Guide to setting up Windows Smart Card Logon using EJBCA

Windows Configuration Guide

Table of contents

1 Configuring the Windows server

This guide will show you how to configure your Windows Server 2003 Domain Controller for MicroSoft SmartCard Logon. The installation of a Domain Controller and DNS-Server is also described, so you could get this working from scratch.

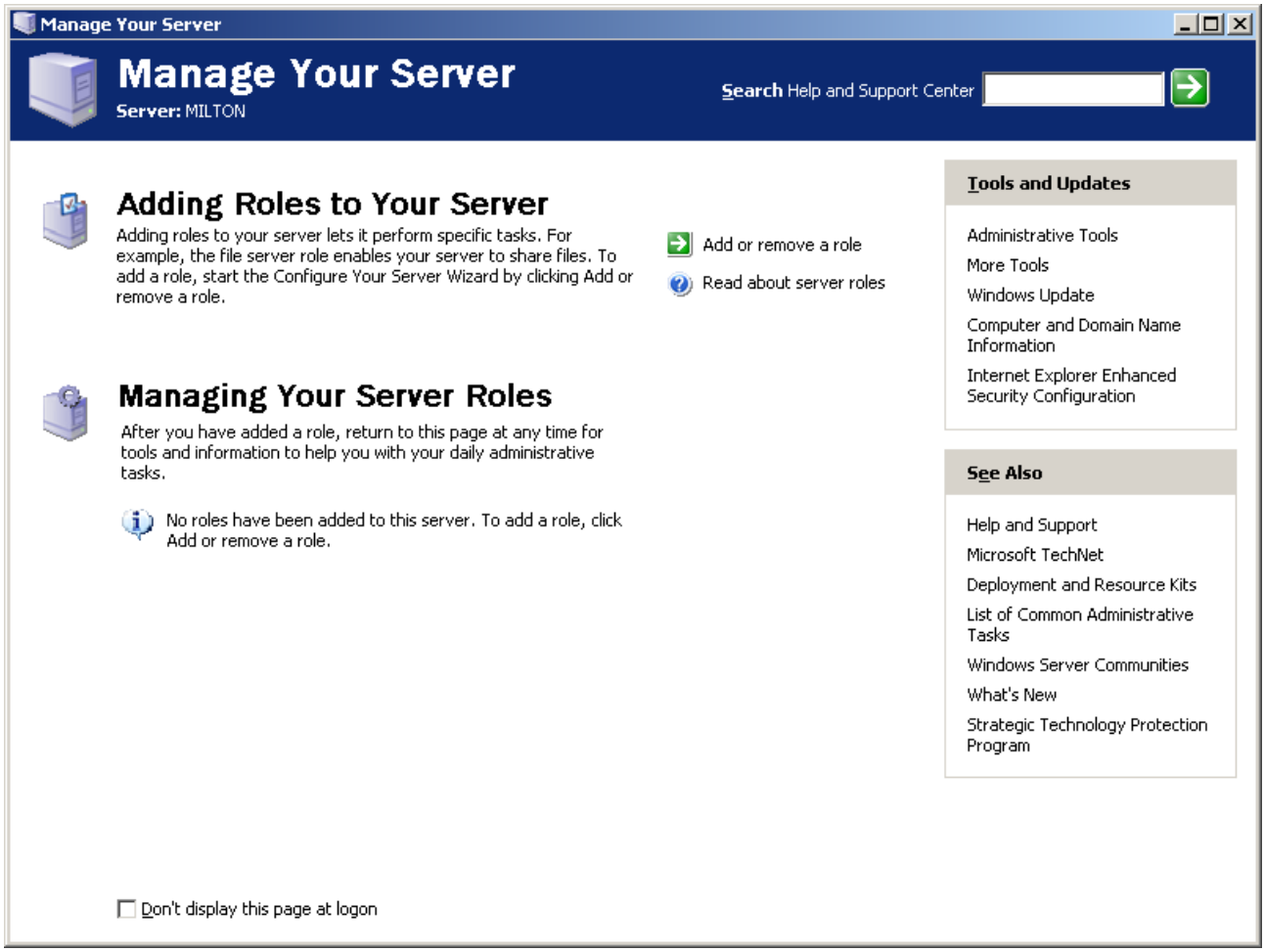
1.1 Prerequisites

Windows Server 2003 Enterprise Edition with SP2. Standard Edition will probably work, but is not as throughly tested as Enterprise Edition.
MS SCL can not be disallowed in the Group Policy.

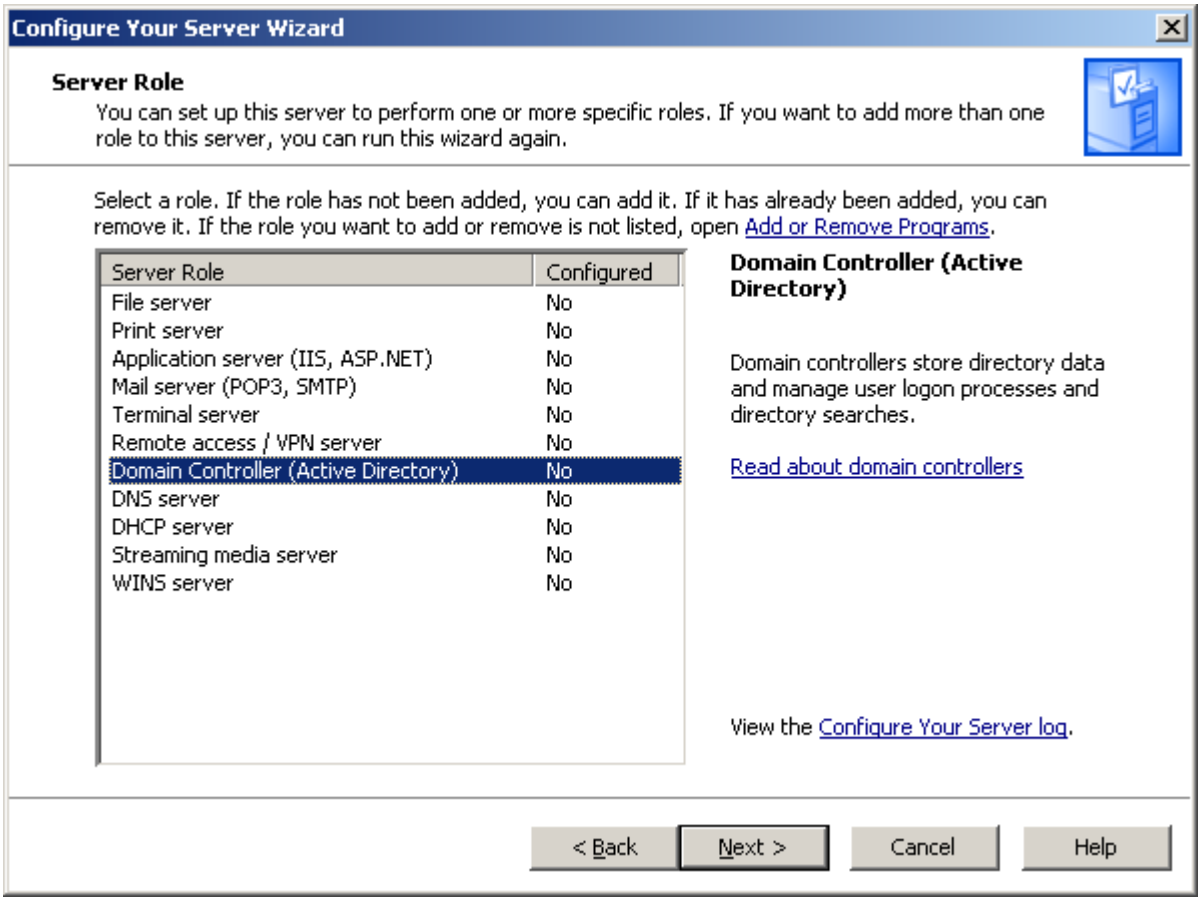
1.2 Creating a domain controllers

Omit this step if you already have an existing installation of Active Directory.

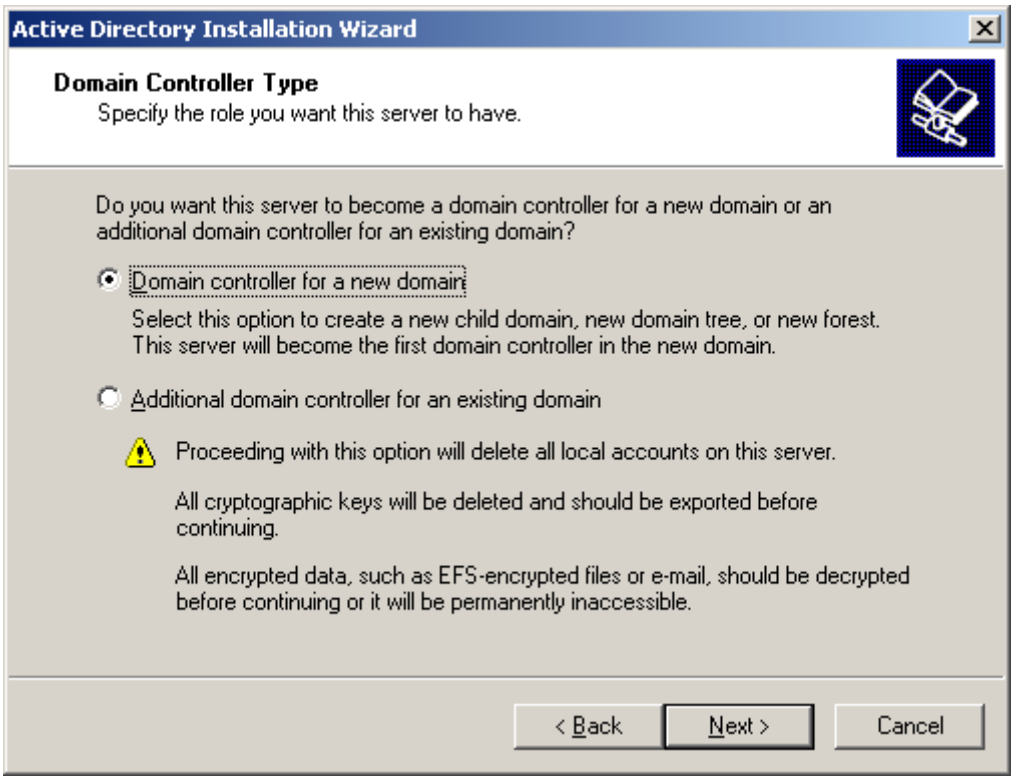
1. Start ”Manage Your Server”
2. Select ”Add or remove a role”



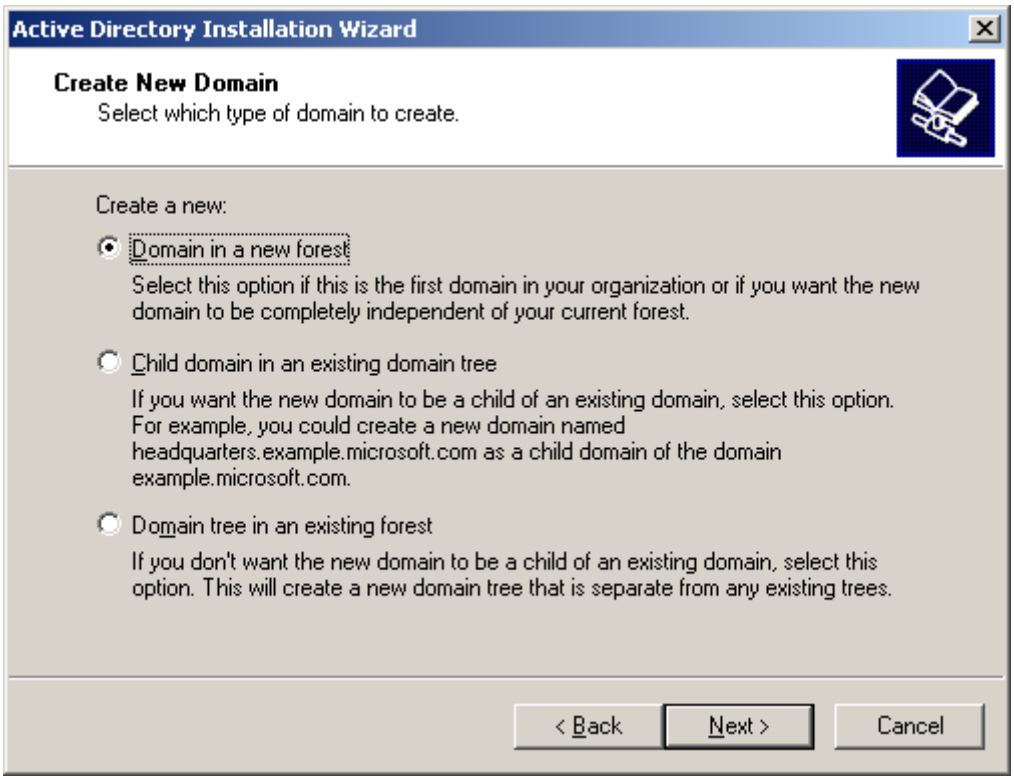
3. Click ”Next”
4. Select ”Domain Controller (Active Directory)” and click ”Next”



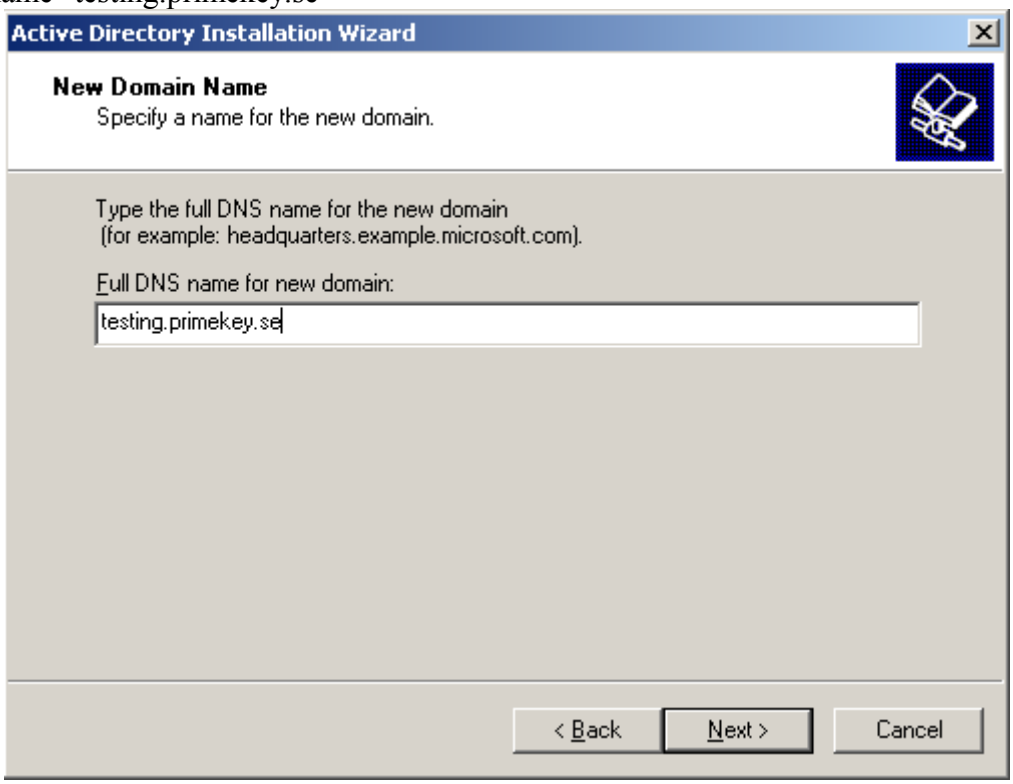
5. Click ”Next”
6. Click ”Next”
7. Click ”Next”
8. Click ”Next”
9. Select ”Domain controller for a new domain” and click ”Next”



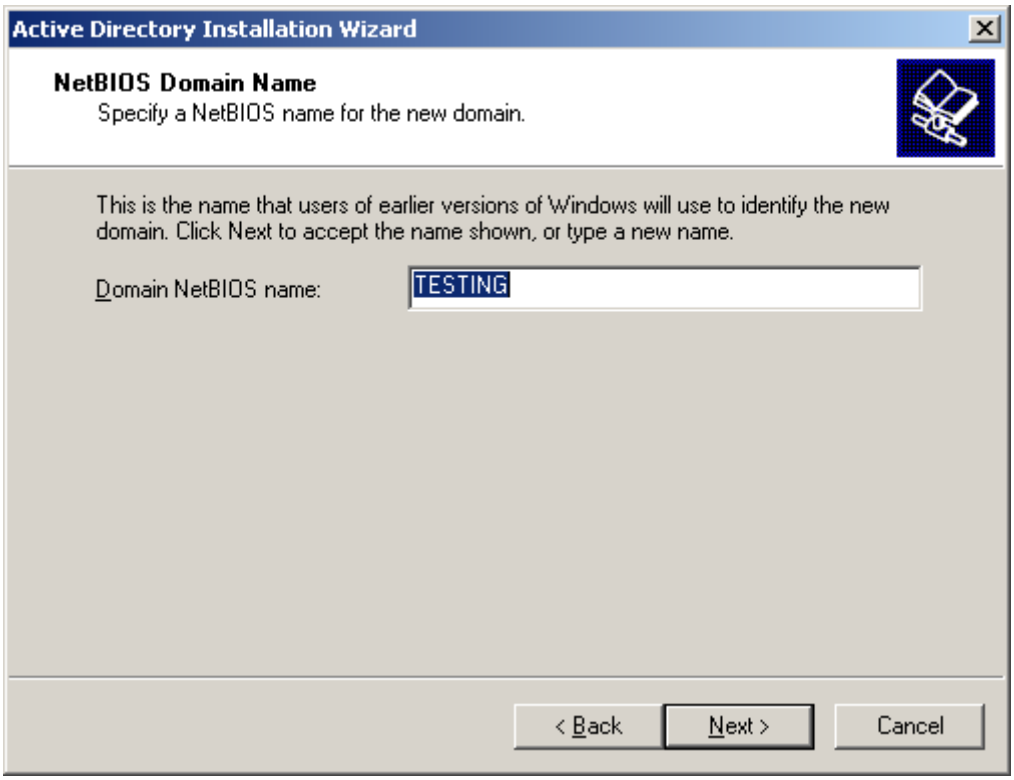
10. Select ”Domain in a new forest” and click ”Next”



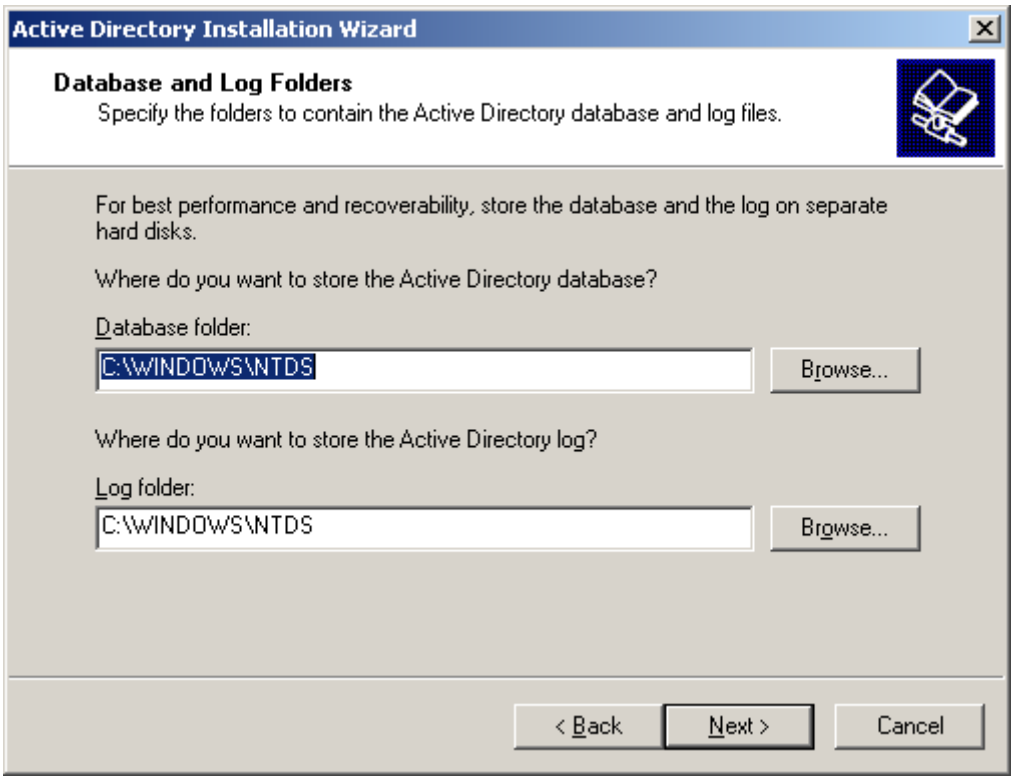
11. DNS name "testing.primekey.se"



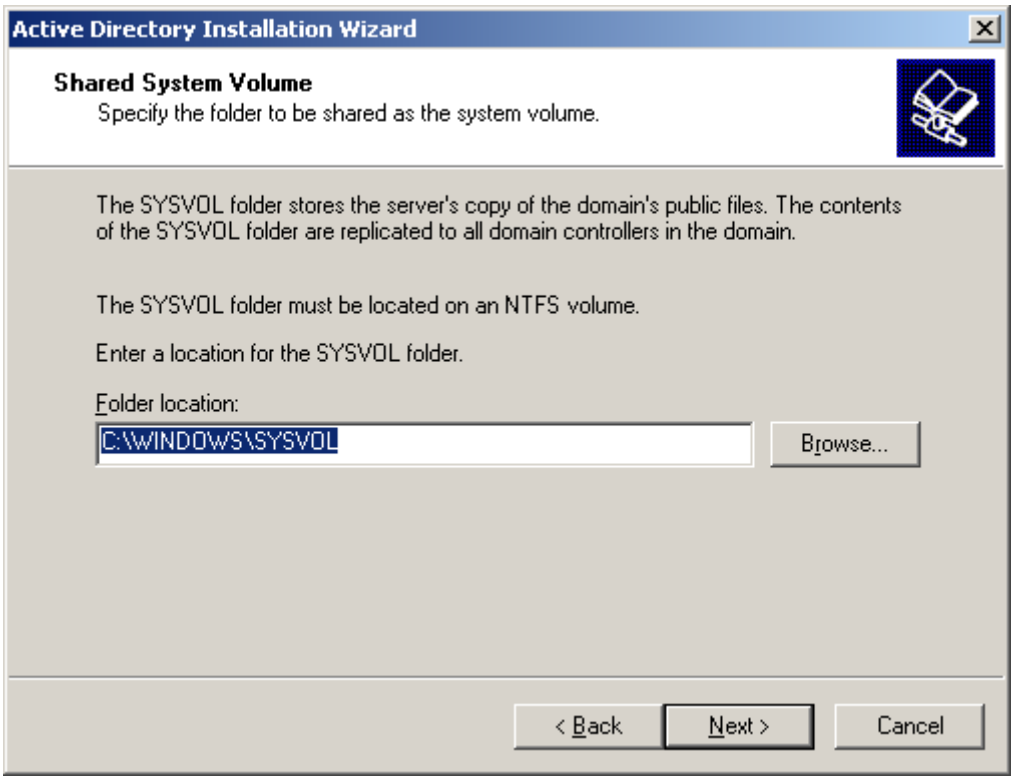
12. Domain NetBIOS name "TESTING" and click ”Next”



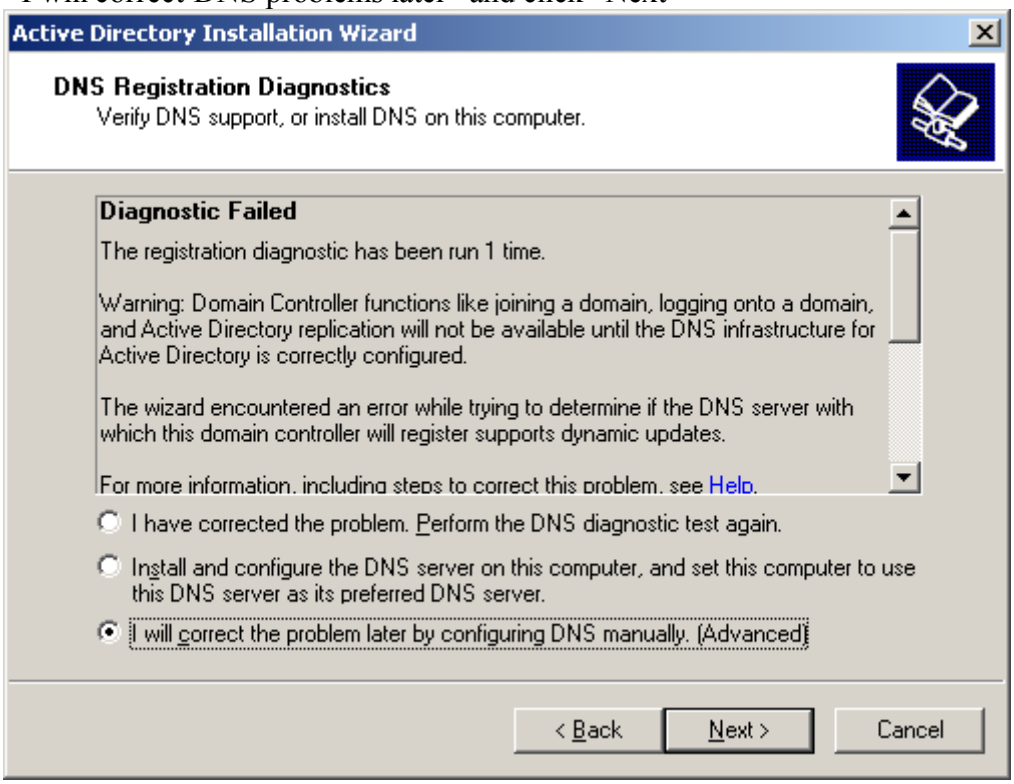
13. Click ”Next”



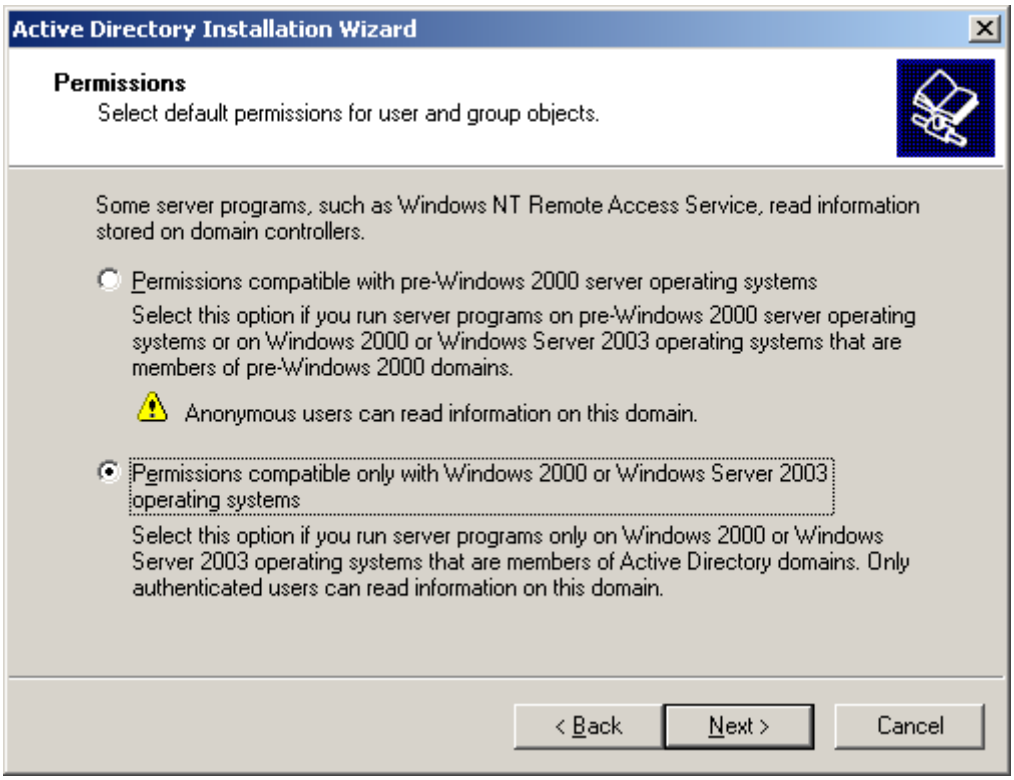
14. Click ”Next”



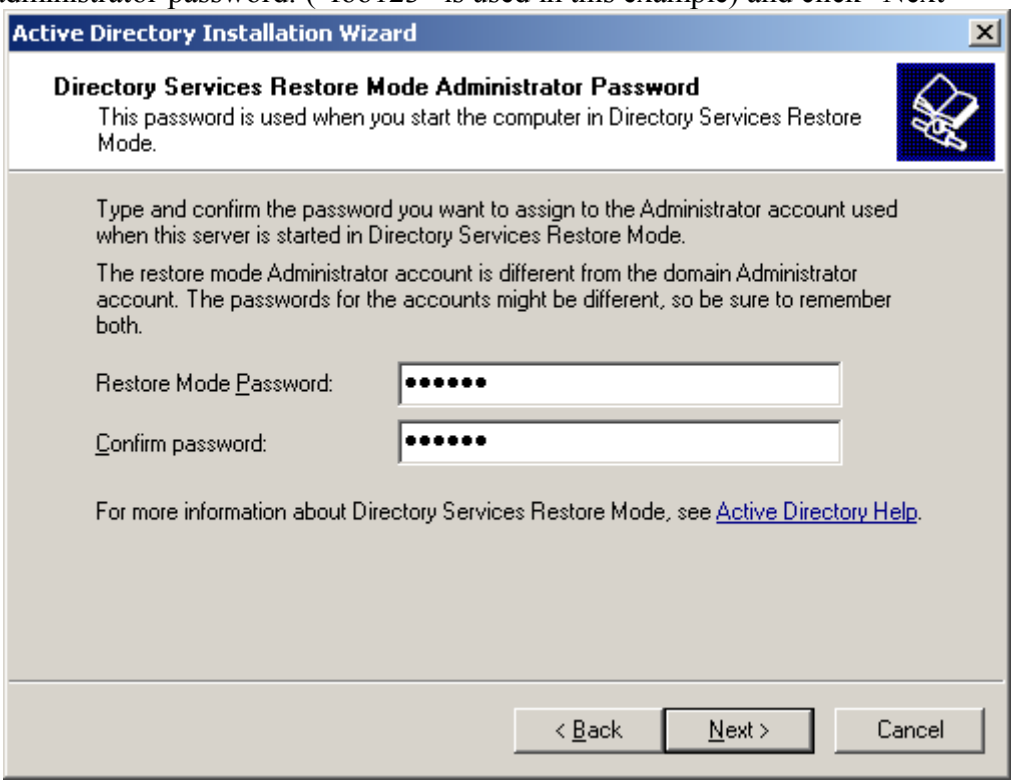
15. Select ” I will correct DNS problems later” and click ”Next”



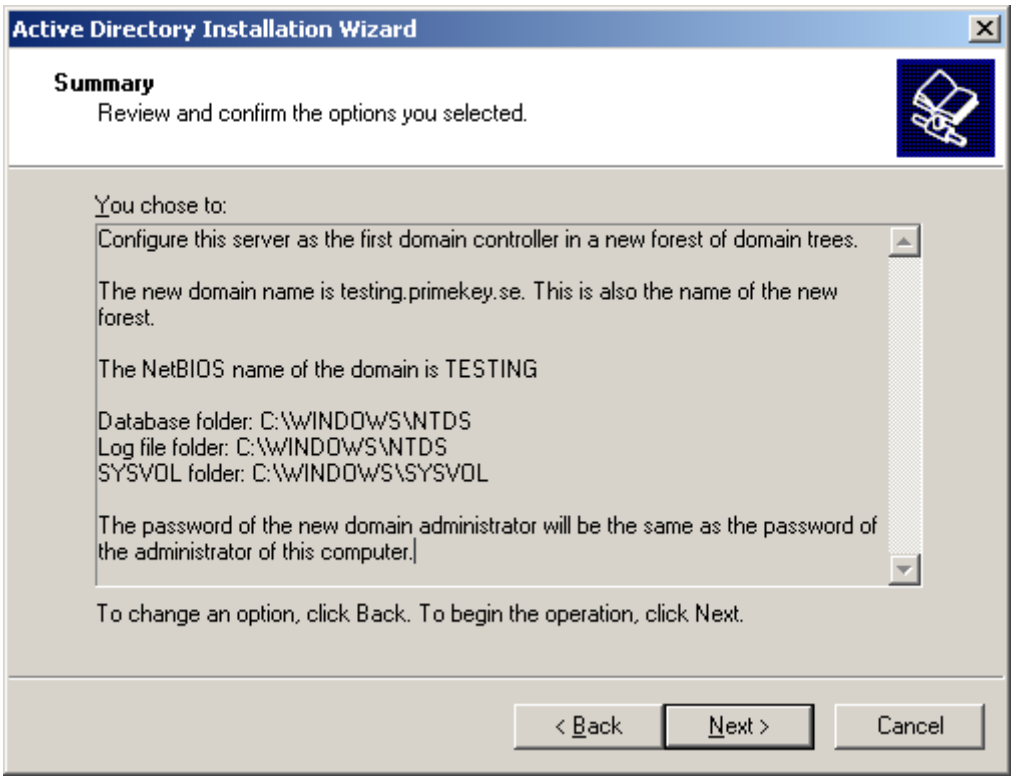
16. Select ”Permissions compatible only with Windows 2000 and Windows Server 2003” and click ”Next”



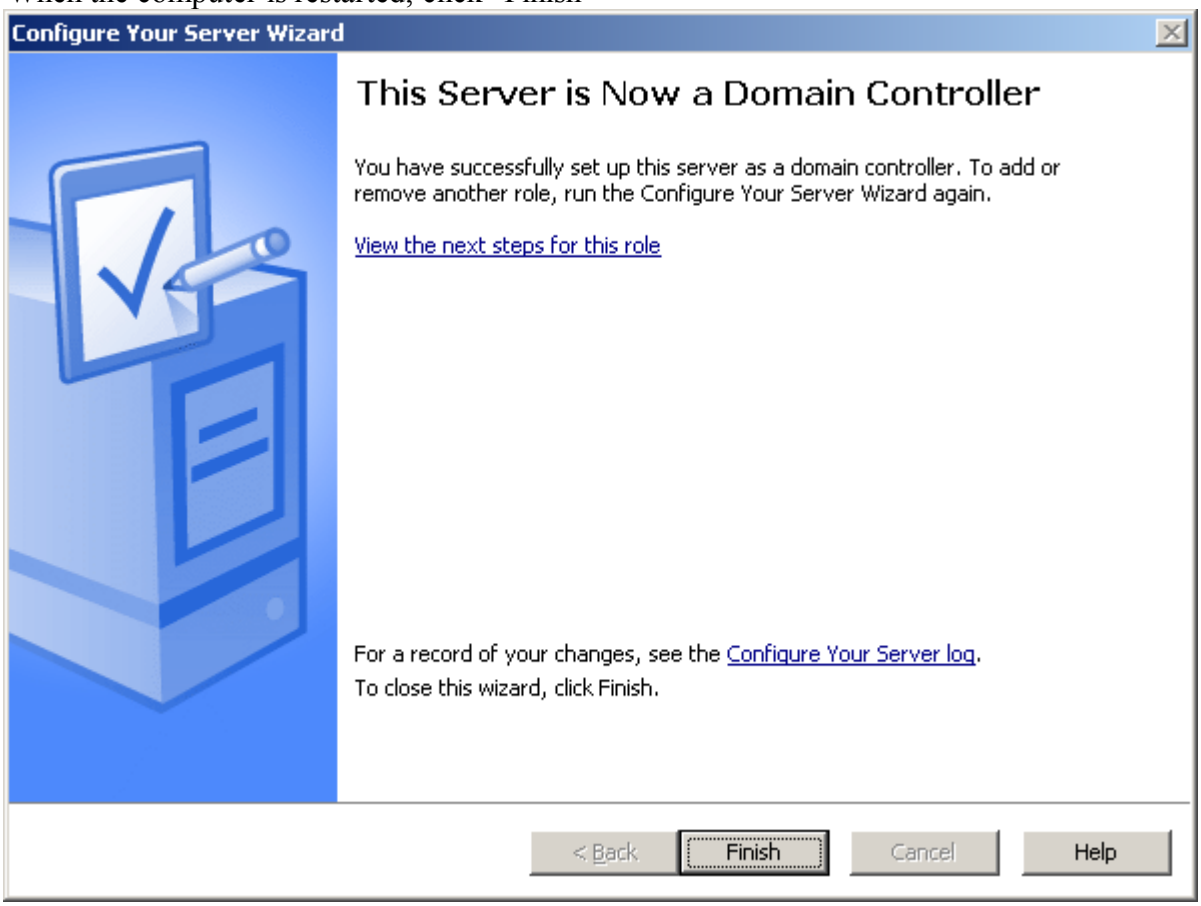
17. Enter administrator password. (”foo123” is used in this example) and click ”Next”



18. Click ”Next”



19. Click ”Finish”
20. Click ”Restart now”
21. When the computer is restarted, click ”Finish”



You now have a working domain controller.

1.3 Install a DNS server

Omit this if you have a working DNS already.

Set a static IP address, if this isn't already the case.
Start “Manage Your Server” → Add or remove a role → Next → DNS Server → Next → Next → (Insert install media if prompted → “This computer”) → Next → Create a forward lookup zone, Next → This server maintains the zone, Next → Zone name “testing.primekey.se”, Next → Allow only secure dynamic updates, Next → Yes, enter primary and secondary DNS servers, Next → Finish (Ignore “Error, the zone already exists”) → Finish

1.4 Setup DNS

Add the DNS name of the ca host “ca.testing.primekey.se” to the DNS record if it doesn't exit.
Reboot.

1.5 Generate a certificate request for each domain controller.

Run "1. GenerateDCCertRequest.vbs" (provided with this guide) and get a visual confirmation "Done!". This script produces "DomainControllerCertRequest-<hostname>.req" containing the request and a "DomainControllerInfo-<hostname>.txt" .

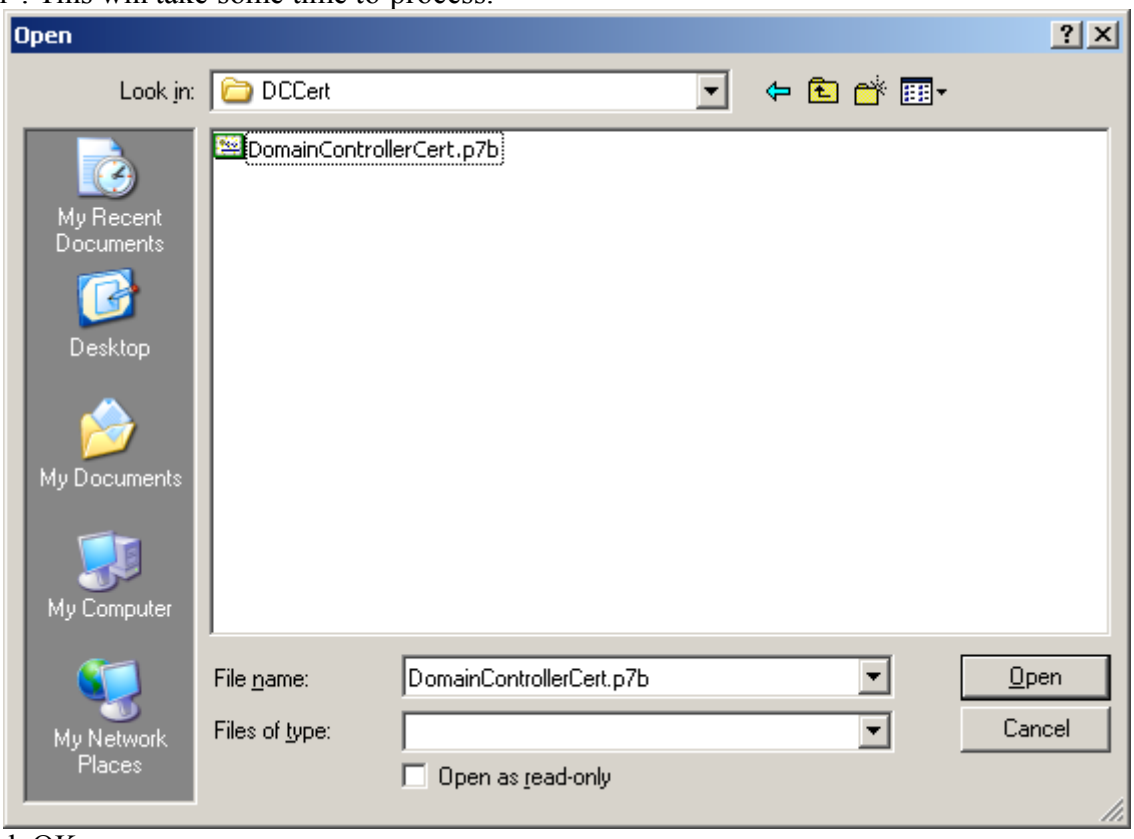
Both these are needed during the PKI set up and must be provided for every Domain Controller to the person responsible for issuing the certificates. In this example we only use one DC.

1.6 Install and publish certificate on each Domain Controller

To be able to continue with this step, you should have received a Domain Controller certificate for every DC and a certificate of the issuing CA.

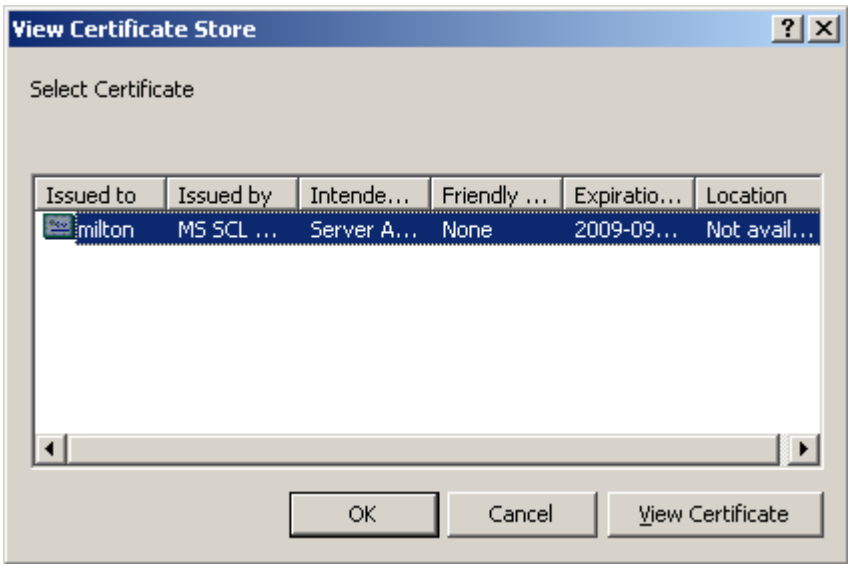
1. "2. InstallDomainControllerCert.vbs" on each Domain Controller

2. Select "DomainControllerCert-<hostname>.p7b" when prompted for the DC certificate and click "Open". This will take some time to process.

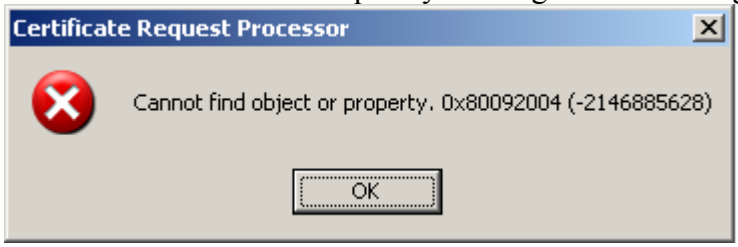


3. Click OK

4. The certificate should be visible in the last step if everything went fine.



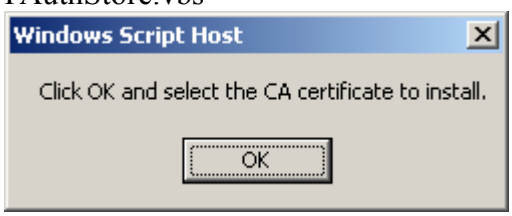
Troubleshoot: If there isn't a valid certificate request you will get the following error:



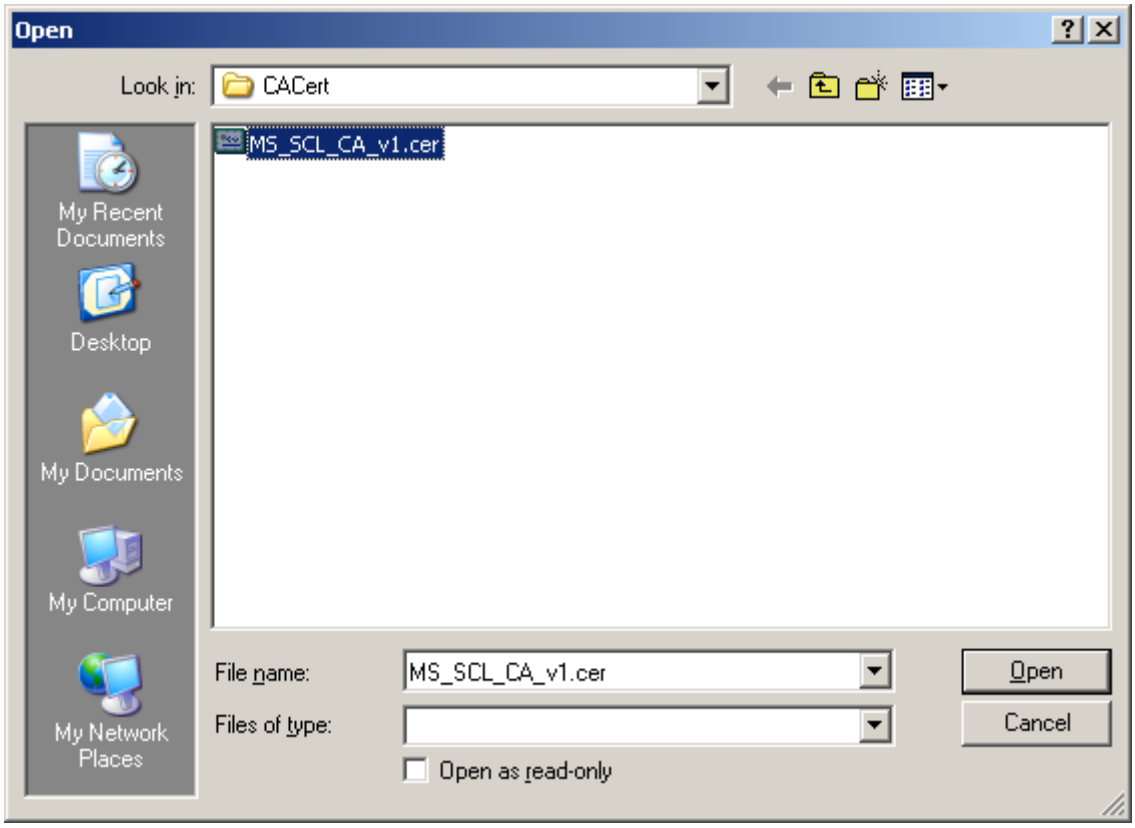
Solve this by creating a new certificate request, get a new certificate from the CA and repeat this step from the top.

1.7 Import the CA certificate to "Enterprise NTAuth store"

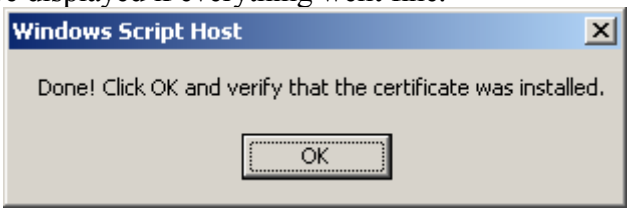
1. Run “3. ImportCACertToNTAuthStore.vbs”

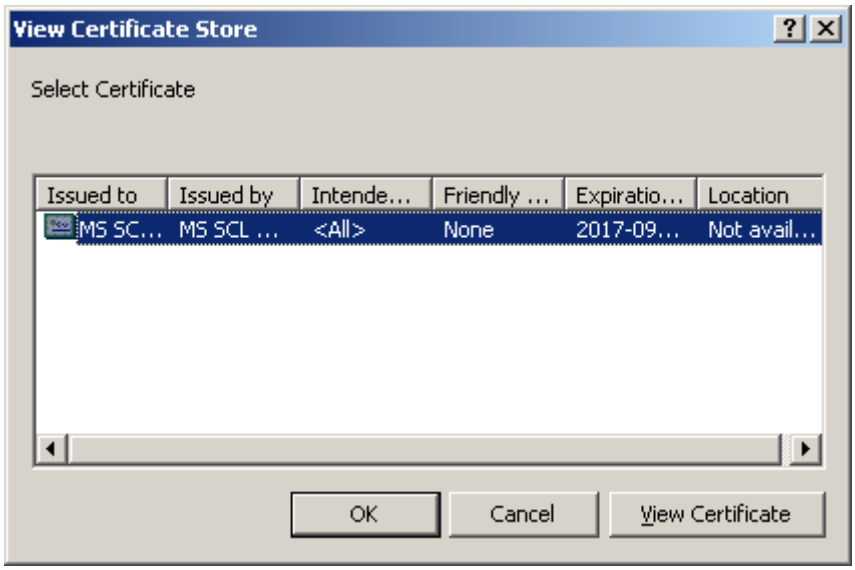


2. Select the CA certificate when prompted. This will take some time to process.



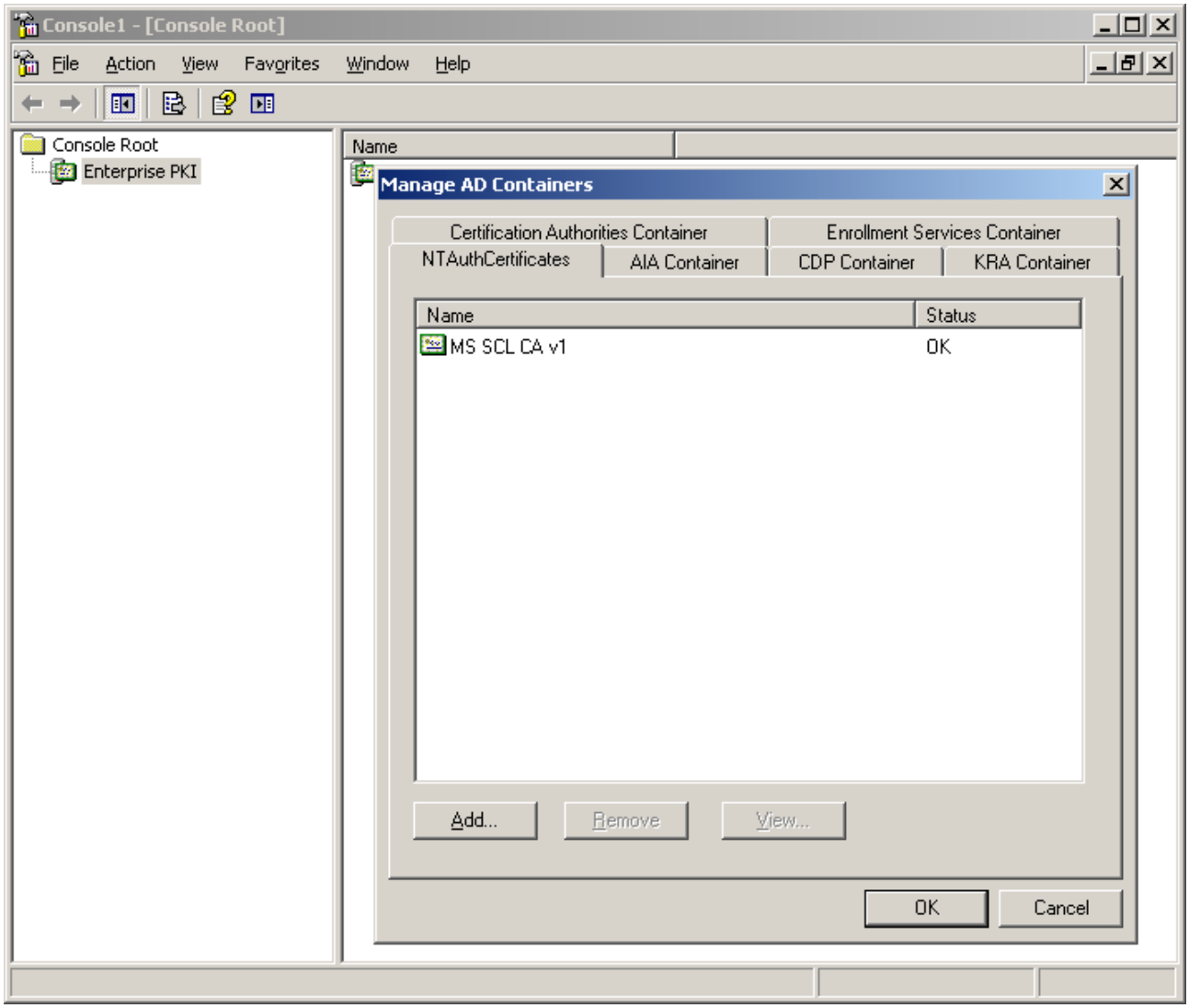
3. The certificate should be displayed if everything went fine.





Troubleshoot: Download and install the "Windows Server 2003 Resource Kit Tools". The package is available from http://www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en. All default options can be used during install.

1. Run "mmc"
2. Add the "Enterprise PKI" snap-in.
3. Right-click "Enterprise PKI" in the main window and select "Manage AD Containers".
4. Remove the old certificate and retry the import from the top.



1.8 Adding a Windows XP client to the domain

This section is to able to test our new domain controller. Feel free to ignore it if you already have clients.

Start → Control Panel → System → Computer name → Change → Select "Domain", Enter "testing.primekey.se" → Login with a valid username and password for the domain → OK → Reboot

1.9 Push CA certificate to all clients

You can add the CA certificate to all client machines by adding it to the Domain Security Policy.

1.9.1 Add the CA certificate to the Domain Security Policy

On the Domain Controller:

Start → Administrative Tools → Domain Security Policy → Public Key Policies → Trusted Root Certification Authorities → Right-click and choose "Import" → Next → Choose the CA certificate in "File to Import" → Next → Next → Finish

1.9.2 Install certificate on every client machine

This should happen automatically every 8 hours. To force the update run "gpupdate /force" on the client(s).

1.10 Enroll an end user

1.10.1 Install Card Reader

Install OmniKey driver (or similar) on all client machines.

1.10.2 Install CSP

Install NetID 4.4.5.7 (or similar) on all client machines. Reboot the clients.

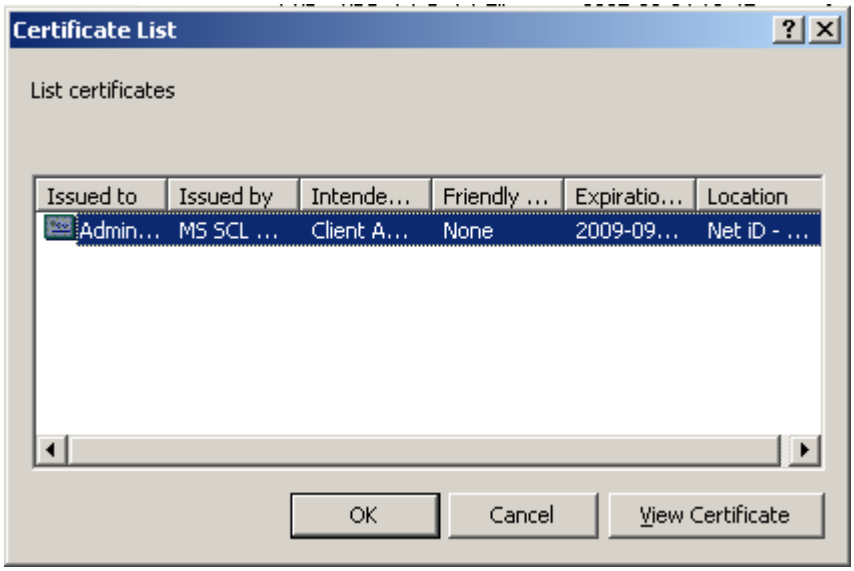
1.10.3 Put a MS SCL certificate on a smartcard

This section requires that the user to enrol has been added to in EJBCA Administration GUI. This is done in "Create an end user" section from the "EJBCA-SmartCardLogon-Guide-PKI".

Enroll user and put the certificate on a smartcard with the EJBCA Public Web Pages and NetID (or another CSP that have the same functionality). Make sure that the LED on the card reader stops flashing before you remove the card.

Internet explorer, EJBCA 3.3.1:
EJBCA Public Web Pages → Cerficate Enrollment → For you browser → Username "AdministratorMSSCL-001 " (Should be given to you.)
Password " foo123" (Should be given to you.)
→ Select "NetId – CSP" (or the one you are using) as CSP → Click OK

Troubleshoot: On a Windows Server 2003 client you can run "4. VerifySmartCardForLogon.vbs" to verify that the certificate was installed. (Requires certutil.exe to be installed.)



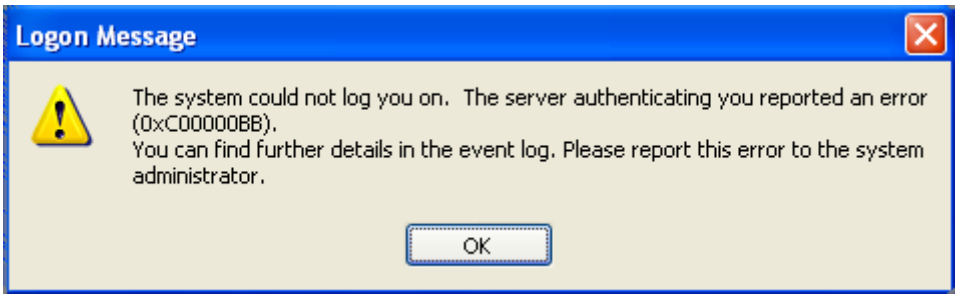
1.10.4 Verify that CRL Distribution Point is reachable

1. Use your favorite tool to look at the certificate on the smartcard. (E.g. "4. VerifySmartCardForLogon.vbs and press "View Certificate".)
2. Locate the CRL Distribution Point.
3. Enter this http-URL in your favorite browser and verify that you get a proper response. (E.g. not "404 Error..." etc)

1.10.5 Verify Smart Card Logon

1. Logoff client
2. Insert the smartcard containing the MS SCL Certificate for the Administrator when prompted for login credentials.
3. Enter the PIN-code and you should be logged on.

Troubleshoot: If you get "The system could not log you on. The server authenticating you reported an error (0xC00000BB)..." you can try to reboot the Domain Controller.



1.10.6 Adding another user

1. Add the user "Manages Your Server" → "Manage users and computers in Active Directory" → Right-click "testing.primekey.se, Users" → "New" → "User" → Tester@testing.primekey.se → password "FooBar123"

2. Create new end entity in EJBCA Administration GUI or have someone doing this for you.
3. Enrol through EJBCA Public Web Pages.

2 Optional configuration

2.1 Lock clients when smart cards are removed

Domain Security Policy Settings → Local policies → Security Options → Interactive Logon: Smart card removal behavior → Lock Workstation

2.2 Disable normal logon

Domain Security Policy Settings → Local policies → Security Options → Interactive Logon: Require smart card → Enable