Oracle® Enterprise Single Sign-on Anywhere

How-To: Creating and Exporting an SSL Certificate
for ESSO-Anywhere

Release 11.1.1.5.0

21024-01

March 2011

Oracle Enterprise Single Sign-on Anywhere How-To: Creating and Exporting an SSL Certificate for ESSO-Anywhere

Release 11.1.1.5.0

21024-01

Table of Contents

Introduction

About This Guide

This document describes how to create and export an SSL certificate for use with ESSO-Anywhere. Instructions for users of standalone and enterprise certificate authorities (CAs) are provided.
The instructions in this document apply to the following operating systems:

- For standalone CAs, Windows 2000 Server and Windows Server 2003 operating systems are supported in both Standard and Enterprise editions.
- For enterprise CAs, only Windows Server 2003 Enterprise Edition is supported. No other versions and/or editions are supported.

Prerequisites

Readers of this document should have a thorough understanding of the Windows server operating systems, SSL certificate technology, and related concepts.

Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

Term or Abbreviation	Description
ESSO-LM	Enterprise Single Sign-On Logon Manager
ESSO-Anywhere	Enterprise Single Sign-On Anywhere
Agent	ESSO-LM client-side software
Console	ESSO-LM Administrative Console

Accessing ESSO-Anywhere Documentation

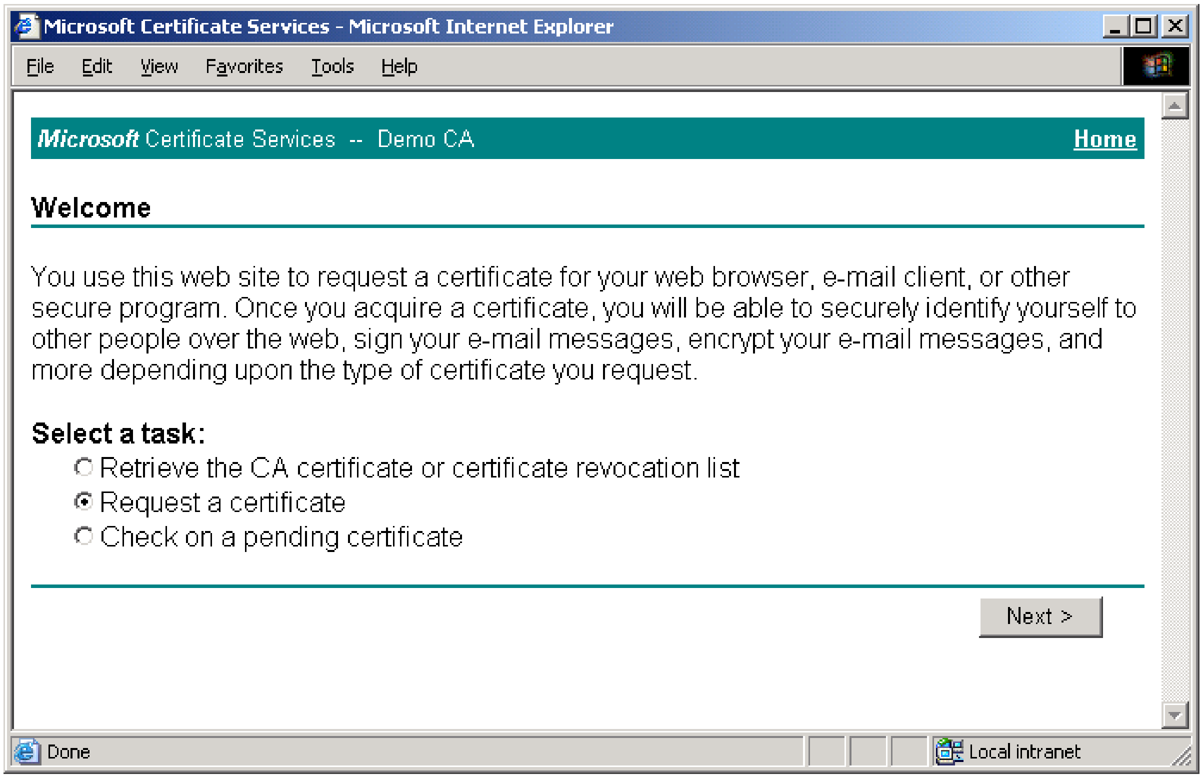
We continually strive to keep ESSO-Anywhere documentation accurate and up to date.
For the latest version of this and other ESSO-Anywhere documents, visit the following URL:

http://download.oracle.com/docs/cd/E21040_01/index.htm

Creating an SSL Certificate with a Standalone Certificate Authority

To create an SSL certificate on Windows Server 2000 and Windows Server 2003 using a standalone certificate authority, do the following:

1. Navigate to the Microsoft Certificate Server enrollment page by accessing the following URL in a Web browser:
   `http://<server>:<port>/certsrv`
2. In the page that appears, select **Request a Certificate** and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Home
Next >
Done
Local intranet

Microsoft Certificate Services -- Demo CA

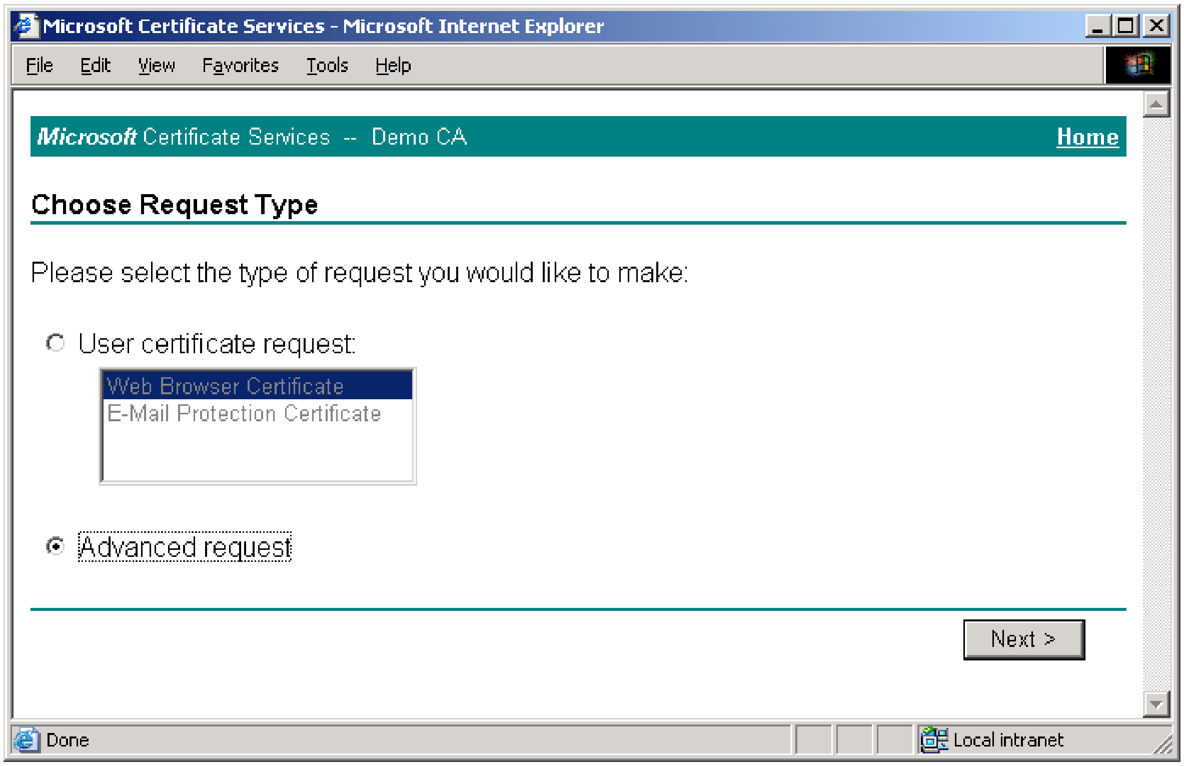
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

3. In the page that appears, select **Advanced request** and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Home
Next >
Done
Local intranet

Microsoft Certificate Services -- Demo CA

Choose Request Type

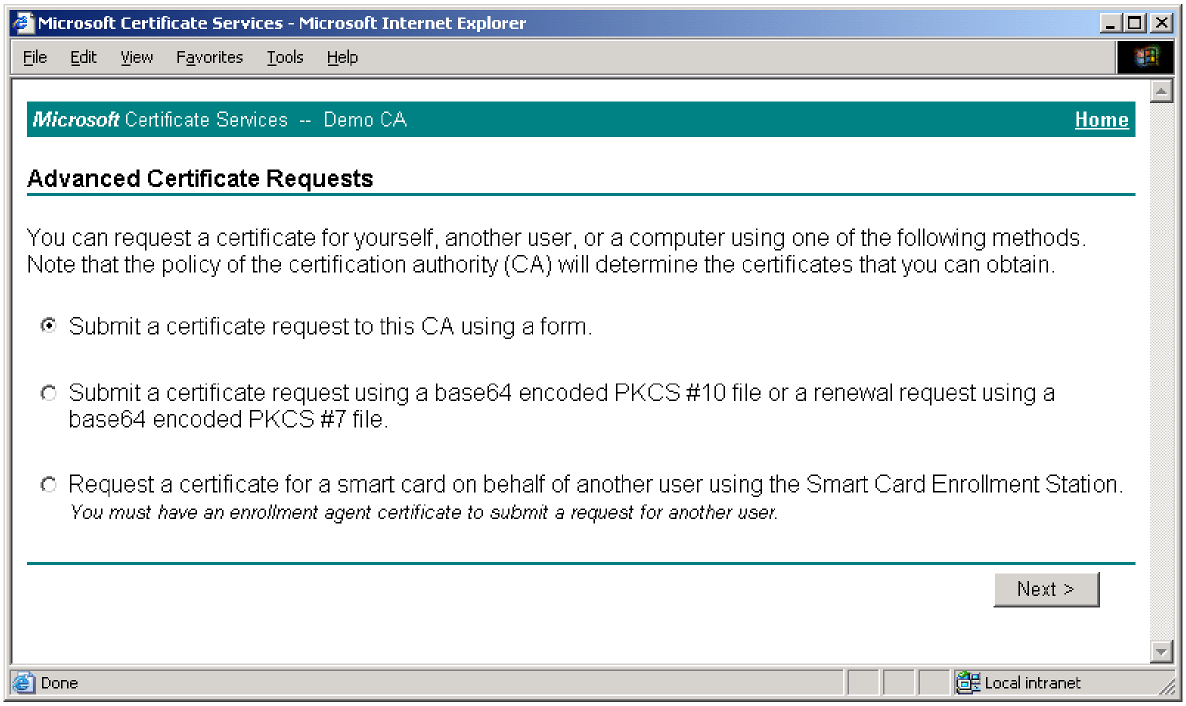
Please select the type of request you would like to make:

○ User certificate request:

Web Browser Certificate
E-Mail Protection Certificate

● Advanced request

4. In the page that appears, select **Submit a certificate request to this CA using a form**, and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Home
Next >
Done
Local intranet

Microsoft Certificate Services -- Demo CA

Advanced Certificate Requests

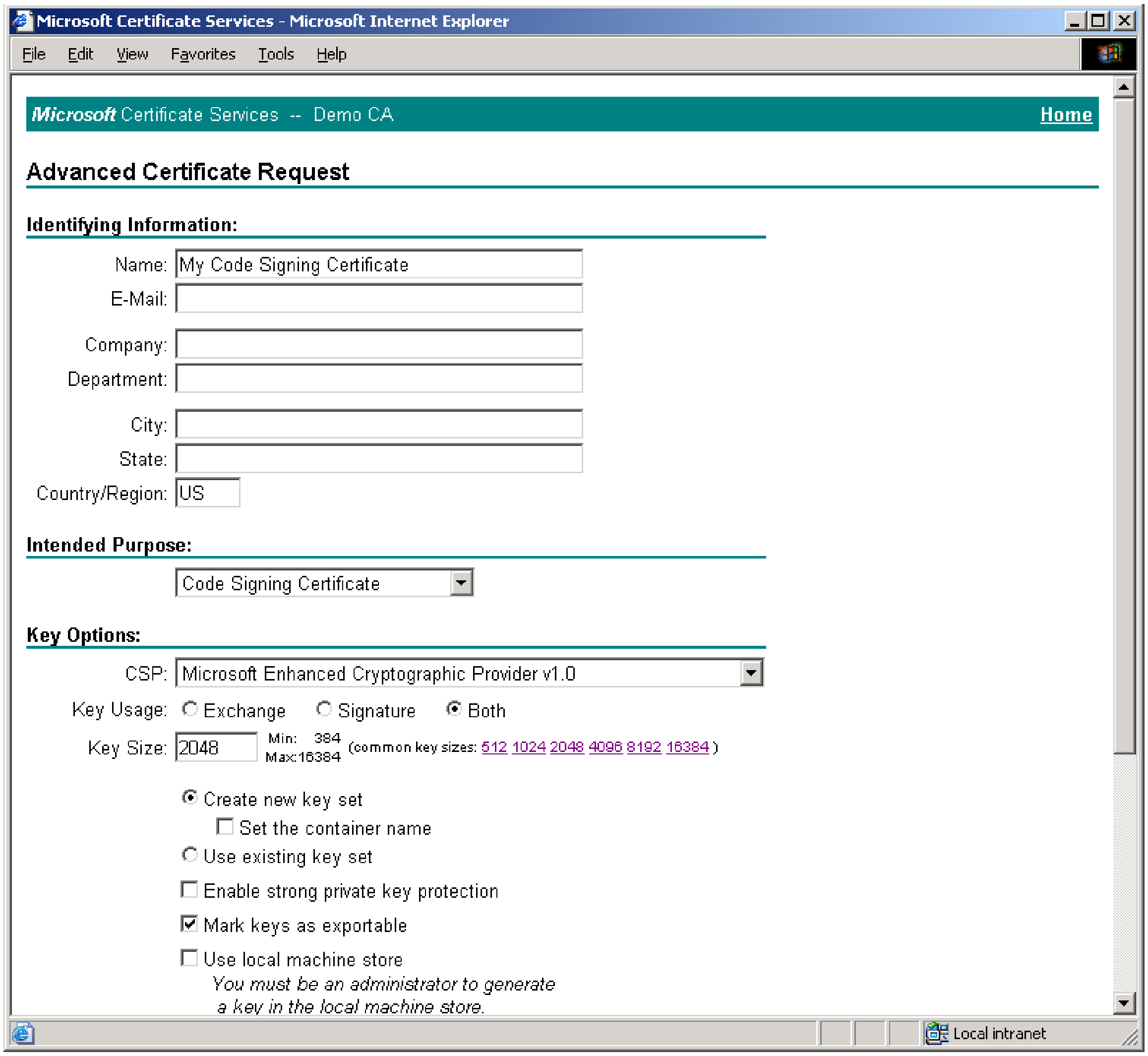
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

● Submit a certificate request to this CA using a form.

○ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

5. In the page that appears, do the following:
   a. Fill in the fields in the “Identifying Information” section as appropriate.
   b. In the “Intended Purpose” drop-down list, select **Code Signing Certificate**.
   c. In the “Key Options” section, make the choices appropriate to your environment.
   d. Click **Submit**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home
Local intranet

Advanced Certificate Request

Identifying Information:

Name: My Code Signing Certificate
E-Mail:
Company:
Department:
City:
State:
Country/Region: US

Intended Purpose:

Code Signing Certificate

Key Options:

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ○ Exchange ○ Signature ● Both

Key Size: 2048 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Create new key set

□ Set the container name

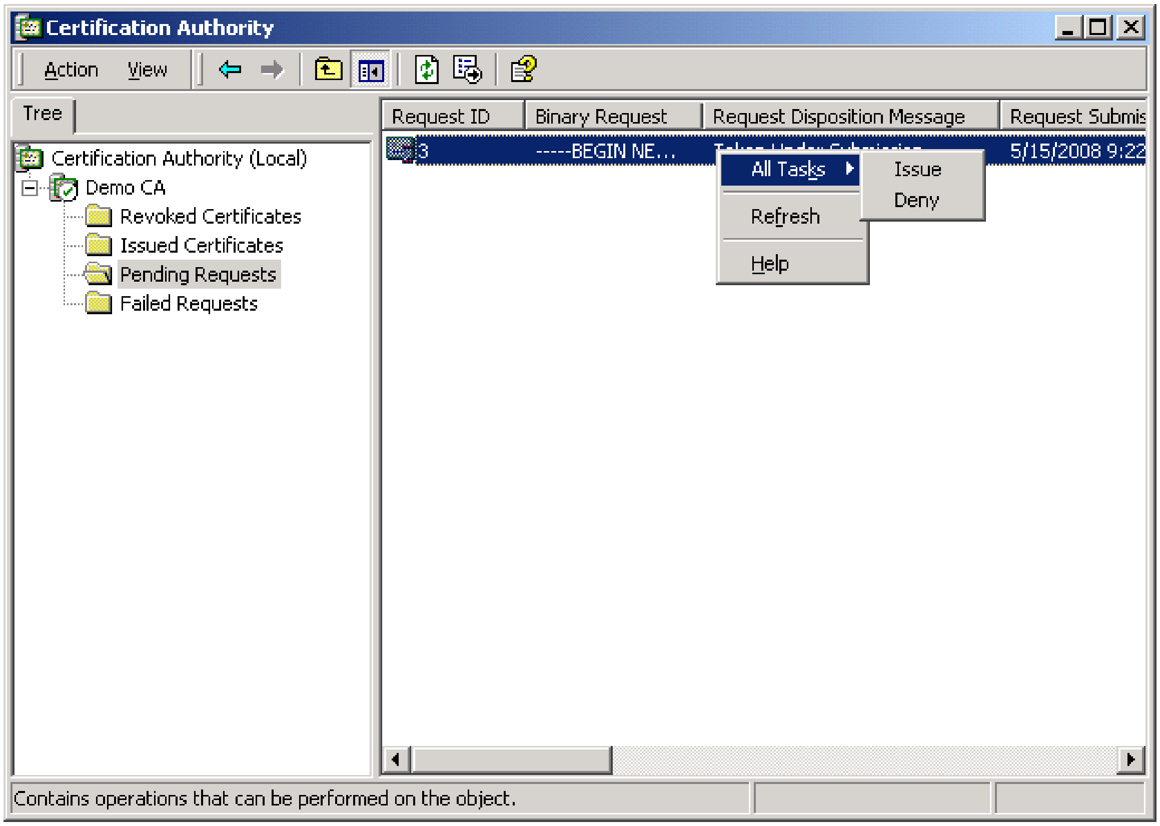
○ Use existing key set

□ Enable strong private key protection

☑ Mark keys as exportable

□ Use local machine store
You must be an administrator to generate a key in the local machine store.

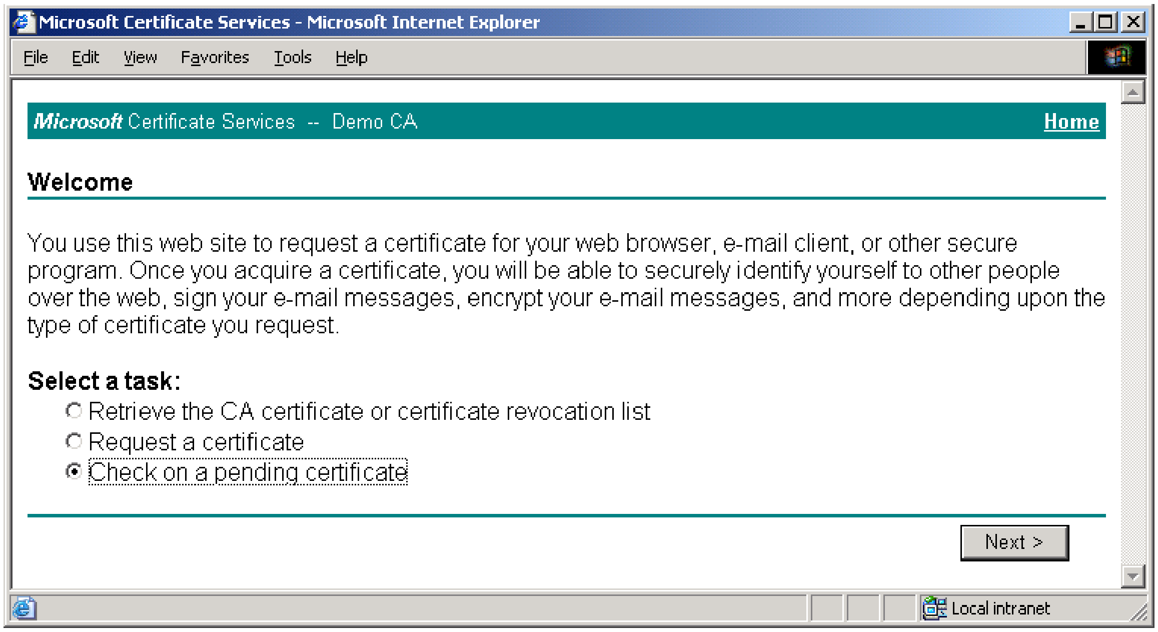
6. Depending on whether you have direct control over the certificate authority, do one of the following:
   - If you do not have direct control over the CA, wait until the certificate is approved by the CA administrator, then proceed to the next step.
   - If you have direct control over the CA, approve the certificate using the Certificate Authority tool, as shown below:



Request ID	Binary Request	Request Disposition Message	Request Submis
3	-----BEGIN NE...	Taken Under Submission	5/15/2008 9:22

Contains operations that can be performed on the object.

7. Once the certificate request has been approved, return to Microsoft Certificate Server's enrollment page, select **Check on a pending certificate**, and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home

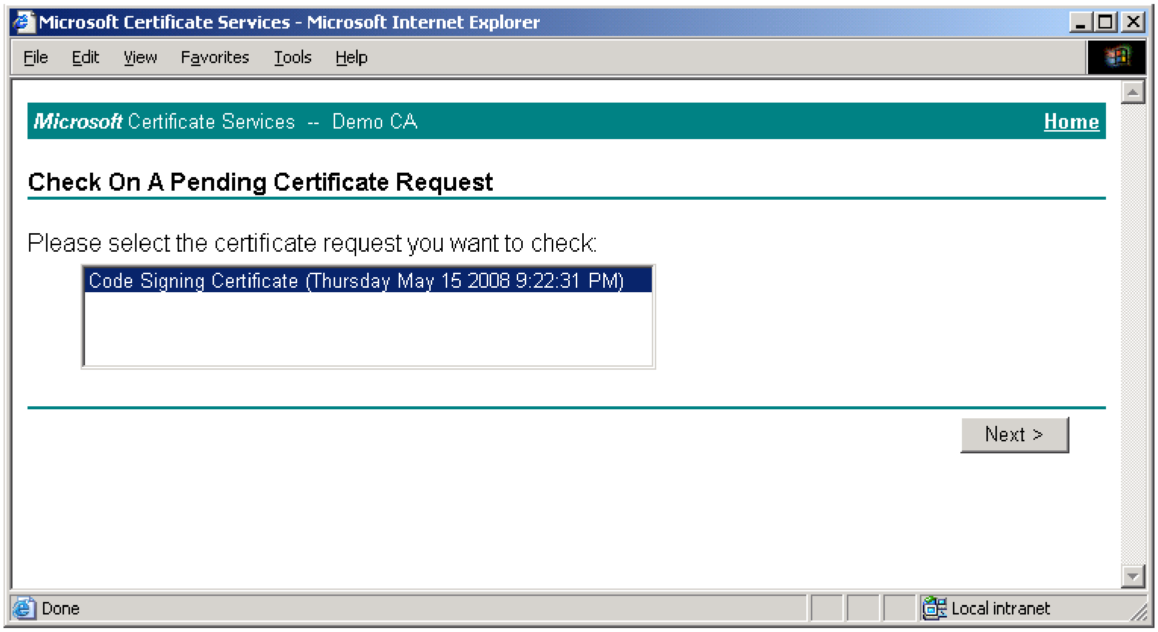
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
○ Request a certificate
● Check on a pending certificate

8. In the page that appears, select the target certificate request and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home

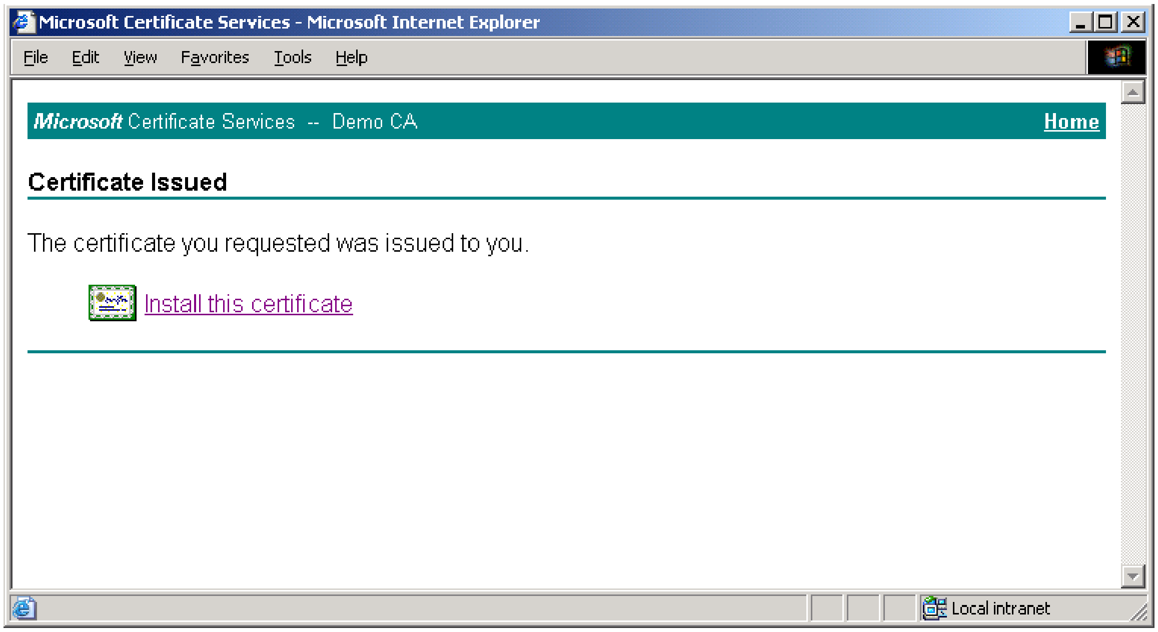
Check On A Pending Certificate Request

Please select the certificate request you want to check:

Code Signing Certificate (Thursday May 15 2008 9:22:31 PM)

Next >
Done
Local intranet

9. In the page that appears, click the **Install the certificate** link.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Home
Local intranet

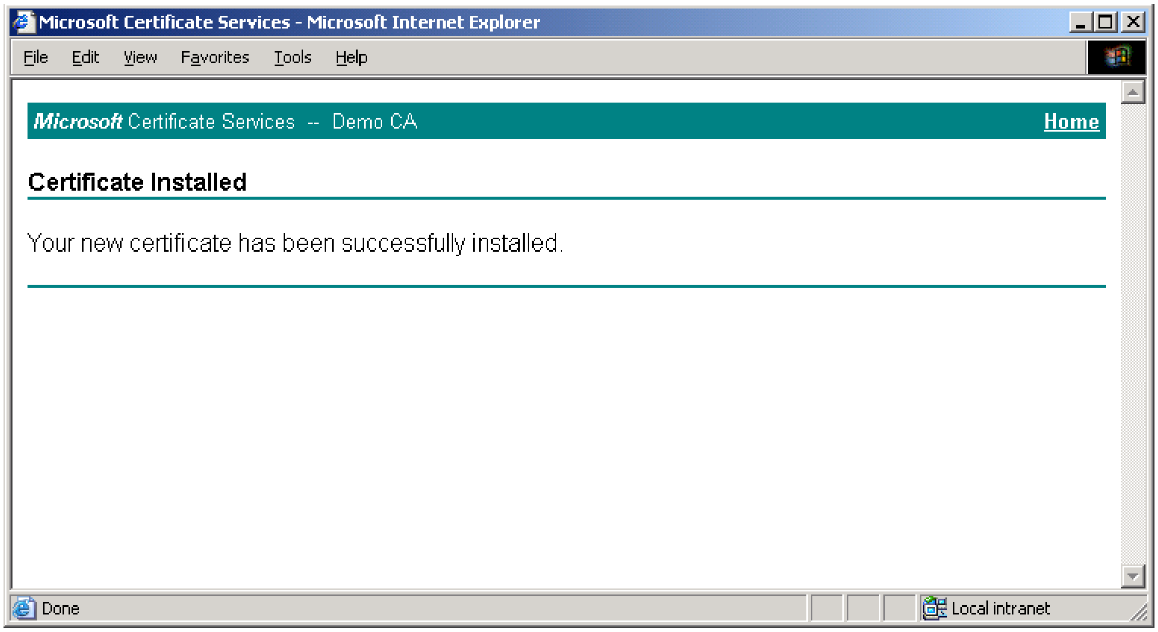
Microsoft Certificate Services -- Demo CA

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

When the certificate is successfully installed, a confirmation page appears:



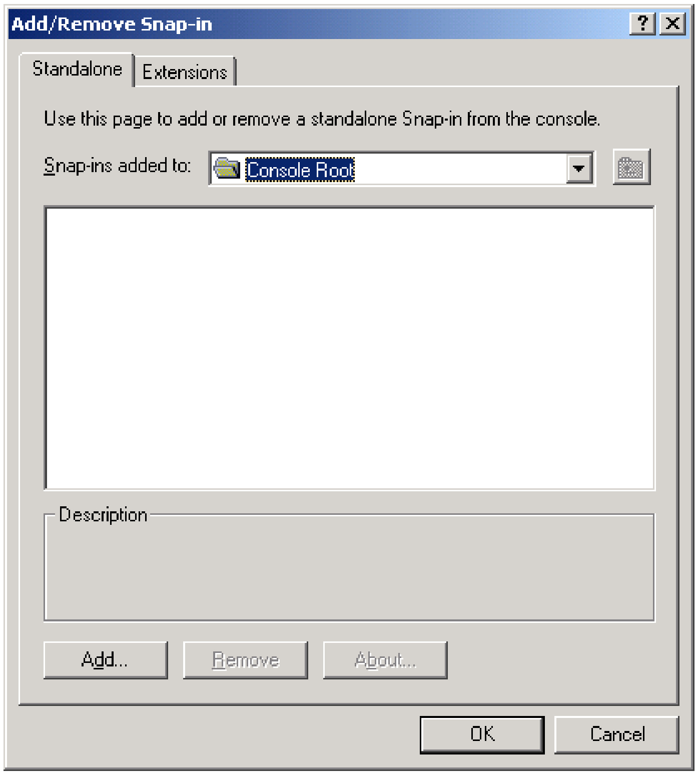
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Home
Done
Local intranet

Microsoft Certificate Services -- Demo CA

Certificate Installed

Your new certificate has been successfully installed.

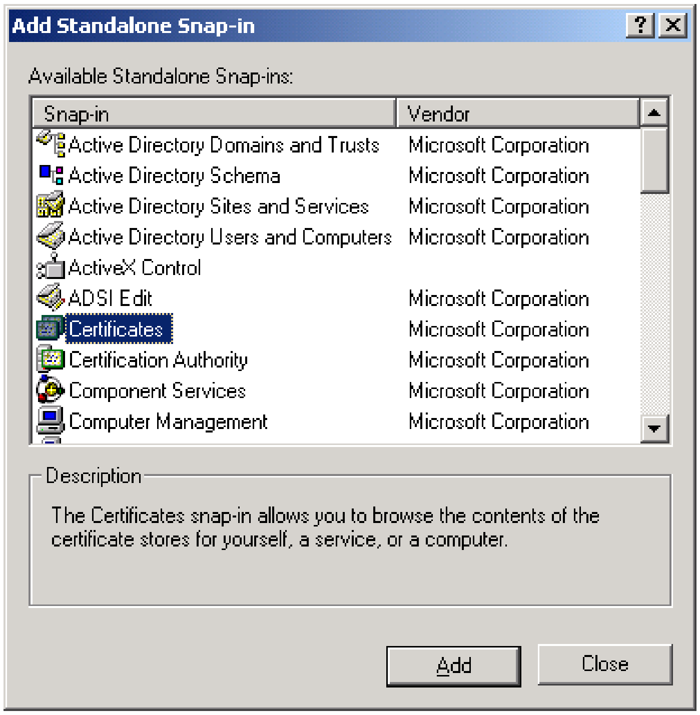
10. Launch the Microsoft Management Console.
11. In the console, add the “Certificates” snap-in:
    a. From the **Console** menu, select **Add/Remove Snap-in**.
    b. In the dialog that appears, click **Add**.



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

Snap-ins added to: Console Root

    c. In the list that appears, select **Certificates** and click **Add**.

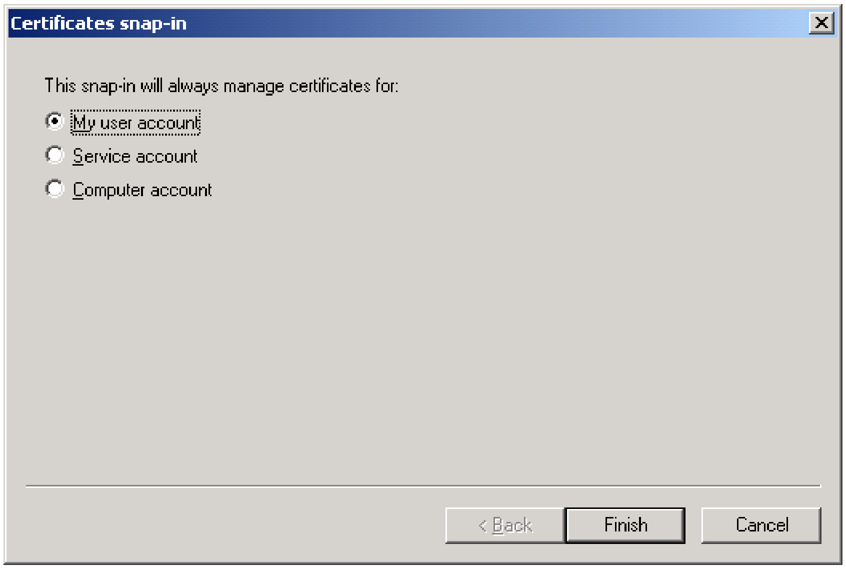


Available Standalone Snap-ins:

Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Schema	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
ADSI Edit	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation

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

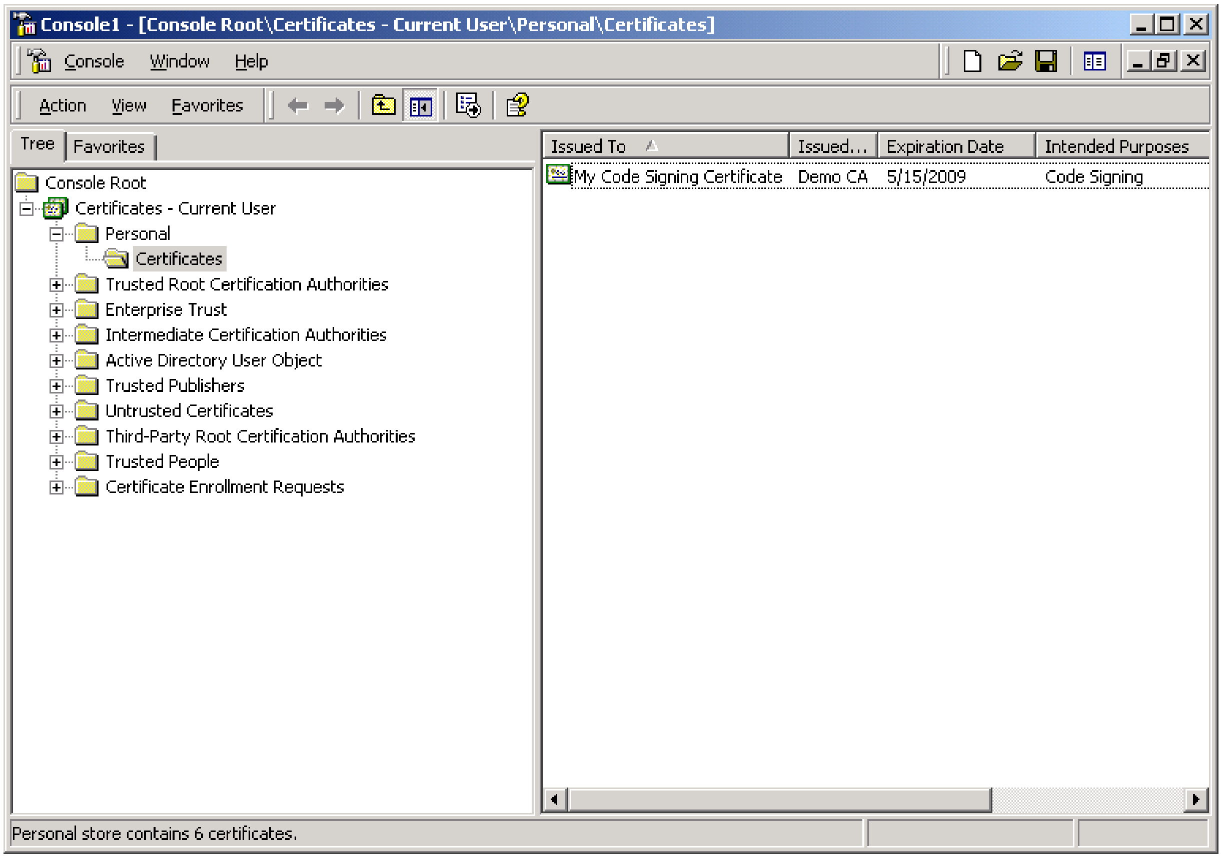
d. In the dialog that appears, select **My user account** and click **Finish**.



This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

12. Close the remaining open dialog boxes inside the Management Console.
13. In the tree in the left-hand pane, navigate to:
    Certificates – Current User → Personal → Certificates.

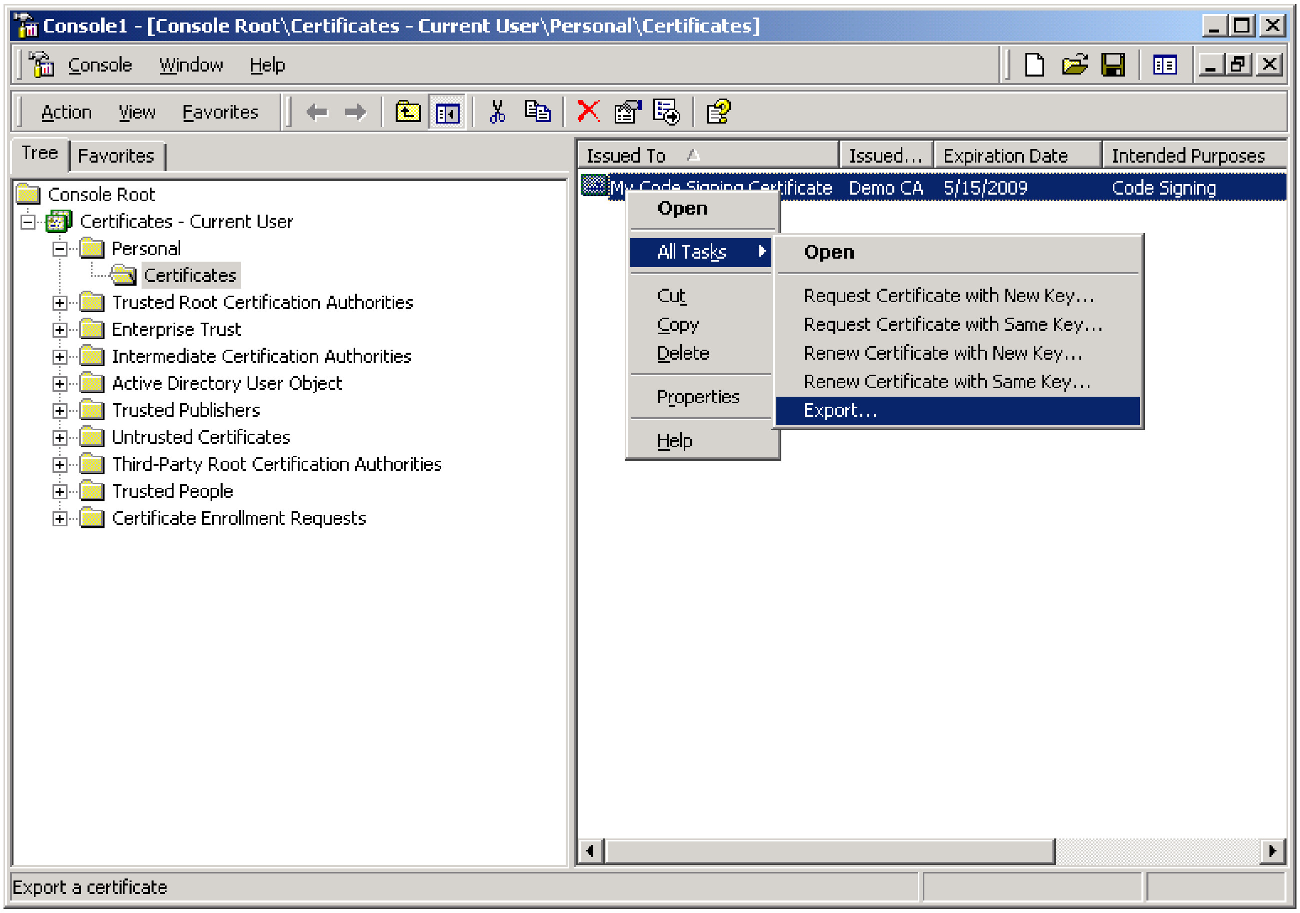

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
Console
Window
Help
Action
View
Favorites
Tree
Favorites

- Console Root
  - Certificates - Current User
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Certificate Enrollment Requests

Issued To	Issued...	Expiration Date	Intended Purposes
My Code Signing Certificate	Demo CA	5/15/2009	Code Signing

Personal store contains 6 certificates.

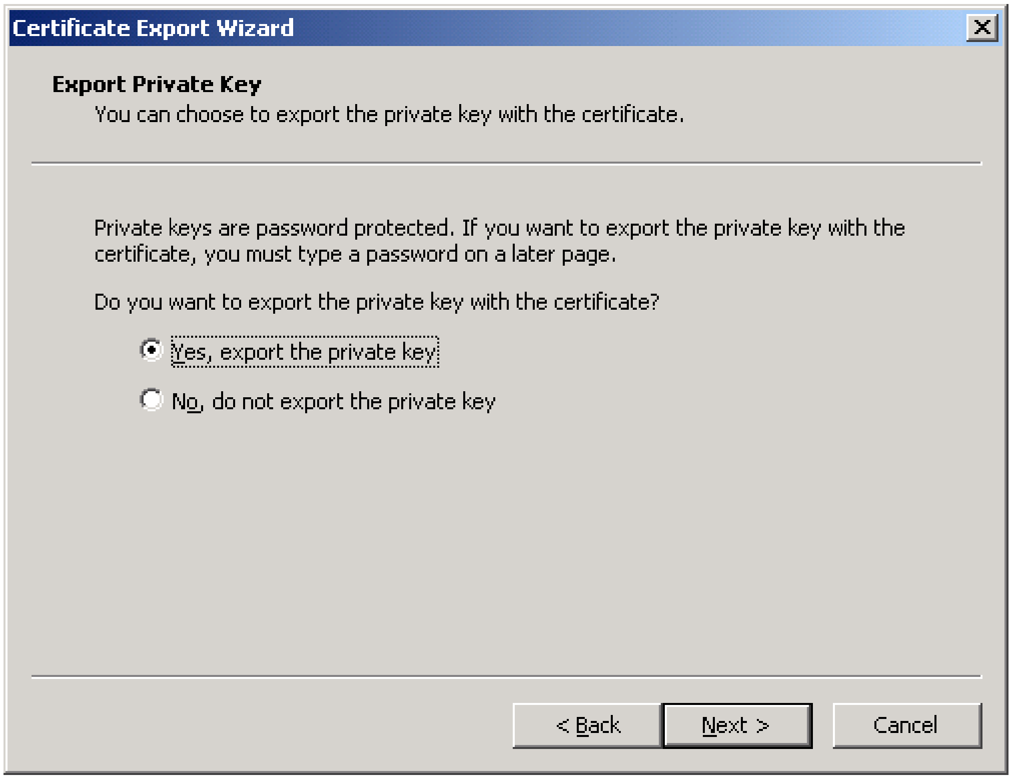
14. In the right-hand pane, right-click the desired certificate, then select **All Tasks → Export** from the context menu.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key…
Request Certificate with Same Key…
Renew Certificate with New Key…
Renew Certificate with Same Key…
Export…
Export a certificate

Issued To	Issued…	Expiration Date	Intended Purposes
My Code Signing Certificate	Demo CA	5/15/2009	Code Signing

15. In the “Certificate Export Wizard” that appears, click **Next**.

16. In the “Export Private Key” screen, select **Yes, export the private key** and click **Next**.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

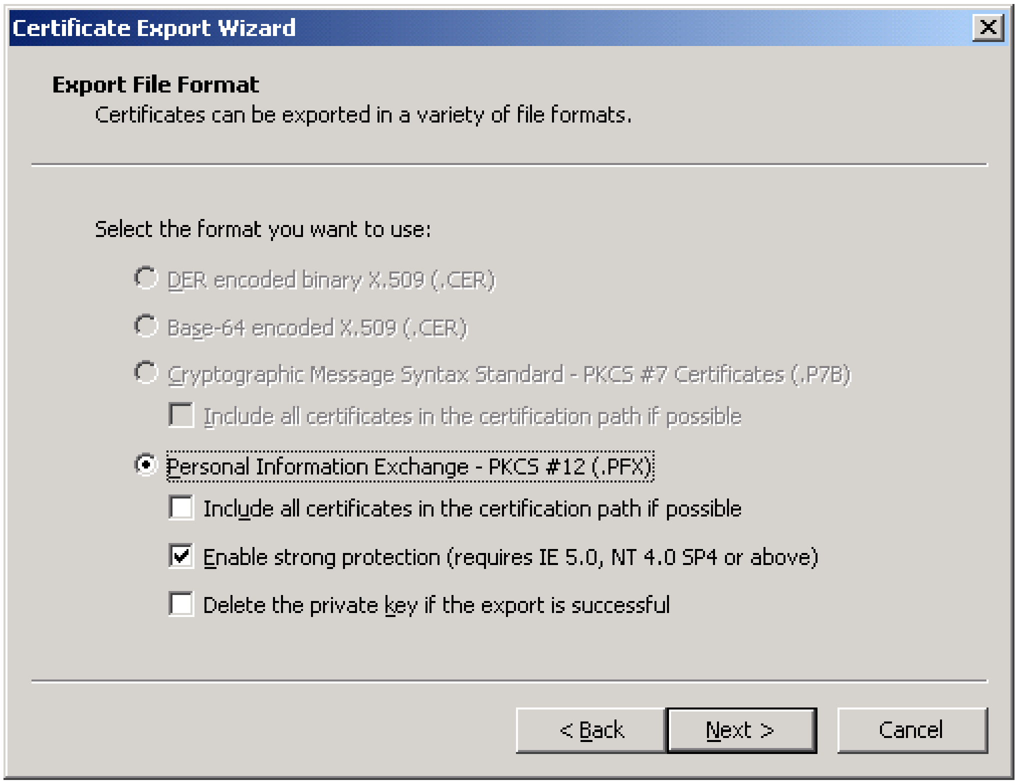
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

17. In the “Export File Format” screen, leave the options at their default values and click **Next**.



Certificate Export Wizard

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

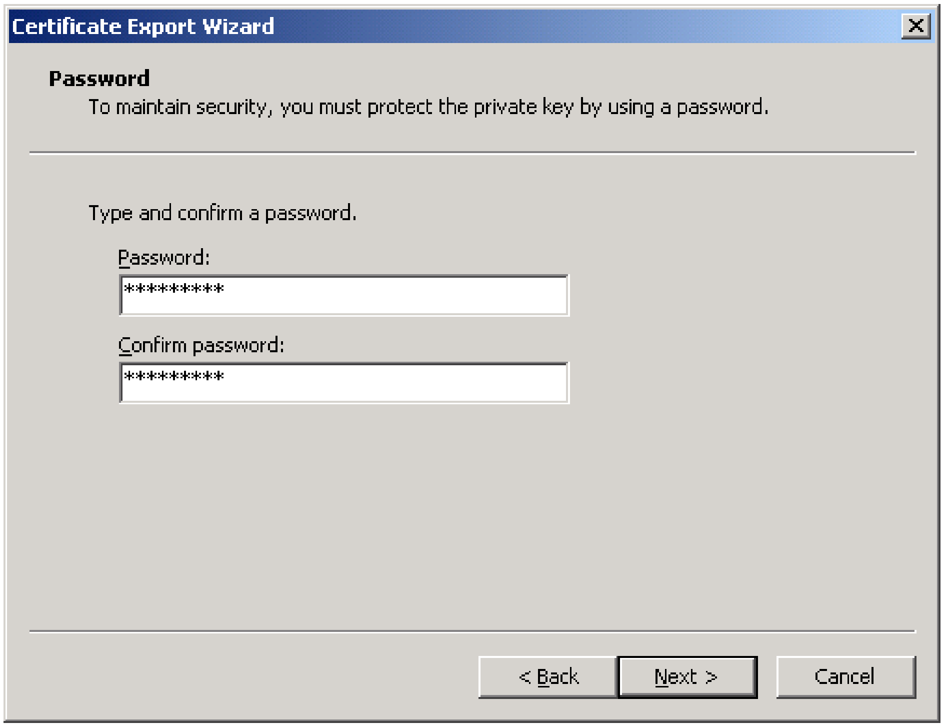
● Personal Information Exchange - PKCS #12 (.PFX)

□ 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

18. In the “Password” screen, enter and confirm a password that will protect the exported file, then click **Next**.



Certificate Export Wizard

Password

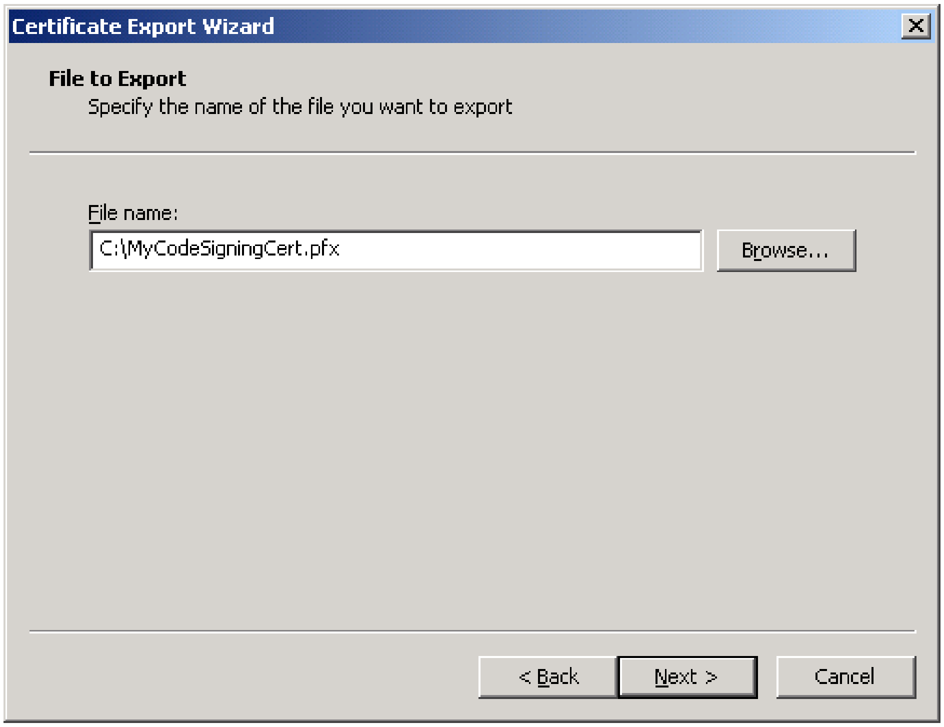
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: *********

Confirm password: *********

19. In the “File to Export” screen, provide an absolute path to and the name of the file to which you want to export the certificate, then click **Next**.



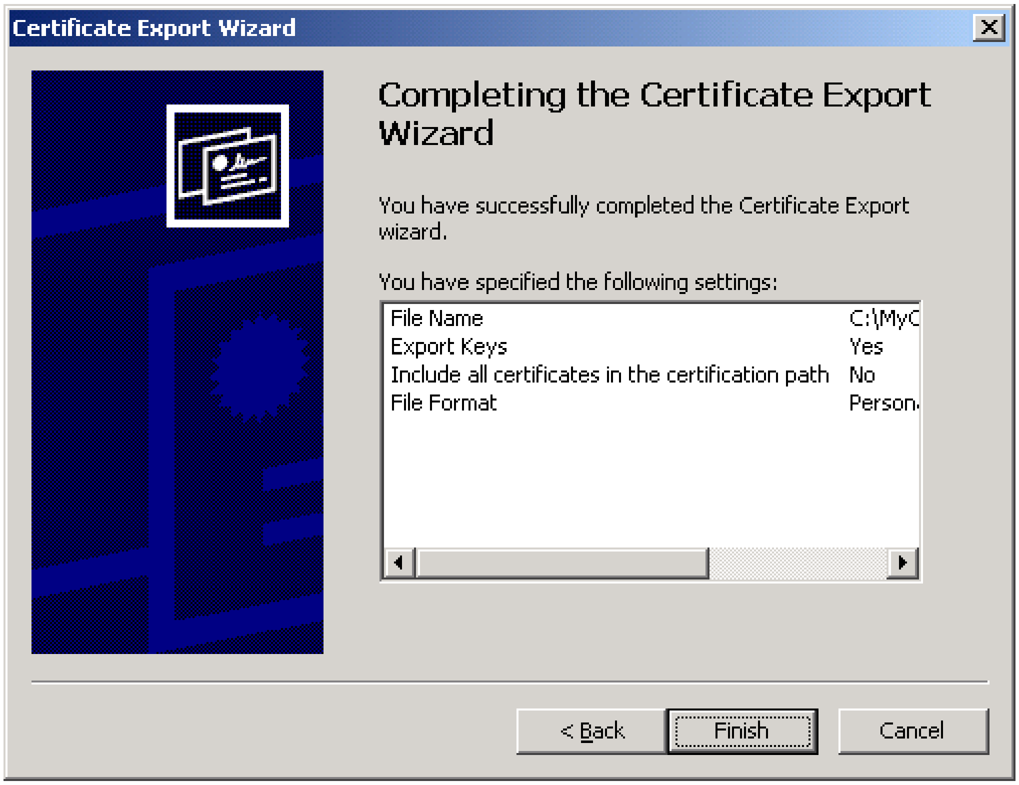
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\MyCodeSigningCert.pfx

20. In the summary screen, click **Finish** to close the wizard.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\MyC
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

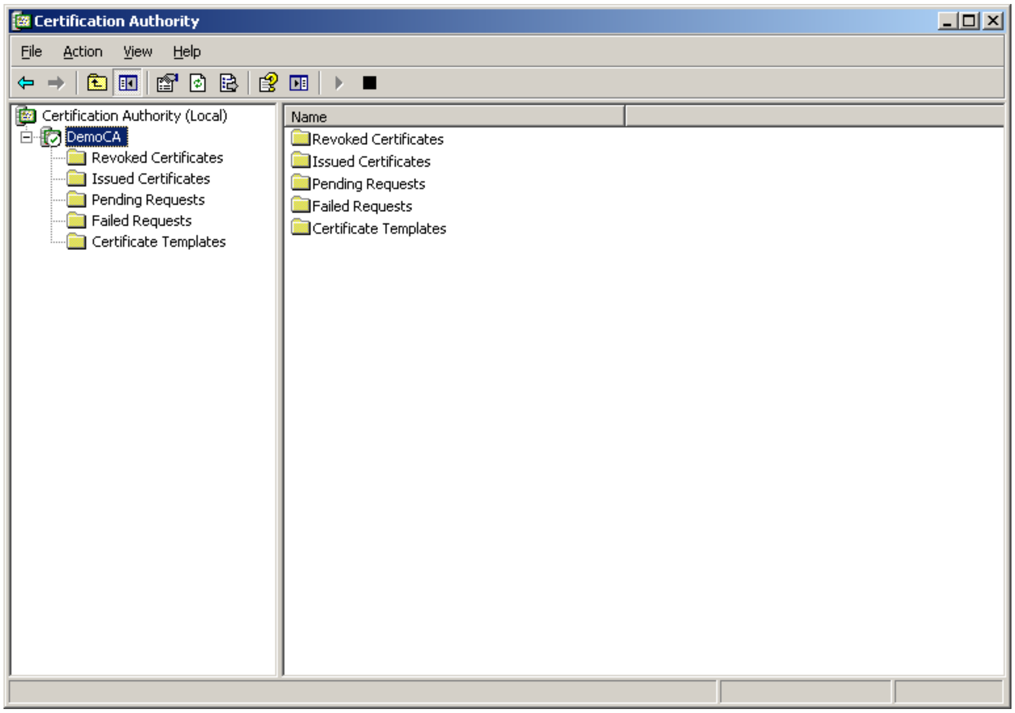
The certificate is now available as a password-protected file at the location you have chosen.

Creating an SSL Certificate with an Enterprise Certificate Authority

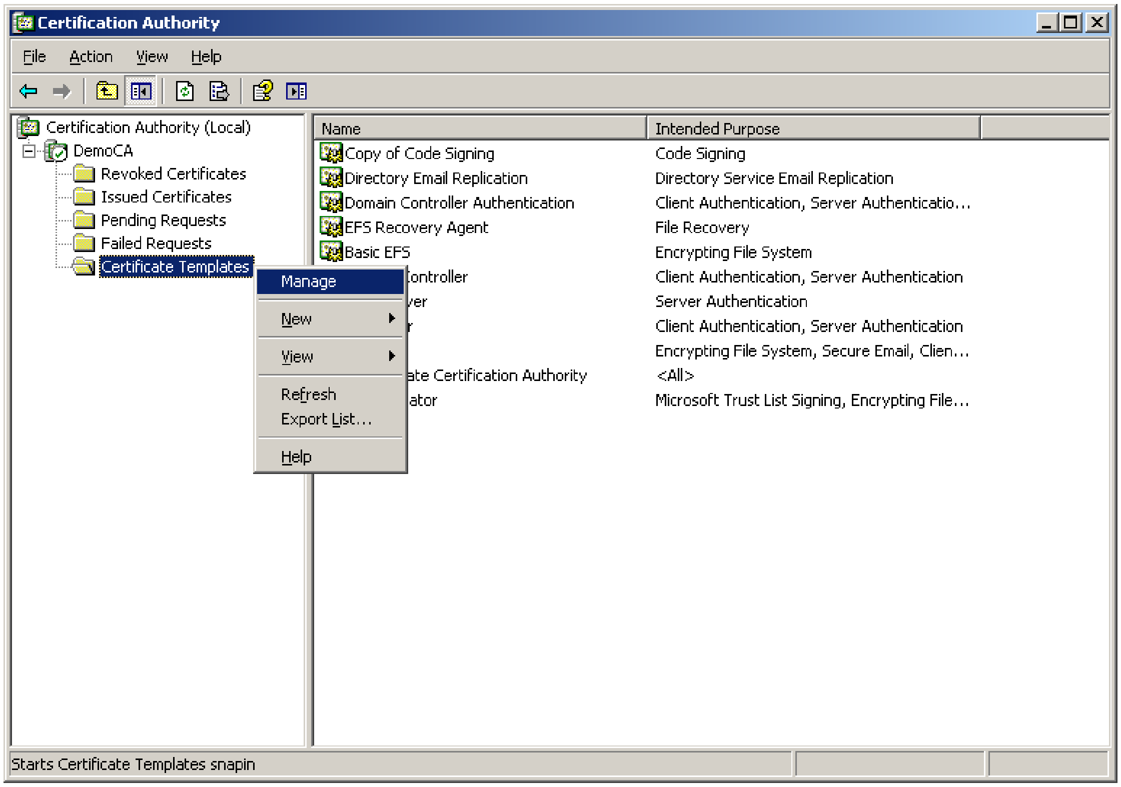
To create an SSL certificate on Windows Server 2003 Enterprise Edition using an enterprise certificate authority, do the following:

Note: Only Windows Server 2003 Enterprise Edition is supported in the enterprise CA scenario. Other versions and/or editions are not supported.

1. Launch the Certificate Authority tool.
2. In the tree in the left-hand pane, expand the root node.



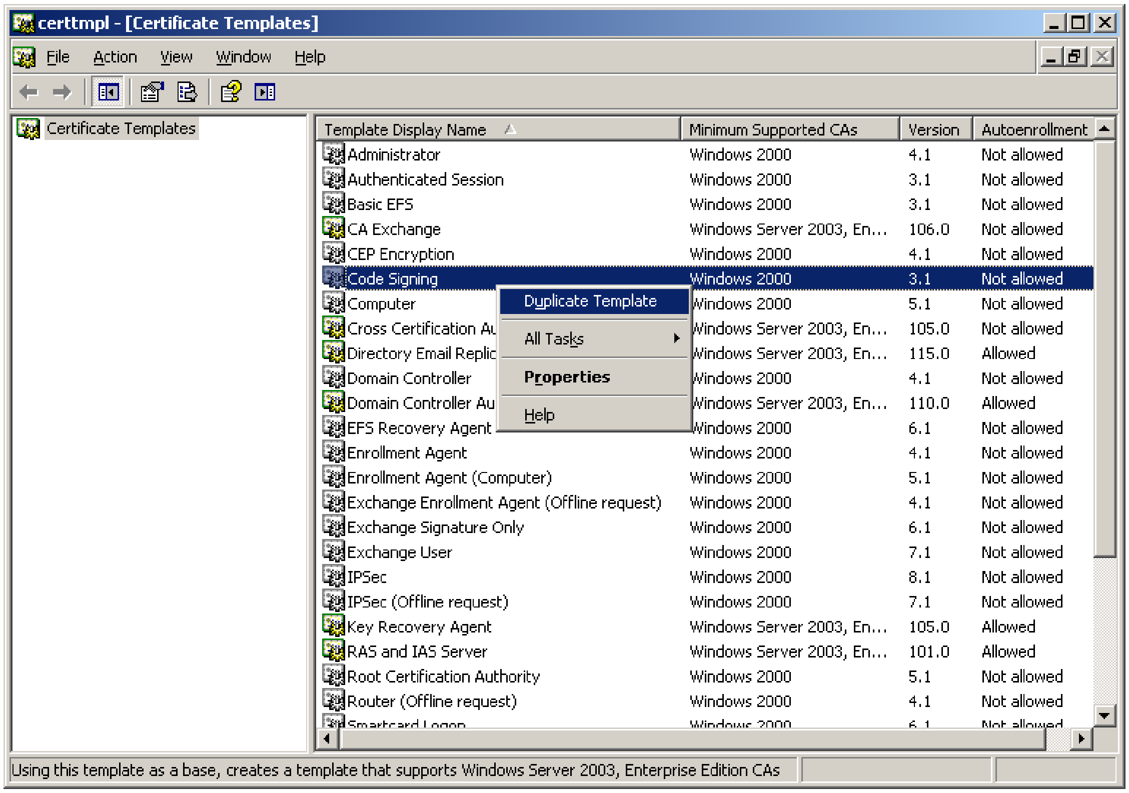
3. Right-click the **Certificate Templates** node, and select **Manage** from the context menu.



Name	Intended Purpose
Copy of Code Signing	Code Signing
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
ontroller	Client Authentication, Server Authentication
ver	Server Authentication
r	Client Authentication, Server Authentication
	Encrypting File System, Secure Email, Clien...
ate Certification Authority	<All>
ator	Microsoft Trust List Signing, Encrypting File...

Starts Certificate Templates snapin

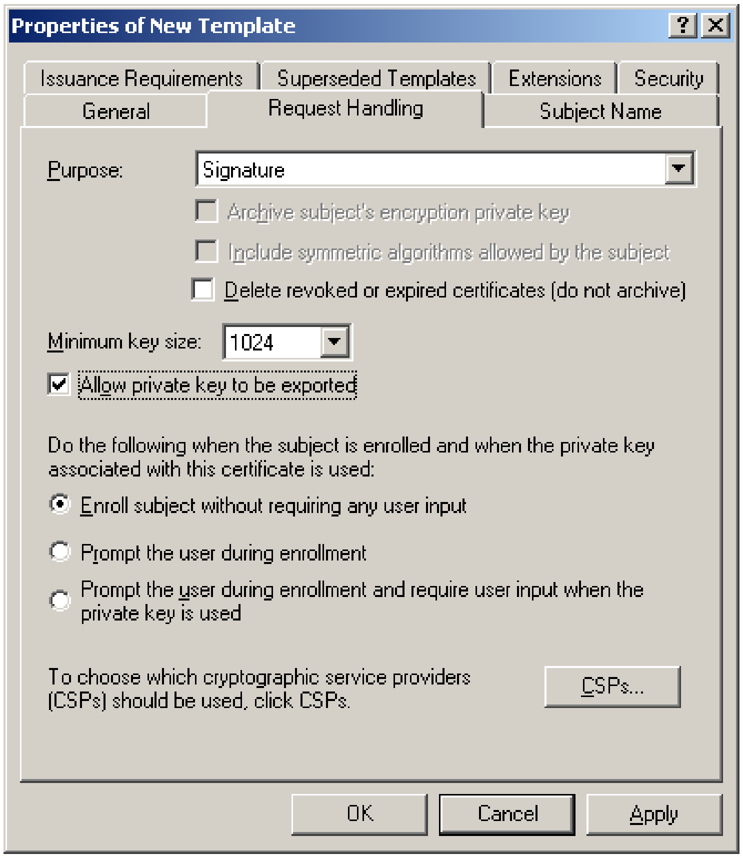
4. In the list of templates in the right-hand pane, right-click the **Code Signing** template and select **Duplicate Template** from the context menu.



Template Display Name	Minimum Supported CAs	Version	Autoenrollment
Administrator	Windows 2000	4.1	Not allowed
Authenticated Session	Windows 2000	3.1	Not allowed
Basic EFS	Windows 2000	3.1	Not allowed
CA Exchange	Windows Server 2003, En...	106.0	Not allowed
CEP Encryption	Windows 2000	4.1	Not allowed
Code Signing	Windows 2000	3.1	Not allowed
Computer	Windows 2000	5.1	Not allowed
Cross Certification Au	Windows Server 2003, En...	105.0	Not allowed
Directory Email Replic	Windows Server 2003, En...	115.0	Allowed
Domain Controller	Windows 2000	4.1	Not allowed
Domain Controller Au	Windows Server 2003, En...	110.0	Allowed
EFS Recovery Agent	Windows 2000	6.1	Not allowed
Enrollment Agent	Windows 2000	4.1	Not allowed
Enrollment Agent (Computer)	Windows 2000	5.1	Not allowed
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	Not allowed
Exchange Signature Only	Windows 2000	6.1	Not allowed
Exchange User	Windows 2000	7.1	Not allowed
IPSec	Windows 2000	8.1	Not allowed
IPSec (Offline request)	Windows 2000	7.1	Not allowed
Key Recovery Agent	Windows Server 2003, En...	105.0	Allowed
RAS and IAS Server	Windows Server 2003, En...	101.0	Allowed
Root Certification Authority	Windows 2000	5.1	Not allowed
Router (Offline request)	Windows 2000	4.1	Not allowed
Smartcard Logon	Windows 2000	6.1	Not allowed

Using this template as a base, creates a template that supports Windows Server 2003, Enterprise Edition CAs

5. In the template properties dialog that appears, do the following:
   a. Select the **Request Handling** tab and select the **Allow private key to be exported** check box.



Purpose: Signature

□ Archive subject's encryption private key

□ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

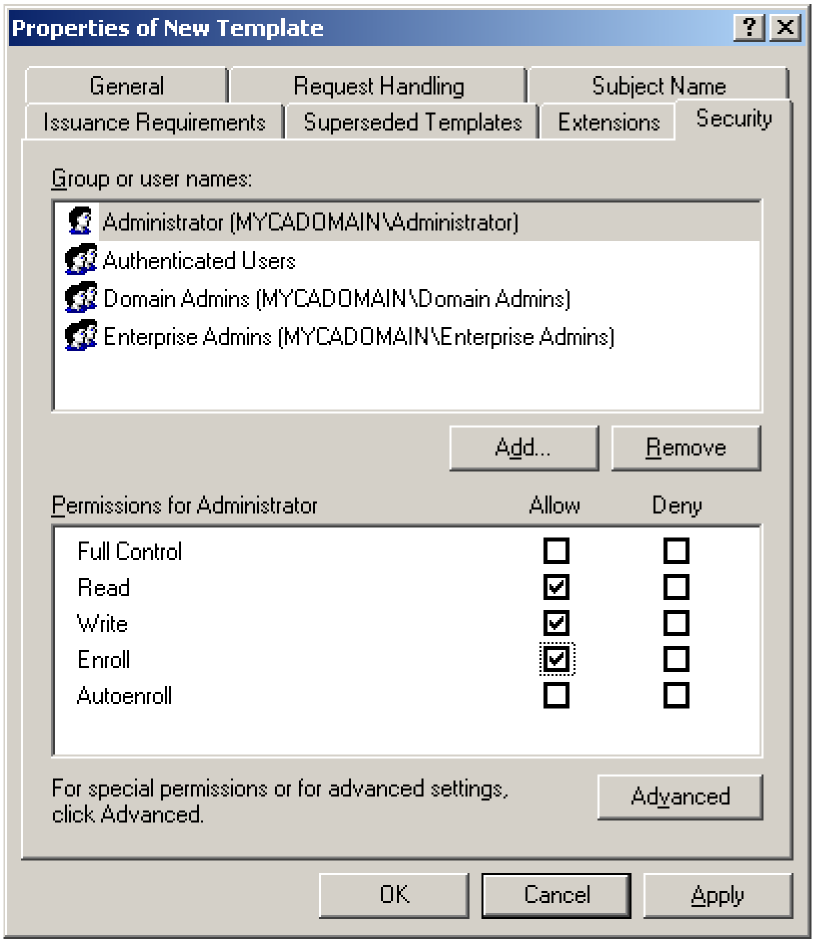
● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

b. Select the **Security** tab and grant the **Enroll** permission to the desired users. For example:



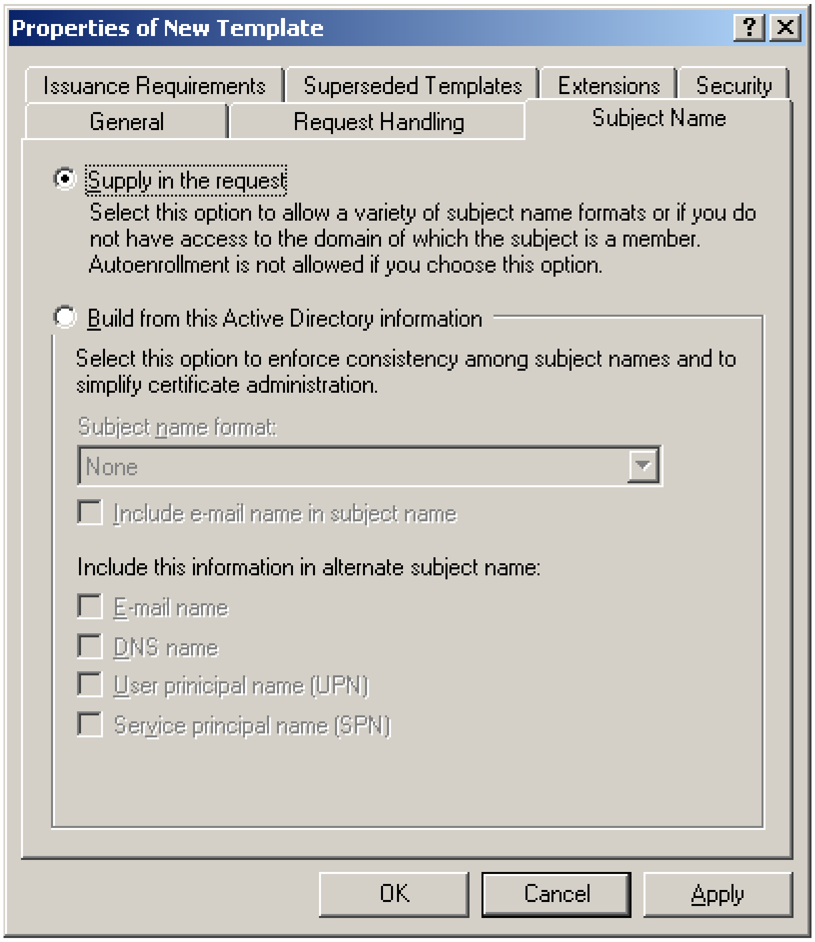
Group or user names:

- Administrator (MYCADOMAIN\Administrator)
- Authenticated Users
- Domain Admins (MYCADOMAIN\Domain Admins)
- Enterprise Admins (MYCADOMAIN\Enterprise Admins)

Permissions for Administrator	Allow	Deny
Full Control	□	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or for advanced settings, click Advanced.

c. If you want to specify the subject name during certificate enrollment, select the **Subject Name** tab and select the **Supply the request** radio button. (If you want to use the default subject name of the enrolling user's account name, skip this step.)



● Supply in the request

Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

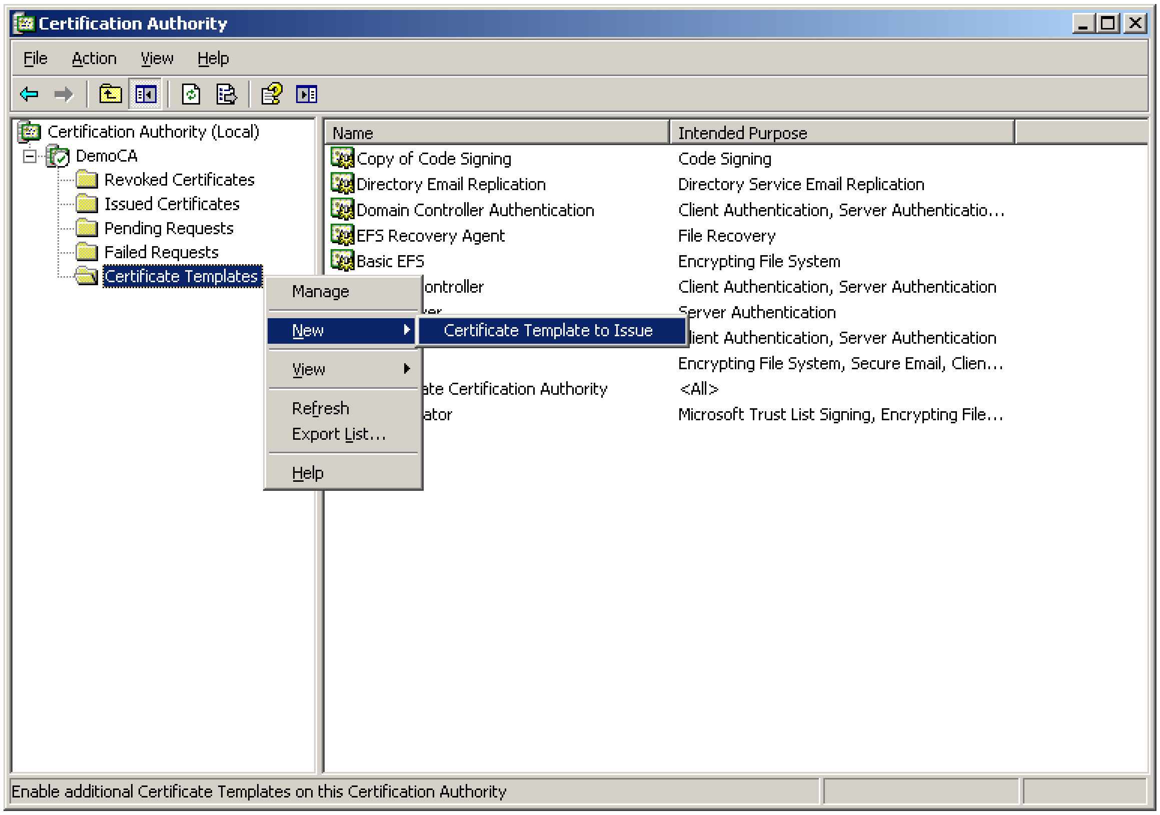
□ DNS name

□ User prinicipal name (UPN)

□ Service principal name (SPN)

d. Configure other template options as desired, then click **OK** to save your changes. The new template appears in the list in the "Certificate Templates" window.

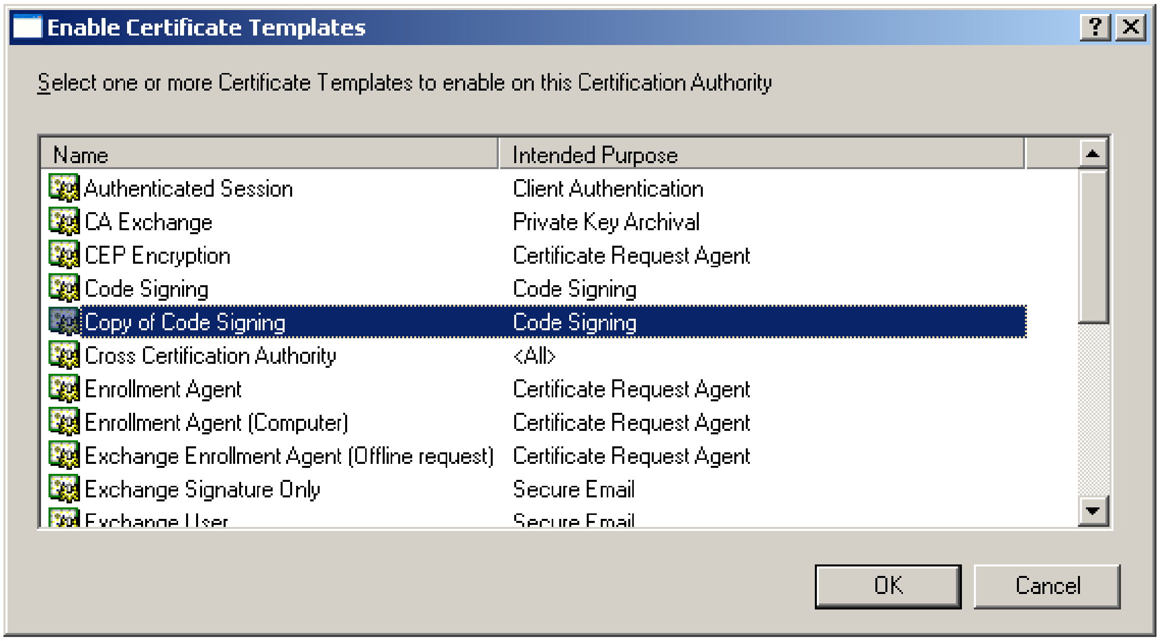
6. Close the “Certificate Templates” window and return to the Certificate Authority tool.
7. In the Certificate Authority tool, right-click the **Certificate Templates** node in the tree and select **New → Certificate Template to Issue** from the context menu.



Name	Intended Purpose
Copy of Code Signing	Code Signing
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
ontroller	Client Authentication, Server Authentication
er	Server Authentication
	lient Authentication, Server Authentication
	Encrypting File System, Secure Email, Clien...
ate Certification Authority	<All>
ator	Microsoft Trust List Signing, Encrypting File...

Enable additional Certificate Templates on this Certification Authority

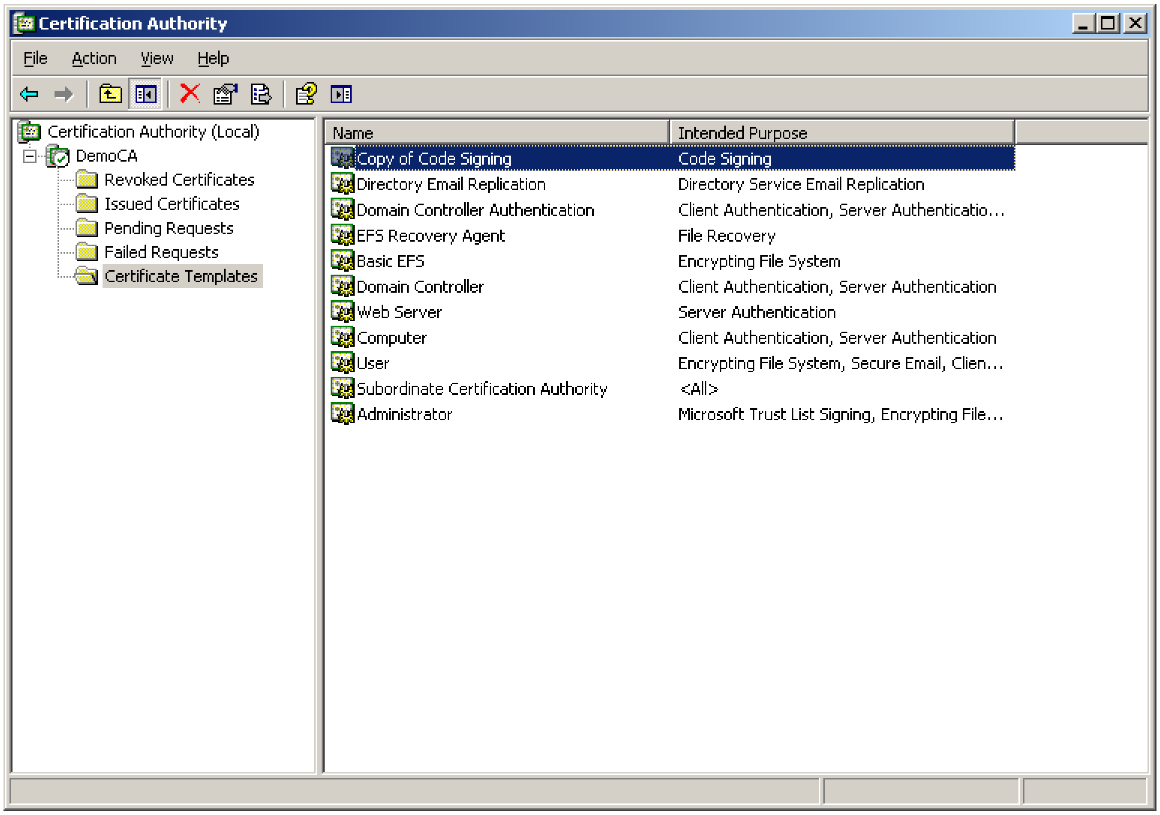
8. In the “Enable Template Certificates” dialog, select the template you created in the previous step, then click **OK**.



Select one or more Certificate Templates to enable on this Certification Authority

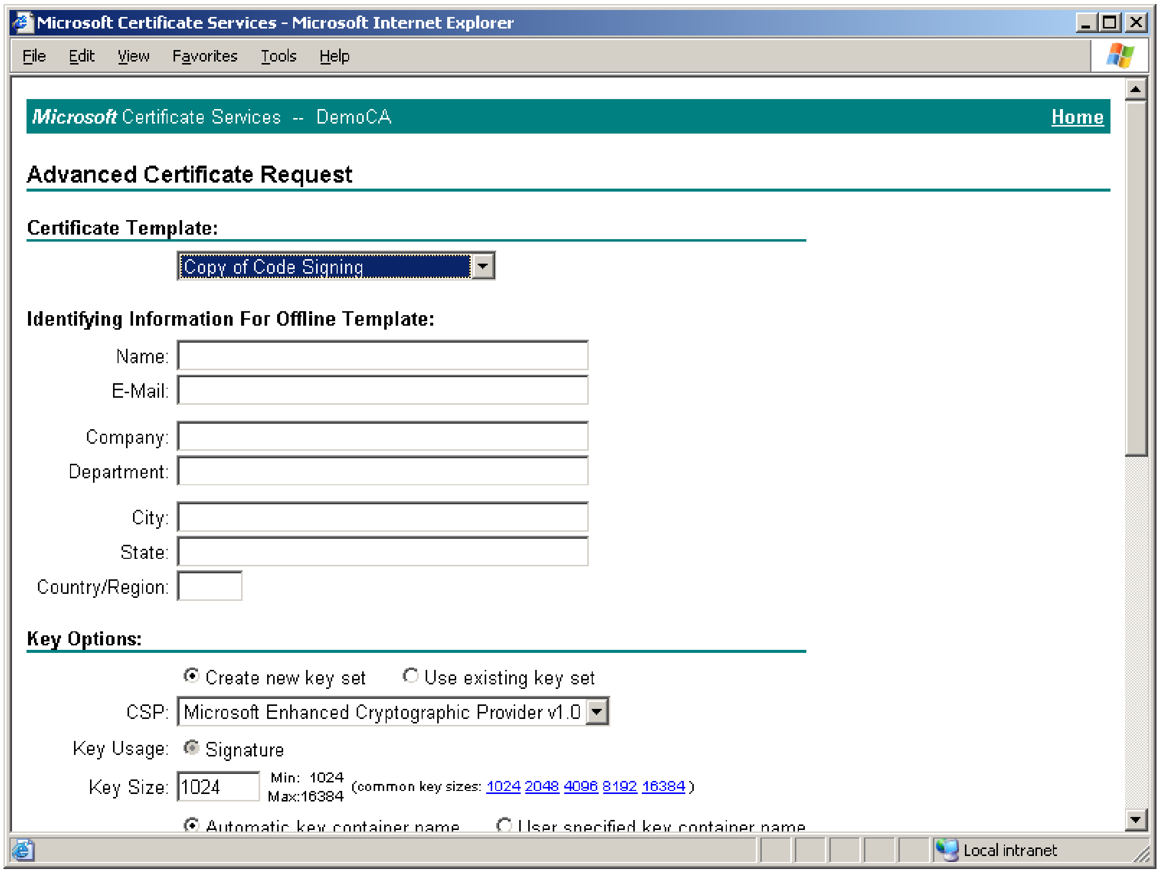
Name	Intended Purpose
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
Code Signing	Code Signing
Copy of Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email

9. Click the **Certificate Templates** node again to refresh the template list and verify that the new template has been successfully enabled.



Name	Intended Purpose
Copy of Code Signing	Code Signing
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

10. In the page that appears, do the following:
    a. Fill in the fields in the “Identifying Information” section as appropriate.
    b. In the “Certificate Template” drop-down list, select your newly created template.
    c. In the “Key Options” section, make the choices appropriate to your environment.
    d. Click **Submit**.


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Local intranet

Microsoft Certificate Services -- DemoCA **Home**

Advanced Certificate Request

Certificate Template:

Copy of Code Signing

Identifying Information For Offline Template:

Name:
E-Mail:
Company:
Department:
City:
State:
Country/Region:

Key Options:

● Create new key set ○ Use existing key set

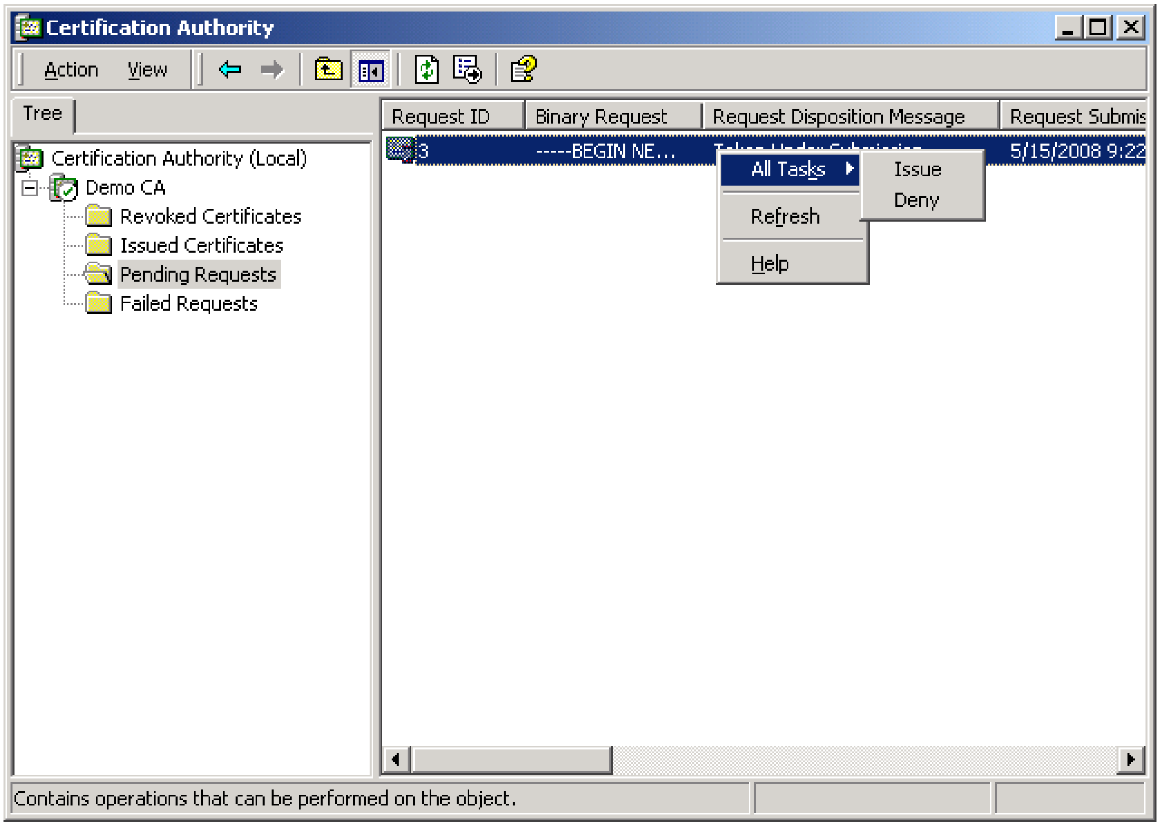
CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ● Signature

Key Size: 1024 Min: 1024 Max:16384 (common key sizes: 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

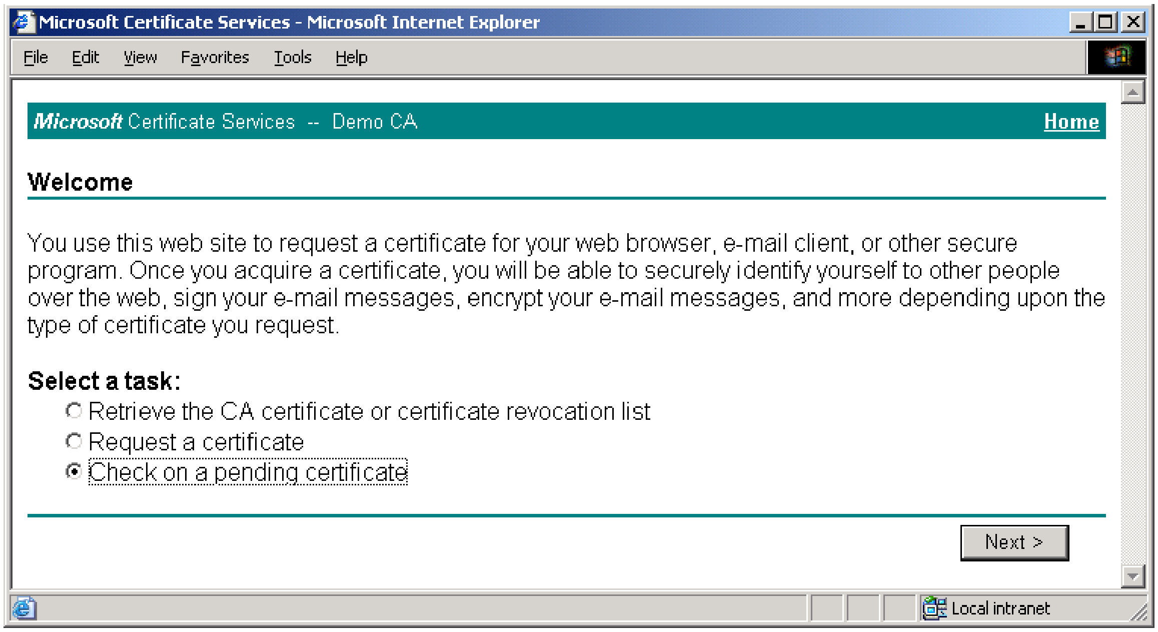
11. Depending on whether you have direct control over the certificate authority, do one of the following:
    - If you do not have direct control over the CA, wait until the certificate is approved by the CA administrator, then proceed to the next step.
    - If you have direct control over the CA, approve the certificate using the Certificate Authority tool, as shown below:



Request ID	Binary Request	Request Disposition Message	Request Submis
3	-----BEGIN NE...		5/15/2008 9:22

Contains operations that can be performed on the object.

12. Once the certificate request has been approved, return to Microsoft Certificate Server's enrollment page, select **Check on a pending certificate**, and click **Next**.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home
Next >
Local intranet

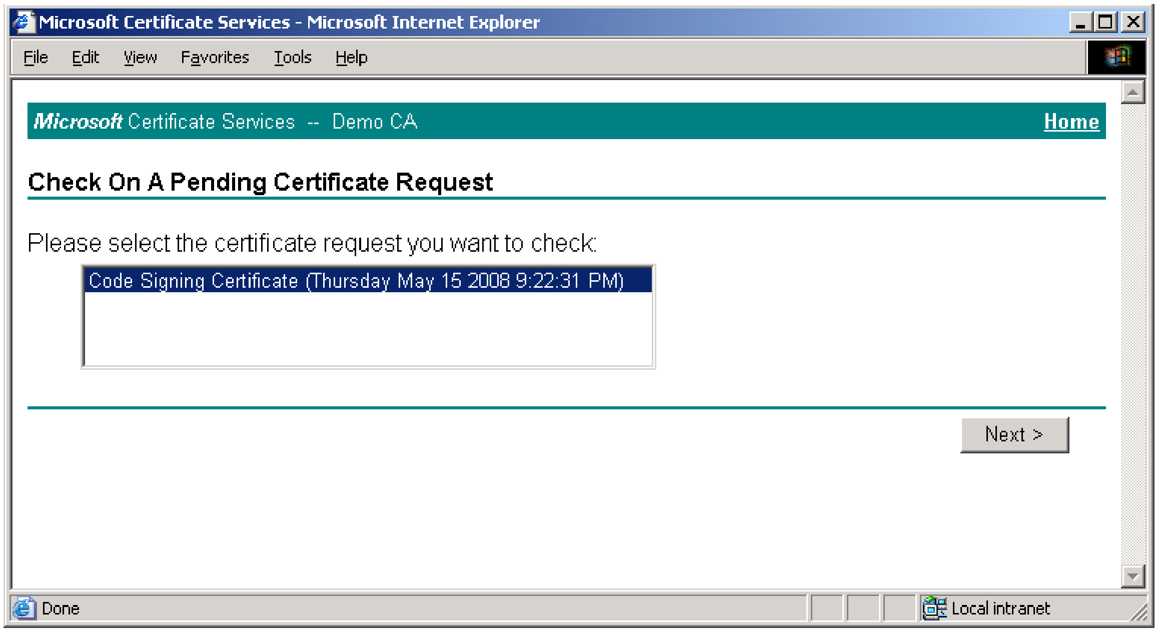
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
○ Request a certificate
● Check on a pending certificate

13. In the page that appears, select the target certificate request and click **Next**.



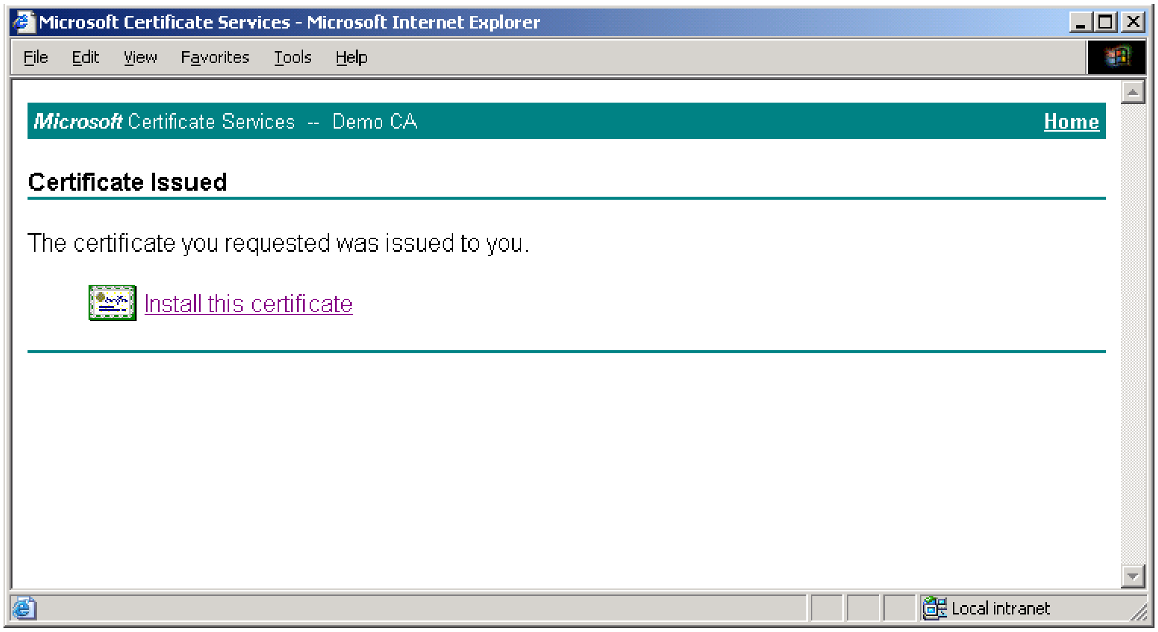
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home
Next >
Done
Local intranet

Check On A Pending Certificate Request

Please select the certificate request you want to check:

Code Signing Certificate (Thursday May 15 2008 9:22:31 PM)

14. In the page that appears, click the **Install the certificate** link.

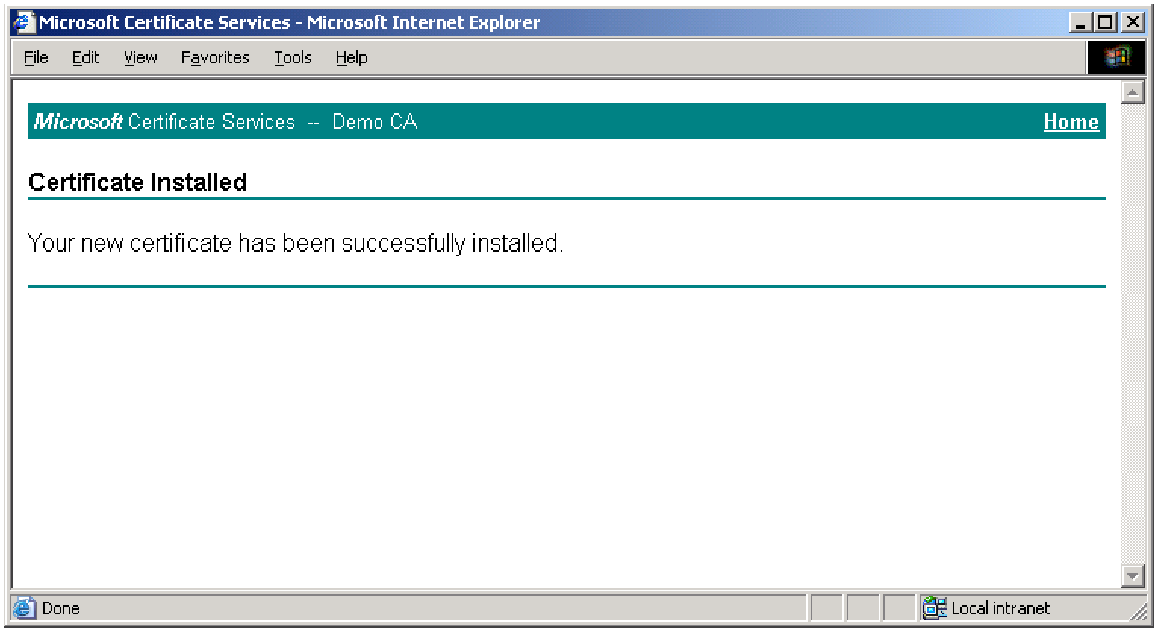

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home
Local intranet

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

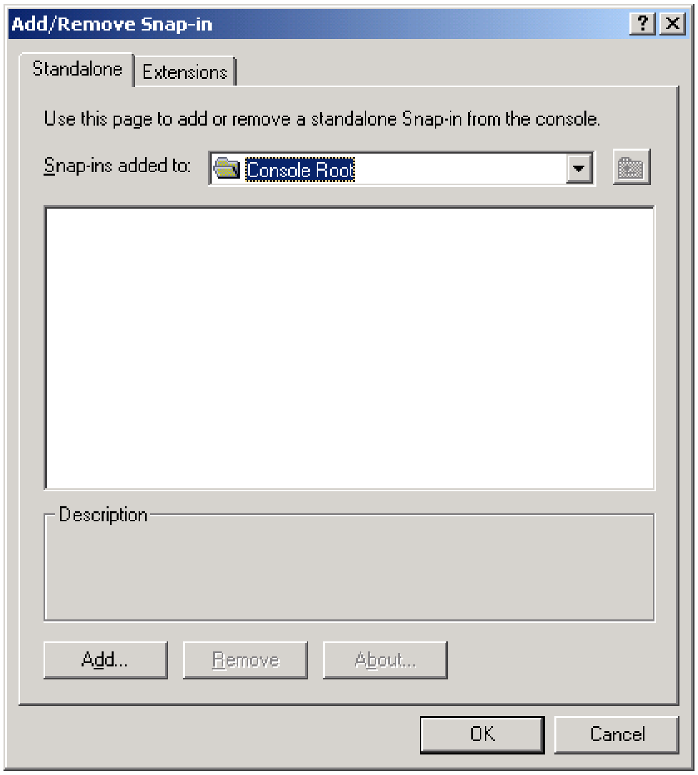
When the certificate is successfully installed, a confirmation page appears:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Microsoft Certificate Services -- Demo CA
Home
Done
Local intranet

Certificate Installed

Your new certificate has been successfully installed.

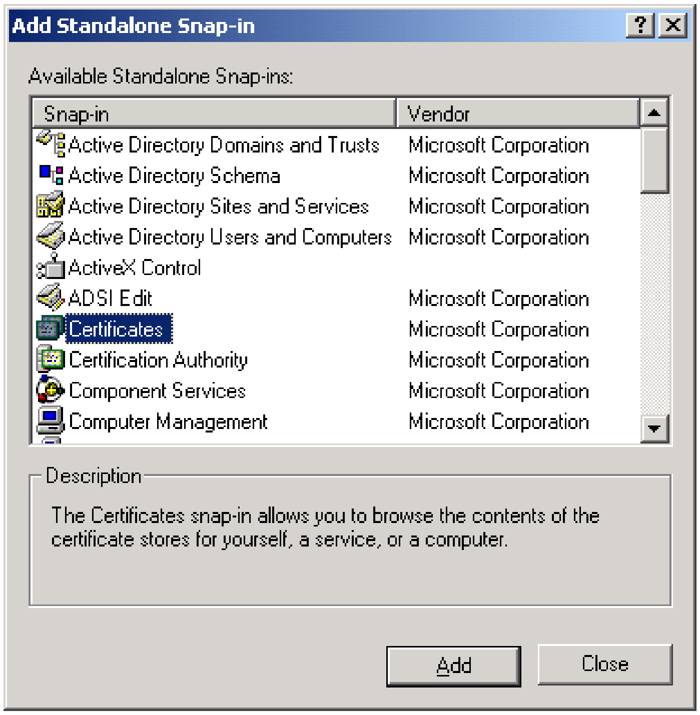
15. Launch the Microsoft Management Console.
16. In the console, add the “Certificates” snap-in:
    a. From the **Console** menu, select **Add/Remove Snap-in**.
    b. In the dialog that appears, click **Add**.



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

Snap-ins added to: Console Root

    c. In the list that appears, select **Certificates** and click **Add**.

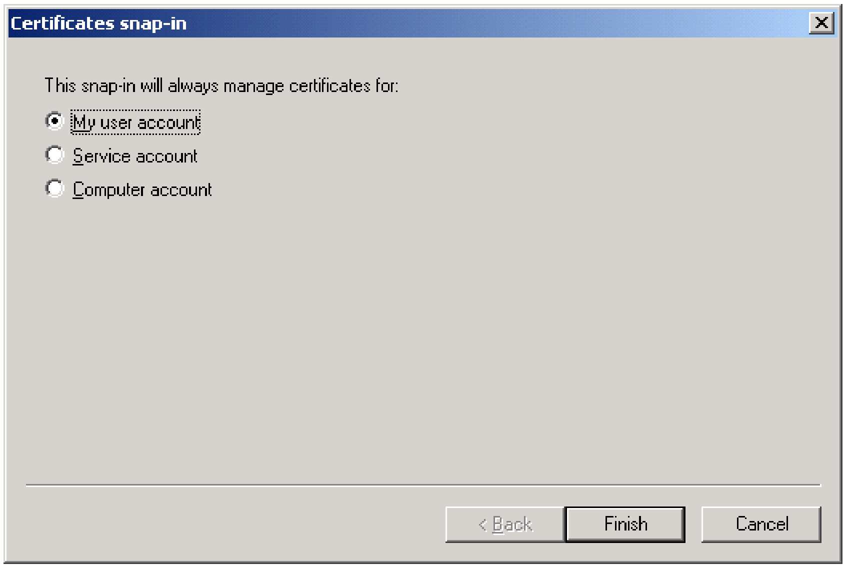


Available Standalone Snap-ins:

Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Schema	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
ADSI Edit	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation

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

d. In the dialog that appears, select **My user account** and click **Finish**.



Certificates snap-in

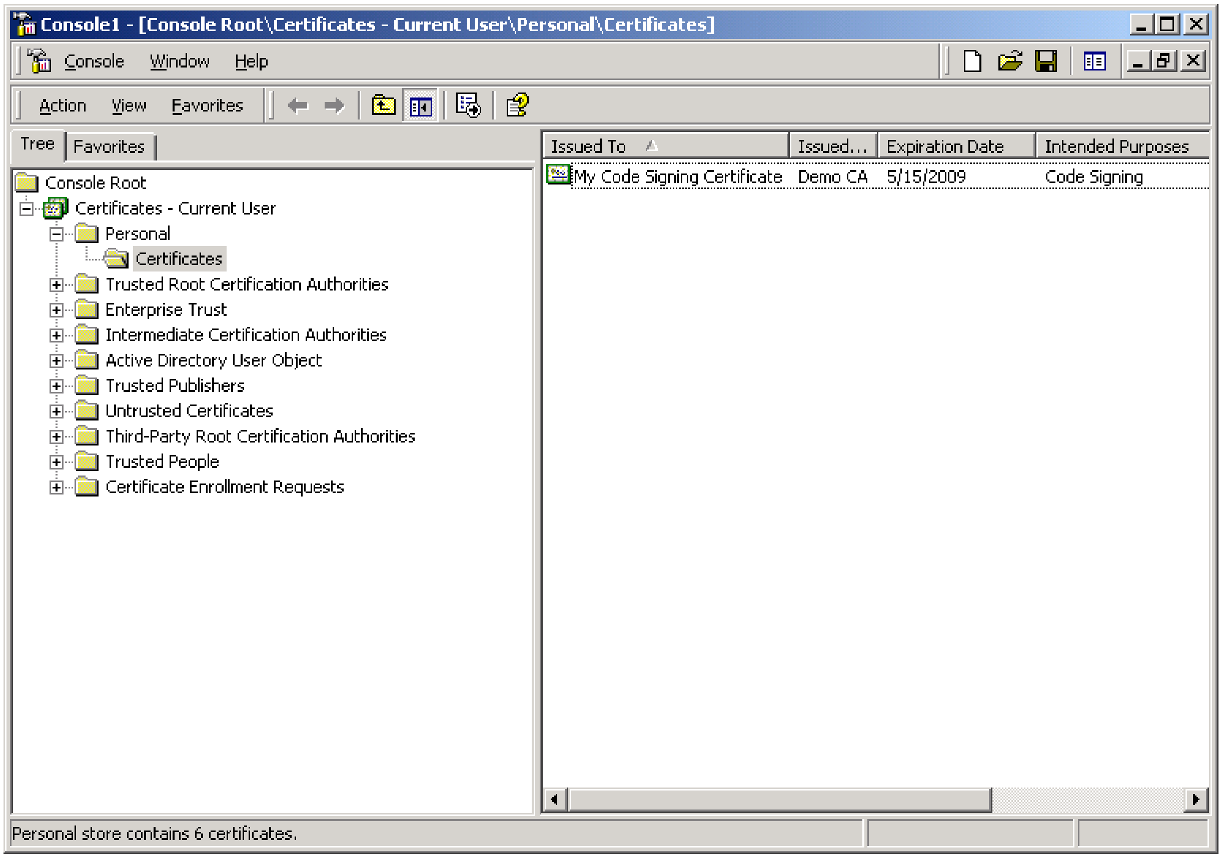
This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

17. Close the remaining open dialog boxes inside the Management Console.
18. In the tree in the left-hand pane, navigate to:
    Certificates – Current User → Personal → Certificates.



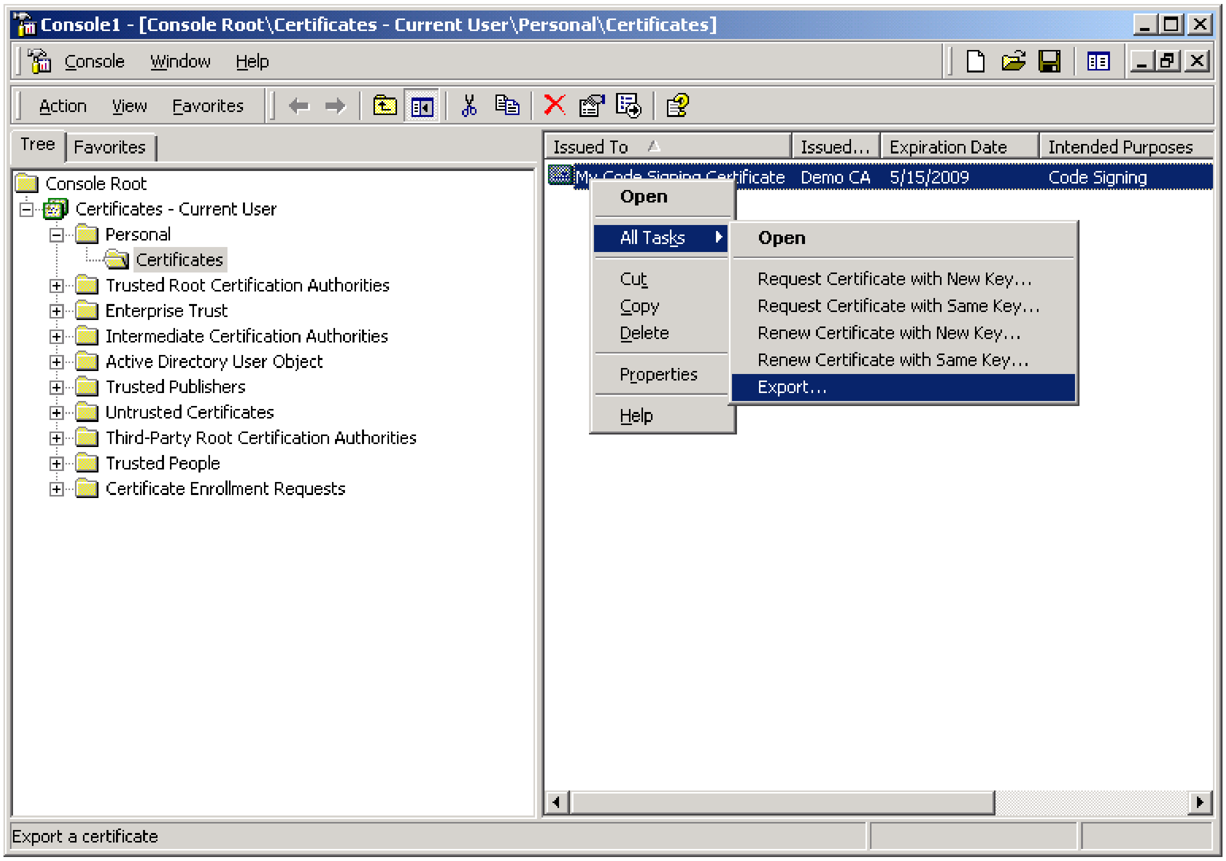
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests

Issued To	Issued...	Expiration Date	Intended Purposes
My Code Signing Certificate	Demo CA	5/15/2009	Code Signing

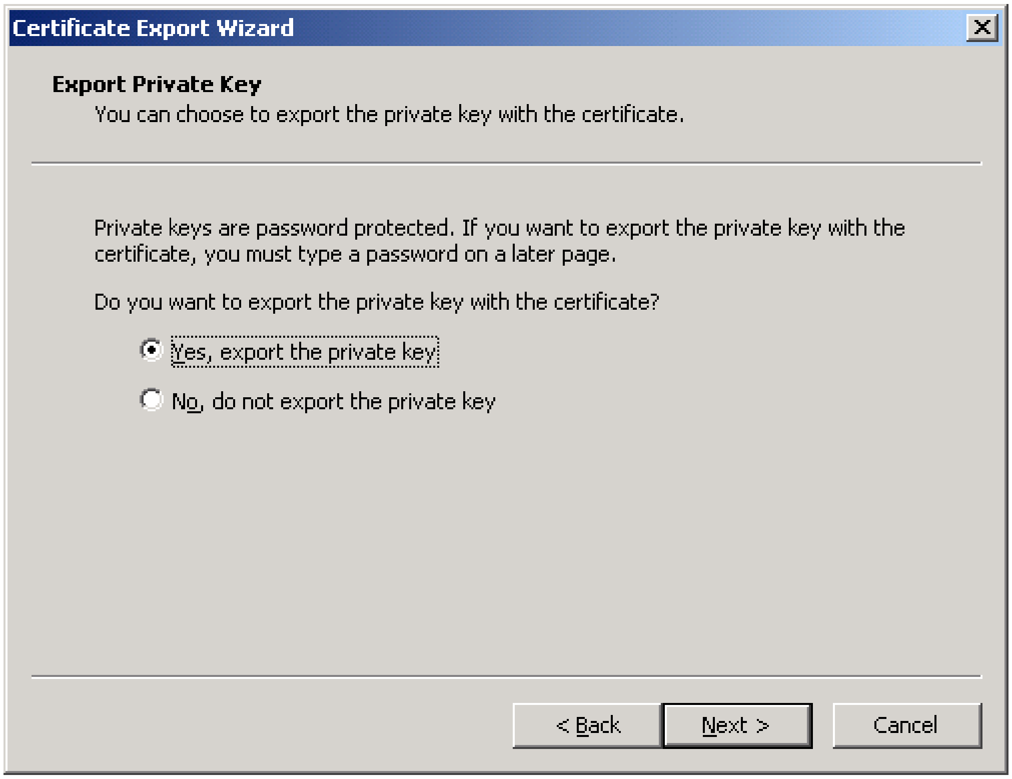
Personal store contains 6 certificates.

19. In the right-hand pane, right-click the desired certificate, then select **All Tasks → Export** from the context menu.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Issued To
Issued...
Expiration Date
Intended Purposes
My Code Signing Certificate
Demo CA
5/15/2009
Code Signing
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Request Certificate with Same Key...
Renew Certificate with New Key...
Renew Certificate with Same Key...
Export...
Export a certificate

20. In the “Certificate Export Wizard” that appears, click **Next**.

21. In the “Export Private Key” screen, select **Yes, export the private key** and click **Next**.



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

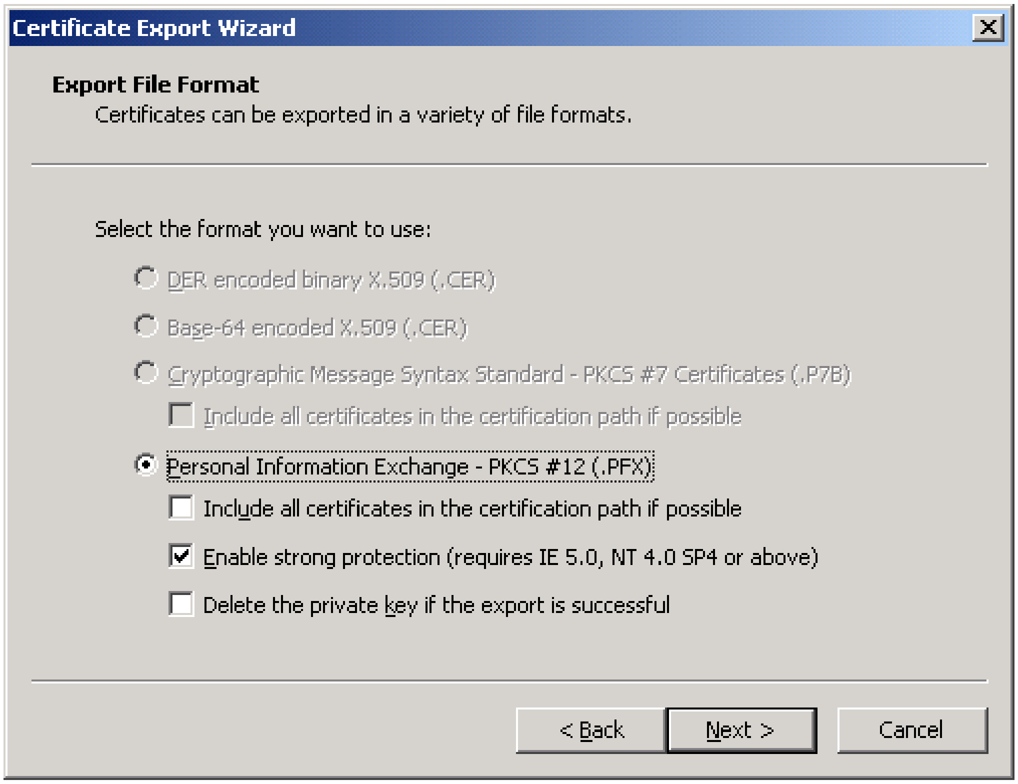
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

22. In the “Export File Format” screen, leave the options at their default values and click **Next**.



Certificate Export Wizard

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

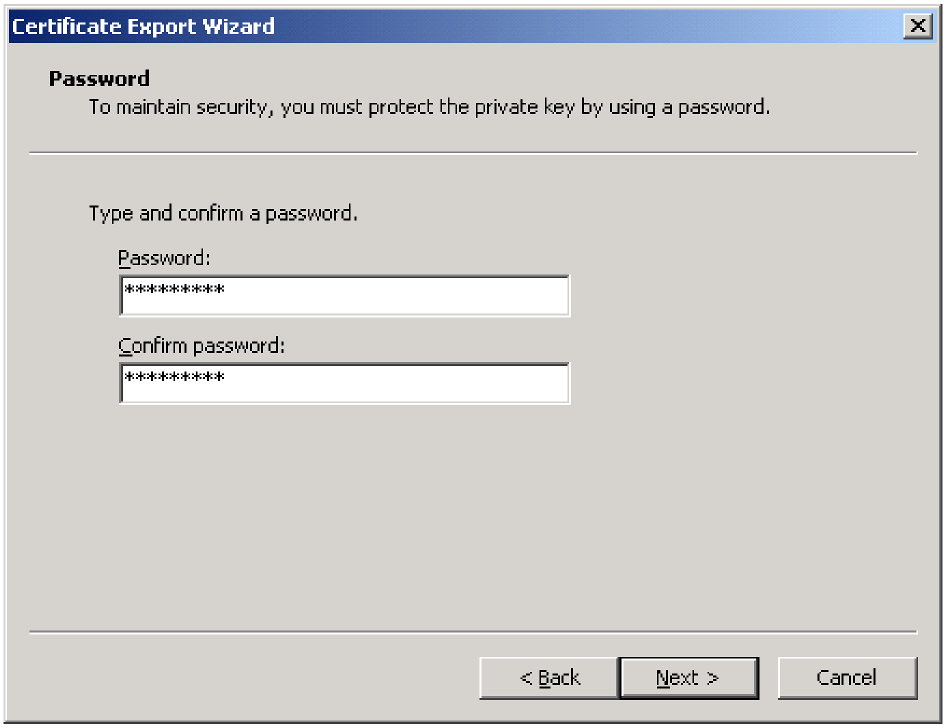
● Personal Information Exchange - PKCS #12 (.PFX)

□ 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

23. In the “Password” screen, enter and confirm a password that will protect the exported file, then click **Next**.



Certificate Export Wizard

Password

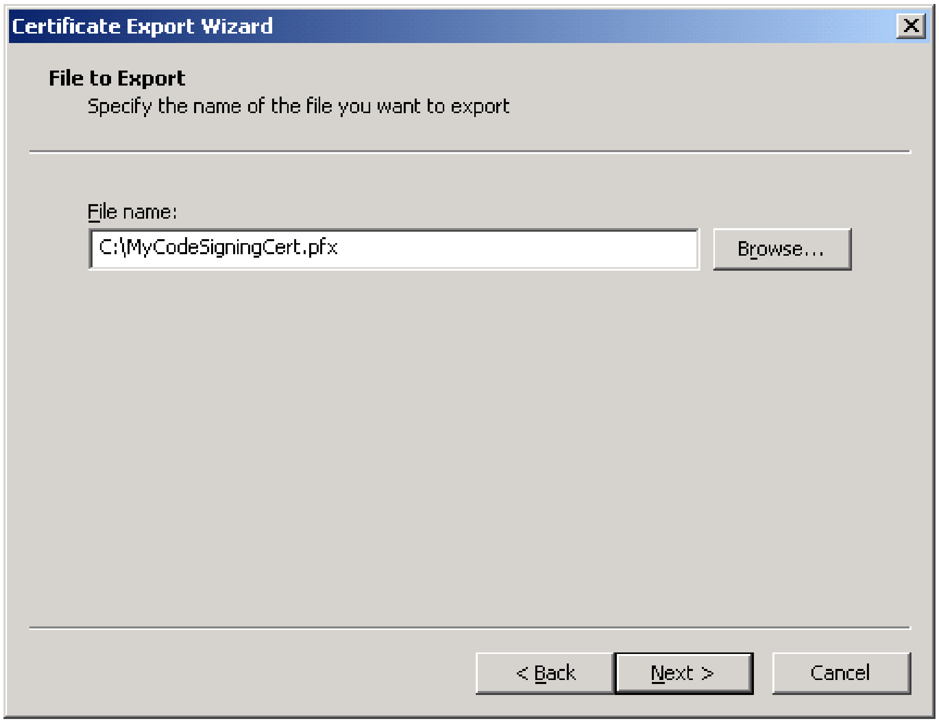
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: **********

Confirm password: **********

24. In the “File to Export” screen, provide an absolute path to and the name of the file to which you want to export the certificate, then click **Next**.



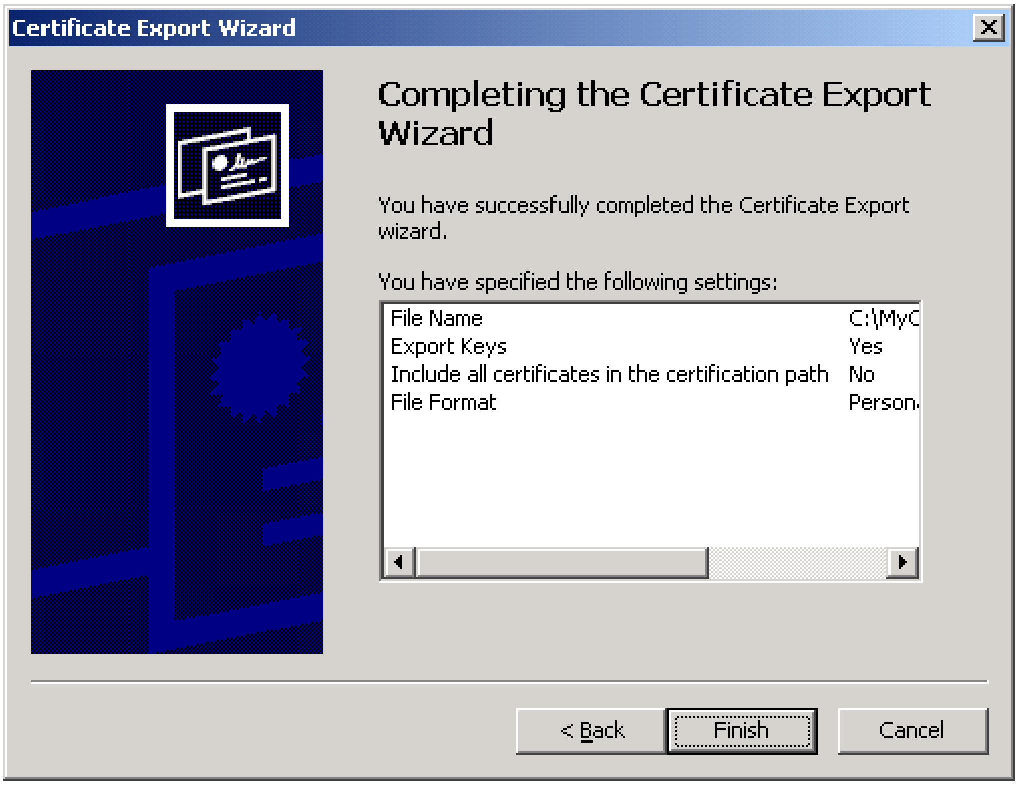
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\MyCodeSigningCert.pfx

25. In the summary screen, click **Finish** to close the wizard.



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\MyC
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

The certificate is now available as a password-protected file at the location you have chosen.