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 XP workstation. Please refer to the “RootCertificateInstall-Vista.docx” document for performing the tasks on a Vista or Windows 7 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

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

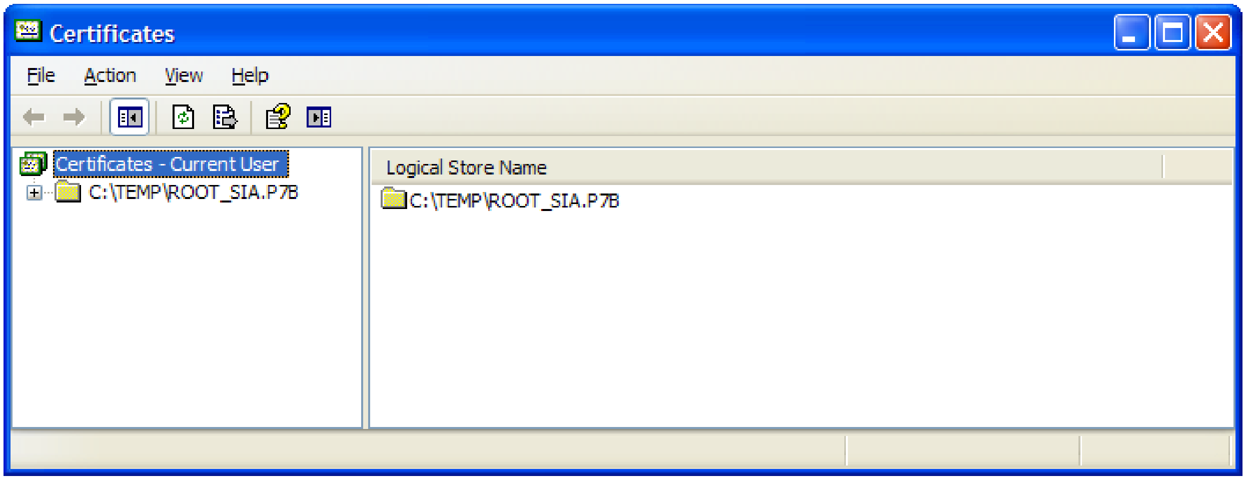
Note that as of December 2010, this URL points to a file that contains the SHA-1 keyed Development Treasury Root Certificate. The URL and/or certificates contained within are subject to change.

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**.

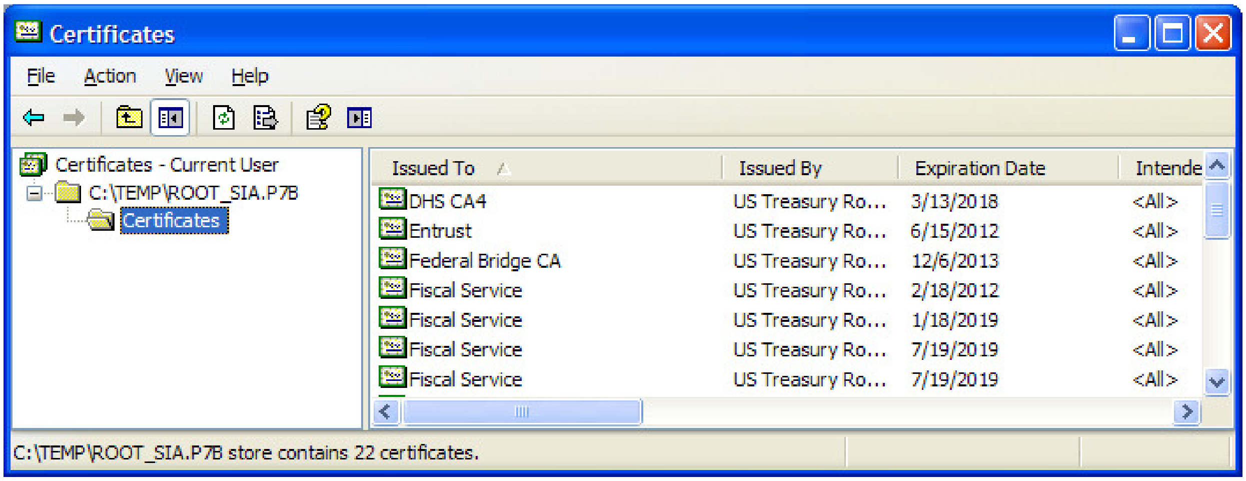
The following screen appears.



Certificates - Current User
C:\TEMP\ROOT_SIA.P7B

Logical Store Name
C:\TEMP\ROOT_SIA.P7B

Navigate to "**Certificates**"

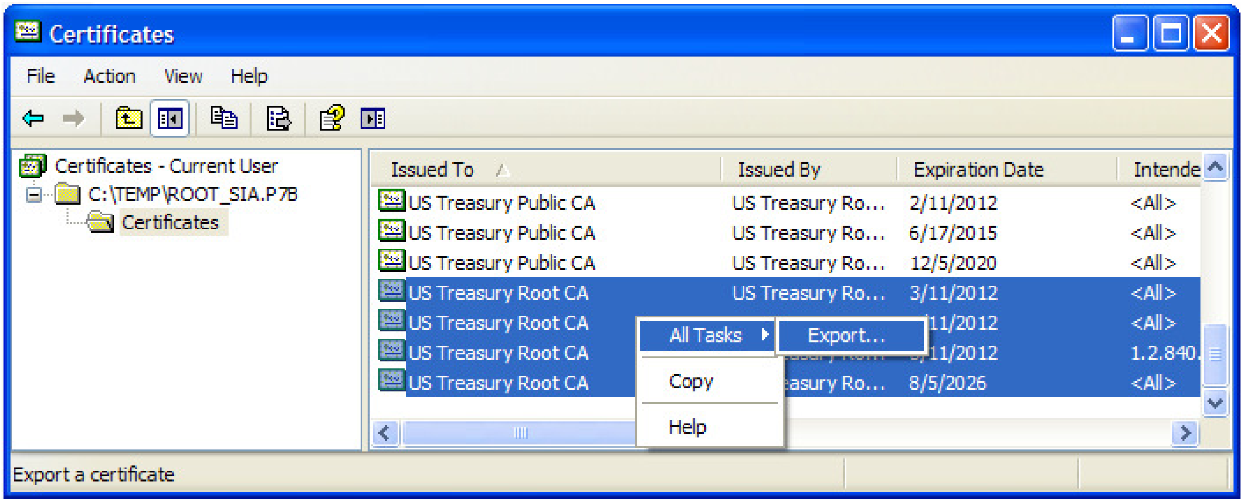


Certificates - Current User
C:\TEMP\ROOT_SIA.P7B
Certificates

Issued To	Issued By	Expiration Date	Intende
DHS CA4	US Treasury Ro...	3/13/2018	<All>
Entrust	US Treasury Ro...	6/15/2012	<All>
Federal Bridge CA	US Treasury Ro...	12/6/2013	<All>
Fiscal Service	US Treasury Ro...	2/18/2012	<All>
Fiscal Service	US Treasury Ro...	1/18/2019	<All>
Fiscal Service	US Treasury Ro...	7/19/2019	<All>
Fiscal Service	US Treasury Ro...	7/19/2019	<All>

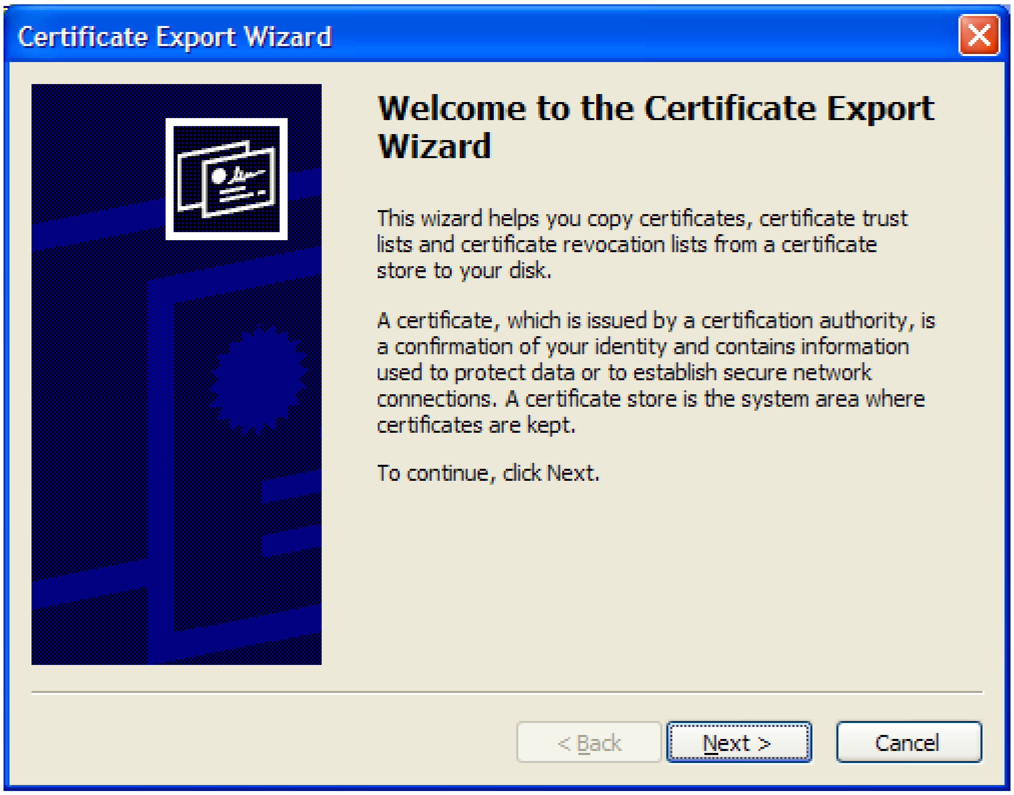
C:\TEMP\ROOT_SIA.P7B store contains 22 certificates.

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…**"



Issued To	Issued By	Expiration Date	Intende
US Treasury Public CA	US Treasury Ro...	2/11/2012	<All>
US Treasury Public CA	US Treasury Ro...	6/17/2015	<All>
US Treasury Public CA	US Treasury Ro...	12/5/2020	<All>
US Treasury Root CA	US Treasury Ro...	3/11/2012	<All>
US Treasury Root CA		11/2012	<All>
US Treasury Root CA		/11/2012	1.2.840.
US Treasury Root CA	asury Ro...	8/5/2026	<All>

The Certificate Export Wizard displays. Click the "**Next**" button



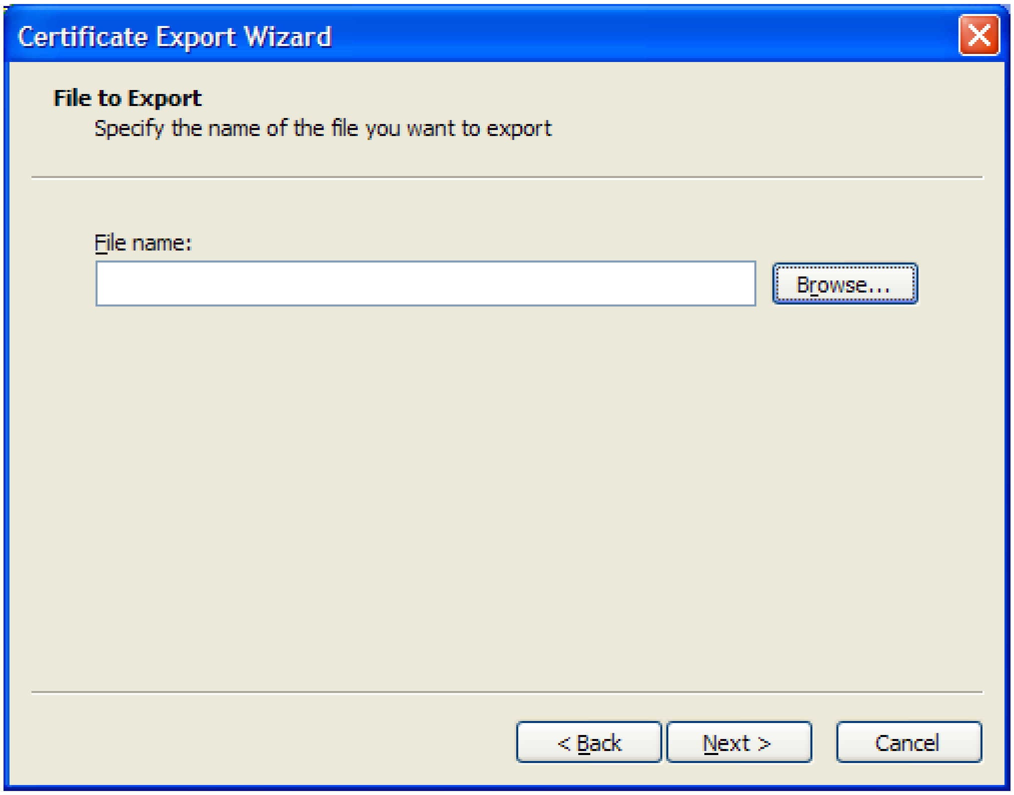
Welcome to the Certificate Export Wizard

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

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



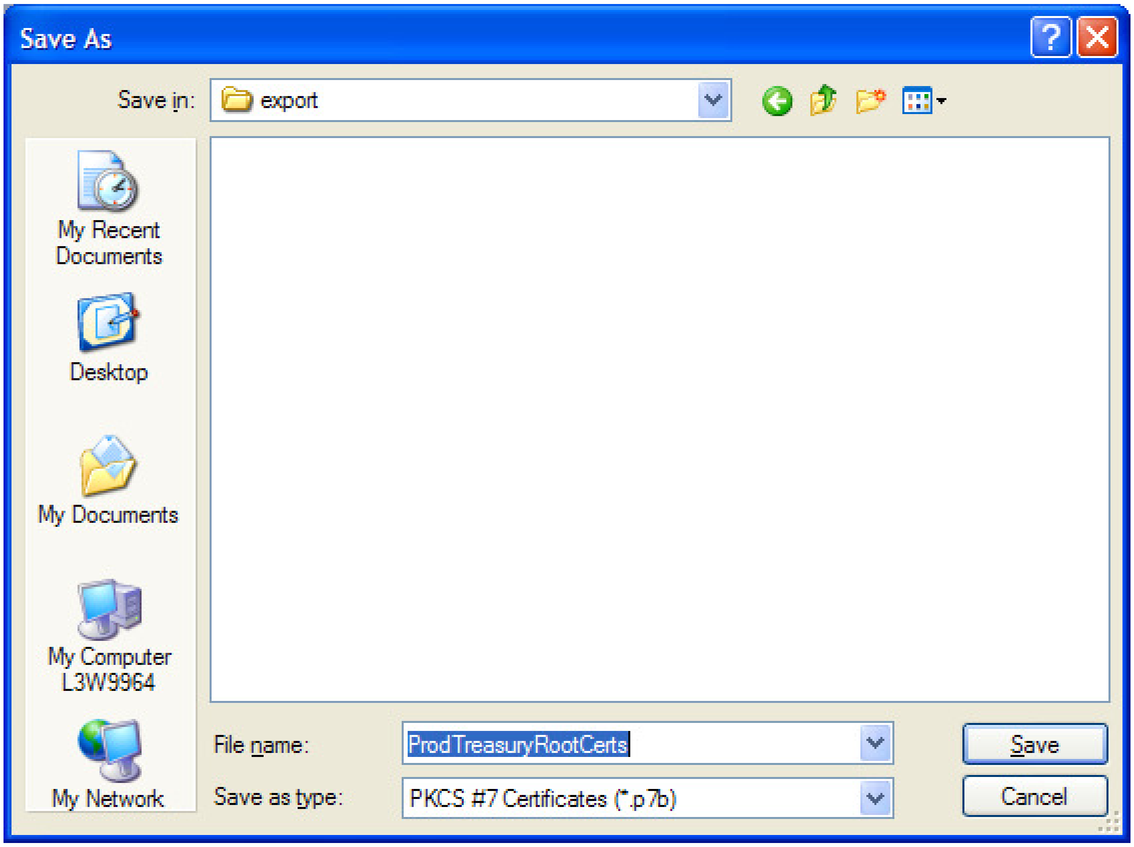
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

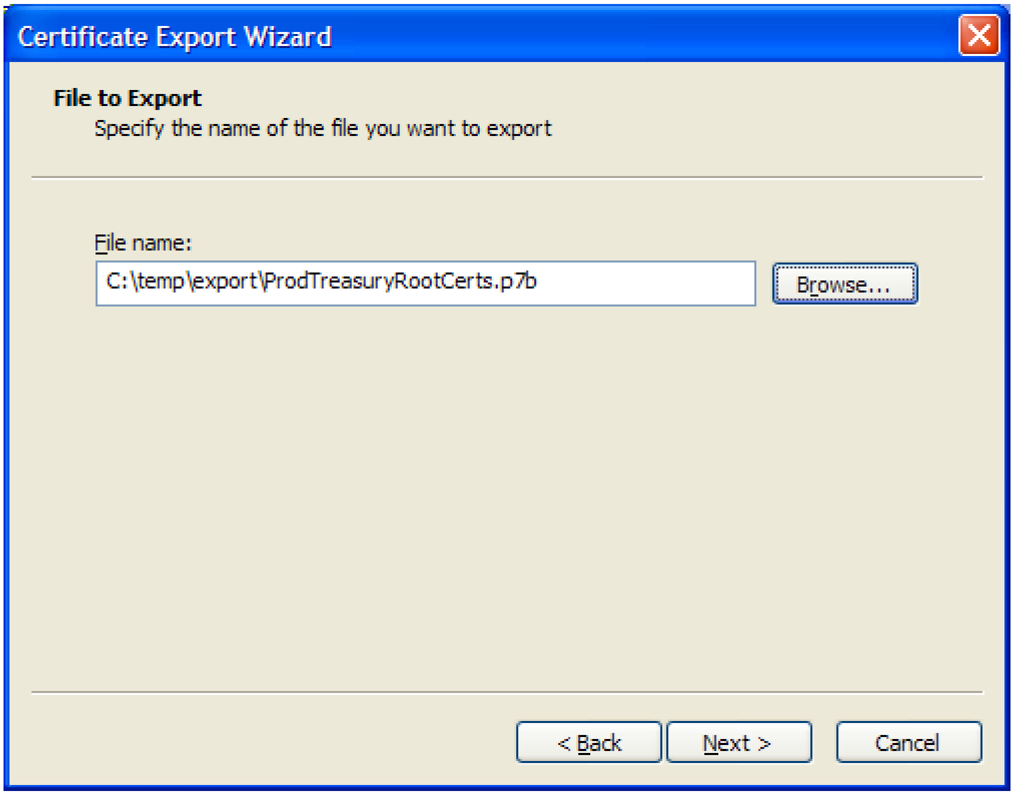
Type in file name and click the “**Save**” button



File name: ProdTreasuryRootCerts

Save as type: PKCS #7 Certificates (*.p7b)

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



Certificate Export Wizard

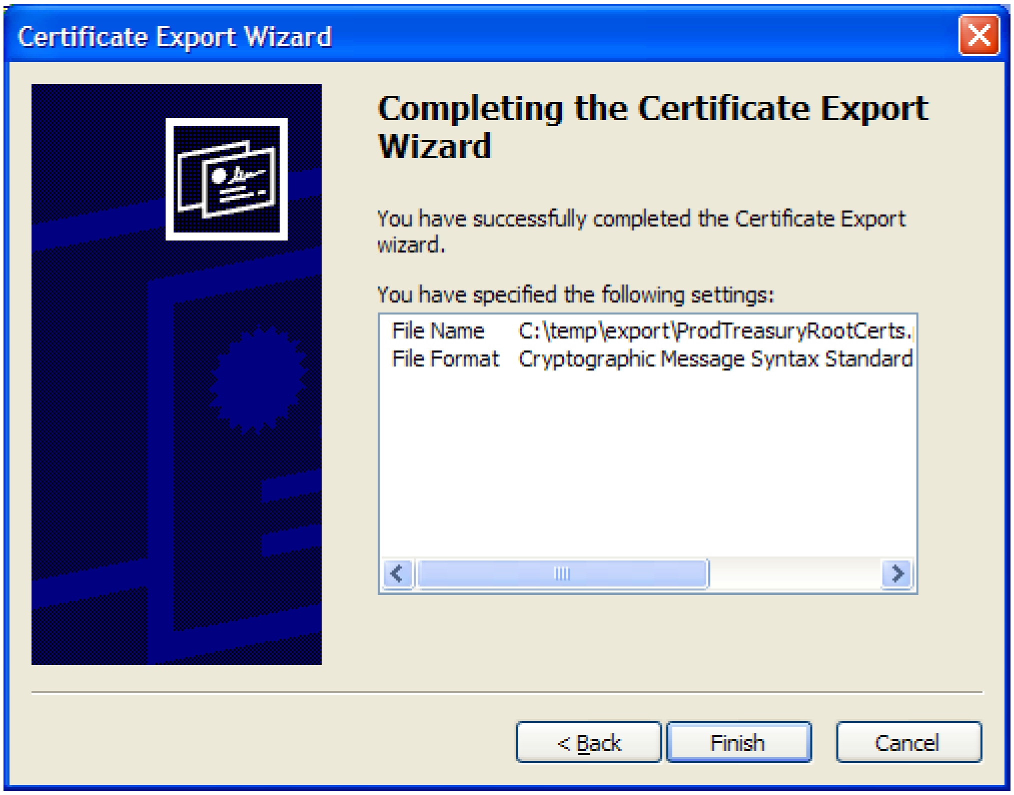
File to Export

Specify the name of the file you want to export

File name:

C:\temp\export\ProdTreasuryRootCerts.p7b

Click the “**Finish**” button



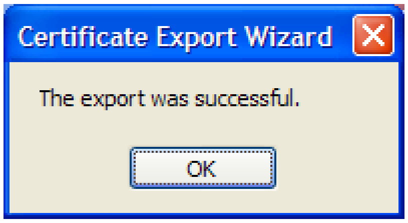
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\temp\export\ProdTreasuryRootCerts.
File Format	Cryptographic Message Syntax Standard

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



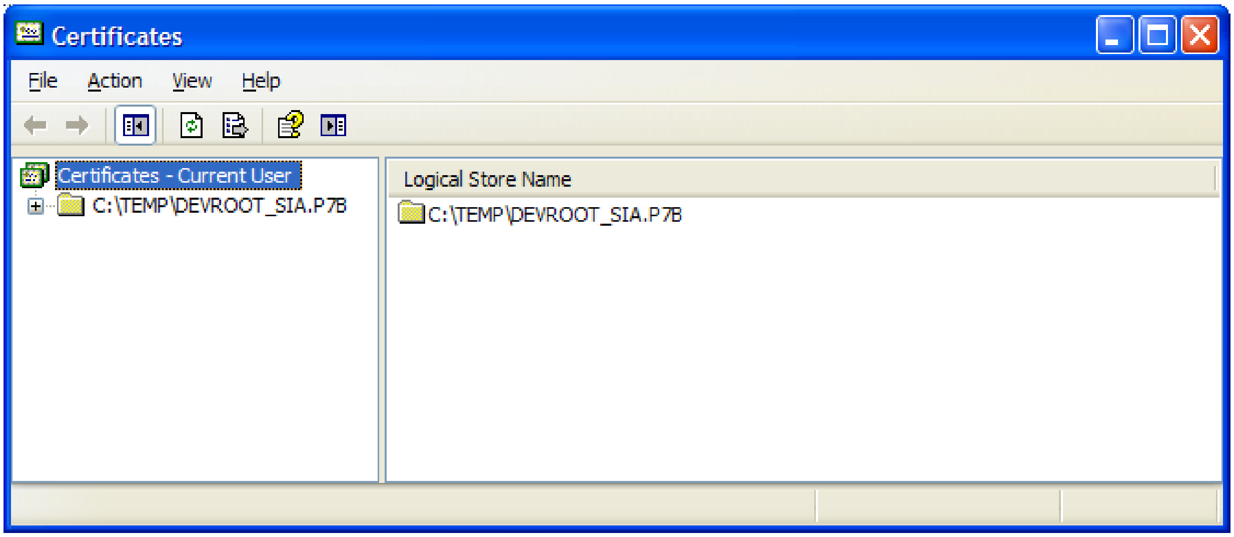
The export was successful.

Close the “**Certificates**” application.

Export the Development Treasury Root Certificate

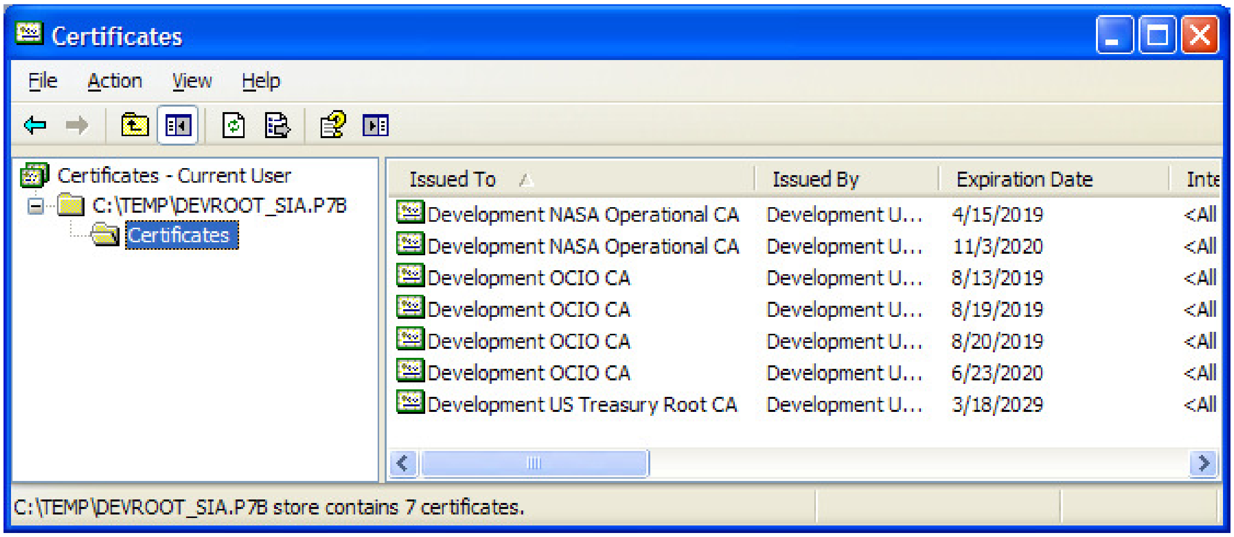
Double-click on the downloaded development certificate container file, **devroot_sia.p7b**.

The following screen appears.



Logical Store Name
C:\TEMP\DEVROOT_SIA.P7B

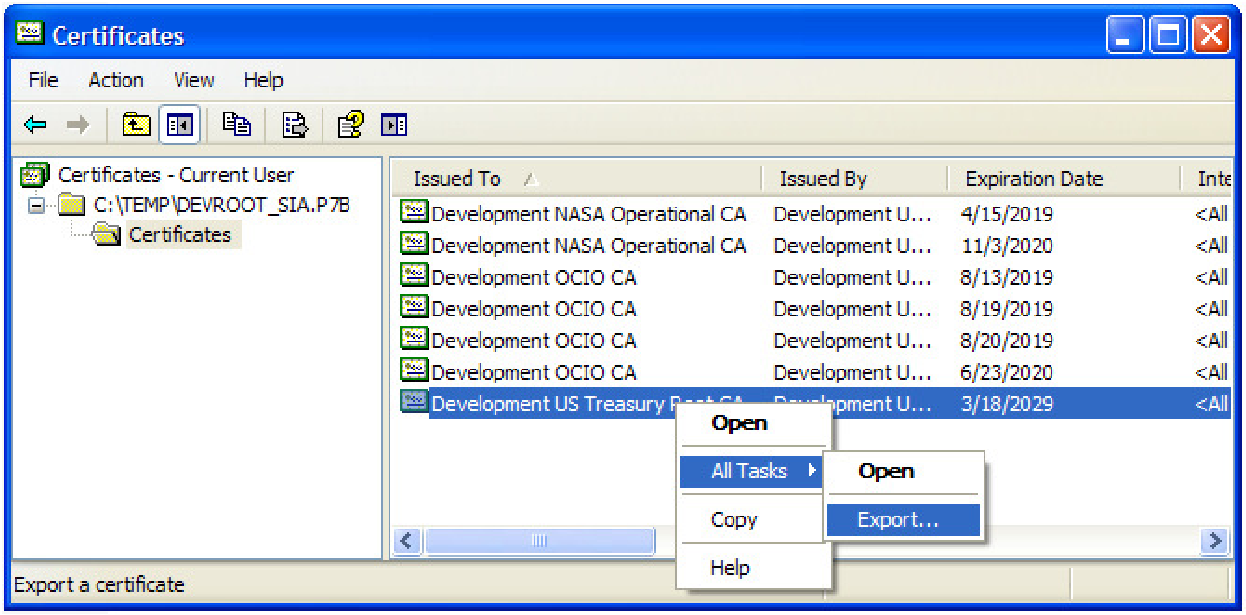
Navigate to "**Certificates**"



Issued To	Issued By	Expiration Date	Inte
Development NASA Operational CA	Development U...	4/15/2019	<All
Development NASA Operational CA	Development U...	11/3/2020	<All
Development OCIO CA	Development U...	8/13/2019	<All
Development OCIO CA	Development U...	8/19/2019	<All
Development OCIO CA	Development U...	8/20/2019	<All
Development OCIO CA	Development U...	6/23/2020	<All
Development US Treasury Root CA	Development U...	3/18/2029	<All

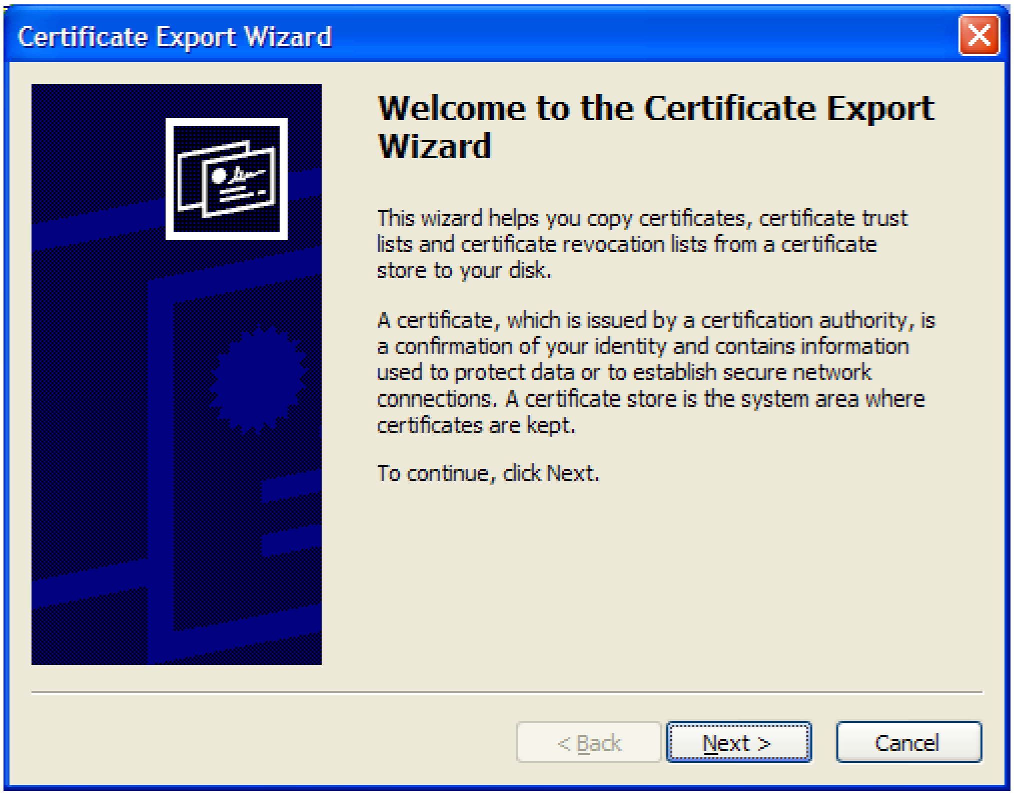
C:\TEMP\DEVROOT_SIA.P7B store contains 7 certificates.

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



Issued To	Issued By	Expiration Date	Inte
Development NASA Operational CA	Development U...	4/15/2019	<All
Development NASA Operational CA	Development U...	11/3/2020	<All
Development OCIO CA	Development U...	8/13/2019	<All
Development OCIO CA	Development U...	8/19/2019	<All
Development OCIO CA	Development U...	8/20/2019	<All
Development OCIO CA	Development U...	6/23/2020	<All
Development US Treasury R	Development U...	3/18/2029	<All

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



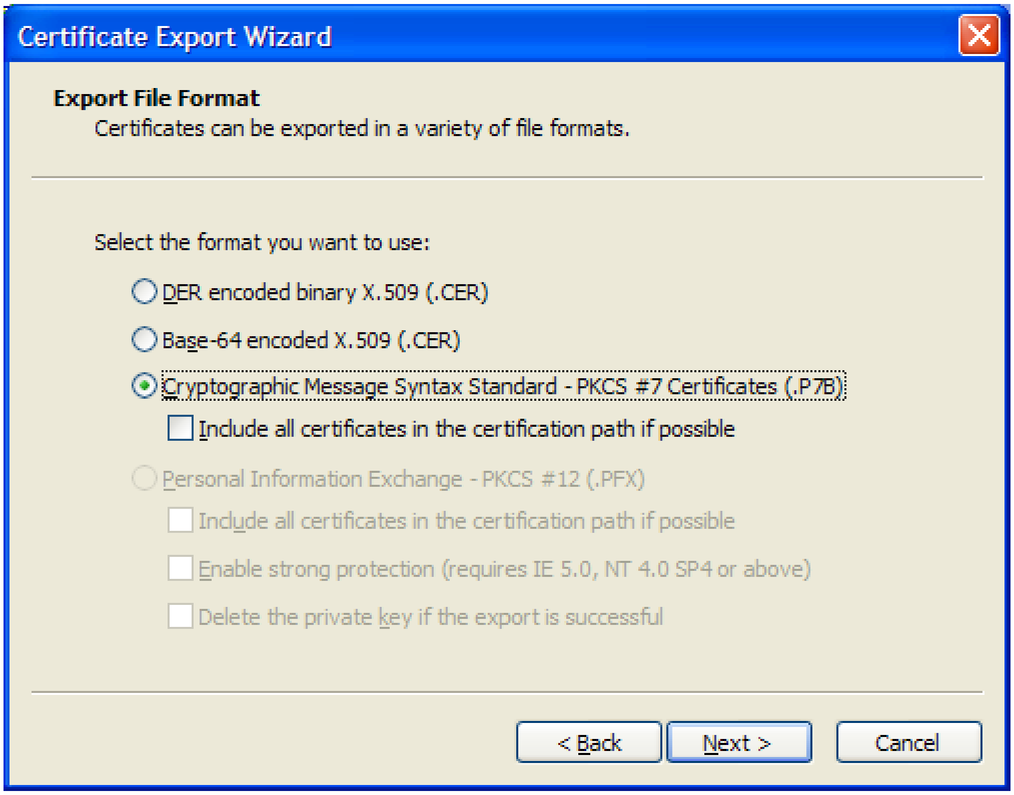
Welcome to the Certificate Export Wizard

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

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.

Select “**Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**” and click the “**Next**” button. Note that this screen only appears when selecting a single certificate to export, as is the case for the Development Treasury Root Certificate (the .CER formats can only contain one certificate).



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

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

□ Include all certificates in the certification path if possible

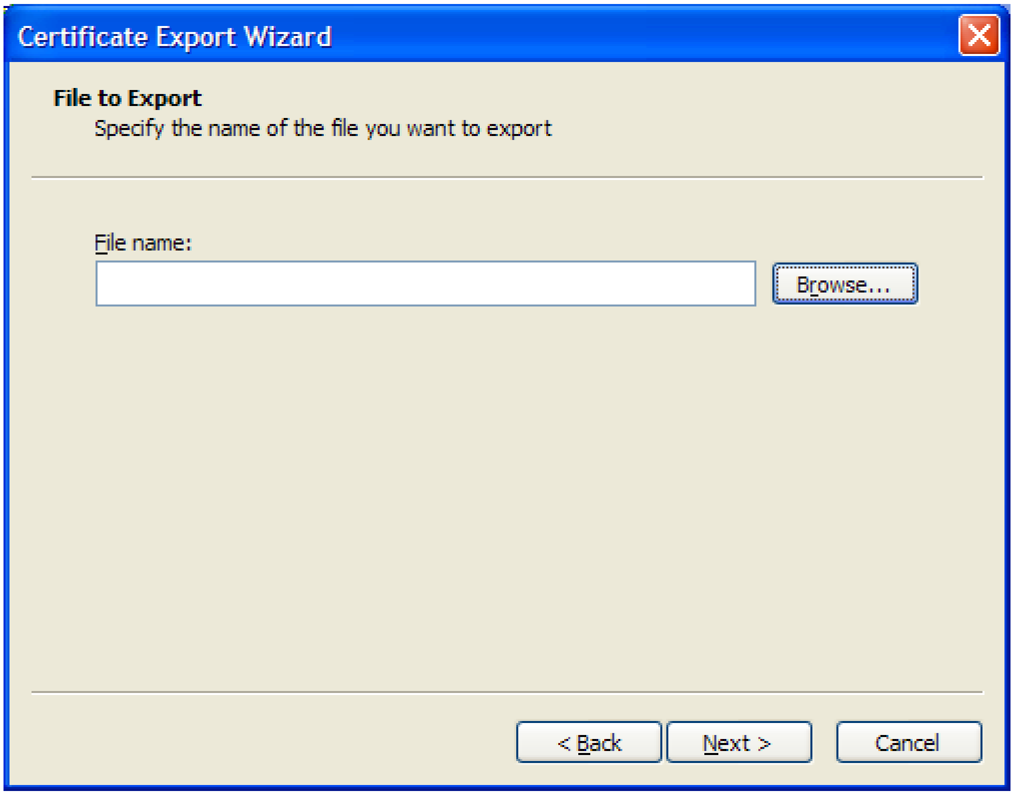
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

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

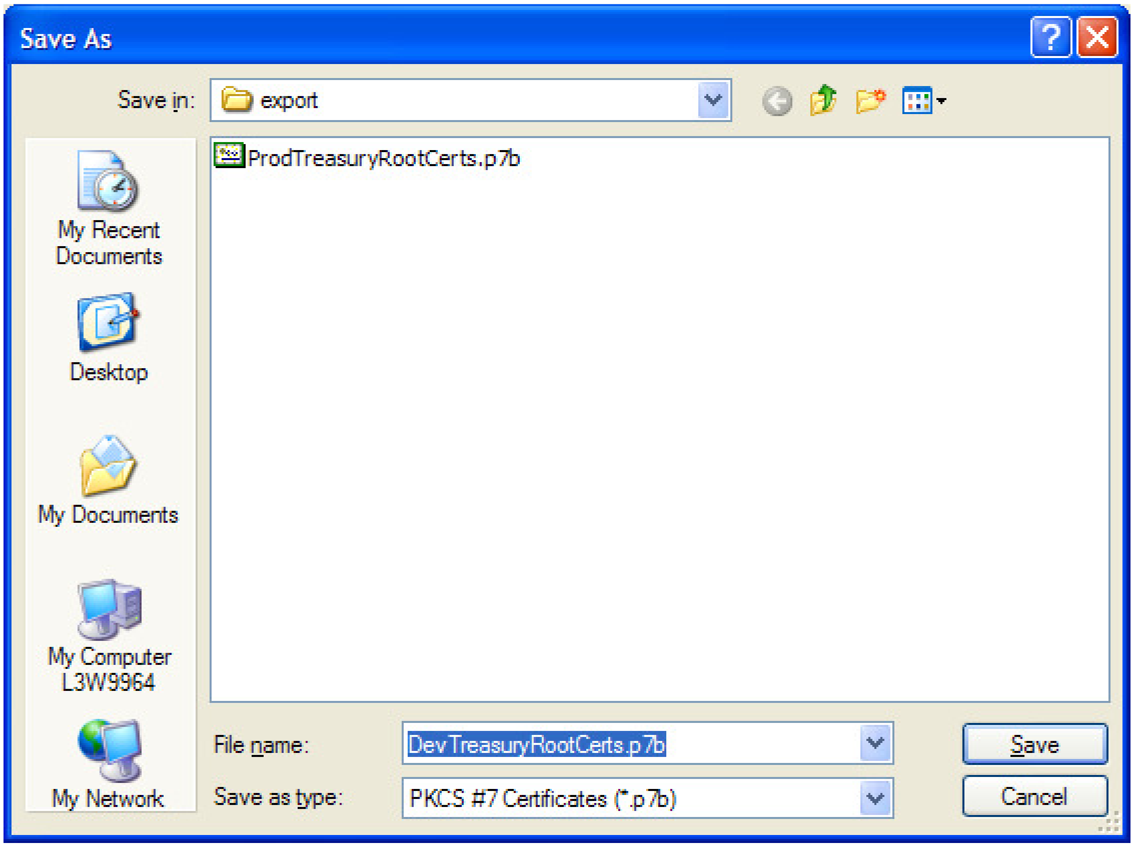


File to Export

Specify the name of the file you want to export

File name:

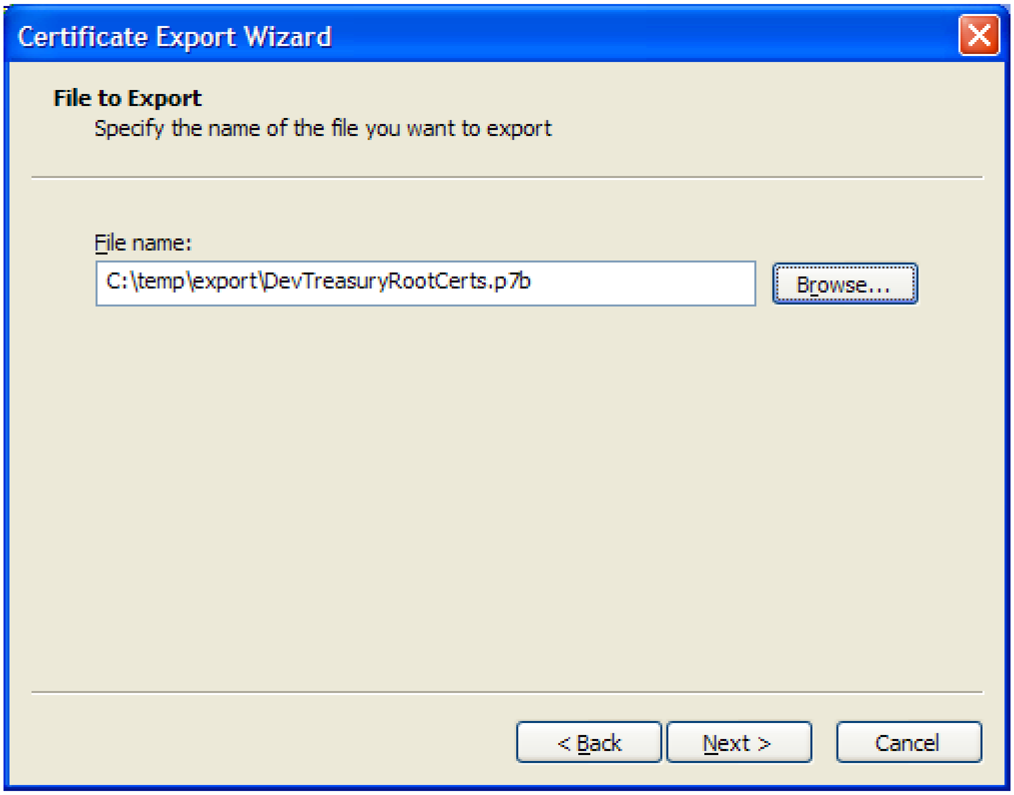
Type in file name and click the "**Save**" button. Ensure that the file name is different than the file name used for exporting the production certificates.



File name: DevTreasuryRootCerts.p7b

Save as type: PKCS #7 Certificates (*.p7b)

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



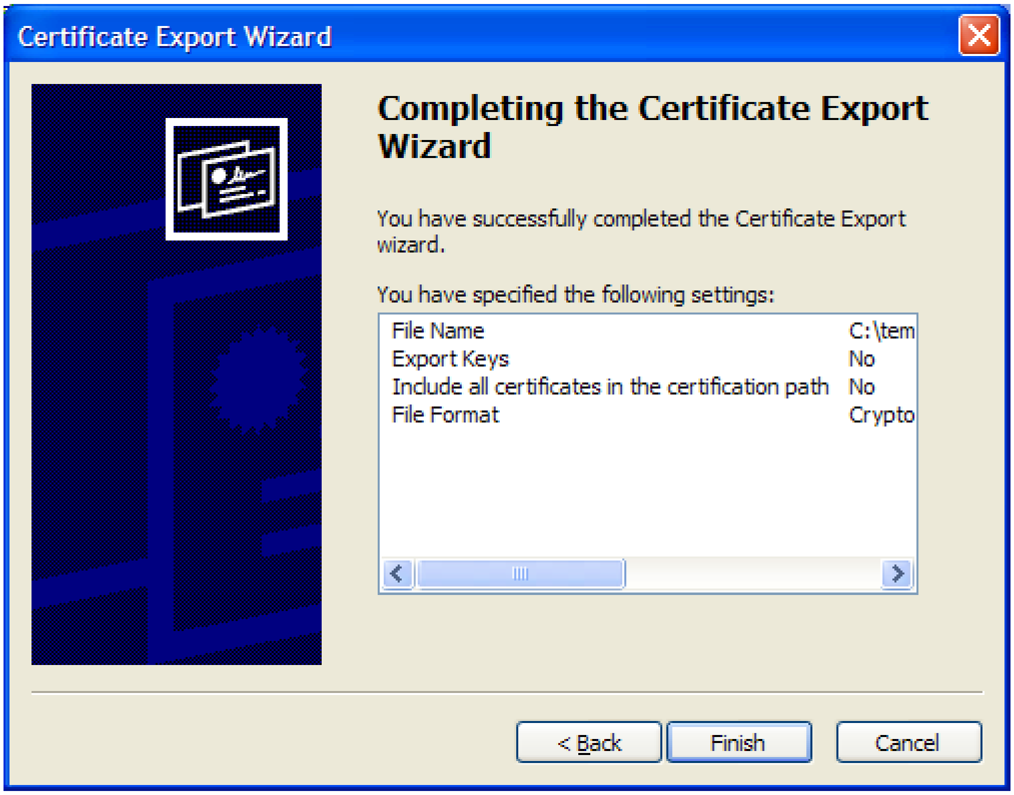
File to Export

Specify the name of the file you want to export

File name:

C:\temp\export\DevTreasuryRootCerts.p7b

Click the “**Finish**” button



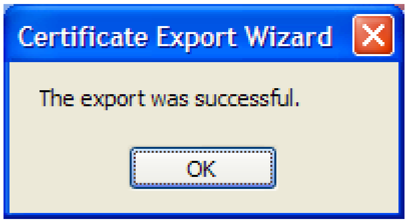
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\tem
Export Keys	No
Include all certificates in the certification path	No
File Format	Crypto

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



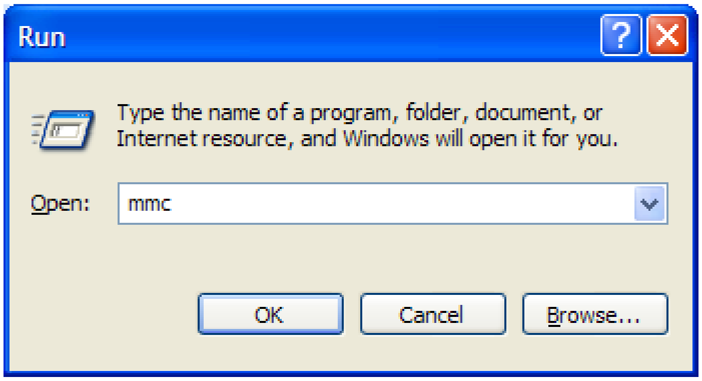
The export was successful.

Close the “**Certificates**” application.

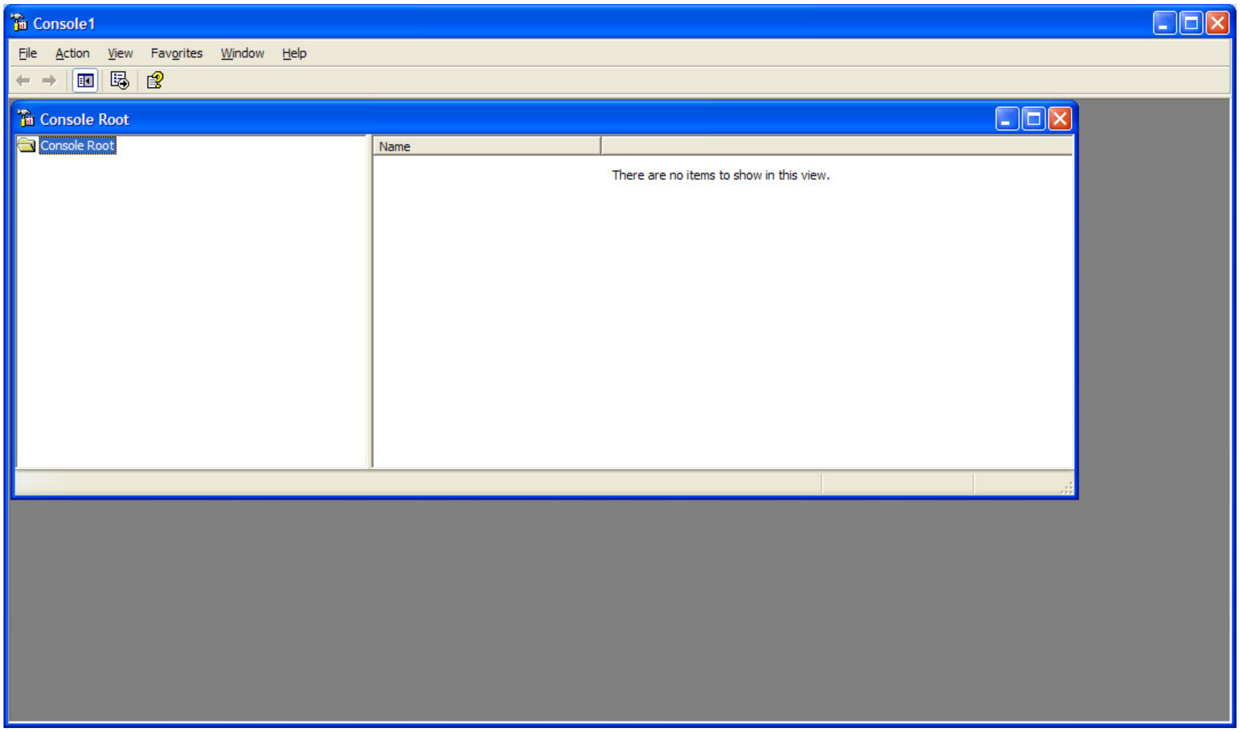
Task 3: Import the Treasury Root Certificates into the local computer trust store

Import the Production Treasury Root Certificates

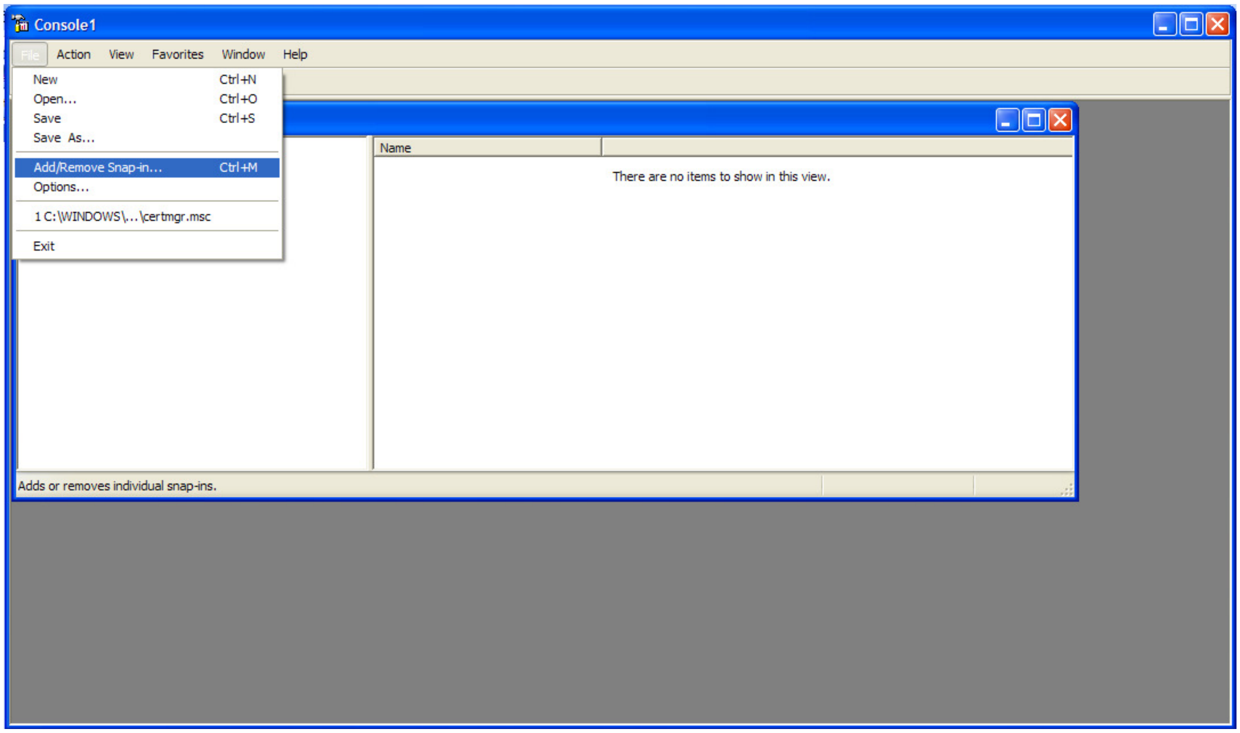
Click “**Start -> Run…**”, type “**mmc**” into the “**Open**” textbox and click “**OK**”


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
mmc
OK
Cancel
Browse...

The following screen appears:



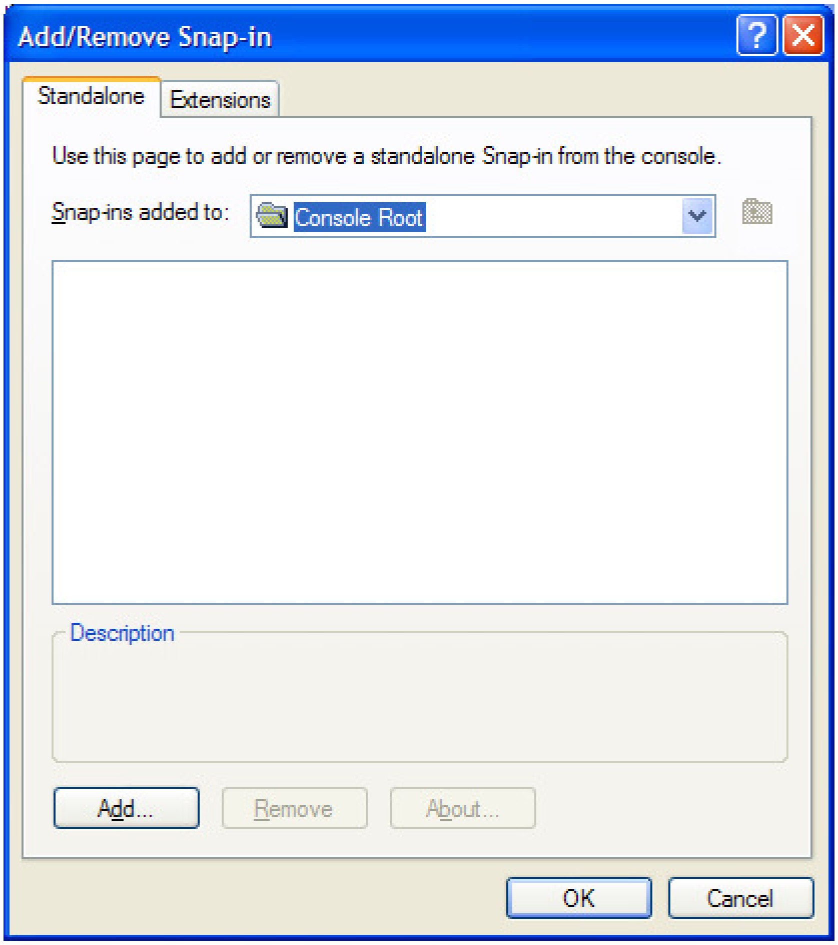
Select “**File -> Add/Remove Snap-in…**”



There are no items to show in this view.

Adds or removes individual snap-ins.

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



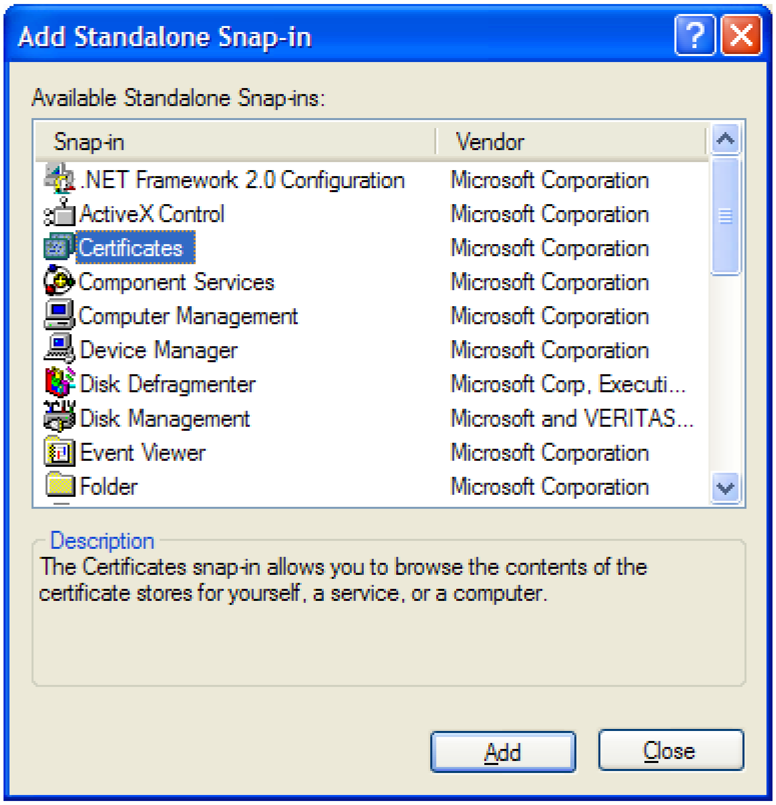
Add/Remove Snap-in

Standalone | Extensions

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

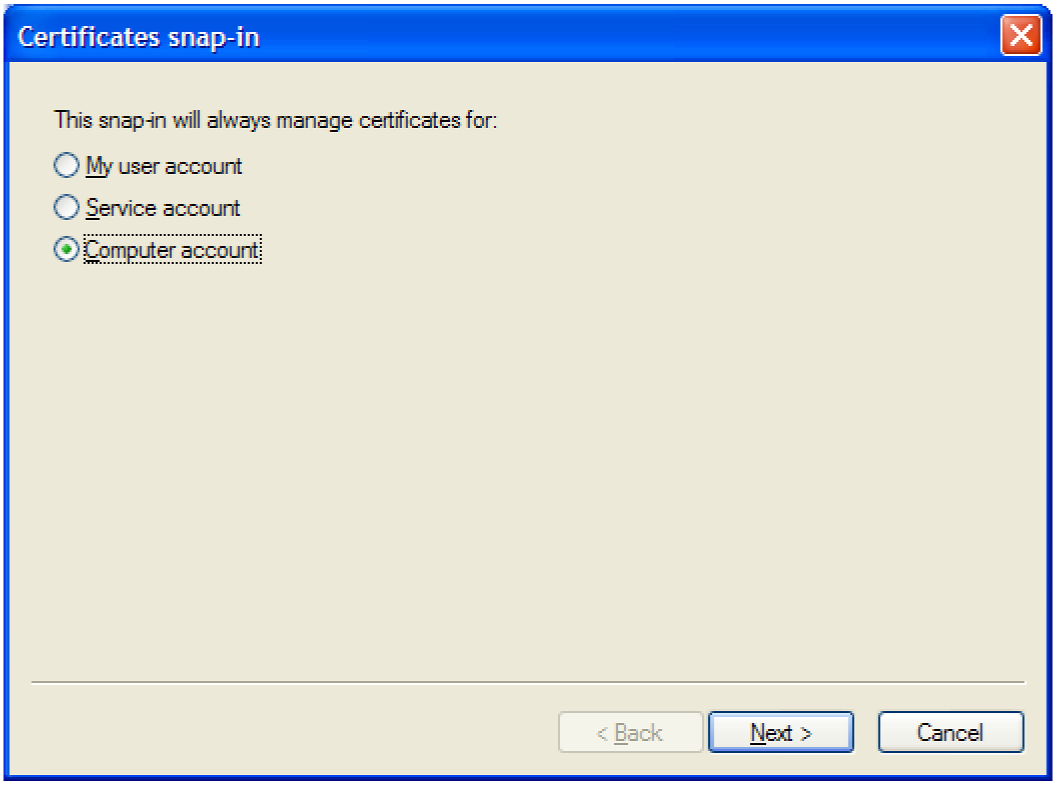
The following screen appears. Select “**Certificates**” and click the “**Add**” button.



Snap-in	Vendor
.NET Framework 2.0 Configuration	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Executi...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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



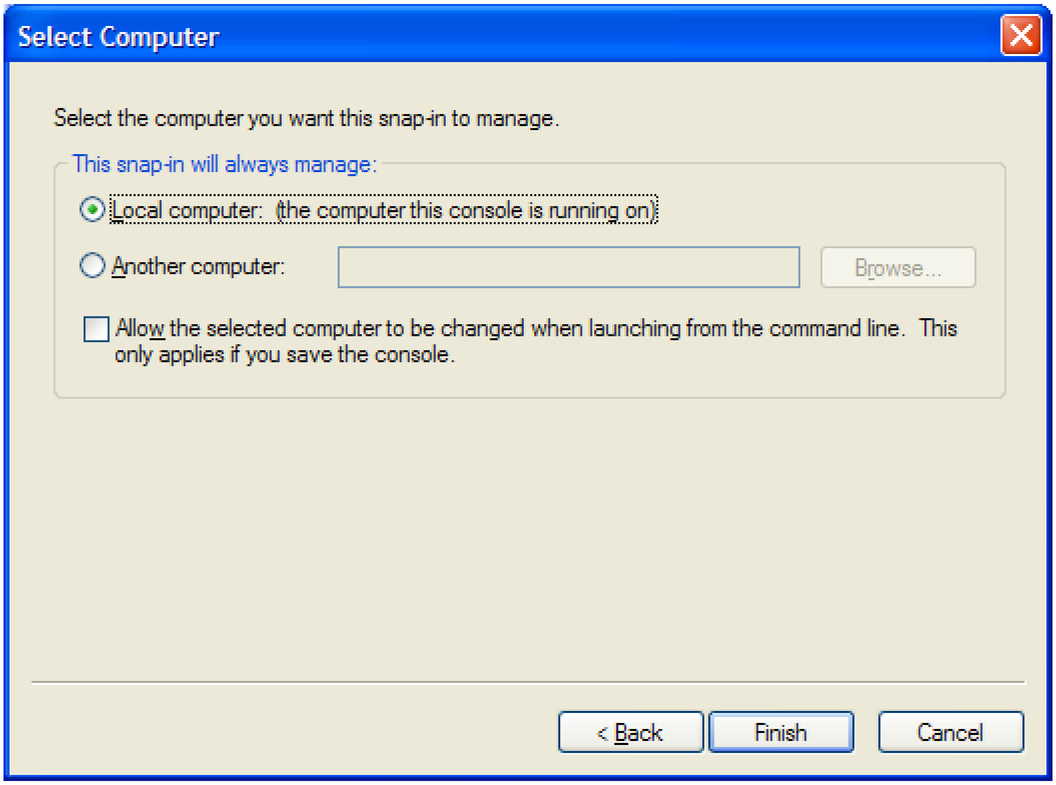
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

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



Select Computer

Select the computer you want this snap-in to manage.

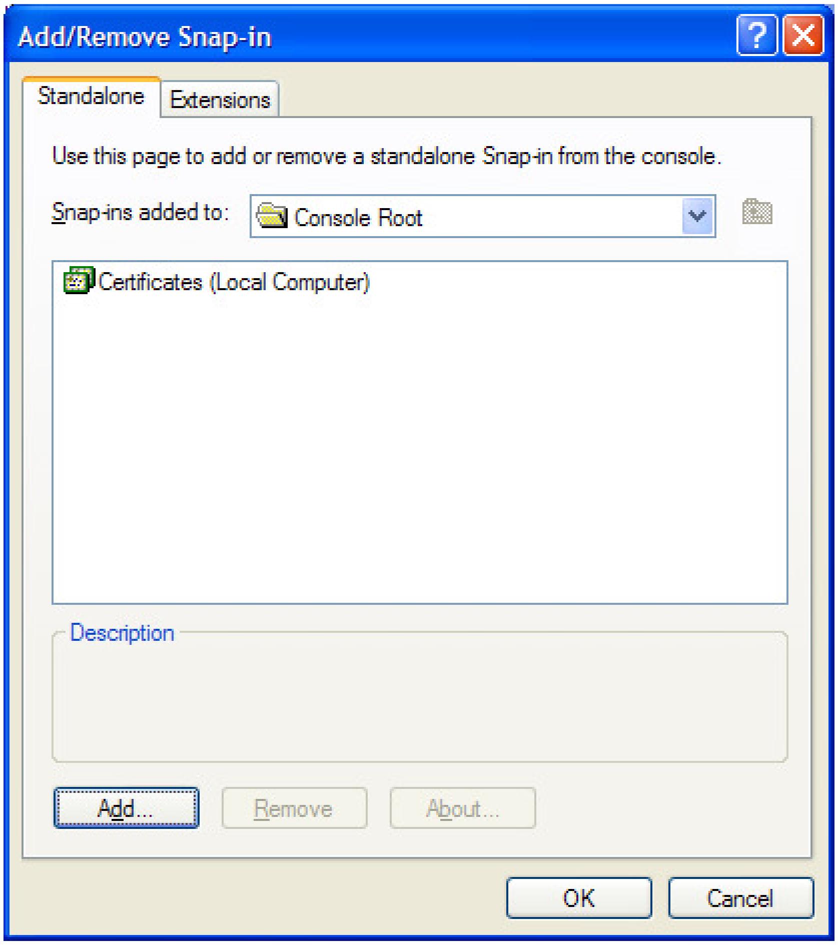
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Click “**Close**” on the “**Add Standalone Snap-In**” screen. The “**Add/Remove Snap-In**” screen appears as shown below with “**Certificates (Local Comuter)**” item listed in the list of snap-ins. Click “**OK**”.

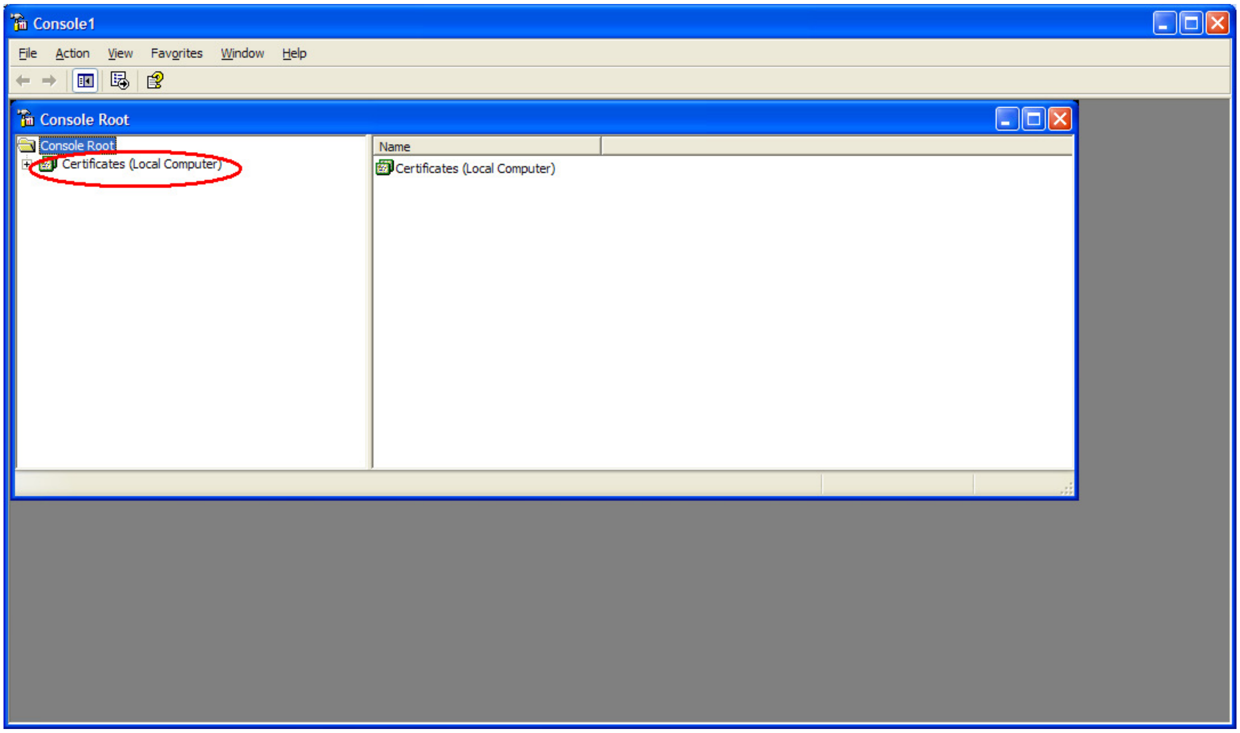


Use this page to add or remove a standalone Snap-in from the console.

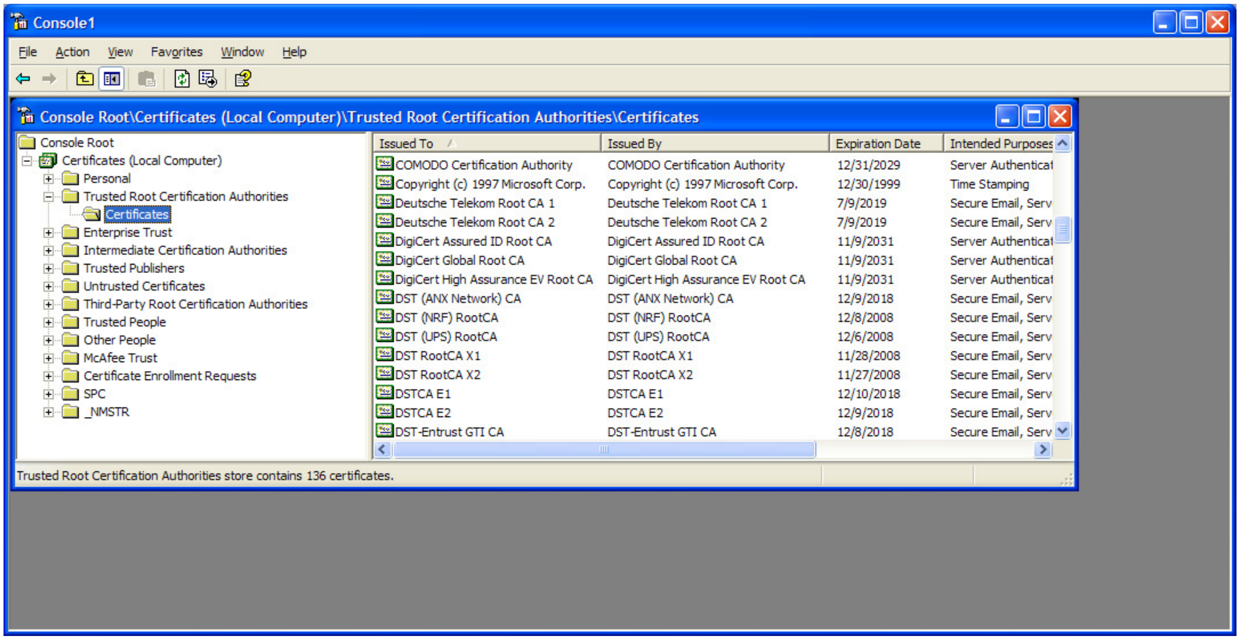
Snap-ins added to: Console Root

Certificates (Local Computer)

The following screen appears. 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 three steps correctly.



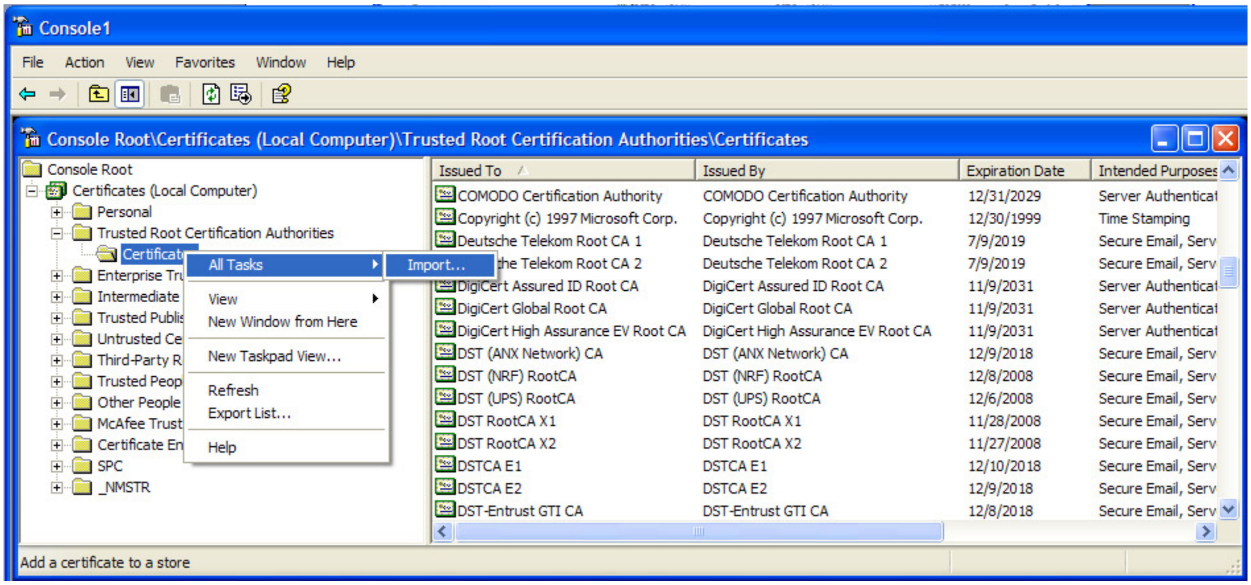
Navigate to "**Console Root -> Certificates (Local Computer)-> Trusted Root Certification Authorities -> Certificates**"


Console1
File
Action
View
Favorites
Window
Help
Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
McAfee Trust
Certificate Enrollment Requests
SPC
_NMSTR

Issued To	Issued By	Expiration Date	Intended Purposes
COMODO Certification Authority	COMODO Certification Authority	12/31/2029	Server Authenticat
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Deutsche Telekom Root CA 1	Deutsche Telekom Root CA 1	7/9/2019	Secure Email, Serv
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serv
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticat
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticat
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	11/9/2031	Server Authenticat
DST (ANX Network) CA	DST (ANX Network) CA	12/9/2018	Secure Email, Serv
DST (NRF) RootCA	DST (NRF) RootCA	12/8/2008	Secure Email, Serv
DST (UPS) RootCA	DST (UPS) RootCA	12/6/2008	Secure Email, Serv
DST RootCA X1	DST RootCA X1	11/28/2008	Secure Email, Serv
DST RootCA X2	DST RootCA X2	11/27/2008	Secure Email, Serv
DSTCA E1	DSTCA E1	12/10/2018	Secure Email, Serv
DSTCA E2	DSTCA E2	12/9/2018	Secure Email, Serv
DST-Entrust GTI CA	DST-Entrust GTI CA	12/8/2018	Secure Email, Serv

Trusted Root Certification Authorities store contains 136 certificates.

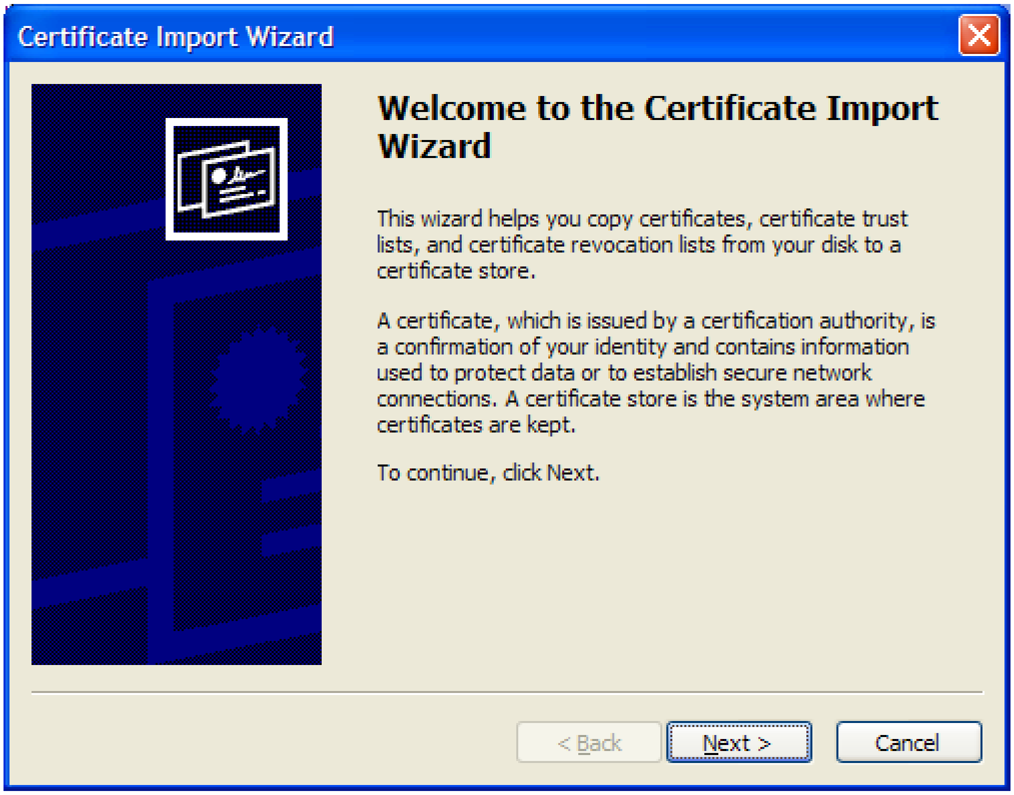
Right mouse click on “**Console Root -> Certificates (Local Computer)-> Trusted Root Certification Authorities -> Certificates**” and select “**All Tasks -> Import…**”



Issued To	Issued By	Expiration Date	Intended Purposes
COMODO Certification Authority	COMODO Certification Authority	12/31/2029	Server Authenticat
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Deutsche Telekom Root CA 1	Deutsche Telekom Root CA 1	7/9/2019	Secure Email, Serv
the Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serv
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticat
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticat
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	11/9/2031	Server Authenticat
DST (ANX Network) CA	DST (ANX Network) CA	12/9/2018	Secure Email, Serv
DST (NRF) RootCA	DST (NRF) RootCA	12/8/2008	Secure Email, Serv
DST (UPS) RootCA	DST (UPS) RootCA	12/6/2008	Secure Email, Serv
DST RootCA X1	DST RootCA X1	11/28/2008	Secure Email, Serv
DST RootCA X2	DST RootCA X2	11/27/2008	Secure Email, Serv
DSTCA E1	DSTCA E1	12/10/2018	Secure Email, Serv
DSTCA E2	DSTCA E2	12/9/2018	Secure Email, Serv
DST-Entrust GTI CA	DST-Entrust GTI CA	12/8/2018	Secure Email, Serv

Add a certificate to a store

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



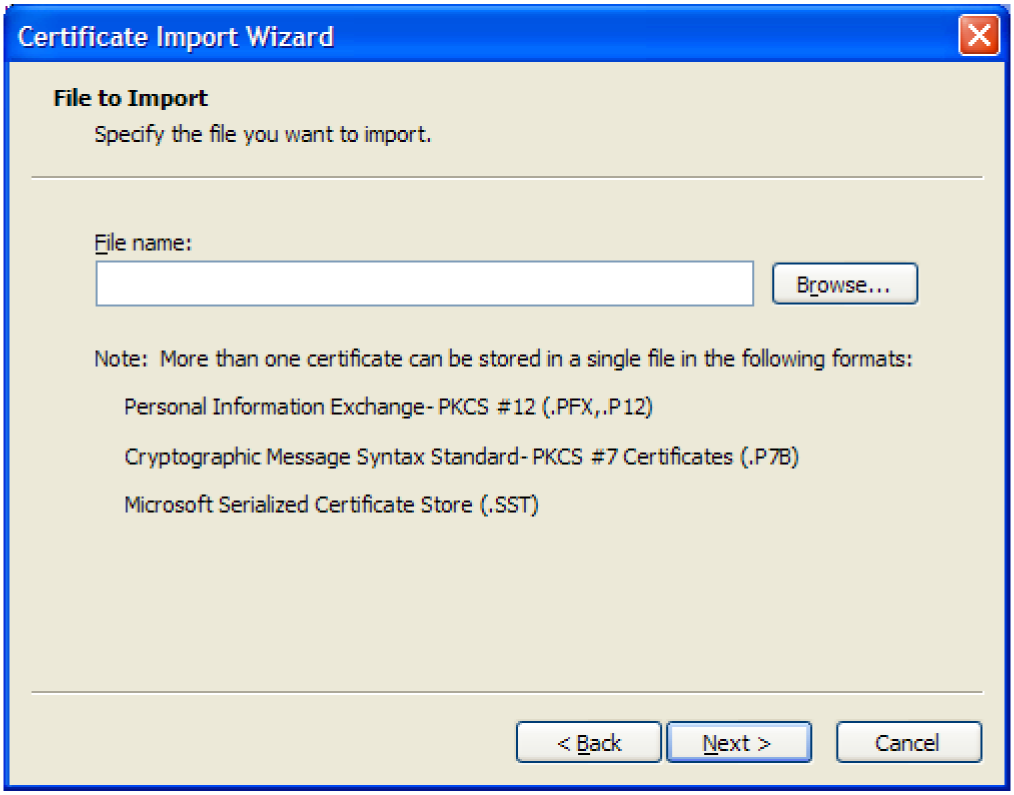
Welcome to the Certificate Import Wizard

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.

The following screen appears. Click the "**Browse…**" button



File to Import

Specify the file you want to import.

File name:

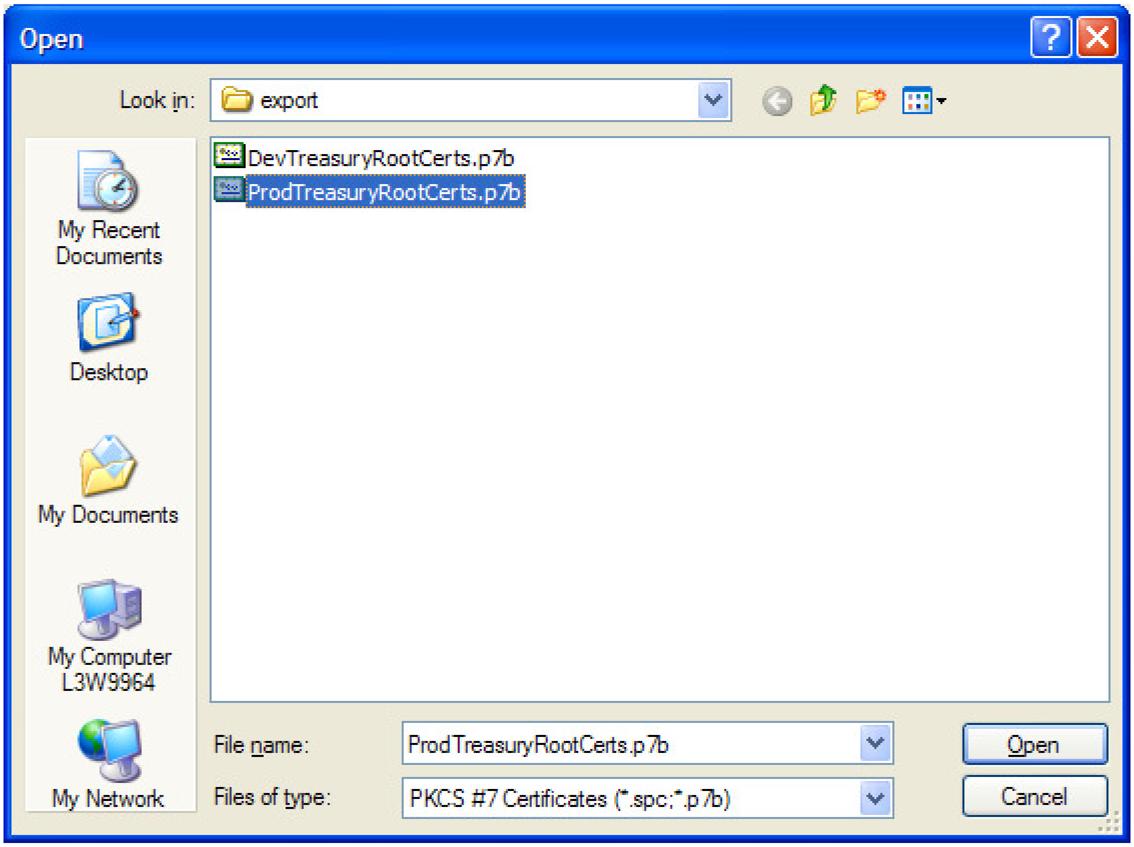
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

Set the file type filter to "**PKCS #7 Certificates (*.spc; *.p7b)**" and navigate to the file containing the production root certificates exported previously in task 2. Select the file and click "**Open**"



Look in: export

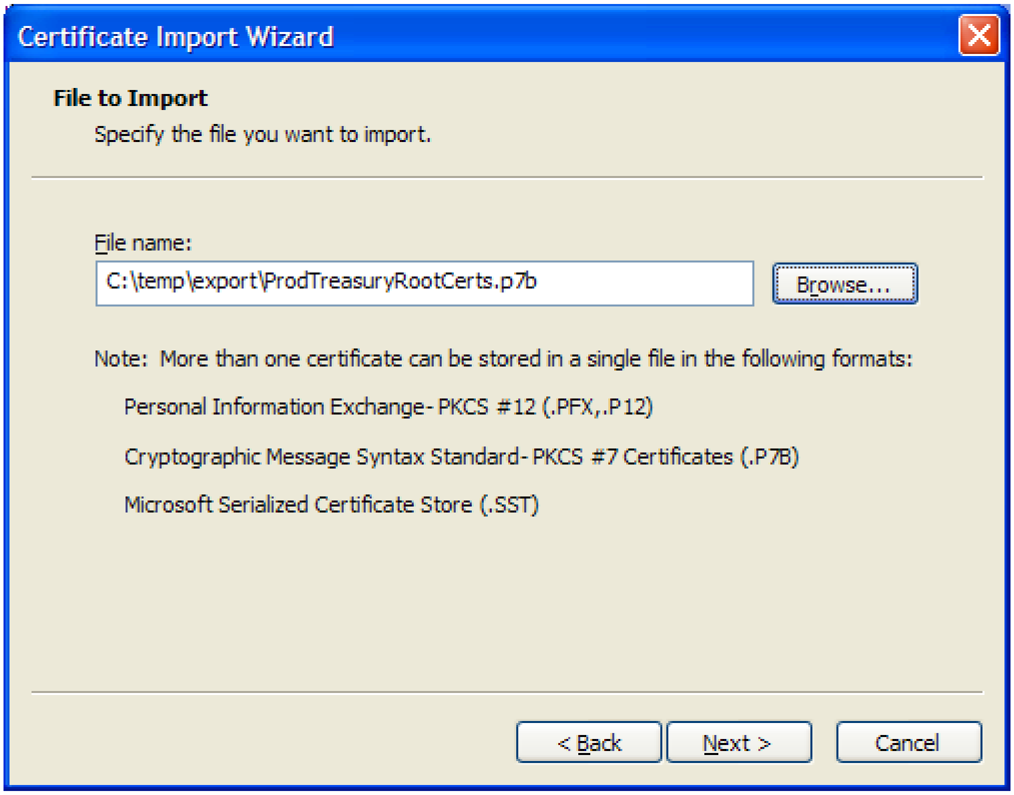
DevTreasuryRootCerts.p7b

ProdTreasuryRootCerts.p7b

File name: ProdTreasuryRootCerts.p7b

Files of type: PKCS #7 Certificates (*.spc;*.p7b)

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



File to Import

Specify the file you want to import.

File name:

C:\temp\export\ProdTreasuryRootCerts.p7b

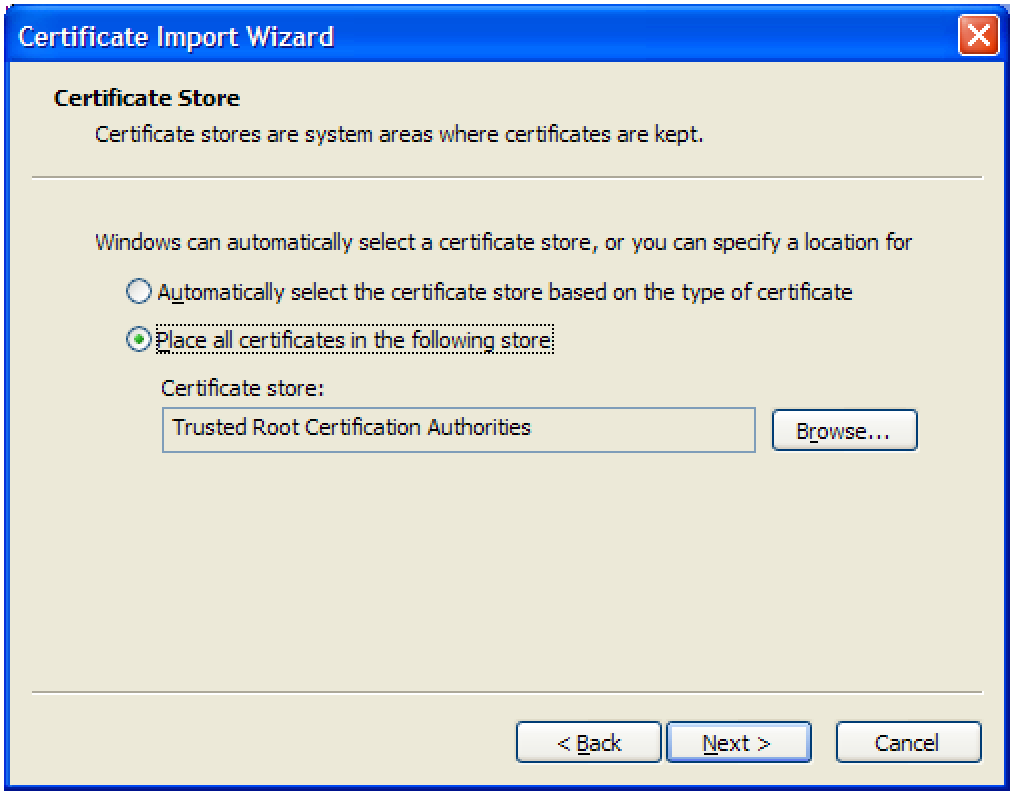
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

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



Certificate Store

Certificate stores are system areas where certificates are kept.

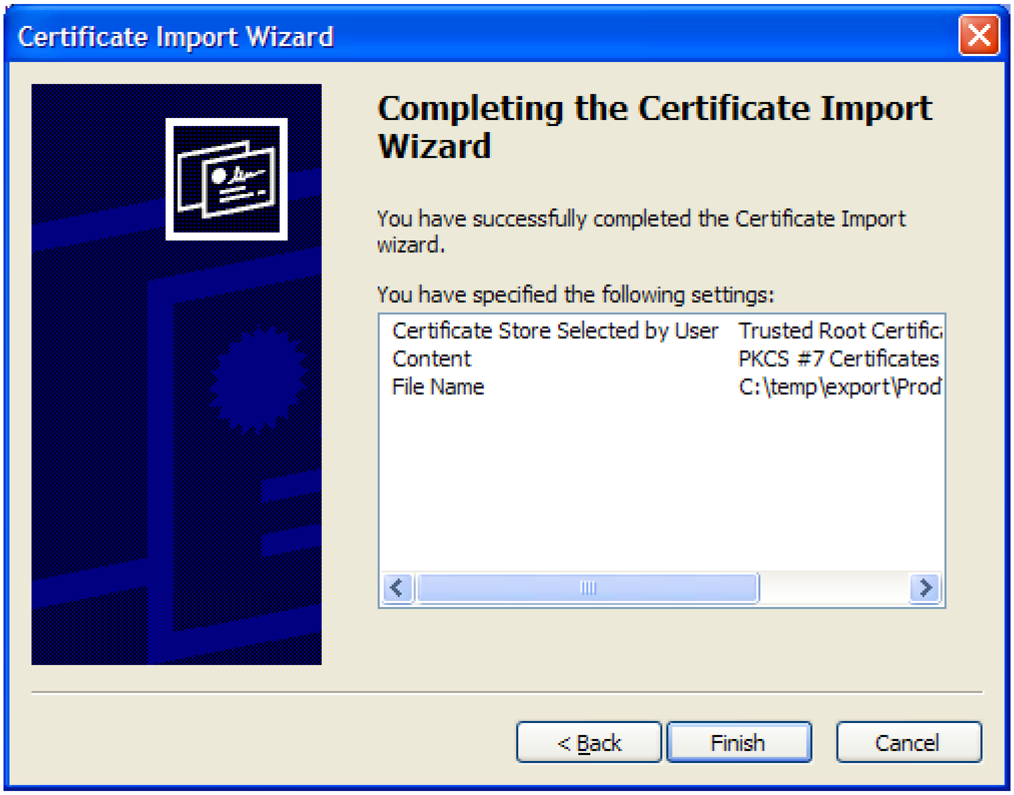
Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

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



Certificate Import Wizard

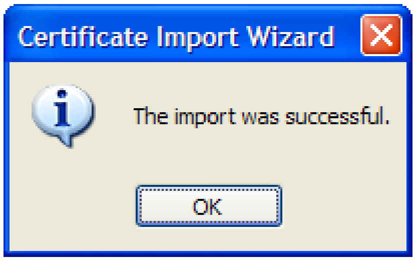
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	PKCS #7 Certificates
File Name	C:\temp\export\Prod

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



Certificate Import Wizard

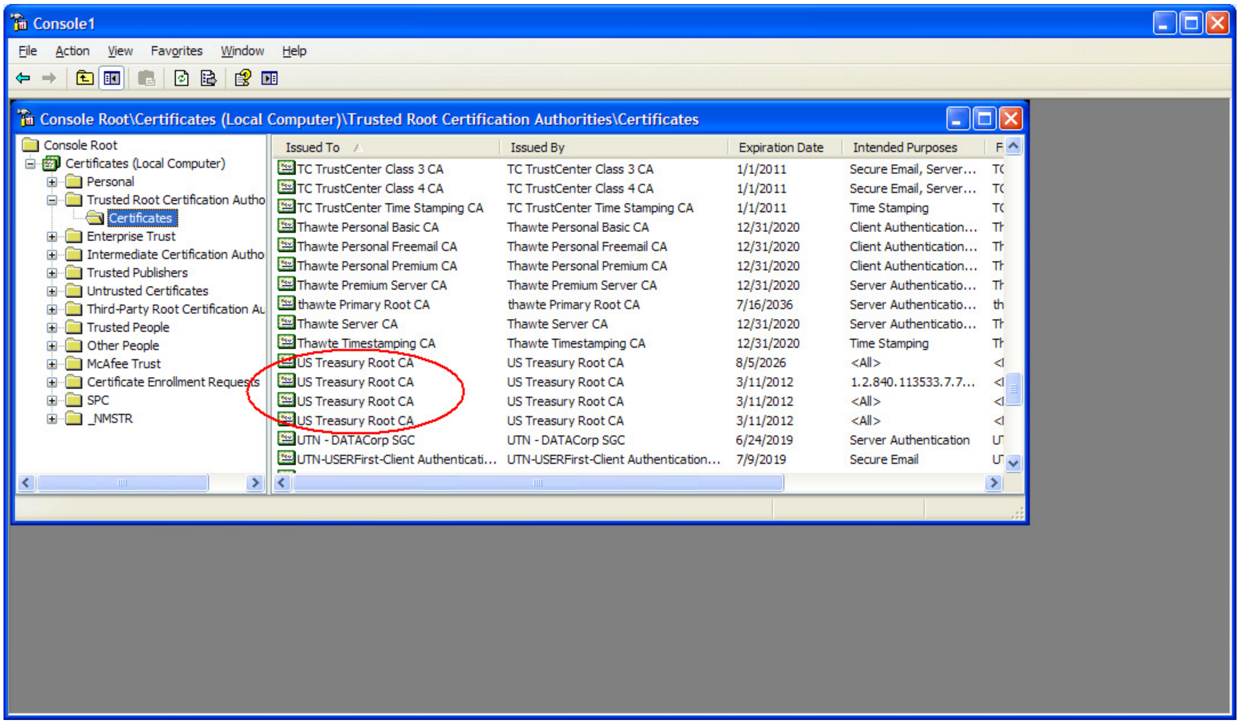
The import was successful.

Import the Development Treasury Root Certificate

Repeat the import process (pages 24-30) for the development root certificate container file exported in task 2 (DevTreasuryRootCerts.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

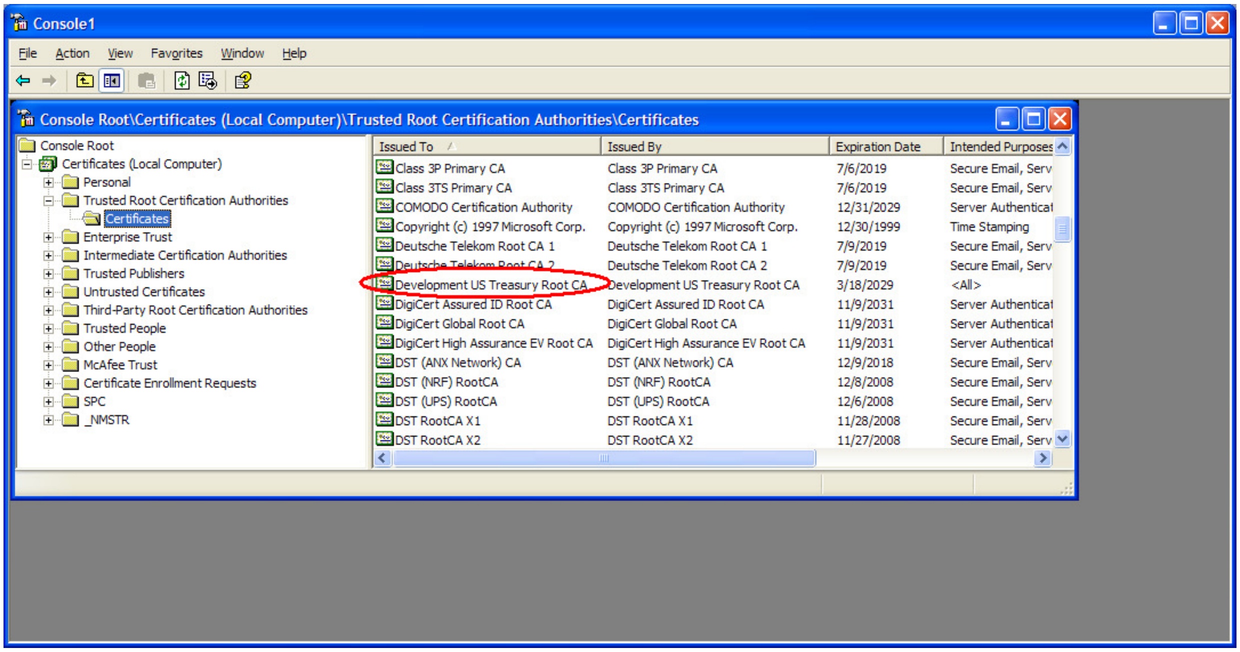
Verify that the “**US Treasury Root CA**” certificates were imported successfully into the “**Trusted Root Certification Authorities**” store of the **Local Computer**. See the certificates encircled in red below to verify.


Console1
File
Action
View
Favorites
Window
Help
Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Autho
Certificates
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Other People
McAfee Trust
Certificate Enrollment Requests
SPC
_NMSTR

Issued To	Issued By	Expiration Date	Intended Purposes	F
TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server...	TC
TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server...	TC
TC TrustCenter Time Stamping CA	TC TrustCenter Time Stamping CA	1/1/2011	Time Stamping	TC
Thawte Personal Basic CA	Thawte Personal Basic CA	12/31/2020	Client Authentication...	Th
Thawte Personal Freemail CA	Thawte Personal Freemail CA	12/31/2020	Client Authentication...	Th
Thawte Personal Premium CA	Thawte Personal Premium CA	12/31/2020	Client Authentication...	Th
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticatio...	Th
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticatio...	th
Thawte Server CA	Thawte Server CA	12/31/2020	Server Authenticatio...	Th
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Th
US Treasury Root CA	US Treasury Root CA	8/5/2026	<All>	<I
US Treasury Root CA	US Treasury Root CA	3/11/2012	1.2.840.113533.7.7...	<I
US Treasury Root CA	US Treasury Root CA	3/11/2012	<All>	<I
US Treasury Root CA	US Treasury Root CA	3/11/2012	<All>	<I
UTN - DATACorp SGC	UTN - DATACorp SGC	6/24/2019	Server Authentication	UT
UTN-USERFirst-Client Authenticati...	UTN-USERFirst-Client Authentication...	7/9/2019	Secure Email	UT

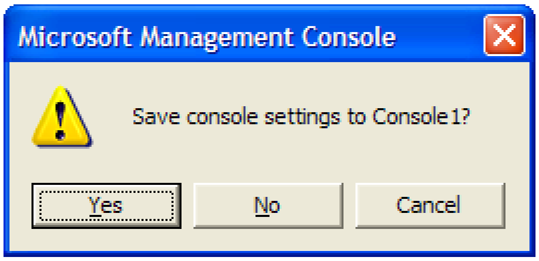
Verify installation of Development Treasury Root Certificate

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.


Console1
File
Action
View
Favorites
Window
Help
Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
McAfee Trust
Certificate Enrollment Requests
SPC
_NMSTR

Issued To	Issued By	Expiration Date	Intended Purposes
Class 3P Primary CA	Class 3P Primary CA	7/6/2019	Secure Email, Serv
Class 3TS Primary CA	Class 3TS Primary CA	7/6/2019	Secure Email, Serv
COMODO Certification Authority	COMODO Certification Authority	12/31/2029	Server Authenticat
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
Deutsche Telekom Root CA 1	Deutsche Telekom Root CA 1	7/9/2019	Secure Email, Serv
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/9/2019	Secure Email, Serv
Development US Treasury Root CA	Development US Treasury Root CA	3/18/2029	<All>
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticat
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticat
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	11/9/2031	Server Authenticat
DST (ANX Network) CA	DST (ANX Network) CA	12/9/2018	Secure Email, Serv
DST (NRF) RootCA	DST (NRF) RootCA	12/8/2008	Secure Email, Serv
DST (UPS) RootCA	DST (UPS) RootCA	12/6/2008	Secure Email, Serv
DST RootCA X1	DST RootCA X1	11/28/2008	Secure Email, Serv
DST RootCA X2	DST RootCA X2	11/27/2008	Secure Email, Serv

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



Save console settings to Console1?

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