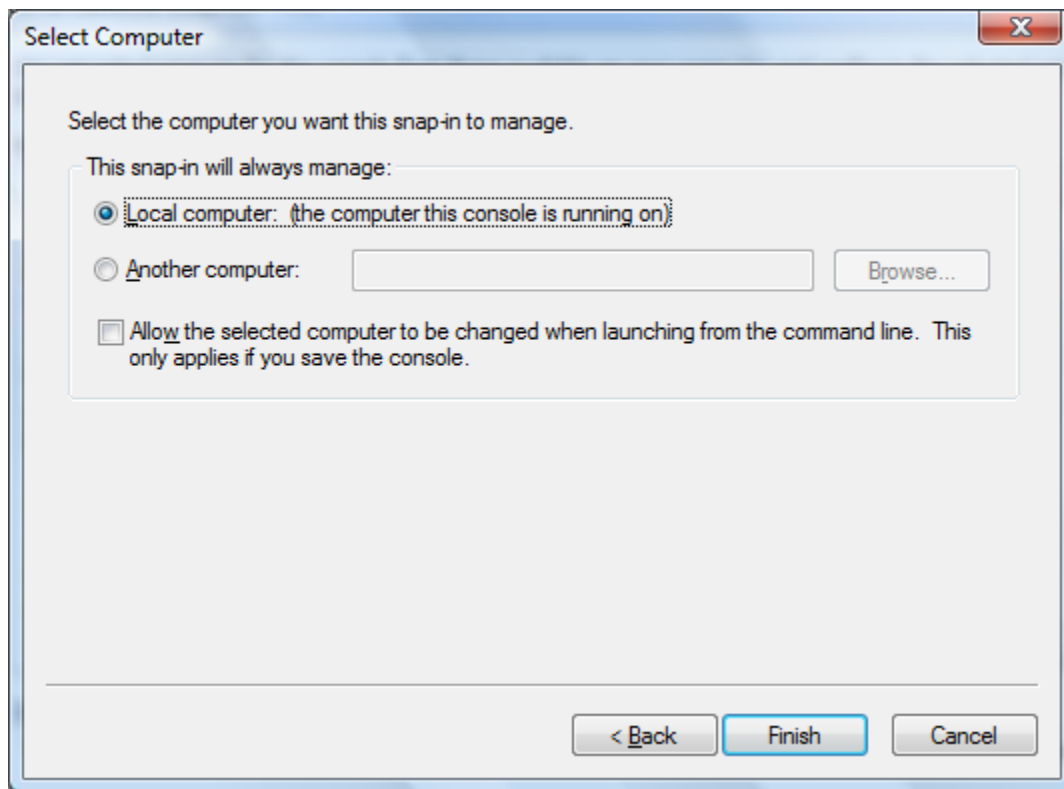




The following screen appears. Ensure that this screen appears. If it does not appear, you are not logged onto the workstation as an administrator. Select the “**Computer account**” option and click the “**Next**” button

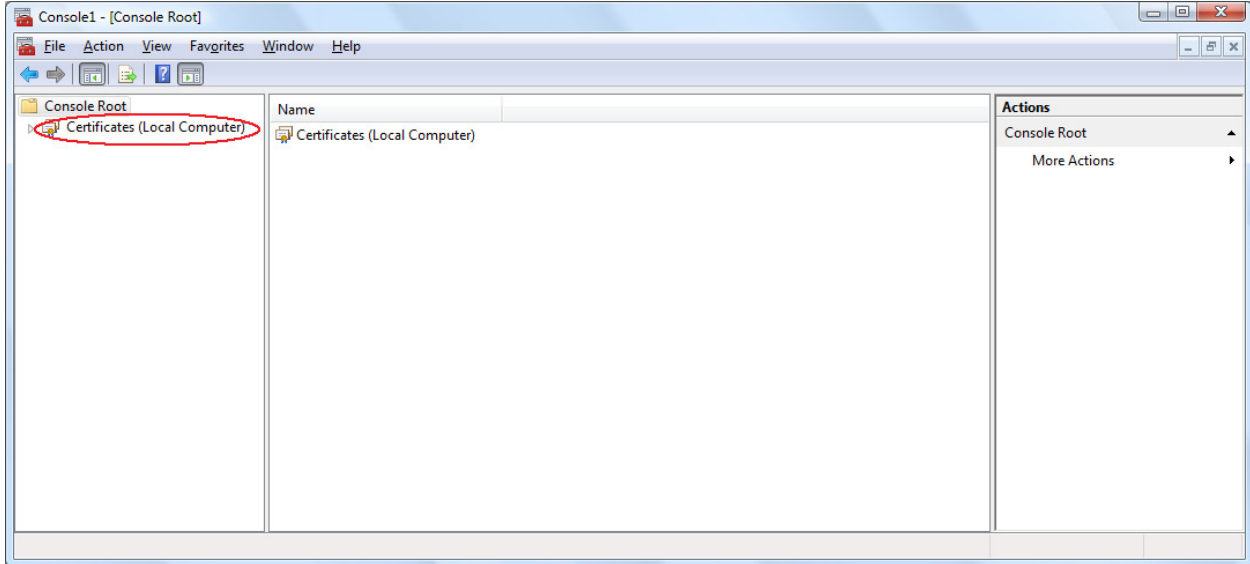


The following screen appears. Ensure the “**Local computer**” option is selected, then click “**Finish**”

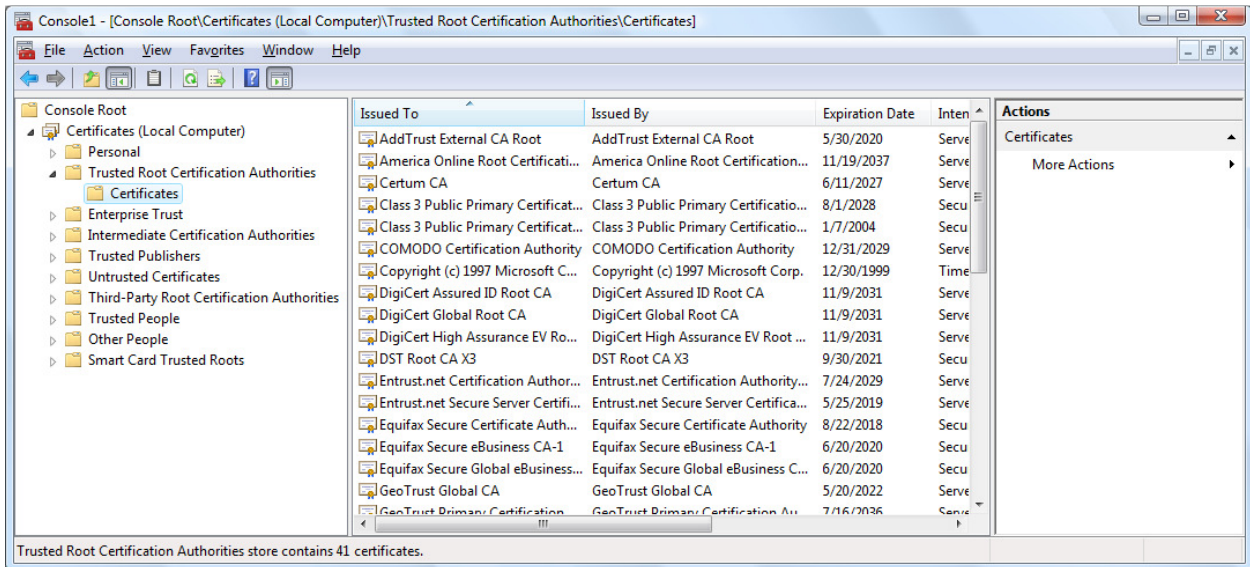


Click “**OK**” on the “Add or Remove Snap-ins” screen.

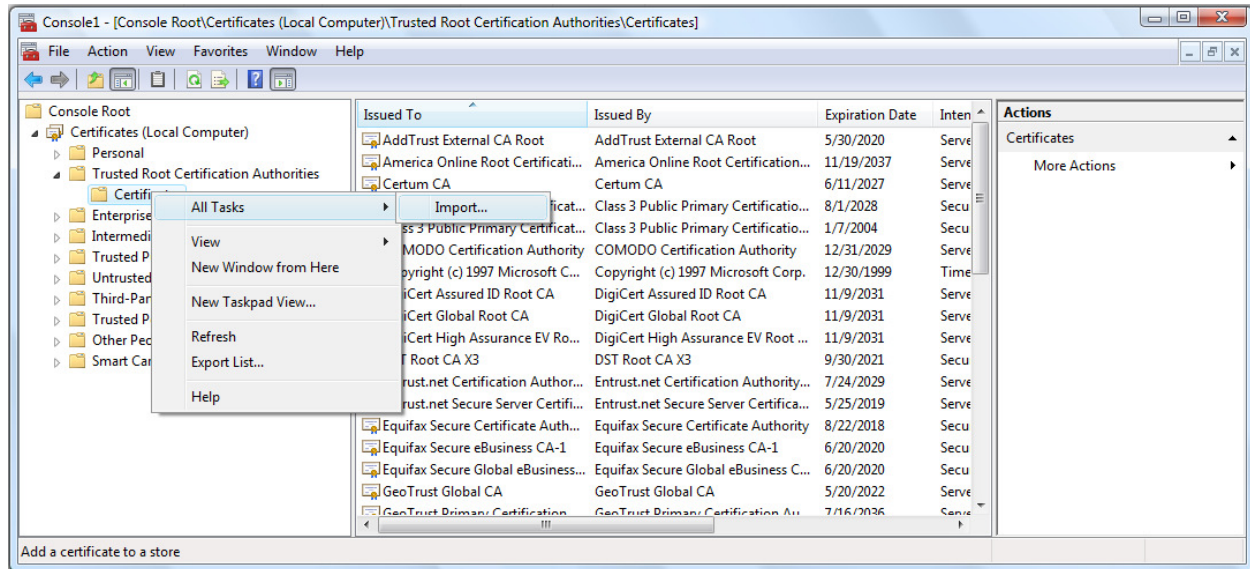
The following screen appears after closing the “Add or Remove Snap-ins” screen. Ensure that “**Certificates (Local Computer)**” appears in the left pane. If instead you see “**Certificates – Current User**”, you are not logged onto the workstation as an administrator or you did not follow the previous two steps correctly.



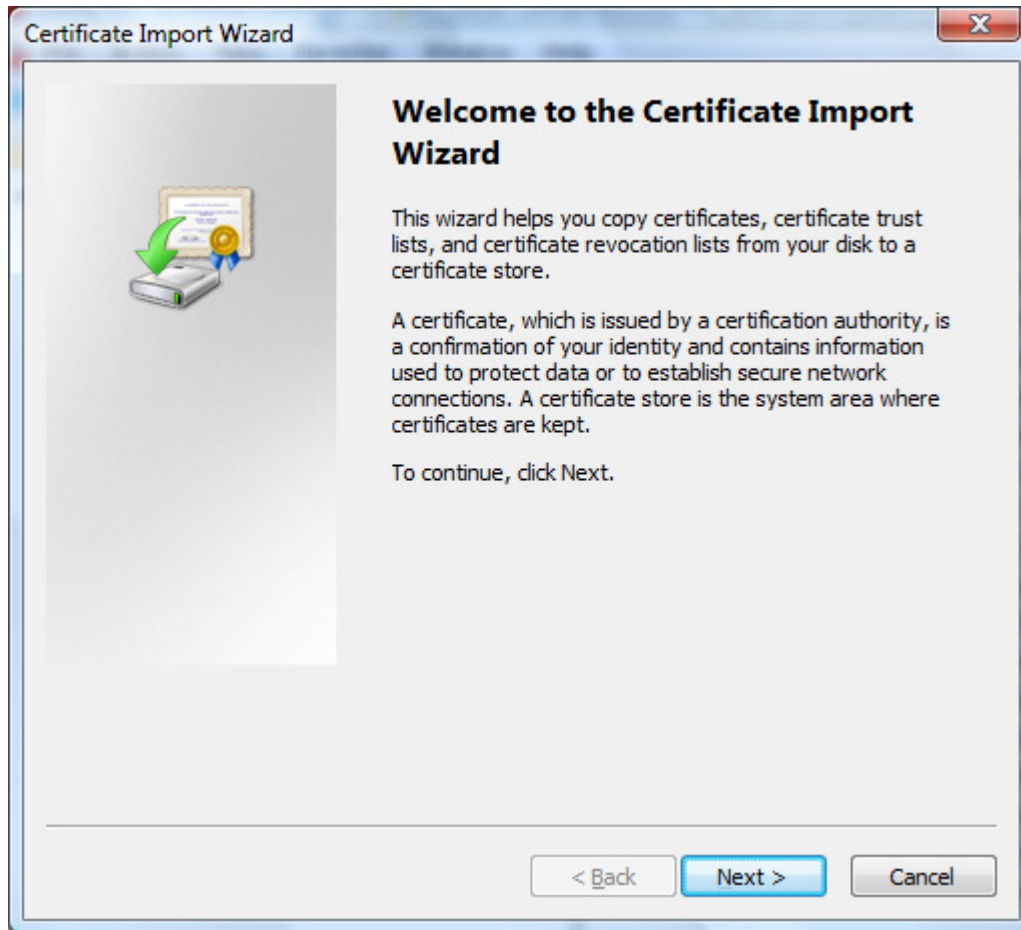
Navigate to “**Console Root -> Certificates (Local Computer)-> Trusted Root Certification Authorities -> Certificates**”



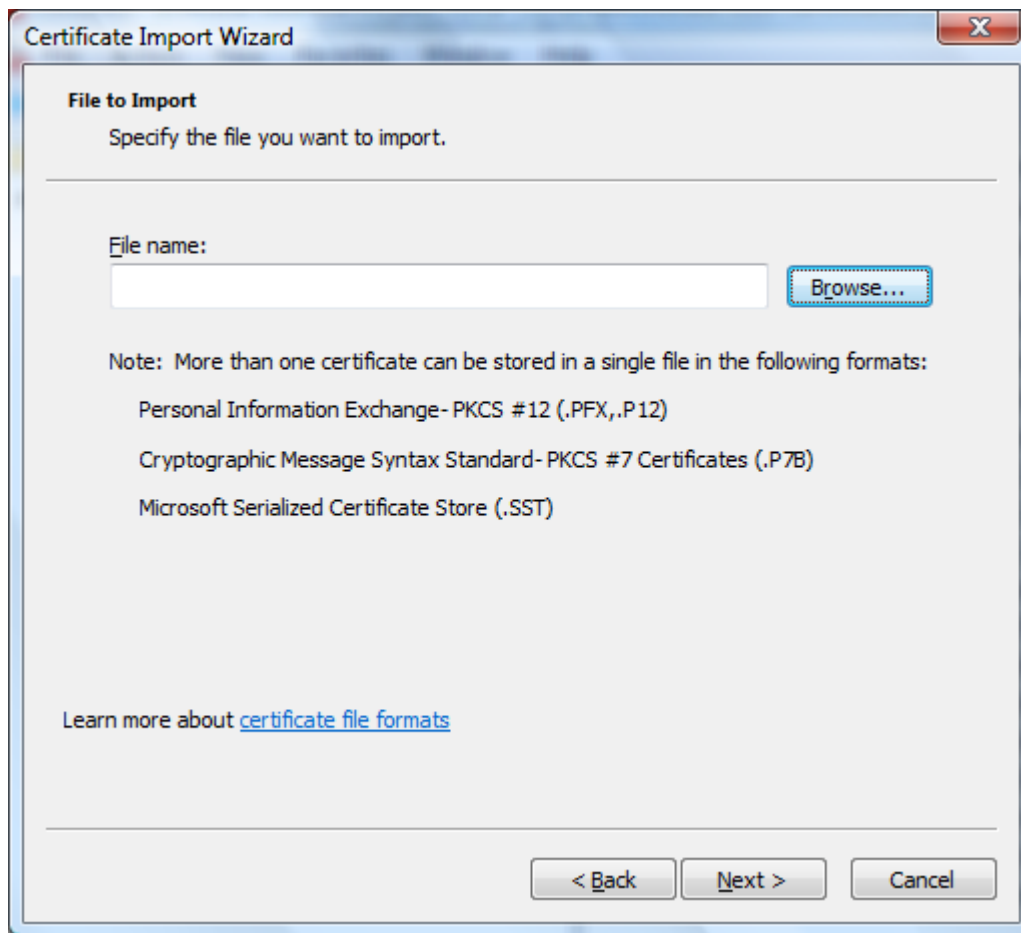
Right mouse click on “Console Root -> Certificates (Local Computer)-> Trusted Root Certification Authorities -> Certificates” and select “All Tasks -> Import...”



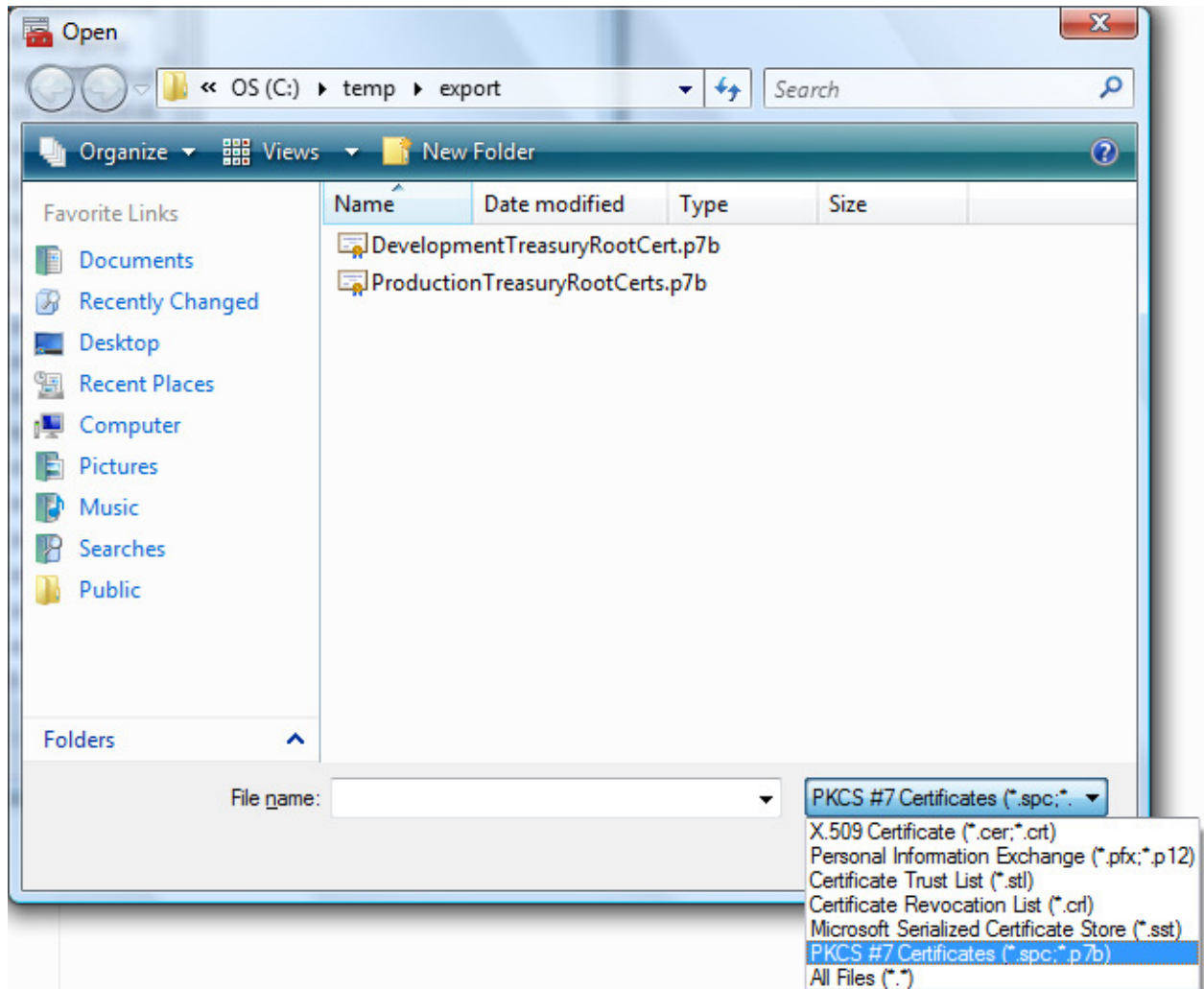
The Certificate Import Wizard displays. Click the “Next” button



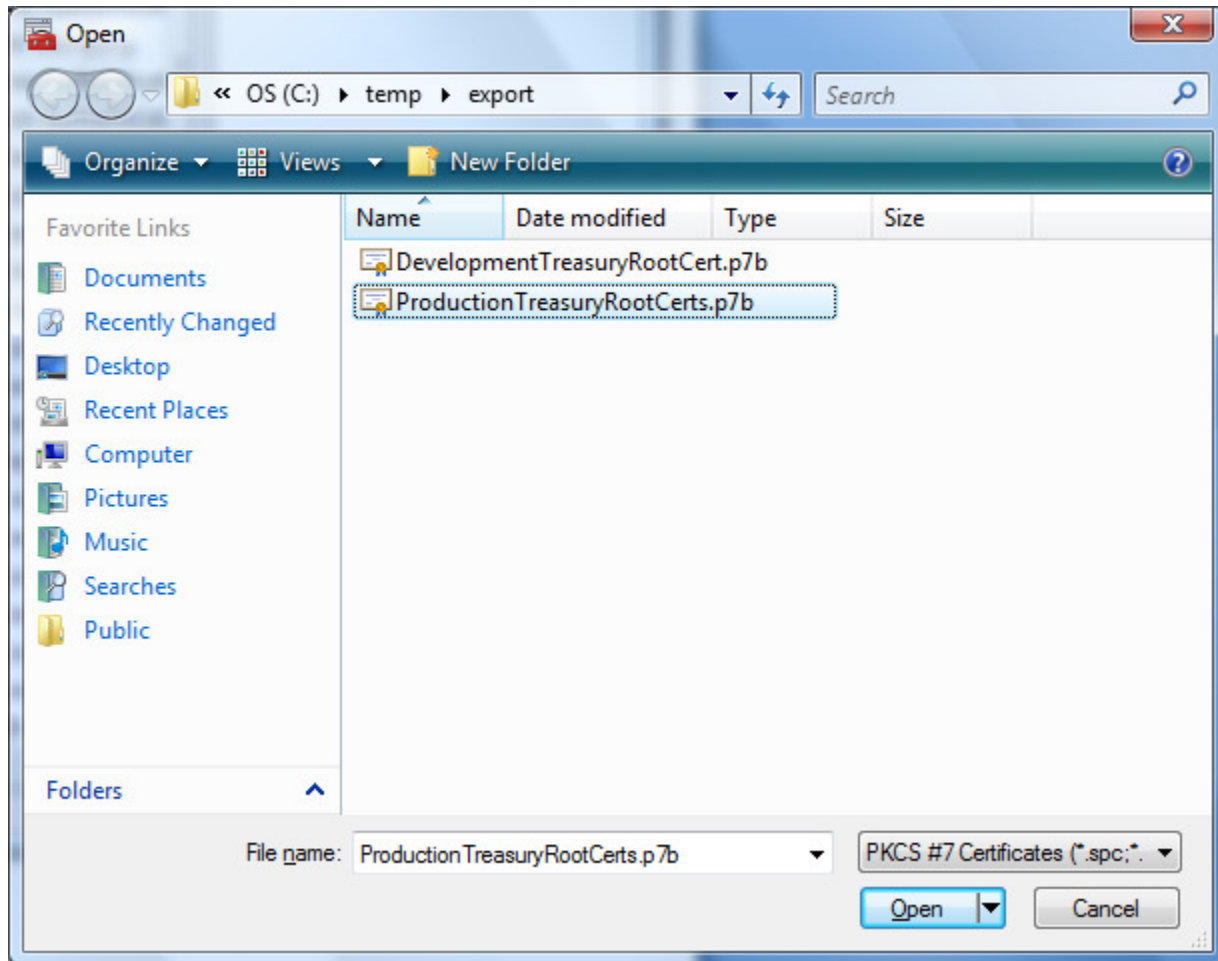
The following screen appears. Click the “Browse...” button



Set the file type filter to “PKCS #7 Certificates (\*.spc; \*.p7b)” and navigate to the production root certificate file exported previously in task 2 (ProductionTreasuryRootCerts.p7b).

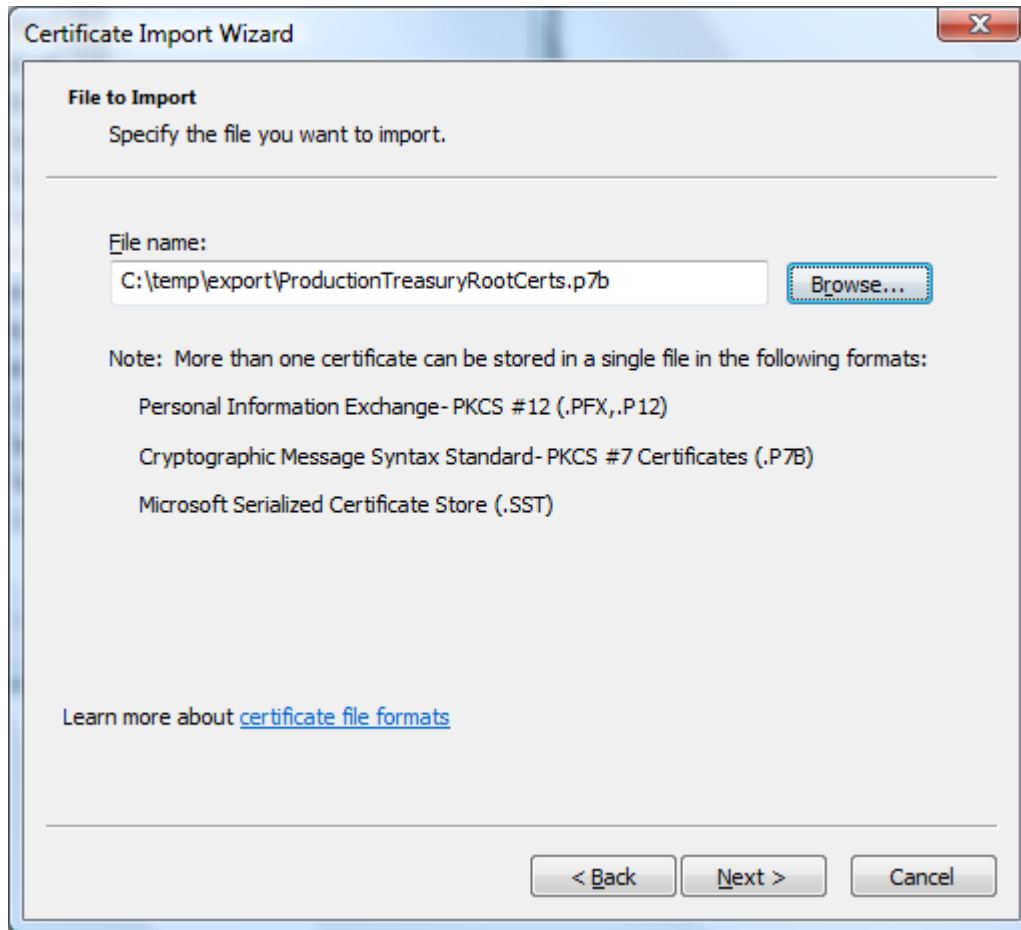


Select the production root certificate container file created in task 2 and click “Open”



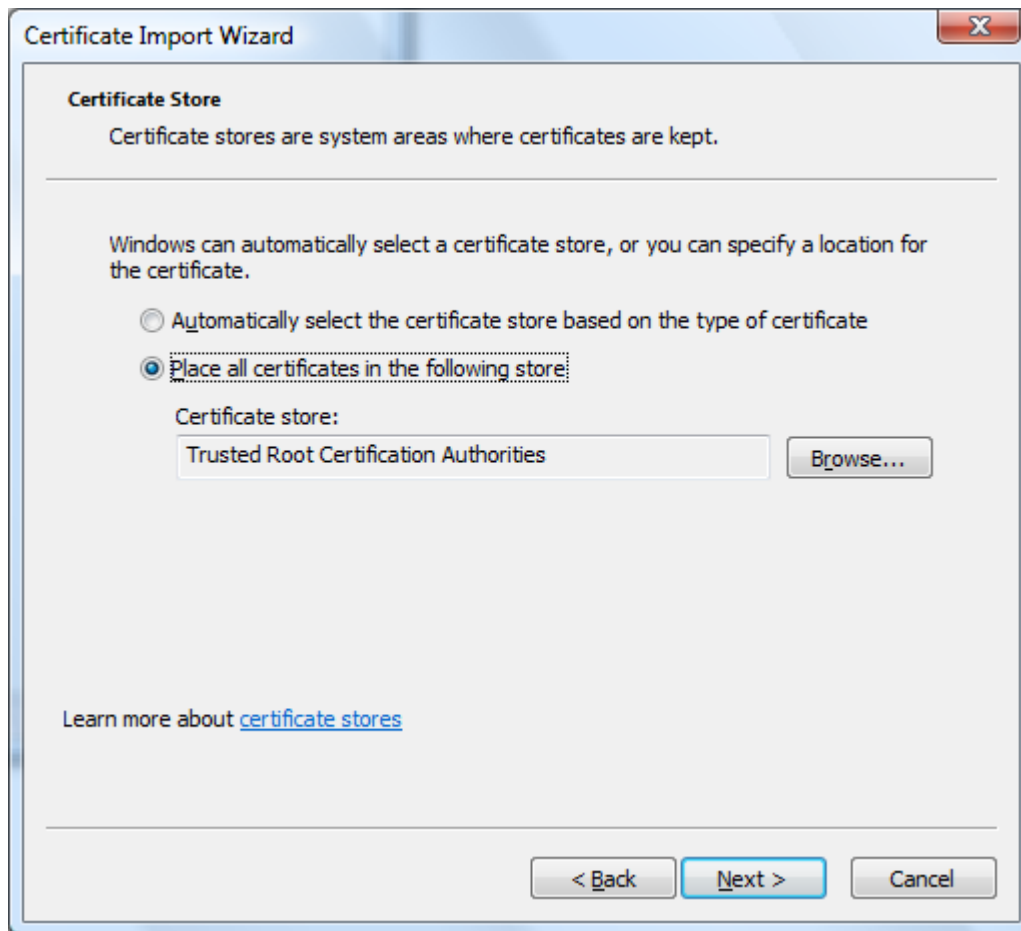


The following screen appears. Verify the name of the file to import and click “Next”

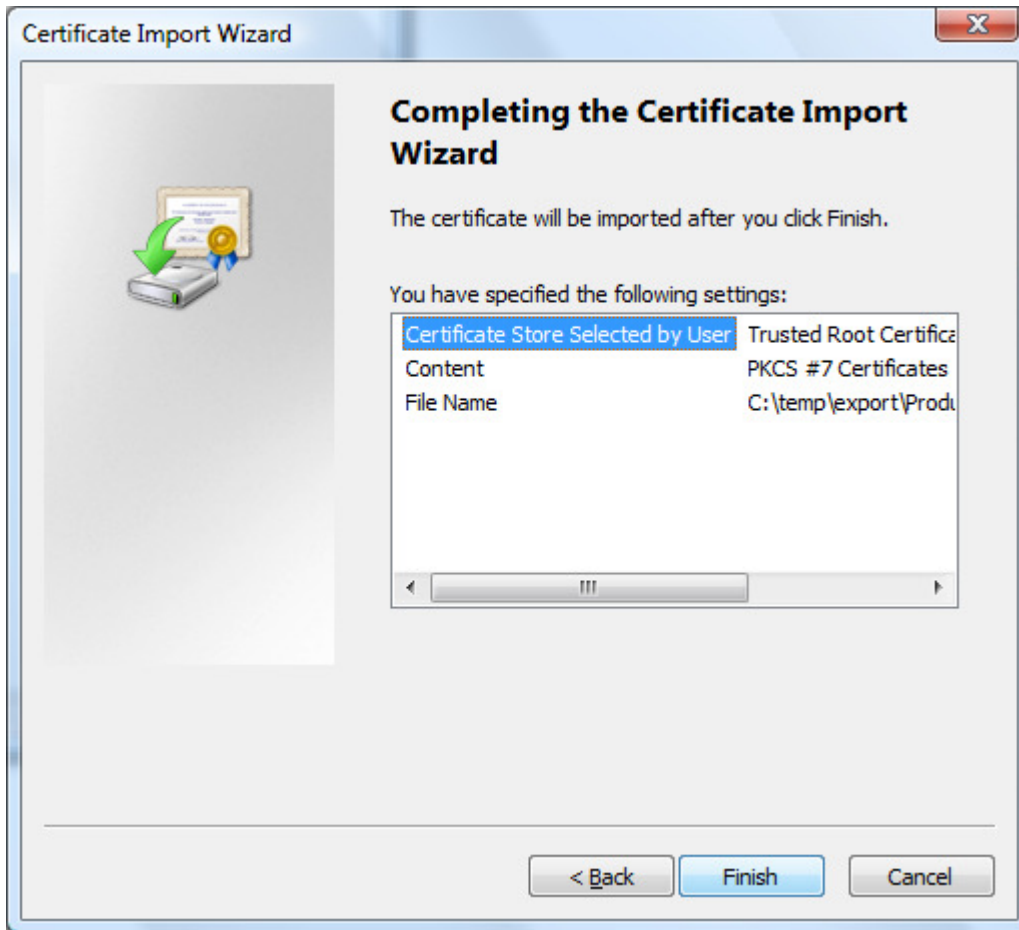


The image shows a Windows dialog box titled "Certificate Import Wizard". The window has a standard title bar with a close button (X) in the top right corner. The main content area is titled "File to Import" and contains the instruction "Specify the file you want to import." Below this is a horizontal line. Underneath the line, the text "File name:" is followed by a text input field containing the path "C:\temp\export\ProductionTreasuryRootCerts.p7b". To the right of the input field is a "Browse..." button. Below the input field and button, there is a "Note:" section with the text: "More than one certificate can be stored in a single file in the following formats:" followed by three bullet points: "Personal Information Exchange- PKCS #12 (.PFX,.P12)", "Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)", and "Microsoft Serialized Certificate Store (.SST)". At the bottom left of the main area, there is a link: "Learn more about [certificate file formats](#)". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

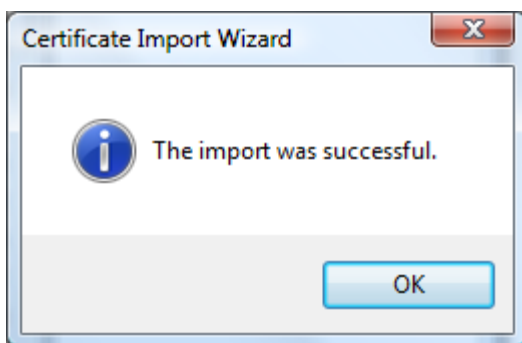
The following screen appears. Verify that the option “**Place all certificates in the following store**” is selected and the Certificate store displayed is “**Trusted Root Certification Authorities**”. Click the “**Next**” button



The following screen appears. Click the **“Finish”** button



You will see the following message if the import was successful. Click **“OK”**.

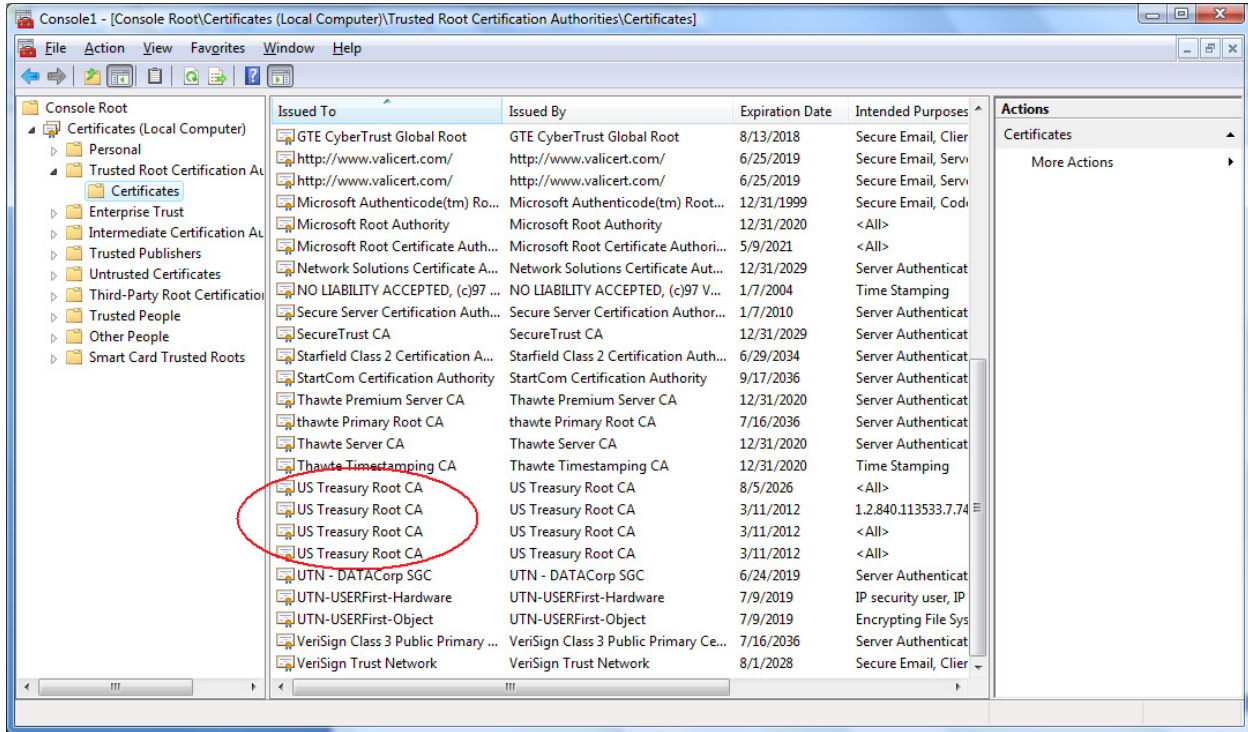


## **Import the Development Treasury Root Certificate**

Repeat the import process (pages 20-27) for the development root certificate container file exported in task 2 (DevelopmentTreasuryRootCert.p7b). Ensure that you specify the file containing the development certificate and that you import into the “Trusted Root Certification Authorities” certificate store.

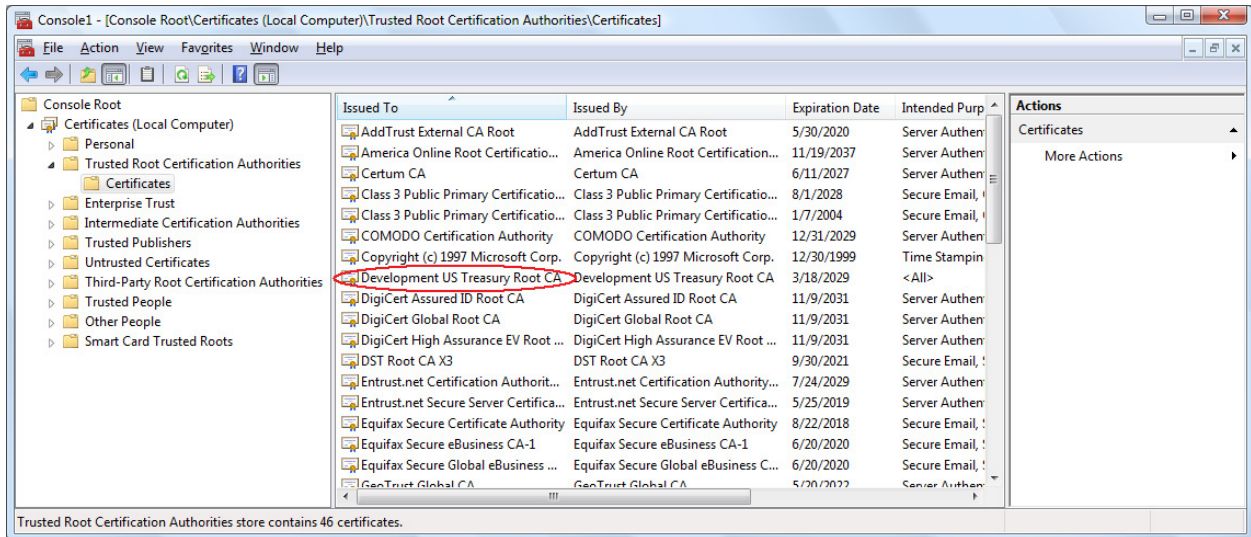
## Verify installation of Production Treasury Root Certificates

Verify that the “US Treasury Root CA” certificates were imported successfully into the “Trusted Root Certification Authorities” store of the Local Computer. See the certificates encircled in red below to verify.

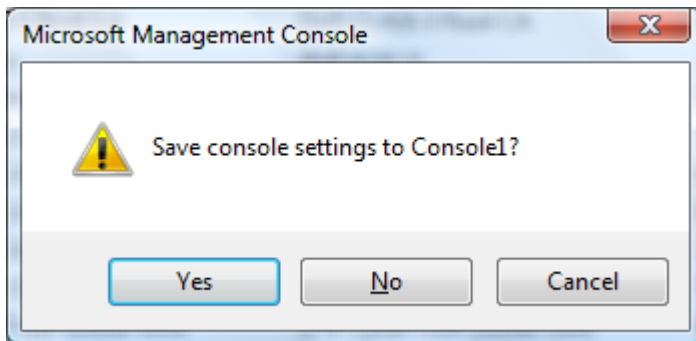


## Verify installation of Development Treasury Root Certificate

Verify that the “**Development US Treasury Root CA**” certificate was imported successfully into the “**Trusted Root Certification Authorities**” store of the **Local Computer**. See the certificate encircled in red to verify.



Close the “**Console1**” application; you will see the following message:



Click “**No**” to close the Microsoft Management Console and complete the Treasury Root Certificate Installation process.

Service: Our Last Name but our First Priority