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 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

Table of Contents	. 3
Introduction	.4
About This Guide	.4
Prerequisites	.4
Terms and Abbreviations	.4
Accessing ESSO-Anywhere Documentation	.4
Creating an SSL Certificate with a Standalone Certificate Authority	. 5
Creating an SSL Certificate with an Enterprise Certificate Authority	17

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.



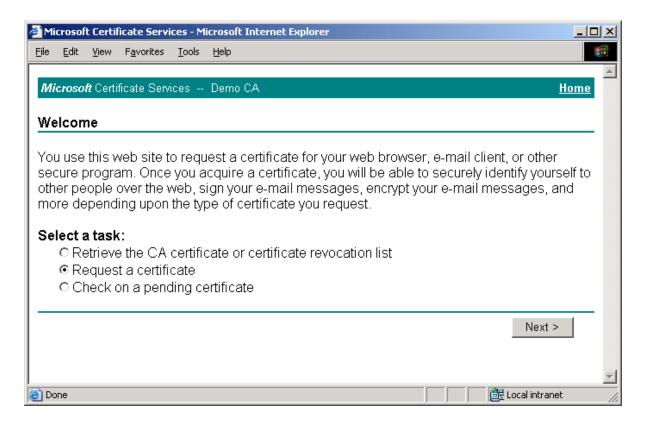
Creating an SSL Certificate with a Standalone Certificate Authority

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

 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**.

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	€ <mark>B</mark>
<i>Microsoft</i> Certificate Services Demo CA	Home
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	
	Next >
E Done	Local intranet

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

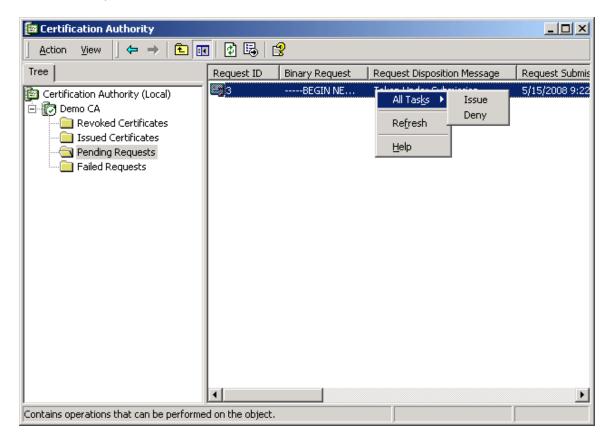
Microsoft Certificate Services - Microsoft Internet Explorer	
<u>Eile E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	10 A
<i>Microsoft</i> Certificate Services Demo CA	<u>Home</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following method Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.	ls.
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 St You must have an enrollment agent certificate to submit a request for another user.	tation.
Next :	>
	-
🗿 Done	net //



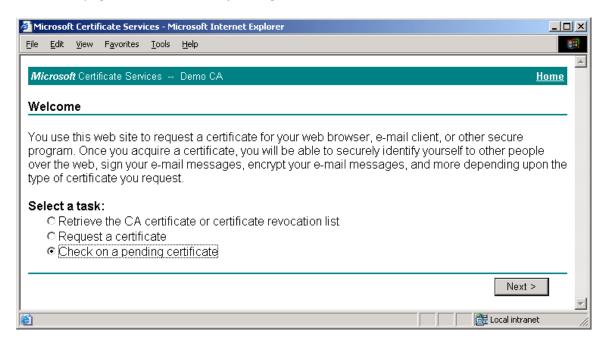
- 5. In the page that appears, do the following:
 - a. Fill in the fields in the "Identifying Information" section as appropriate.
 - b. In the "Intended Purpose" drop-down list, select Code Signing Certificate.
 - c. In the "Key Options" section, make the choices appropriate to your environment.
 -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

🚰 Microsoft Certifi	cate Services - Microsoft Internet Explorer	<u>_ ×</u>
<u>File E</u> dit <u>V</u> iew	Favorites Tools Help	1
Microsoft Certifi	icate Services Demo CA	lome ▲
Advanced Ce	ertificate Request	
Identifying Infor	mation:	
Name:	My Code Signing Certificate	
E-Mail:		
Company:		
Department:		
City:		
State:		
Country/Region:	US	
Intended Purpos	se:	
intended i dipe.	Code Signing Certificate	
Key Options:		
	Microsoft Enhanced Cryptographic Provider v1.0	
	⊂ 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	
	O Use existing key set □ Enable strong private key protection	
	I Mark keys as exportable	
	Use local machine store	
	You must be an administrator to generate a key in the local machine store.	
a	a key in the local machine store.	

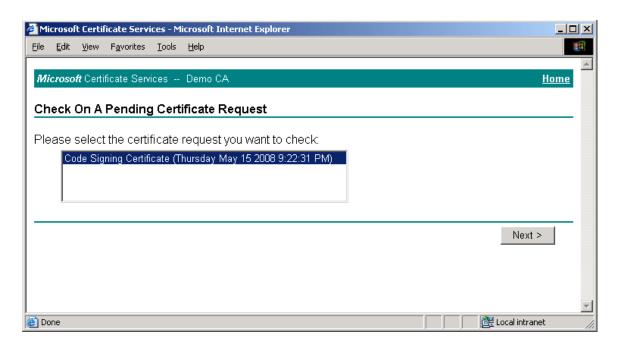
- 6. Depending on whether you have direct control over the certificate authority, do one of the following:
 - If you do not have direct control over the CA, wait until the certificate is approved by the CA administrator, then proceed to the next step.
 - If you have direct control over the CA, approve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



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**.

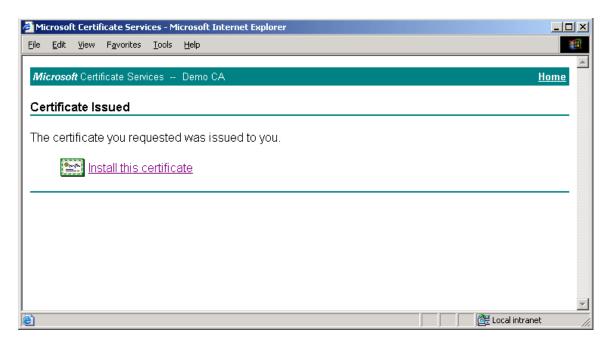


8. In the page that appears, select the target certificate request and click Next.





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



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

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
<u>Eile Edit View Favorites Tools H</u> elp	100 A
<i>Microsoft</i> Certificate Services Demo CA	<u>Home</u>
Certificate Installed	
Your new certificate has been successfully installed.	
	T
🙆 Done	🛛 🔠 Local intranet 🖉



- 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.

Add/Remove Snap-in	? ×
Standalone Extensions	
Use this page to add or remove a standalone Snap-in from the console.	
Snap-ins added to: Sonsole Root	
Description Add <u>Remove</u> About	
OKC.	ancel

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





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

Certificates snap-in	×
This snap-in will always manage certificates for:	
O Service account	
O Computer account	
< Back. Finish Cancel	

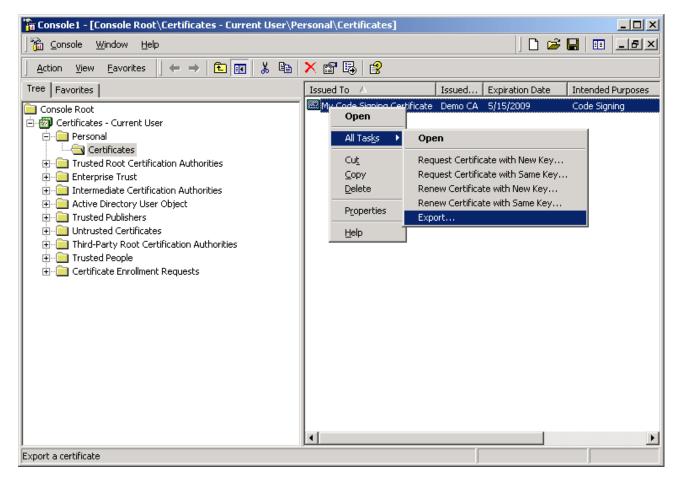
- 12. Close the remaining open dialog boxes inside the Management Console.
- 13. In the tree in the left-hand pane, navigate to:

Certificates –	Current User	\rightarrow Personal \rightarrow	Certificates.

🚡 Console1 - [Console Root\Certificates - Current User\Pe	rsonal\Certificates]			
Console Window Help] 🗋 🖻	
$] \underline{A}$ ction <u>V</u> iew Eavorites $] \leftarrow \rightarrow \mathbf{E} \mathbf$				
Tree Favorites	Issued To 🔺	Issued	Expiration Date	Intended Purposes
Console Root	Wy Code Signing Certificate	Demo CA	5/15/2009	Code Signing
🖻 👹 Certificates - Current User				
⊡				
🗄 💼 Enterprise Trust				
🕀 📄 Intermediate Certification Authorities				
⊕ ☐ Active Directory User Object				
Third-Party Root Certification Authorities				
⊕ ·· 📄 Trusted People				
🗄 💼 Certificate Enrollment Requests				
	•			<u> </u>
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.



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	
O No, do not export the private key	
< <u>B</u> ack <u>N</u> ext > Cancel	

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:	
C DER encoded binary X.509 (,CER)	
C Bage-64 encoded X.509 (,CER)	
C gryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square 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	
< <u>B</u> ack <u>N</u> ext > Ca	ncel



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 u	sing a password.
Type and confirm a password.	
Password:	
ጥጥጥጥጥጥጥ	
Confirm password:	

< <u>B</u> ack	<u>N</u> ext > Cancel

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	Browse
<u> </u>	Next > Cancel





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

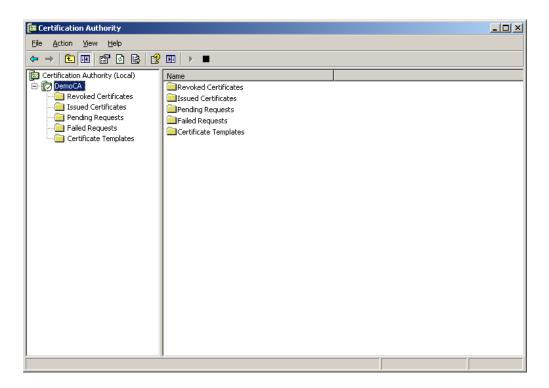
The certificate is now available as a password-protected file at the location you have chosen.

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.

🔯 Certification Authority			_ 🗆 🗵
<u>File Action View H</u> elp			
	2 🖬		
 Certification Authority (Local) DemoCA Revoked Certificates Issued Certificates Pending Requests Faled Requests Certificate Templates 	Name Copy of Code Signing Directory Email Replication Domain Controller Authentication EFS Recovery Agent Basic EFS Manage Vew View Refresh Export List Help	Intended Purpose Code Signing Directory Service Email Replication Client Authentication, Server Authenticatio File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien <all> Microsoft Trust List Signing, Encrypting File</all>	
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.

	elp			_8
🥵 Certificate Templates	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 Duplicate Template	Windows 2000	5.1	Not allowed
	Cross Certification Au All Tasks	Windows Server 2003, En	105.0	Not allowed
	Directory Email Replic	Windows Server 2003, En	115.0	Allowed
	Domain Controller Properties	Windows 2000	4.1	Not allowed
	Domain Controller Au Help	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



- 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.

Properties of New	7 Template	? ×		
Issuance Require General	ements Superseded Templates Request Handling	Extensions Security Subject Name		
<u>P</u> urpose:	Signature Archive subject's encryption p Include symmetric algorithms a Delete revoked or expired certit	flowed 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. 				
	OK C	Cancel <u>Apply</u>		

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

Properties of New Template		? ×		
General Request Handlin Issuance Requirements Superseded Te		t Name ; Security		
Group or user names: Administrator (MYCADOMAIN\Administrator) Authenticated Users Domain Admins (MYCADOMAIN\Domain Admins) Enterprise Admins (MYCADOMAIN\Enterprise Admins)				
Add Remove Permissions for Administrator Allow				
Full Control Read Write Enroll Autoenroll				
For special permissions or for advanced settings, Advanced Click Advanced. OK Cancel Apply				

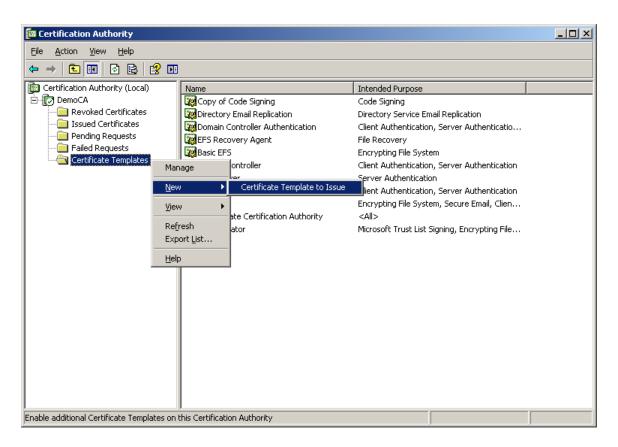
c. If you want to specify the subject name during certificate enrollment, select the
 Subject Name tab and select the Supply the request radio button. (If you want to use the default subject name of the enrolling user's account name, skip this step.)

Properties of New Template
Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name
 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)
OK Cancel Apply

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.
- 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**.

Intended Purpose		A
Code Signing		
Code Signing		
<alb< td=""><td></td><td></td></alb<>		
Certificate Request Agent		
Certificate Request Agent		
Certificate Request Agent		
	Code Signing <all> Certificate Request Agent Certificate Request Agent</all>	Client Authentication Private Key Archival Certificate Request Agent Code Signing Code Signing <all> Certificate Request Agent Certificate Request Agent</all>



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

📴 Certification Authority		_ _ _ _ _ _
<u>File Action View H</u> elp		
	F	
Certification Authority (Local) DemoCA Revoked Certificates Pending Requests Failed Requests Certificate Templates	Name Intended Purpose Copy of Code Signing Code Signing Directory Email Replication Directory Service Email Replication Domain Controller Authentication Client Authentication, Server Authe Basic EFS Encrypting File System Domain Controller Client Authentication, Server Authe Web Server Server Authentication Computer Client Authentication, Server Authe Subordinate Certification Authority <all> Administrator Microsoft Trust List Signing, Encrypt</all>	ntication ntication il, Clien

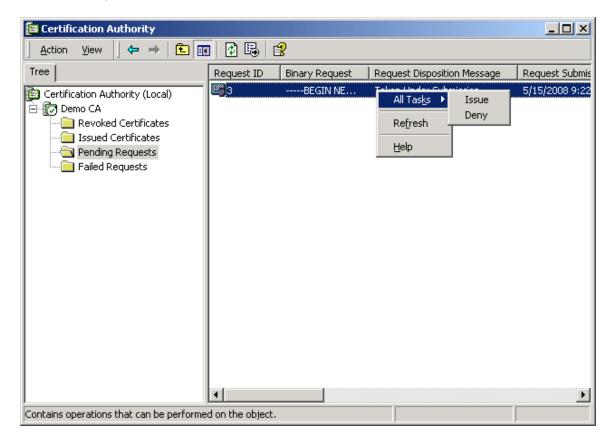
10. In the page that appears, do the following:

- 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.

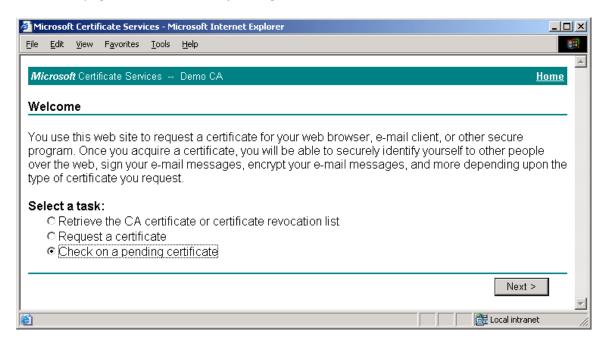
🔮 Microsoft Certifi	cate Services - Microsoft Internet Explorer	
<u>File E</u> dit <u>Y</u> iew	F <u>a</u> vorites <u>I</u> ools <u>H</u> elp	
Microsoft Certifi	cate Services DemoCA	<u>Home</u>
Advanced Ce	ertificate Request	
Certificate Tem		
	Copy of Code Signing	
Identifying Infor	mation For Offline Template:	
Name:		
E-Mail:		
Company:		
Department:		
City:		
State:		
Country/Region:		
Key Options:		
	O 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: <u>1024 2048 4096 8192 16384</u>)	
- h	Automatic key container name O User snecified key container name	
		Local intranet



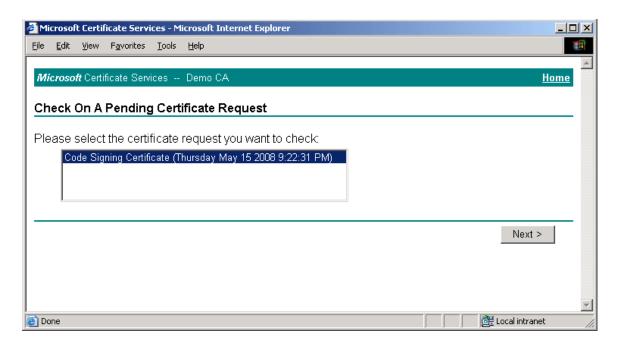
- 11. Depending on whether you have direct control over the certificate authority, do one of the following:
 - If you do not have direct control over the CA, wait until the certificate is approved by the CA administrator, then proceed to the next step.
 - If you have direct control over the CA, approve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

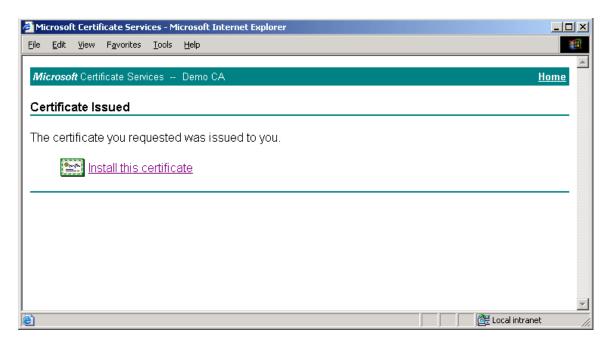


13. In the page that appears, select the target certificate request and click Next.





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



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

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
<u>Eile Edit View Favorites Tools H</u> elp	100 A
<i>Microsoft</i> Certificate Services Demo CA	<u>Home</u>
Certificate Installed	
Your new certificate has been successfully installed.	
	T
🙆 Done	🛛 🔠 Local intranet 🖉



- 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**.

Add/Remove Snap-in	? ×
Standalone Extensions	
Use this page to add or remove a standalone Snap-in from the console.	
Snap-ins added to:	
Description Add Remove	
ОК Са	ancel

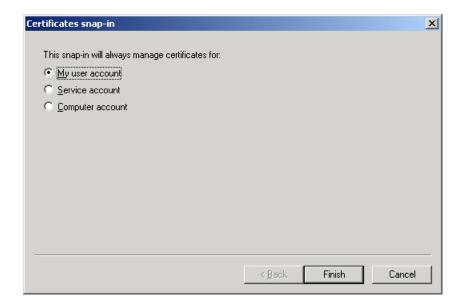
c. In the list that appears, select **Certificates** and click **Add**.

? ×

-
∍
lose
1036



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



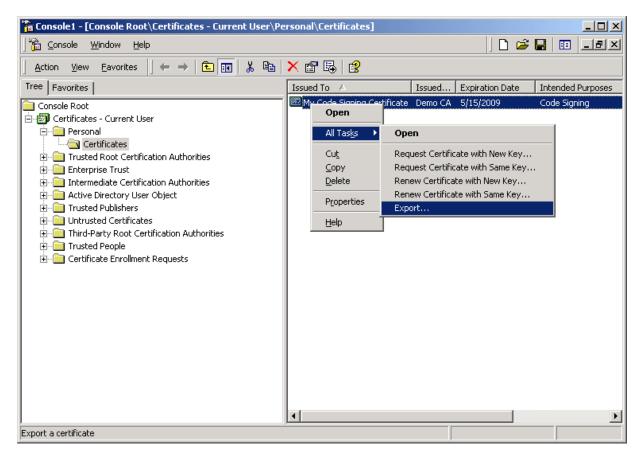
- 17. Close the remaining open dialog boxes inside the Management Console.
- 18. In the tree in the left-hand pane, navigate to:

```
Certificates – Current User \rightarrow Personal \rightarrow Certificates.
```

🚡 Console1 - [Console Root\Certificates - Current User\Pe	rsonal\Certificates]			
] 🚰 ⊆onsole Window Help] 🗋 🖻	; 🖬 🔳 💷 🗵
$ \underline{A}$ ction <u>Vi</u> ew Eavorites $ \underline{A} \leftarrow \rightarrow \underline{E} \boxed{1} \boxed{E} \boxed{2} $				
Tree Favorites	Issued To 🔺	Issued	Expiration Date	Intended Purposes
Console Root	My Code Signing Certificate	Demo CA	5/15/2009	Code Signing
🖻 👹 Certificates - Current User				
⊡				
Trusted Root Certification Authorities				
🗄 💼 Intermediate Certification Authorities				
🗄 💼 Active Directory User Object				
⊕ Untrusted Certificates ⊕ Third-Party Root Certification Authorities				
E Certificate Enrollment Requests				
	•			<u> </u>
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.



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 Exp	ort Wizard			2
Export Priv You can	ite Key hoose to export the private	key with the certif	icate.	
	eys are password protected e, you must type a password		port the private ke	y with the
Do you v	ant to export the private ke	y with the certifica	te?	
•	es, export the private key			
01	o, do not export the privat	e key		
		< <u>B</u> ack	<u>N</u> ext >	Cancel

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

ertificate Export Wizard	X
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C DER encoded binary X.509 (,CER)	
C Bage-64 encoded X.509 (,CER)	
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
\square 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	
< <u>B</u> ack <u>N</u> ext > Cance	3



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

Certificate Export Wizard	X
Password To maintain security, you must protect the private key by using a passwor	d.
Type and confirm a password.	
Password:	

Confirm password:	

< <u>B</u> ack <u>N</u> ext >	Cancel

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	J
File to Export Specify the name of the file you want to e	export
Eile name:	
C:\MyCodeSigningCert.pfx	B <u>r</u> owse
	< <u>B</u> ack <u>N</u> ext > Cancel





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.