Oracle® Enterprise Single Sign-on Anywhere

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

Release 11.1.1.2.0

20452-01

December 2010

ORACLE

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

Release 11.1.1.2.0

20452-01

Copyright © 2010, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free.

Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites.

You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for:

(a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

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

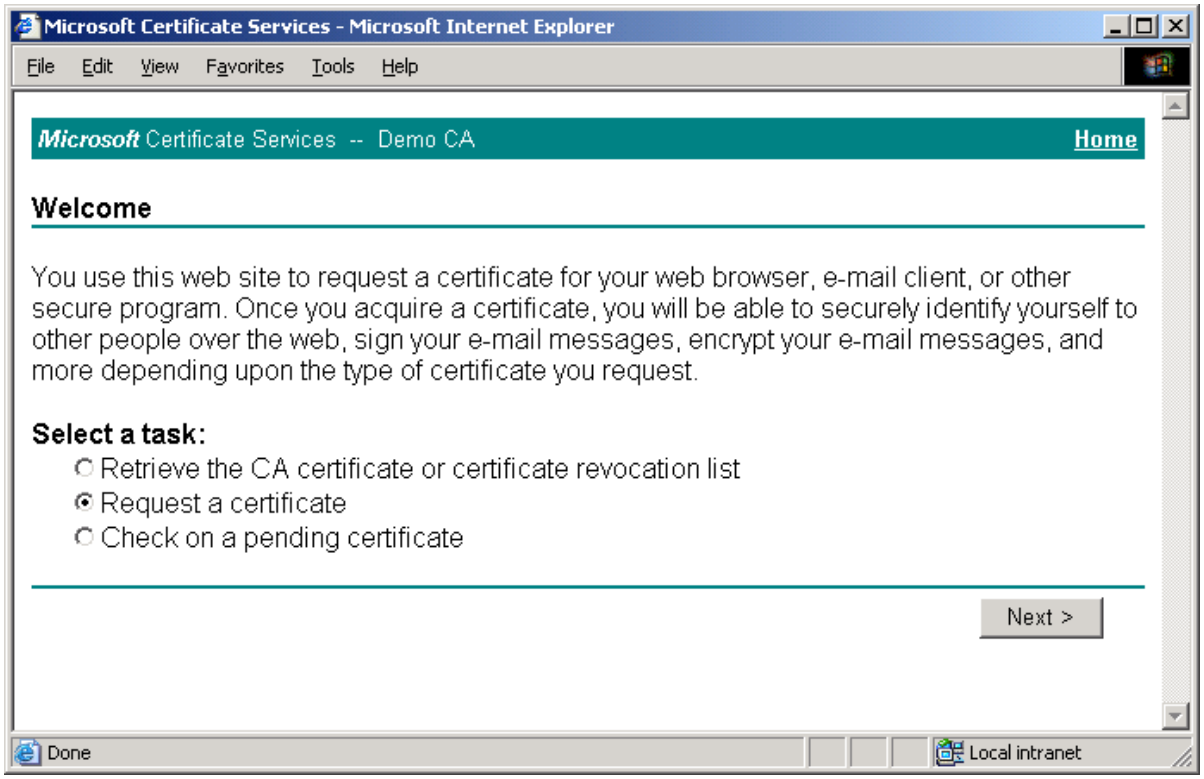
Accessing ESSO-Anywhere Documentation

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:
http://download.oracle.com/docs/cd/E15624_01/index.htm.

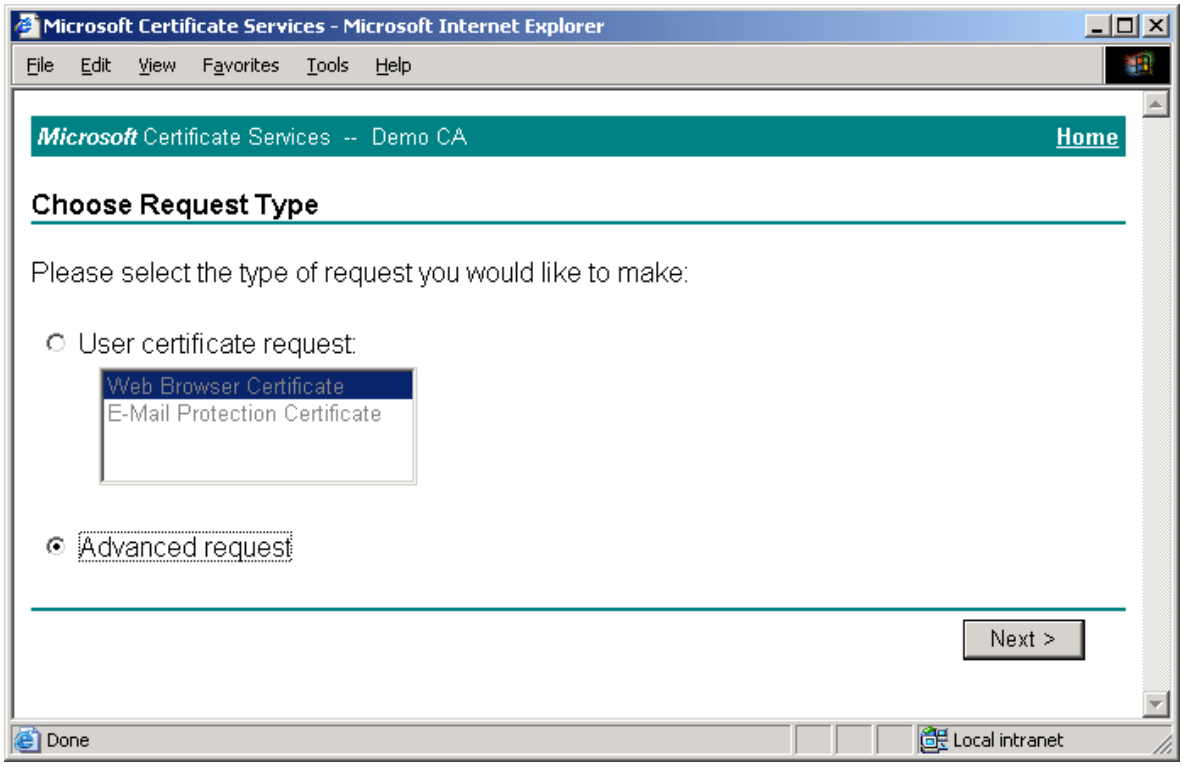
Creating an SSL Certificate with a Standalone Certificate Authority

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

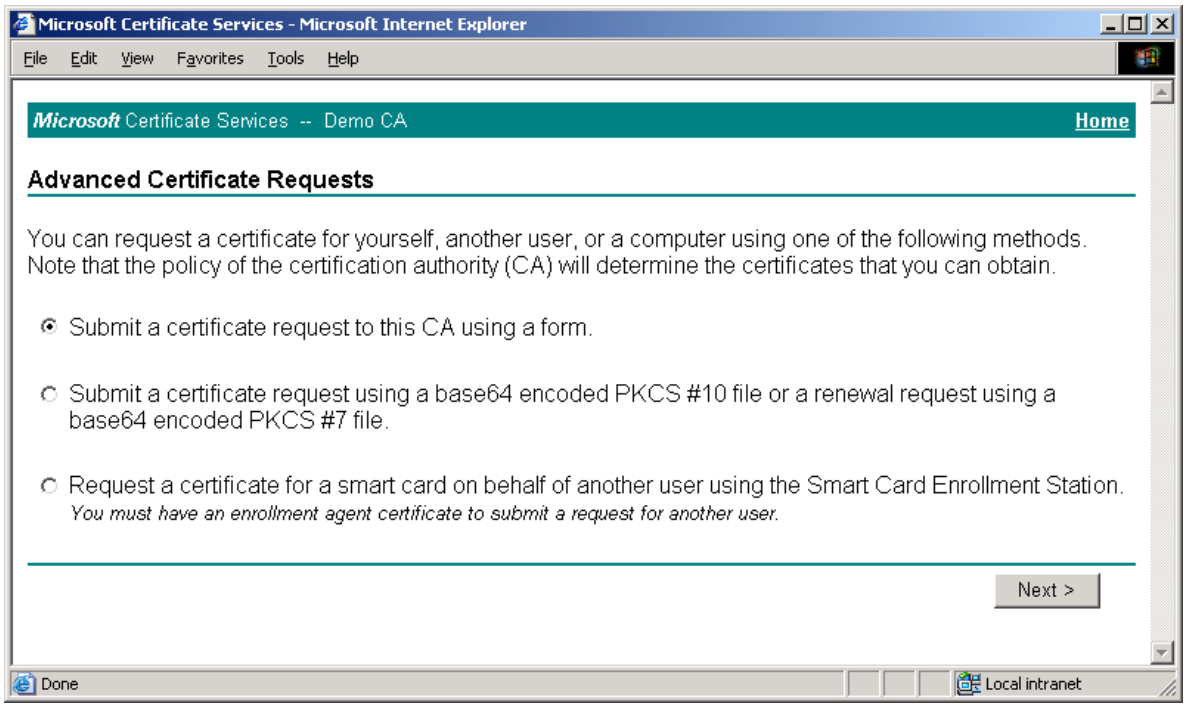
1. Navigate to the Microsoft Certificate Server enrollment page by accessing the following URL in a Web browser:
   `http://<server>:<port>/certsrv`
2. In the page that appears, select **Request a Certificate** and click **Next**.



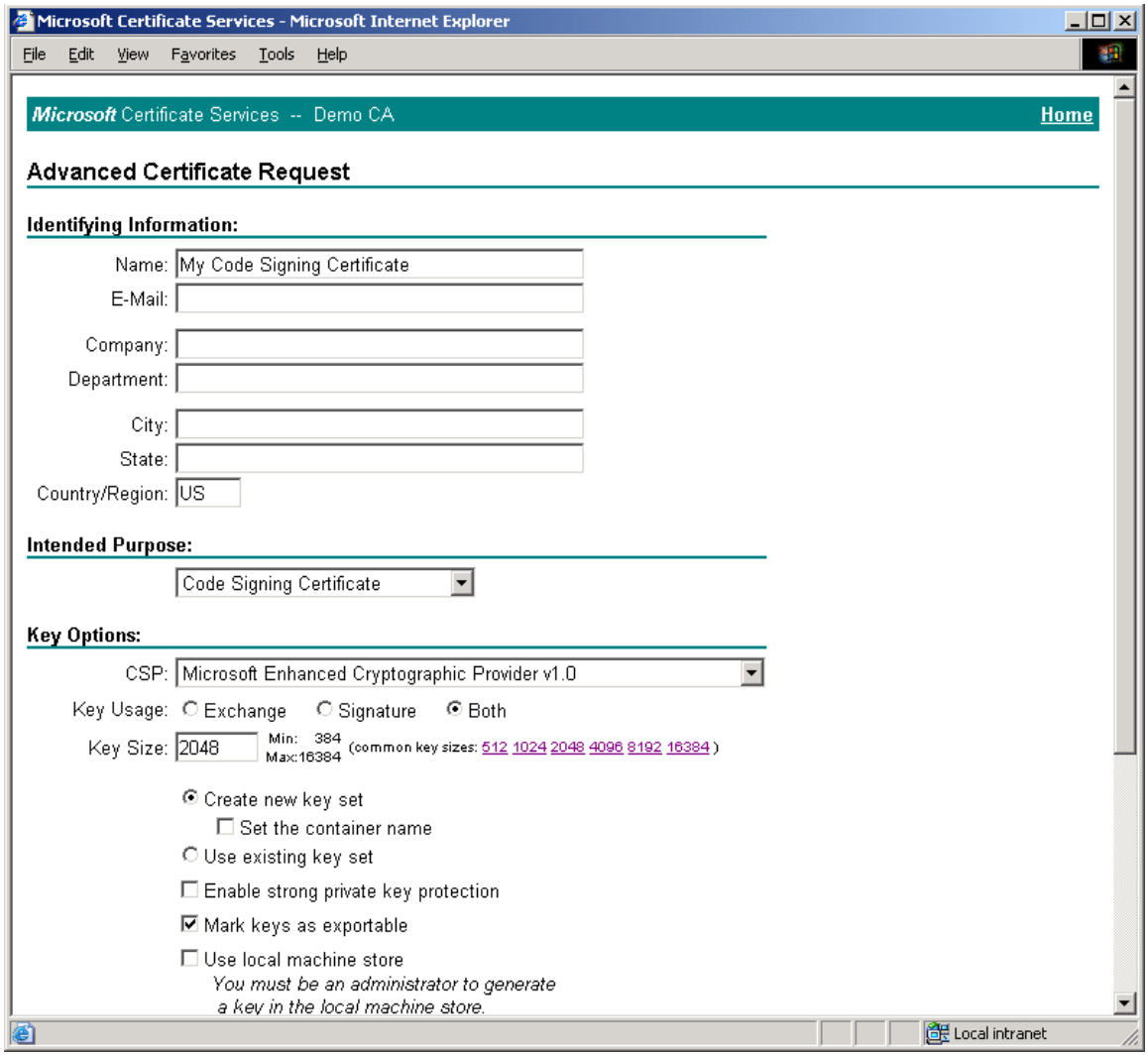
3. In the page that appears, select **Advanced request** and click **Next**.



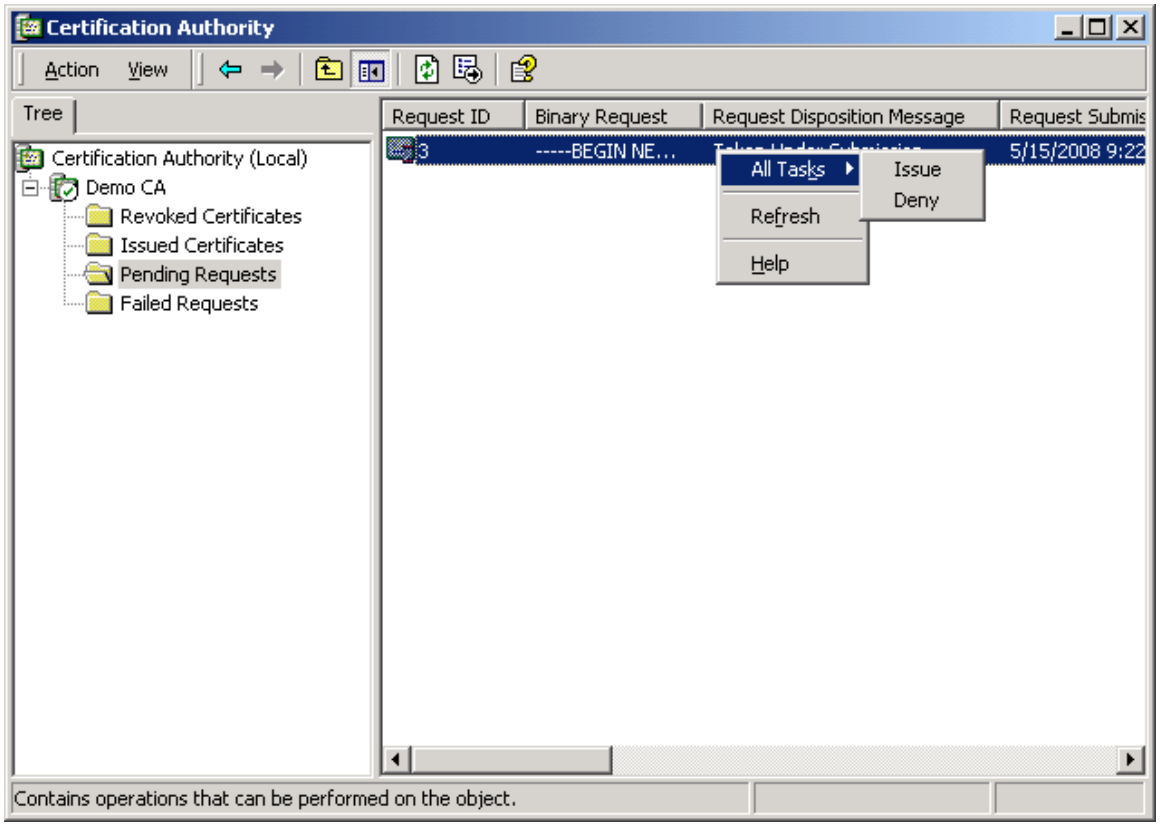
4. In the page that appears, select **Submit a certificate request to this CA using a form**, and click **Next**.



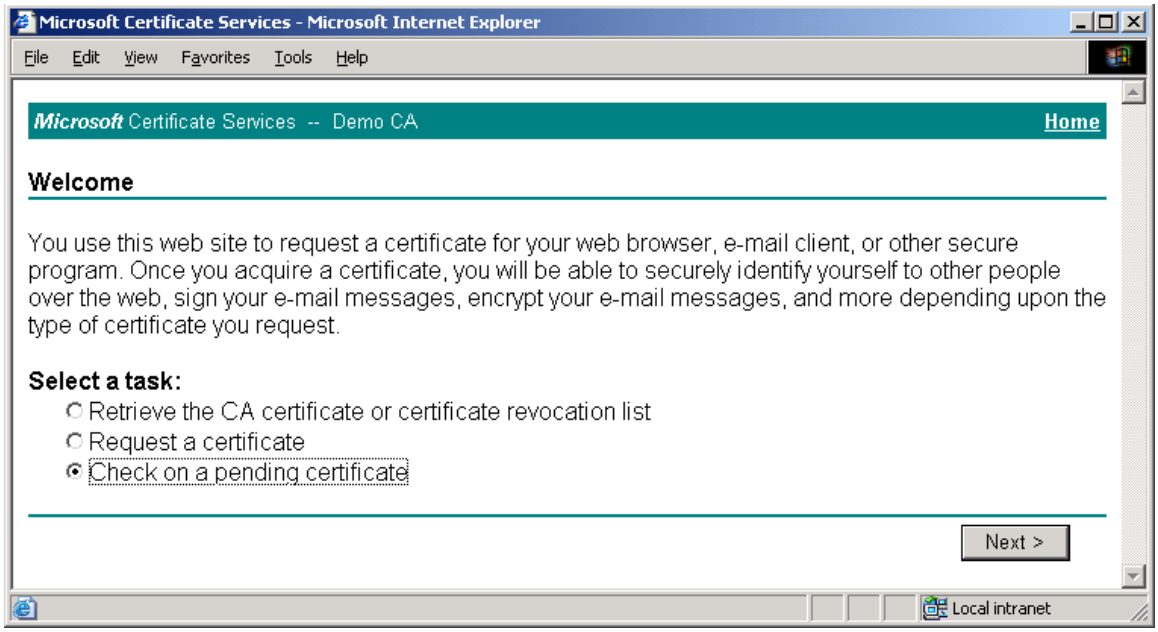
5. In the page that appears, do the following:
   a. Fill in the fields in the “Identifying Information” section as appropriate.
   b. In the “Intended Purpose” drop-down list, select **Code Signing Certificate**.
   c. In the “Key Options” section, make the choices appropriate to your environment.
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



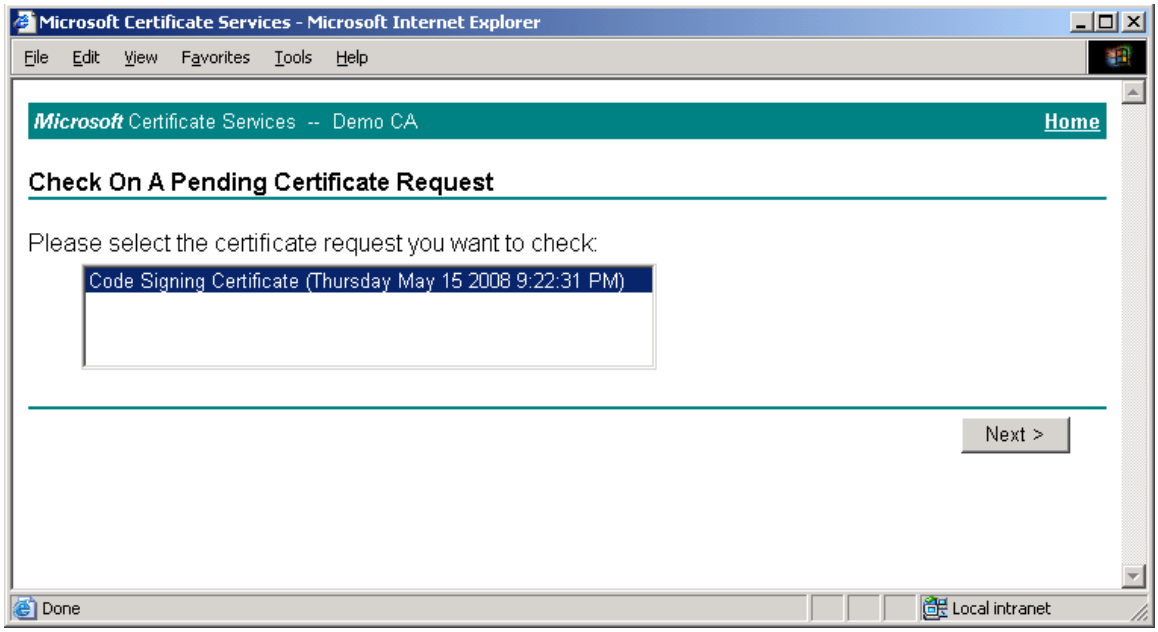
6. Depending on whether you have direct control over the certificate authority, do one of the following:
   - If you do not have direct control over the CA, wait until the certificate is approved by the CA administrator, then proceed to the next step.
   - If you have direct control over the CA, approve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



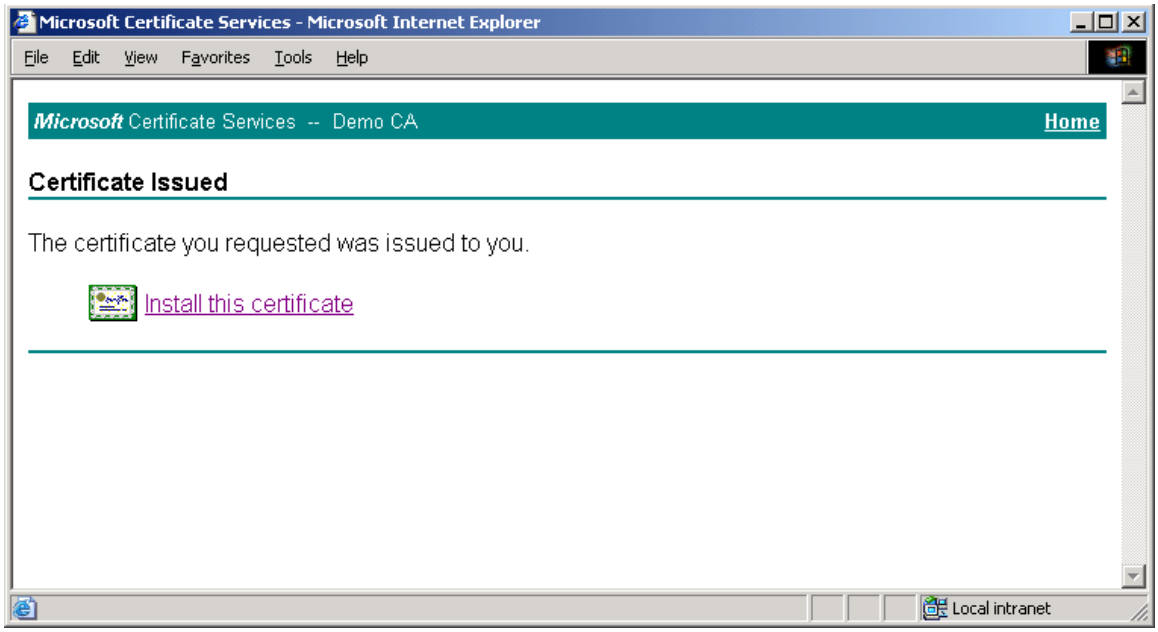
7. Once the certificate request has been approved, return to Microsoft Certificate Server's enrollment page, select **Check on a pending certificate**, and click **Next**.



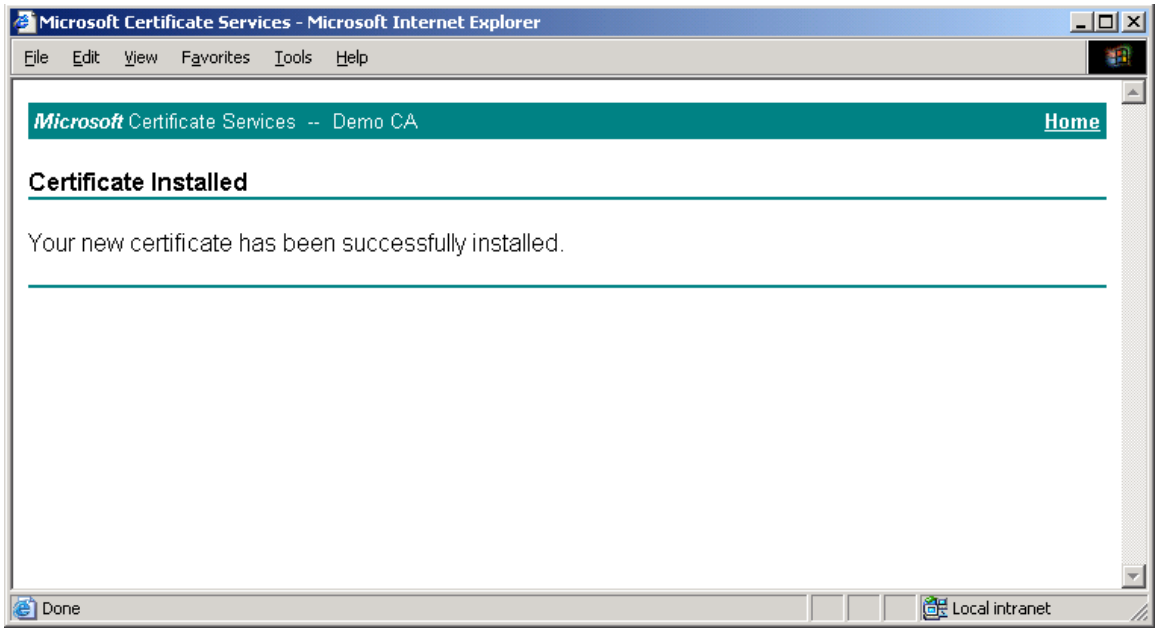
8. In the page that appears, select the target certificate request and click **Next**.



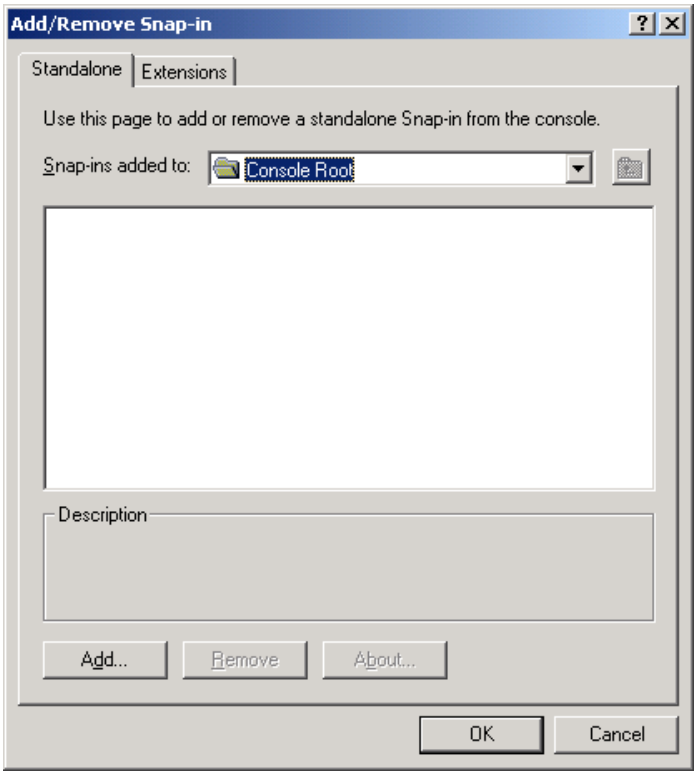
9. In the page that appears, click the **Install the certificate** link.



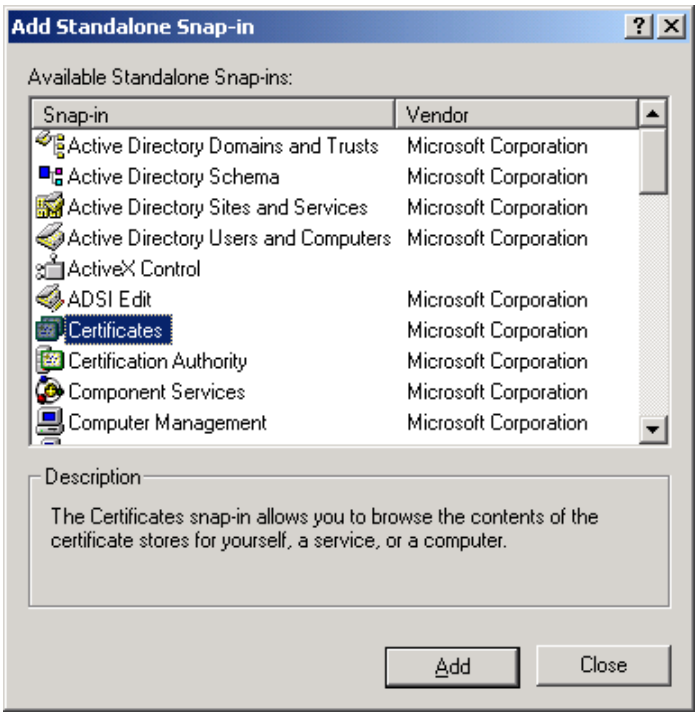
When the certificate is successfully installed, a confirmation page appears:



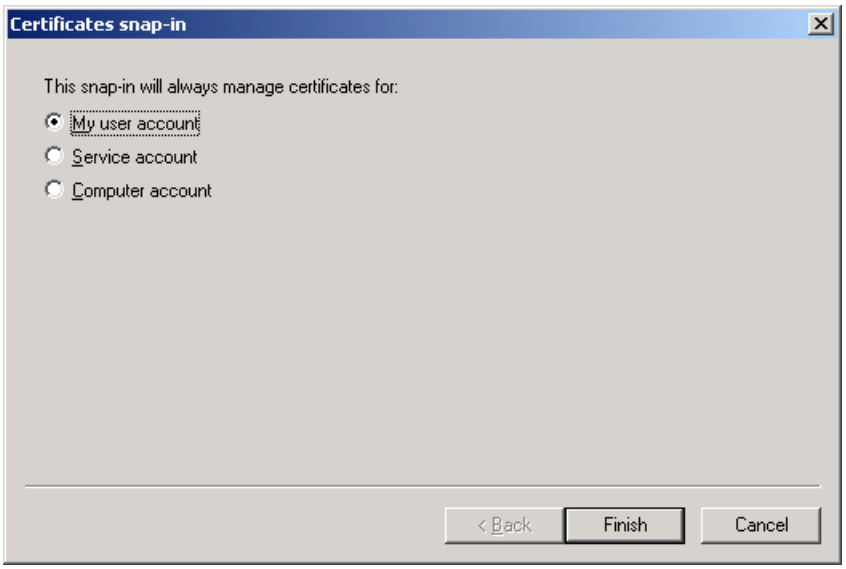
10. Launch the Microsoft Management Console.
11. In the console, add the “Certificates” snap-in:
    a. From the **Console** menu, select **Add/Remove Snap-in**.
    b. In the dialog that appears, click **Add**.



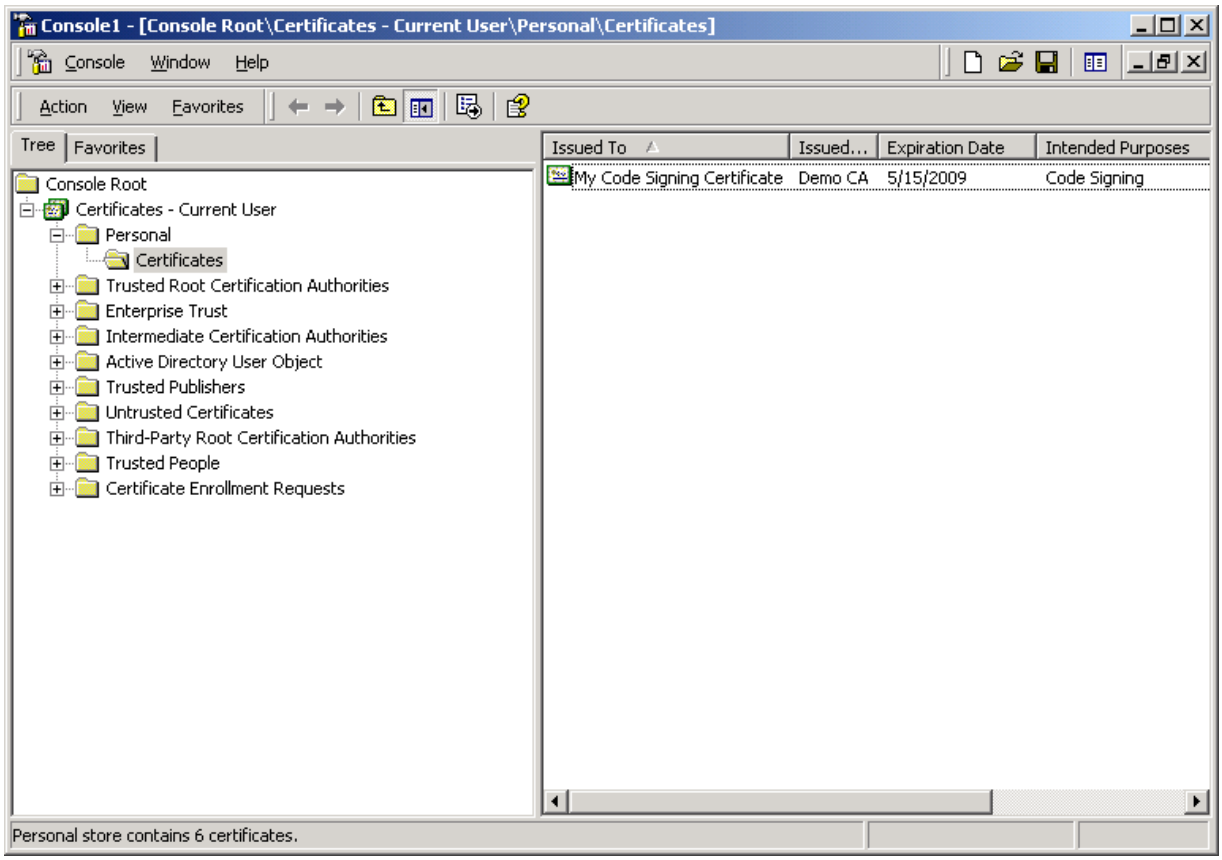
    c. In the list that appears, select **Certificates** and click **Add**.



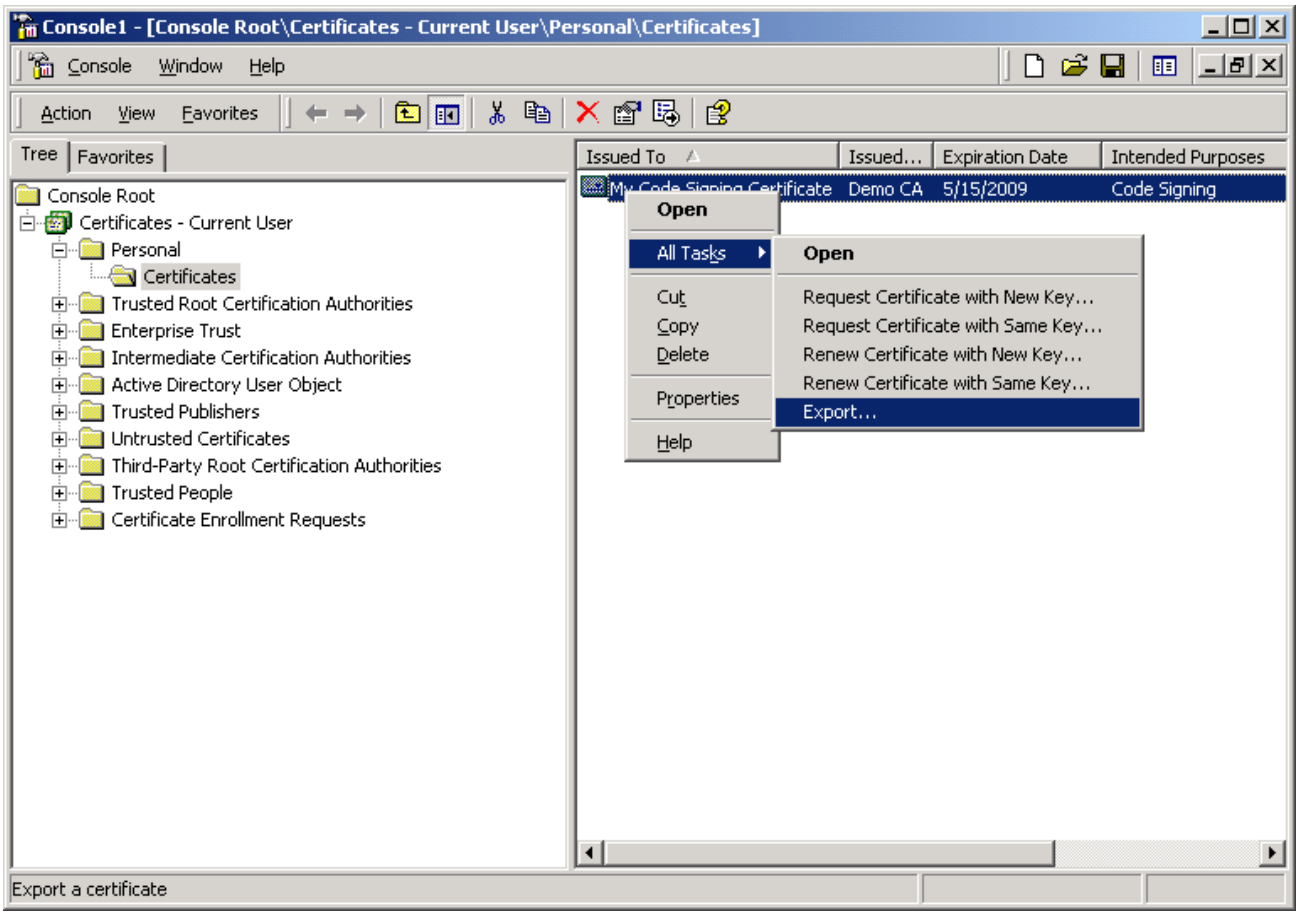
d. In the dialog that appears, select **My user account** and click **Finish**.



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.



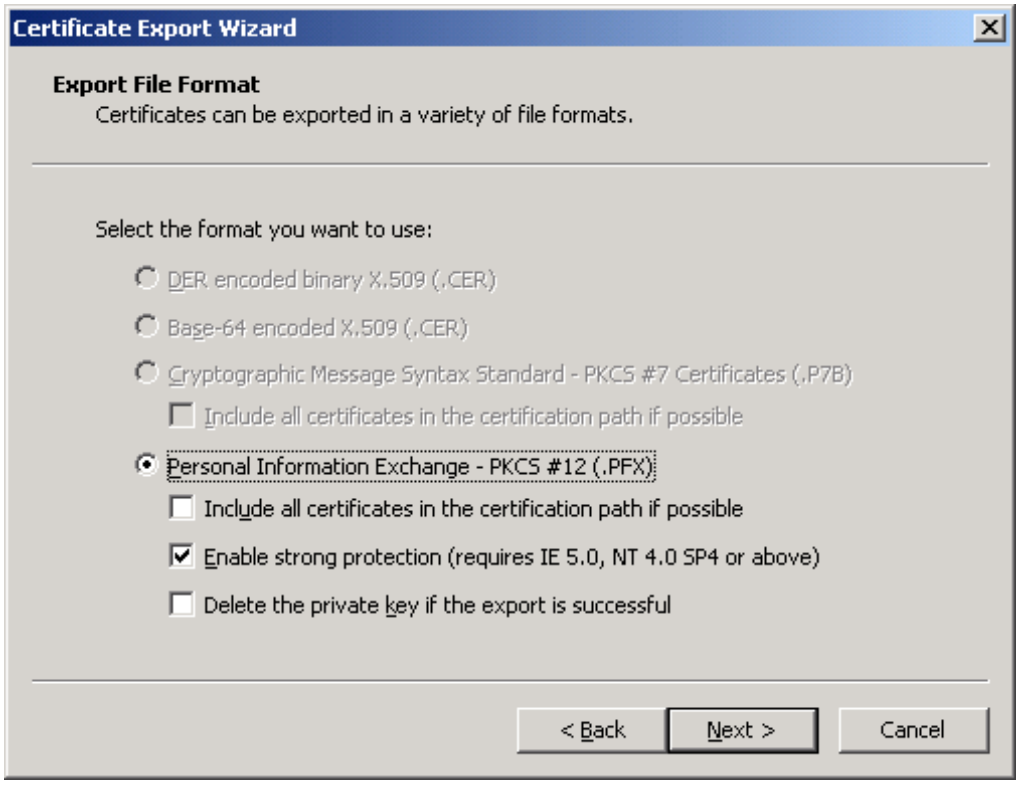
14. In the right-hand pane, right-click the desired certificate, then select **All Tasks → Export** from the context menu.



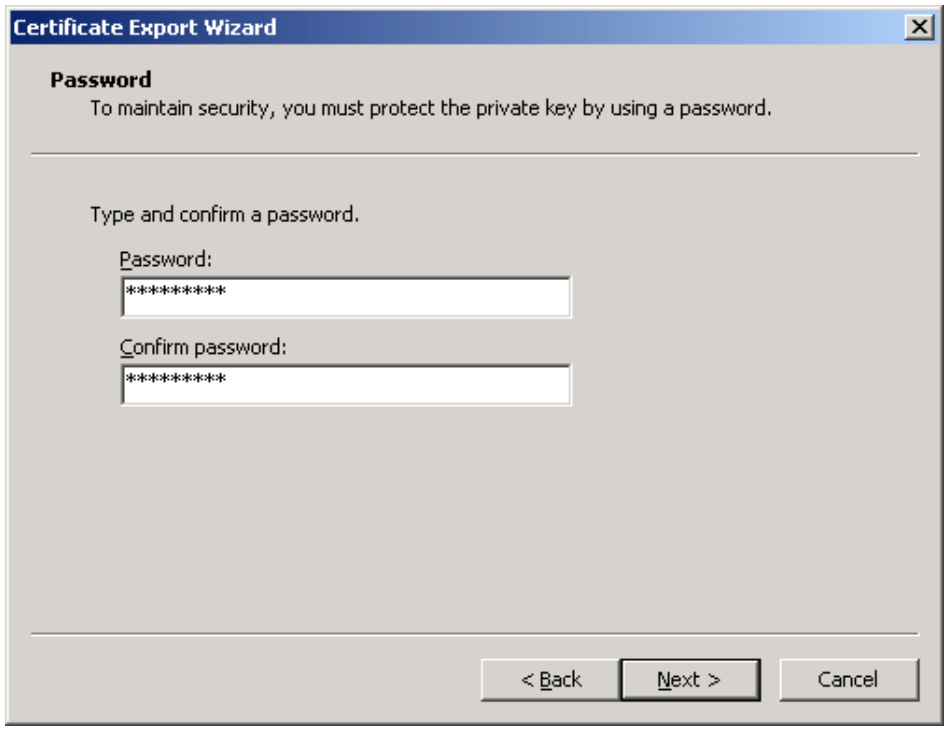
15. In the "Certificate Export Wizard" that appears, click **Next**.

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

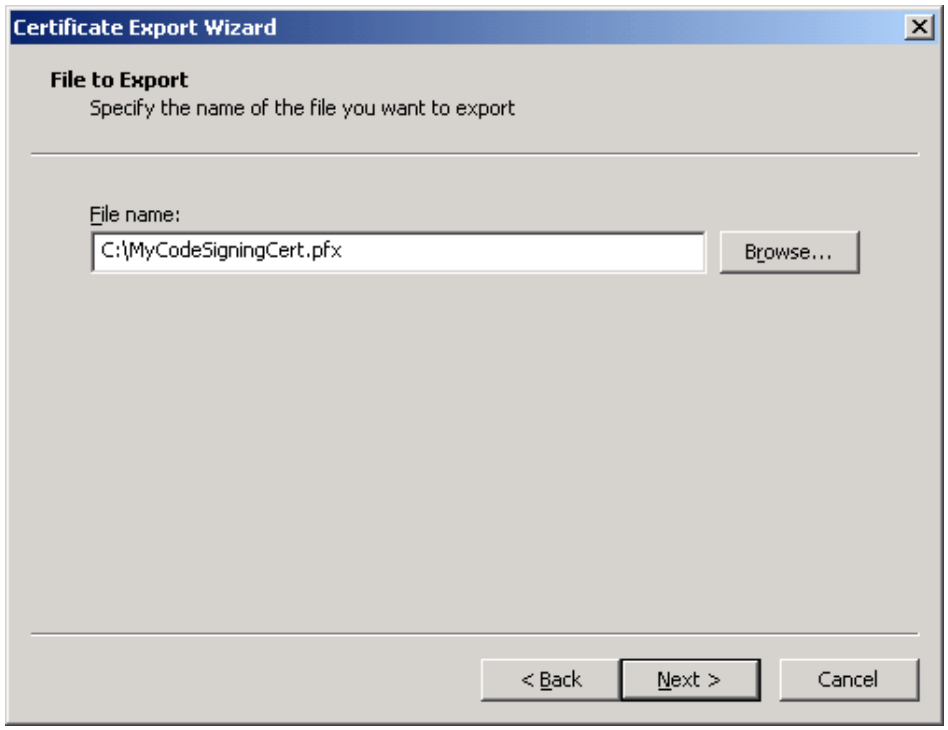
17. In the “Export File Format” screen, leave the options at their default values and click **Next**.



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



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**.



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

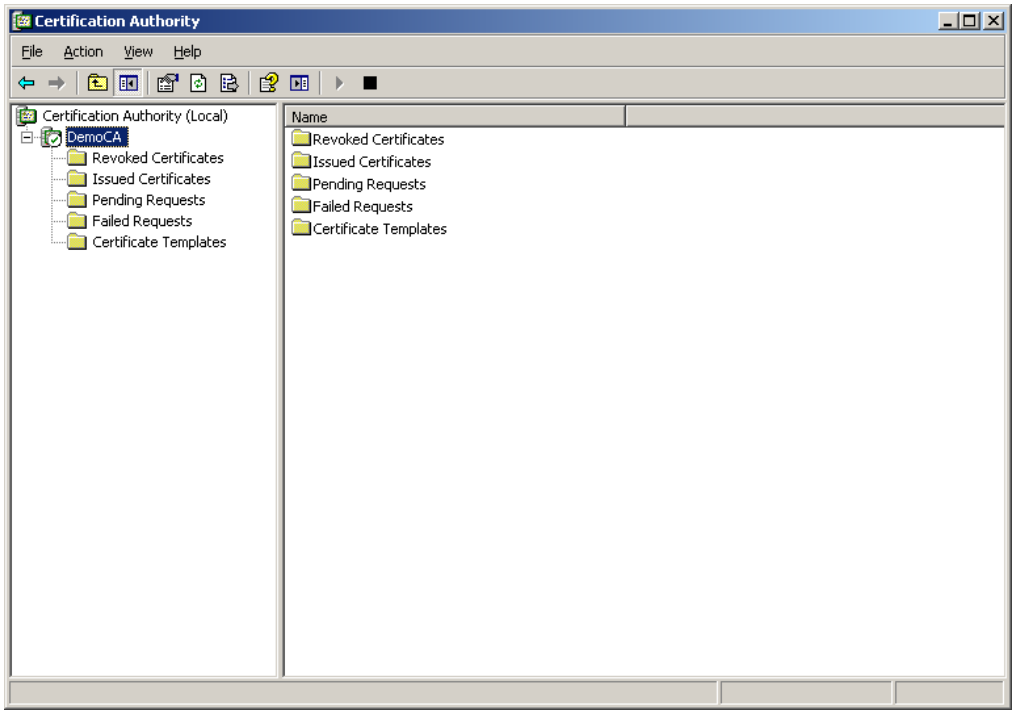
The certificate is now available as a password-protected file at the location you have chosen.

Creating an SSL Certificate with an Enterprise Certificate Authority

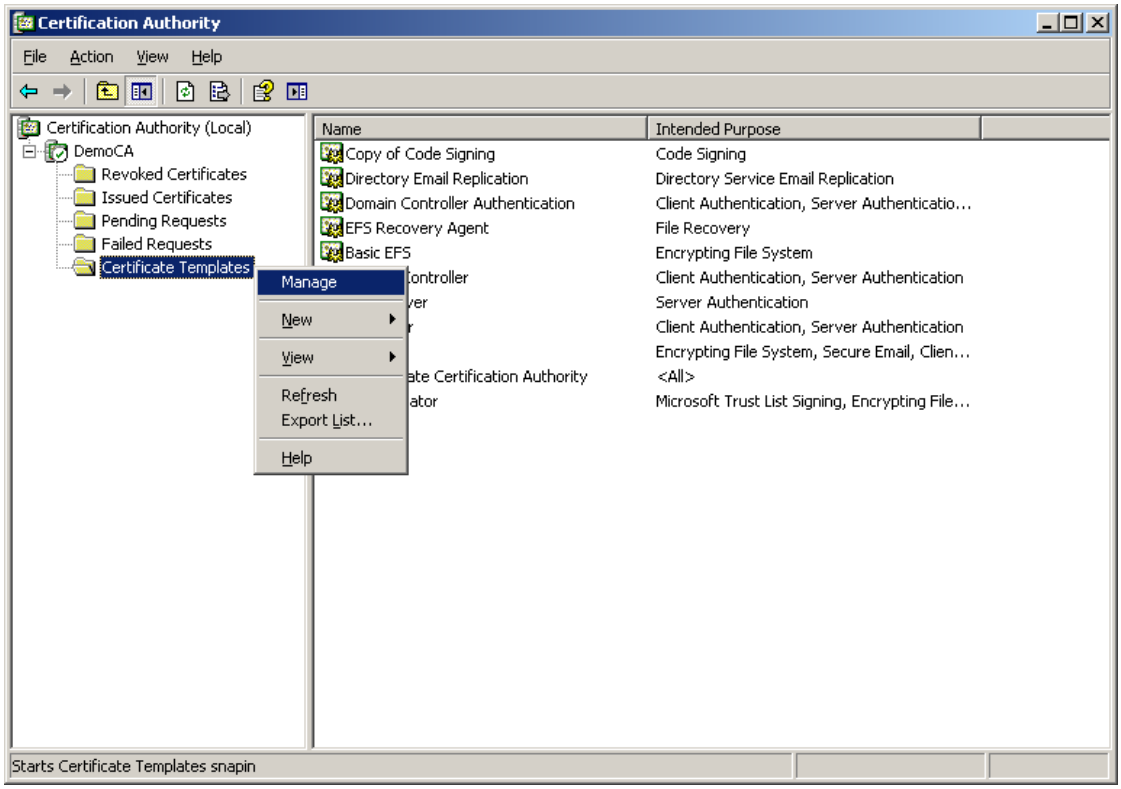
To create an SSL certificate on Windows Server 2003 Enterprise Edition using an enterprise certificate authority, do the following:

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

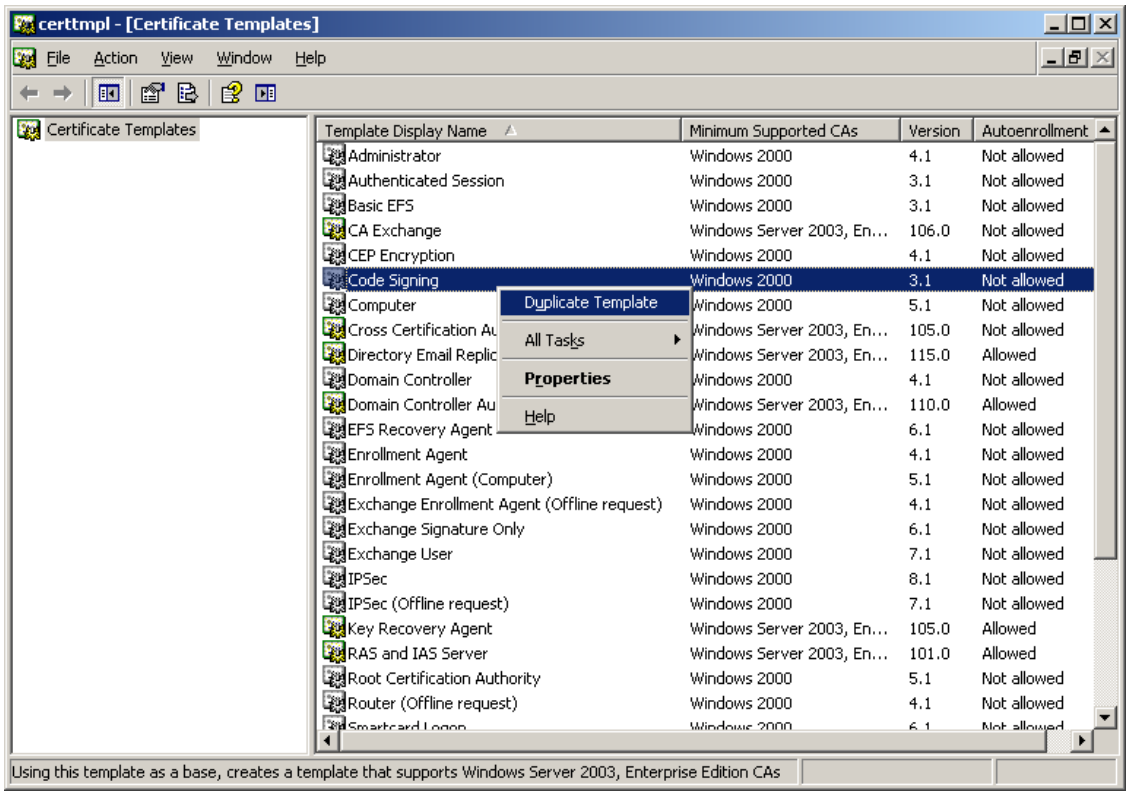
1. Launch the Certificate Authority tool.
2. In the tree in the left-hand pane, expand the root node.



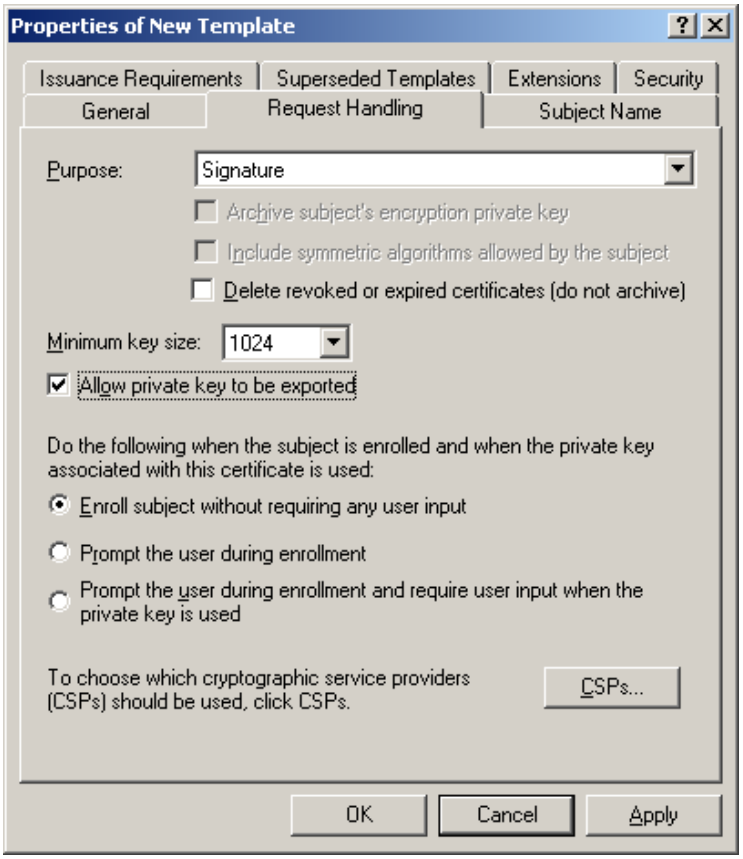
3. Right-click the **Certificate Templates** node, and select **Manage** from the context menu.



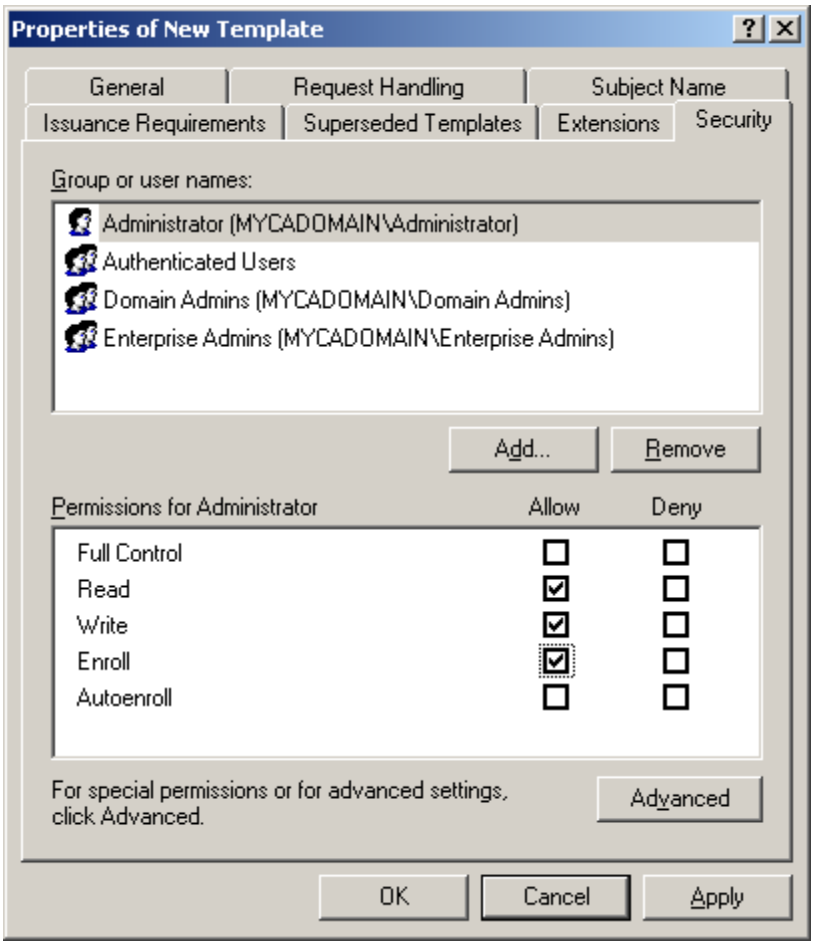
4. In the list of templates in the right-hand pane, right-click the **Code Signing** template and select **Duplicate Template** from the context menu.



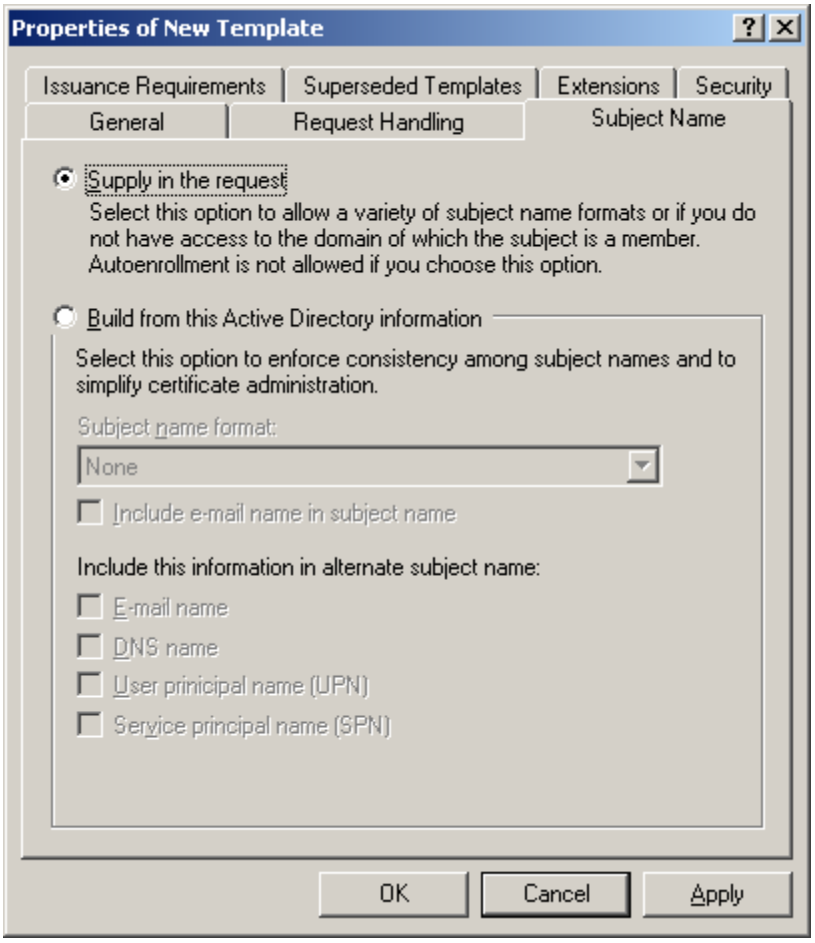
5. In the template properties dialog that appears, do the following:
    a. Select the **Request Handling** tab and select the **Allow private key to be exported** check box.



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

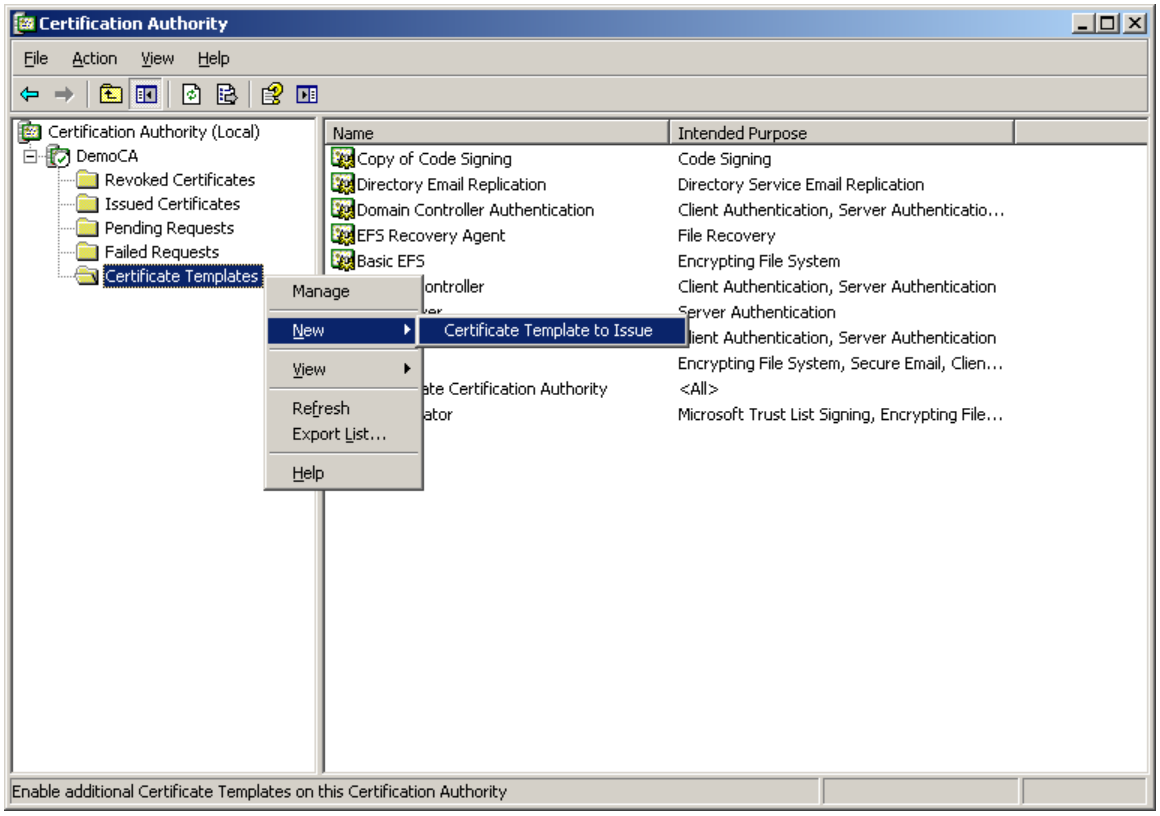


c. If you want to specify the subject name during certificate enrollment, select the **Subject Name** tab and select the **Supply the request** radio button. (If you want to use the default subject name of the enrolling user's account name, skip this step.)

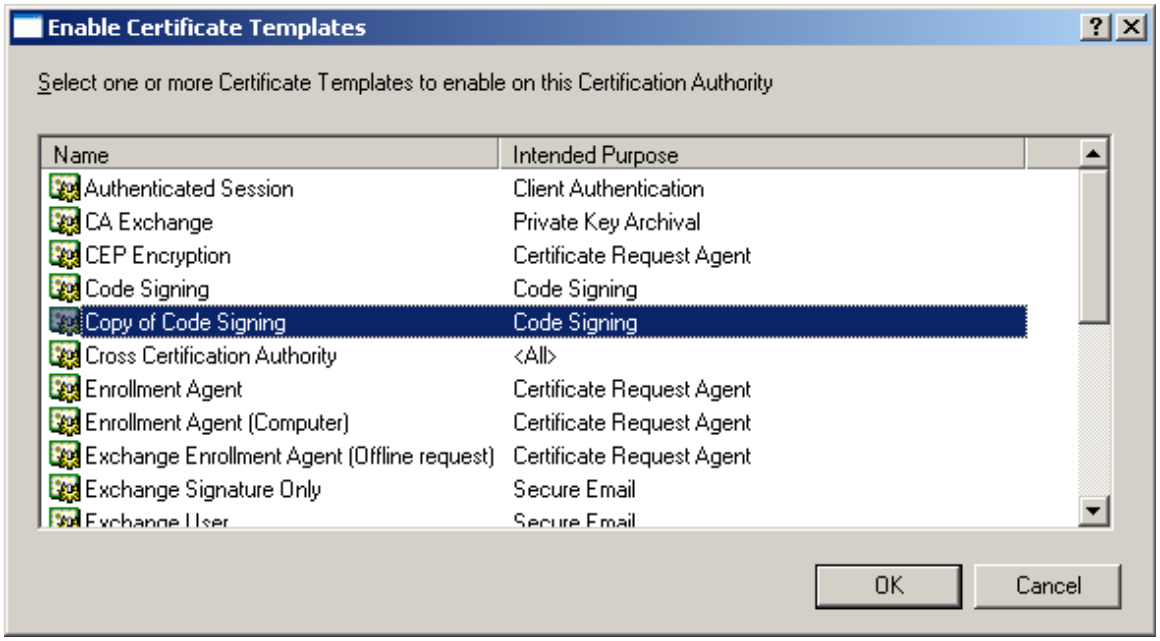


d. Configure other template options as desired, then click **OK** to save your changes. The new template appears in the list in the "Certificate Templates" window.

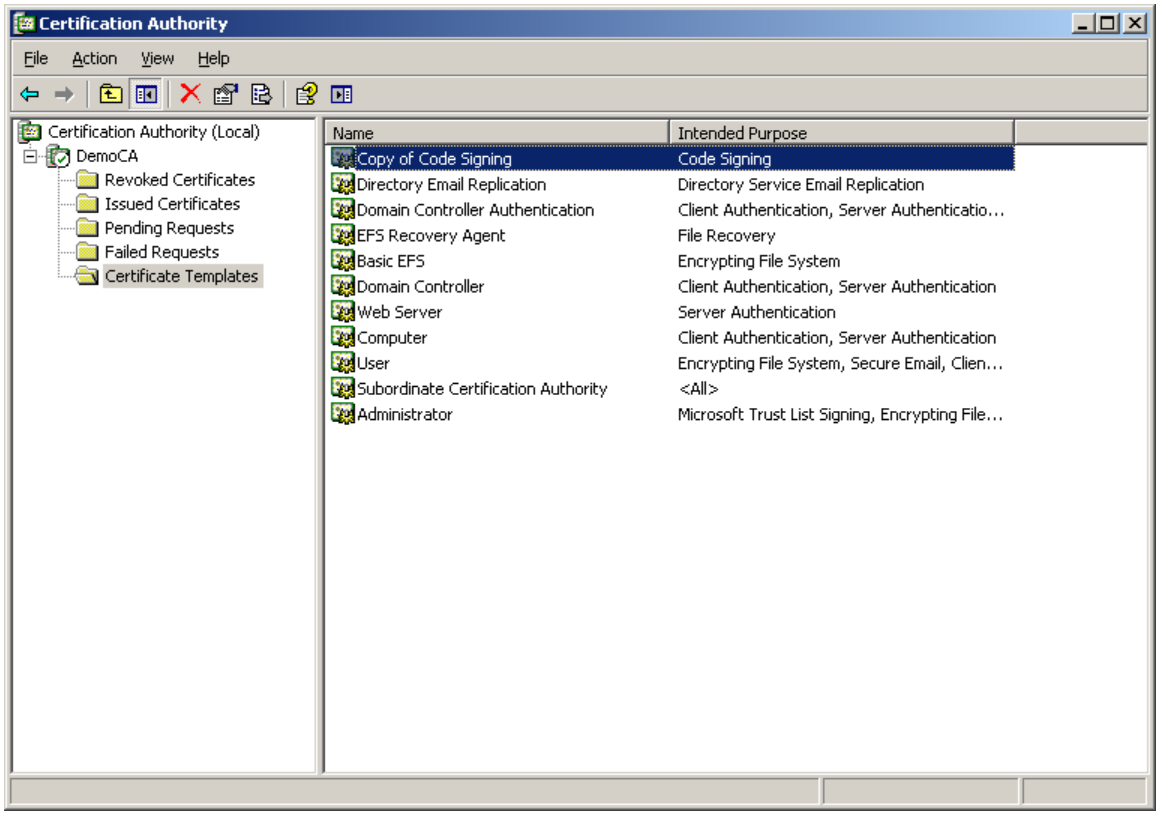
6. Close the “Certificate Templates” window and return to the Certificate Authority tool.
7. In the Certificate Authority tool, right-click the **Certificate Templates** node in the tree and select **New → Certificate Template to Issue** from the context menu.



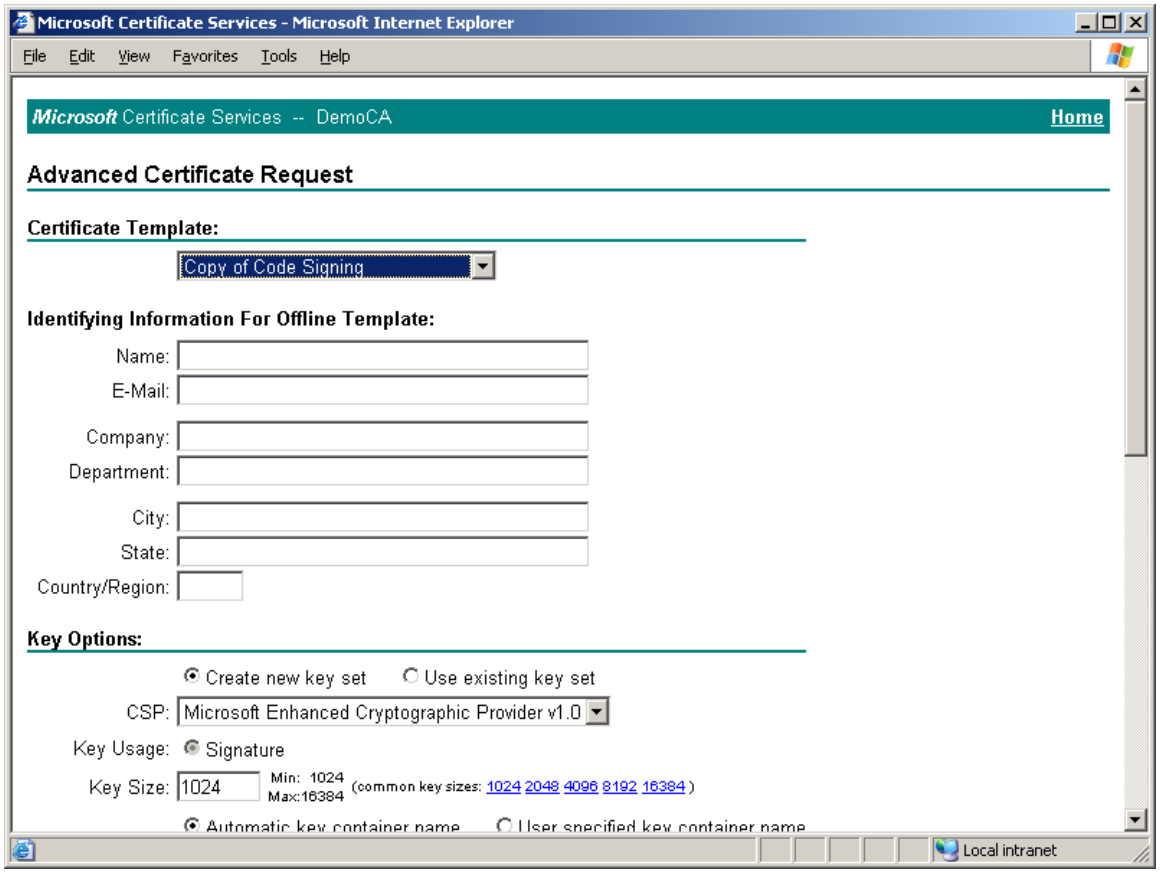
8. In the “Enable Template Certificates” dialog, select the template you created in the previous step, then click **OK**.



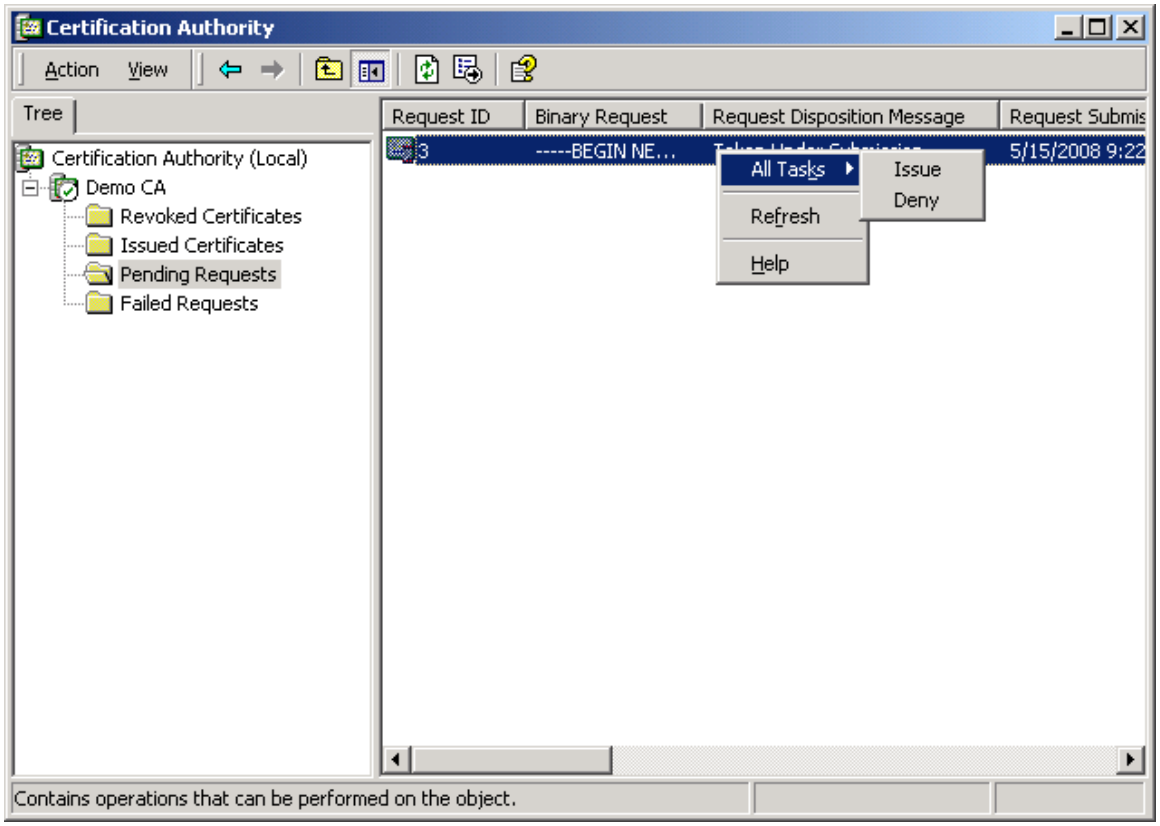
9. Click the **Certificate Templates** node again to refresh the template list and verify that the new template has been successfully enabled.



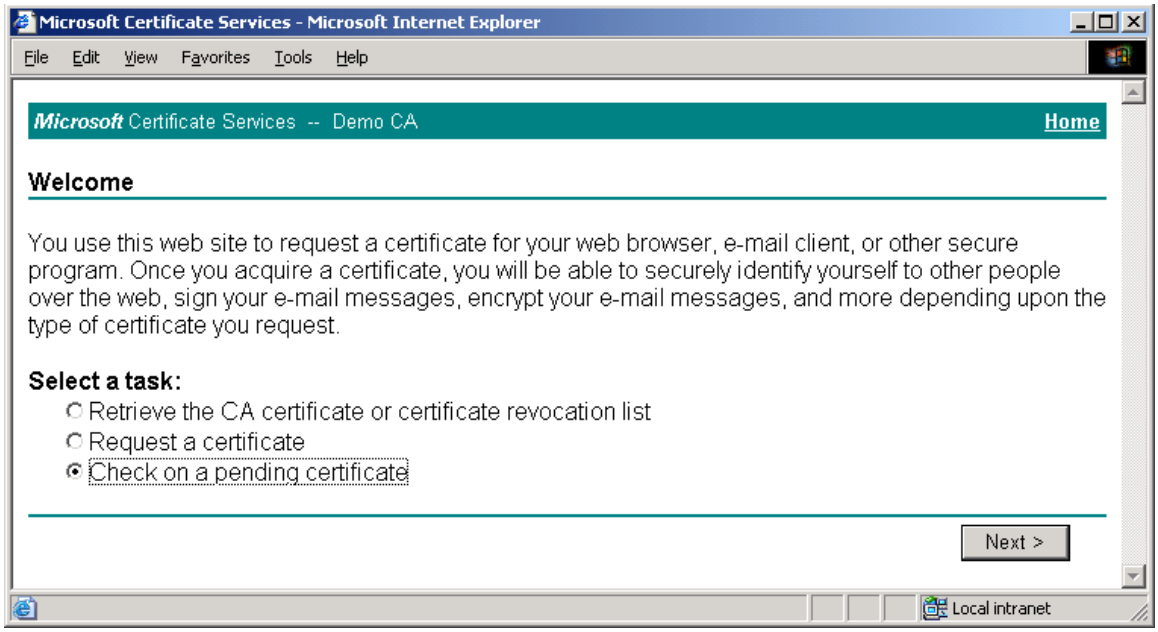
10. In the page that appears, do the following:
    a. Fill in the fields in the “Identifying Information” section as appropriate.
    b. In the “Certificate Template” drop-down list, select your newly created template.
    c. In the “Key Options” section, make the choices appropriate to your environment.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



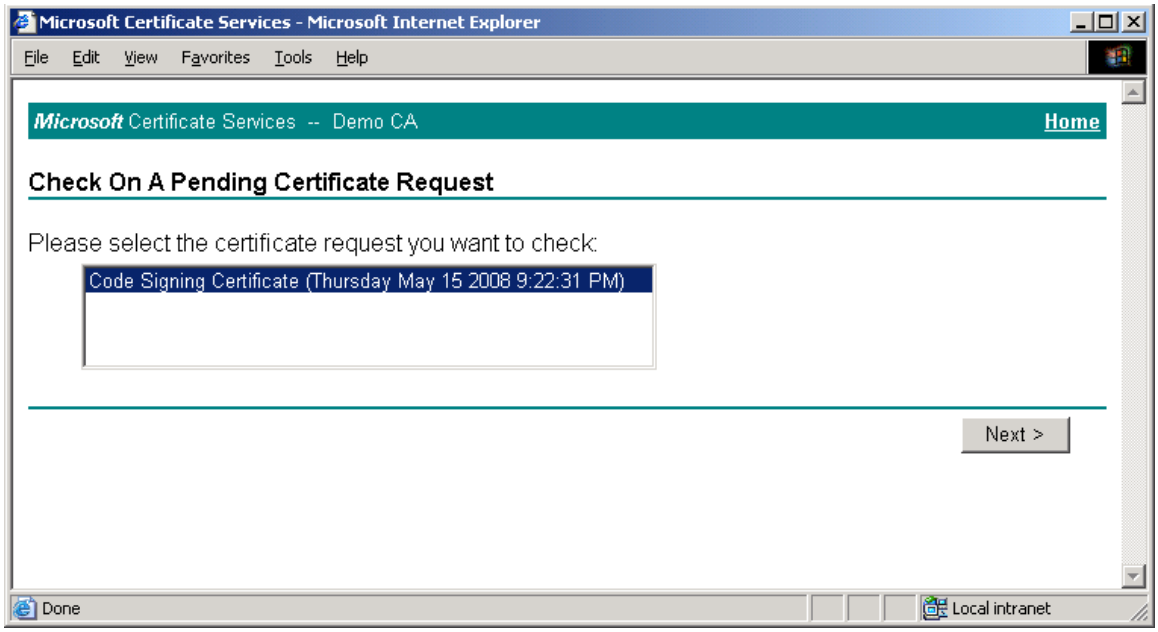
11. Depending on whether you have direct control over the certificate authority, do one of the following:
    - If you do not have direct control over the CA, wait until the certificate is approved by the CA administrator, then proceed to the next step.
    - If you have direct control over the CA, approve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



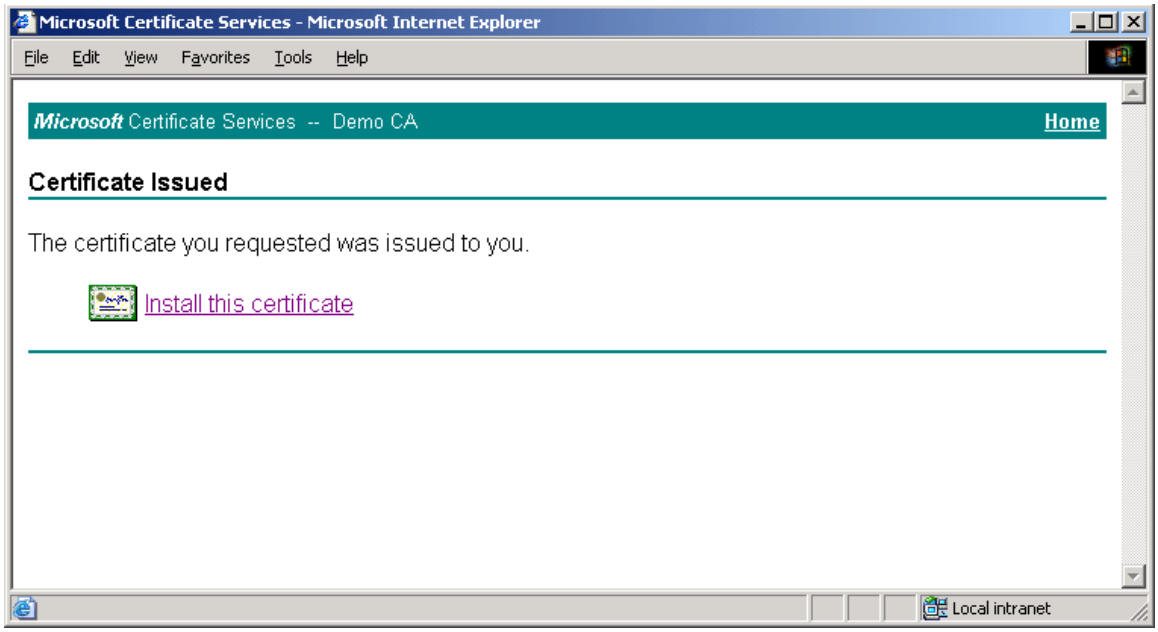
12. Once the certificate request has been approved, return to Microsoft Certificate Server's enrollment page, select **Check on a pending certificate**, and click **Next**.



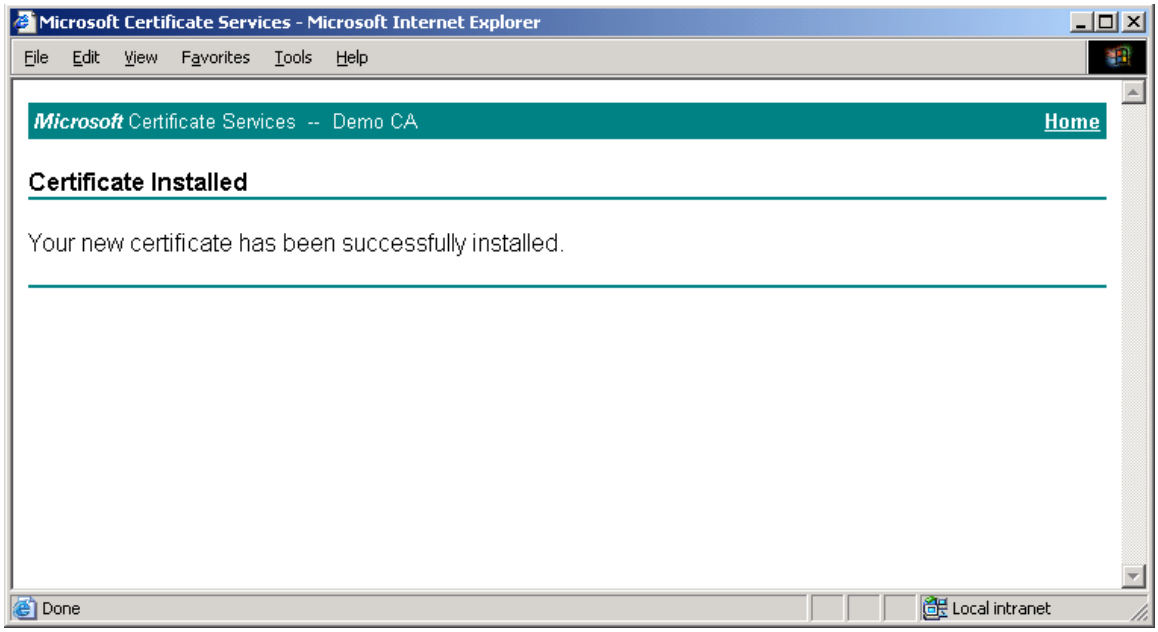
13. In the page that appears, select the target certificate request and click **Next**.



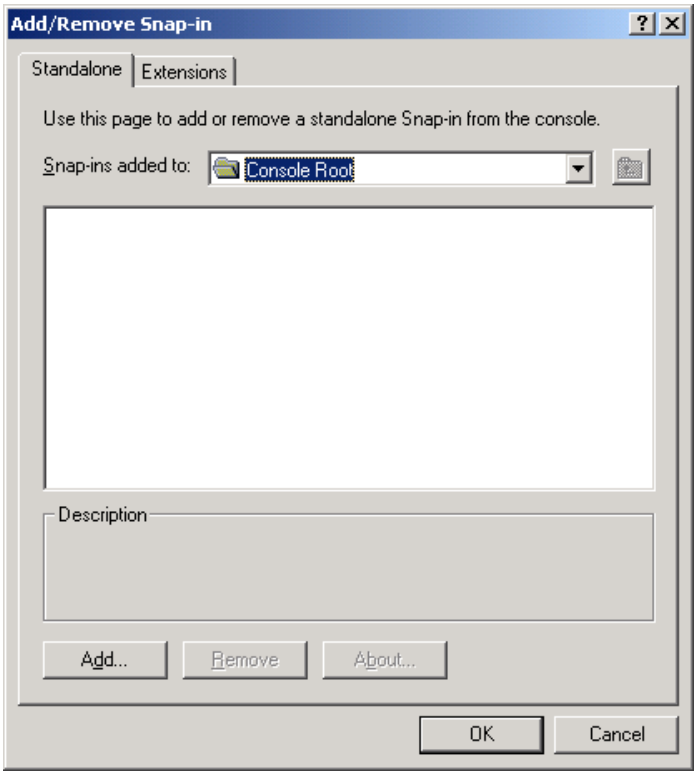
14. In the page that appears, click the **Install the certificate** link.



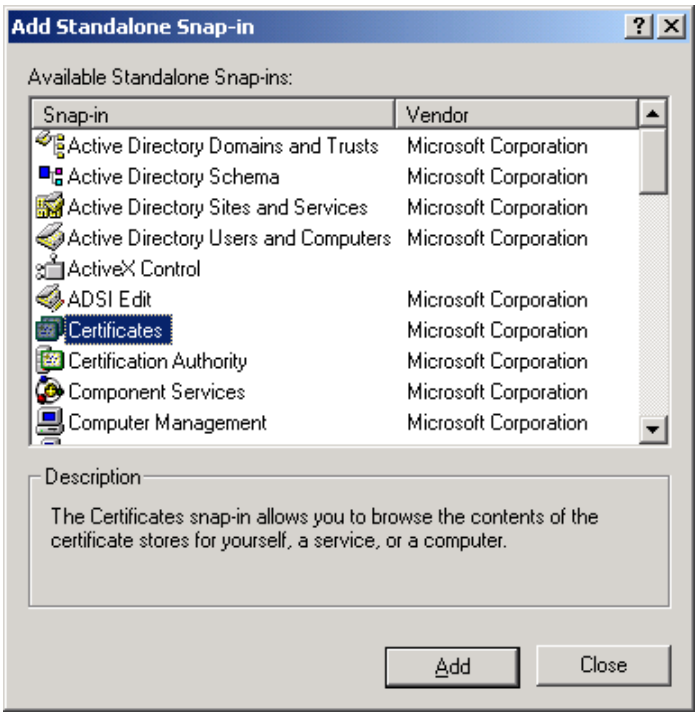
When the certificate is successfully installed, a confirmation page appears:



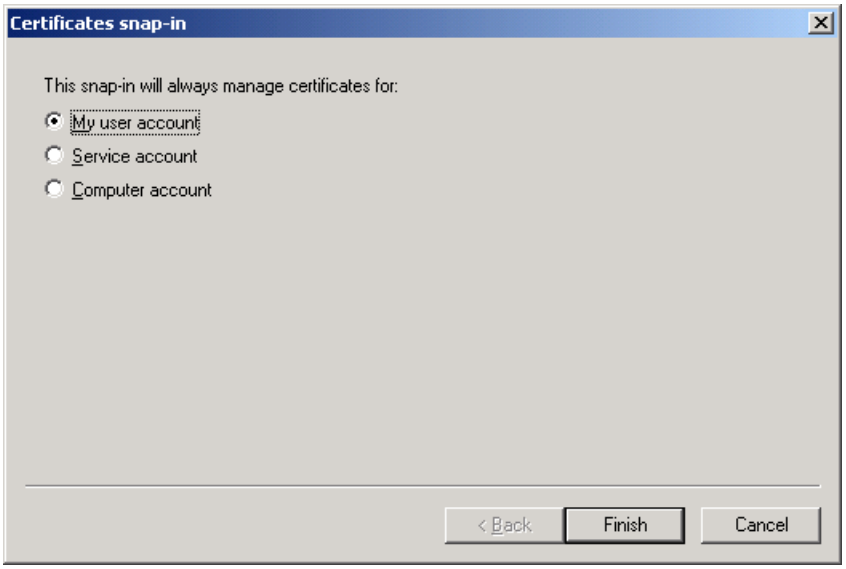
15. Launch the Microsoft Management Console.
16. In the console, add the “Certificates” snap-in:
    a. From the **Console** menu, select **Add/Remove Snap-in**.
    b. In the dialog that appears, click **Add**.



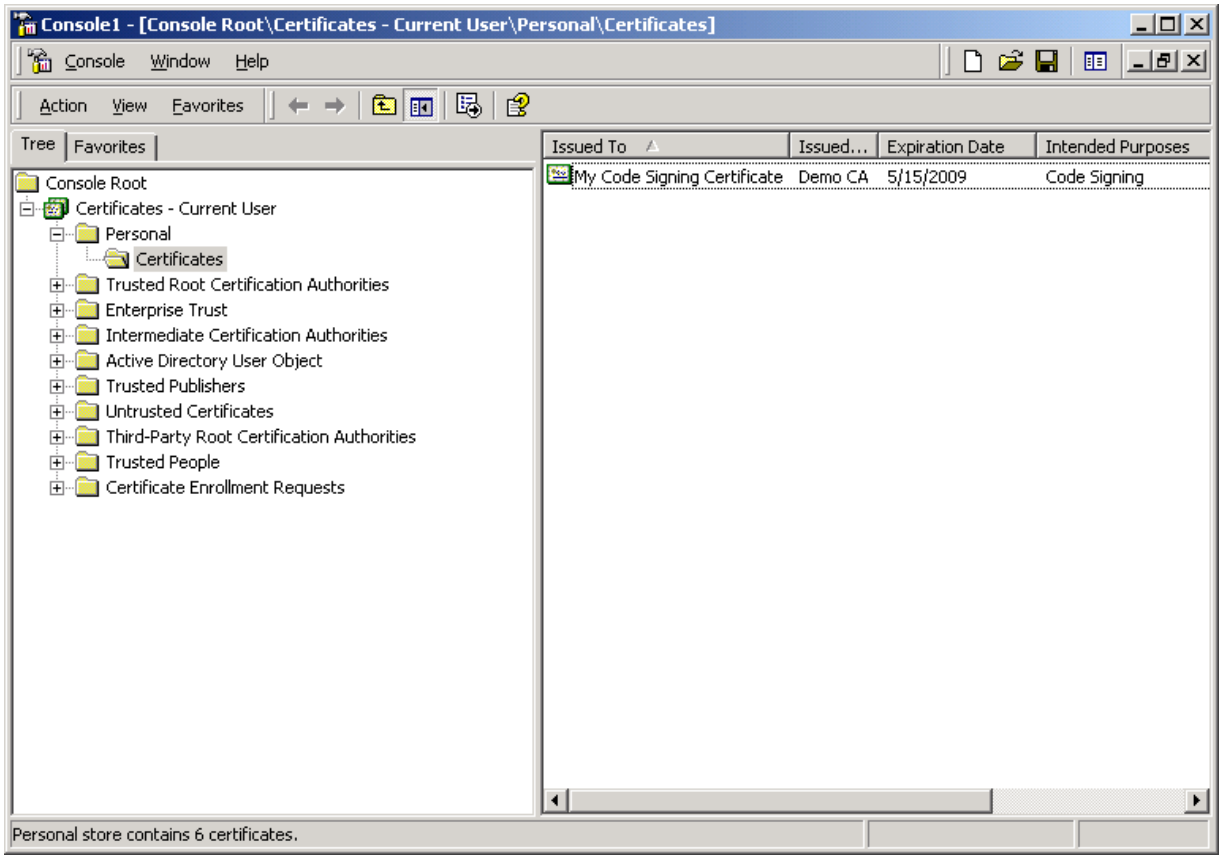
    c. In the list that appears, select **Certificates** and click **Add**.



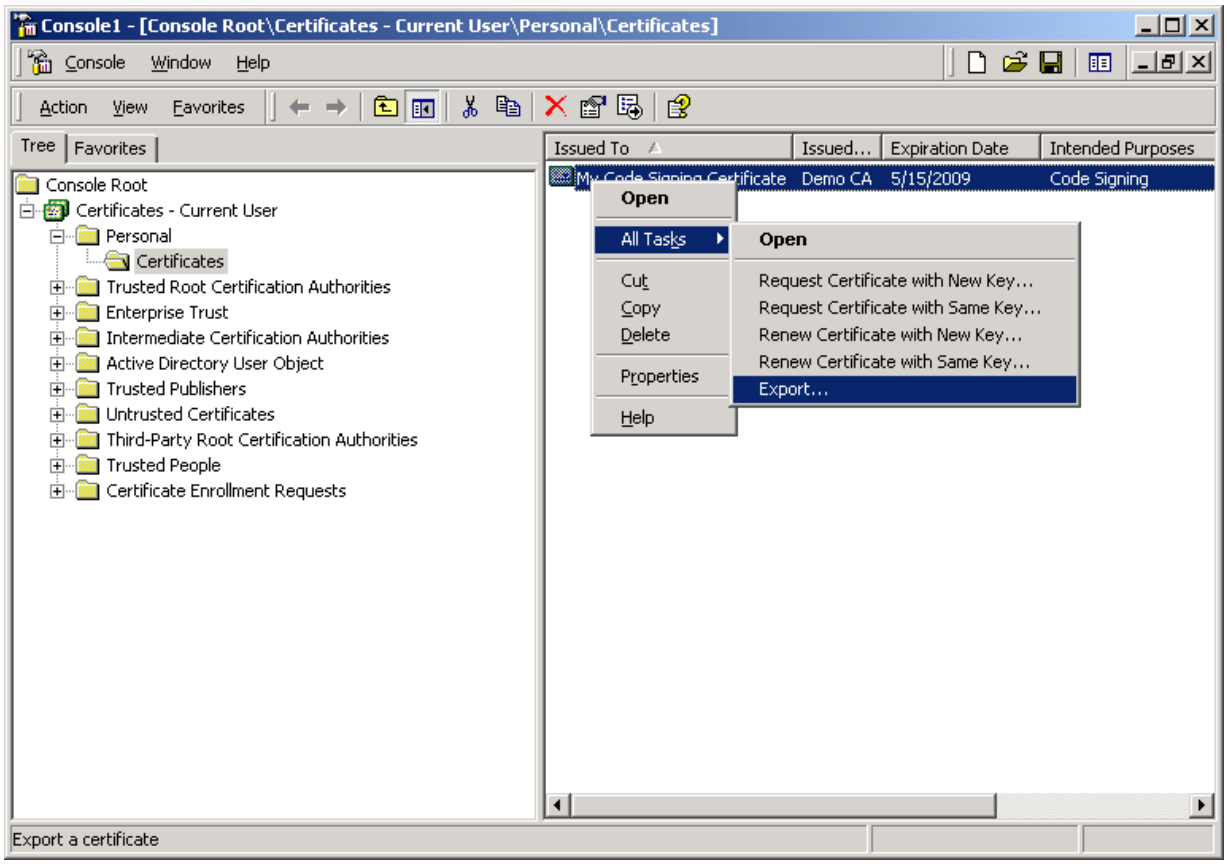
d. In the dialog that appears, select **My user account** and click **Finish**.



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.



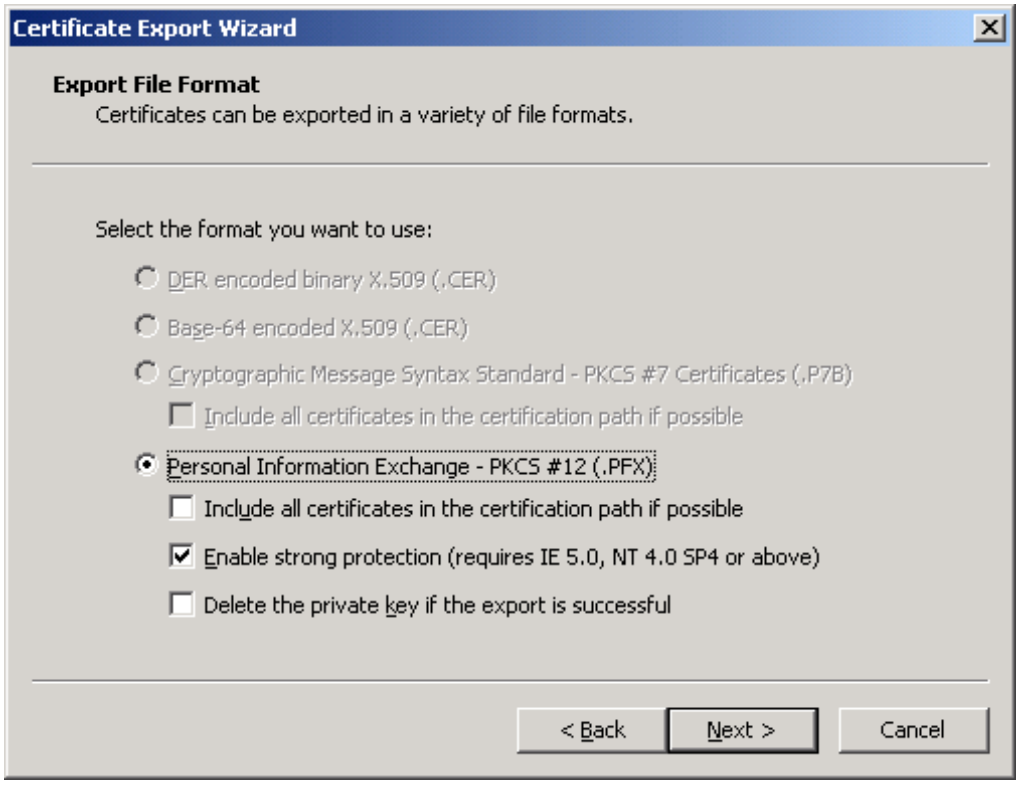
19. In the right-hand pane, right-click the desired certificate, then select **All Tasks → Export** from the context menu.



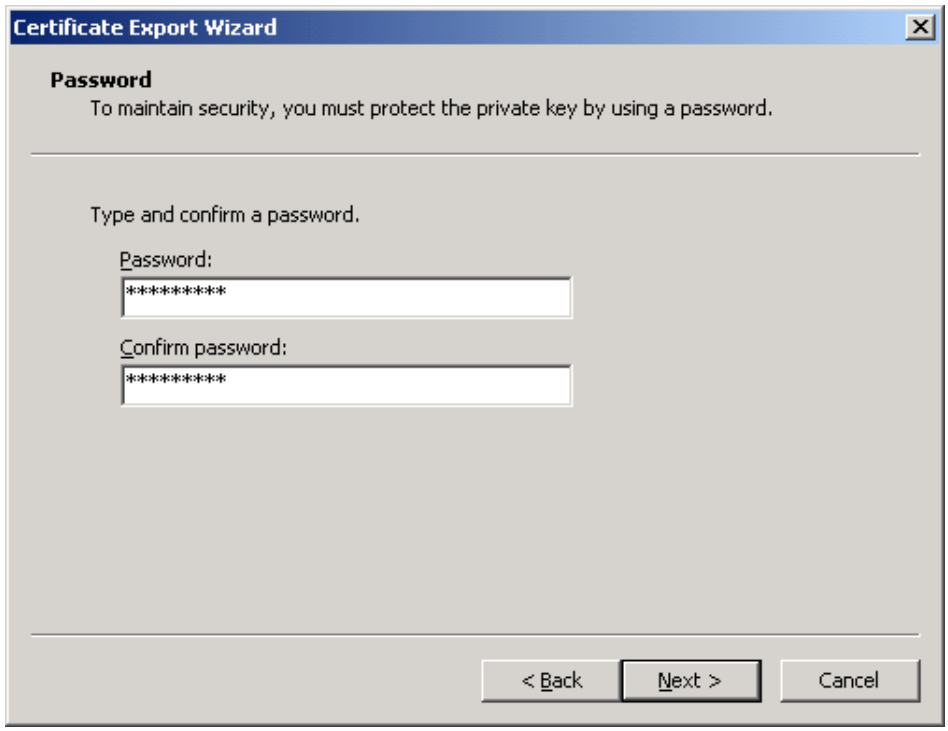
20. In the "Certificate Export Wizard" that appears, click **Next**.

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

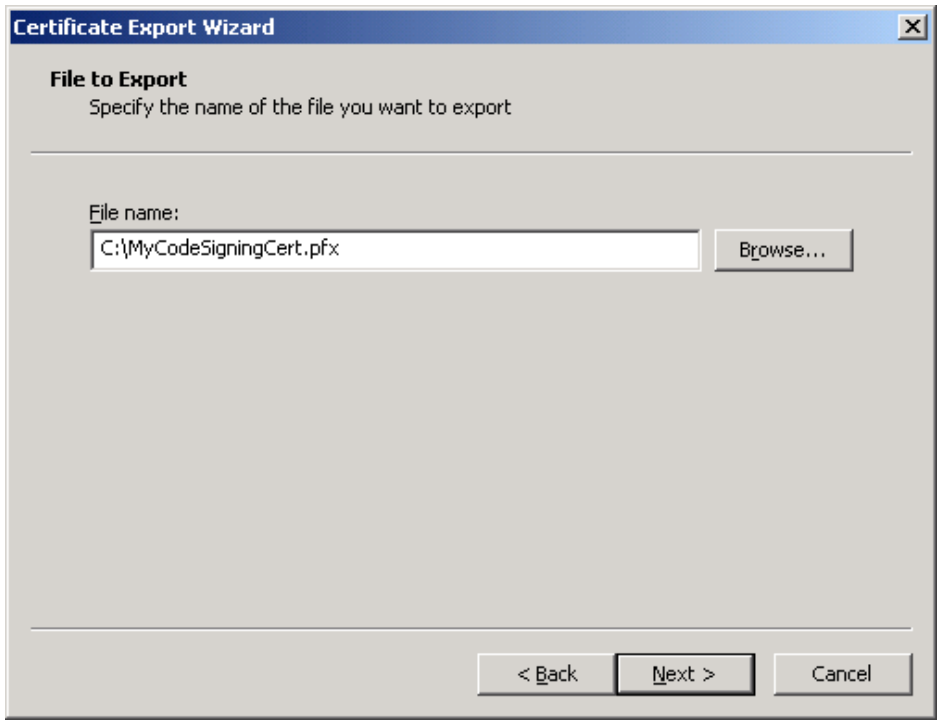
22. In the “Export File Format” screen, leave the options at their default values and click **Next**.



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



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**.



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

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