

EJBCA with GemSAFE Toolbox Part1

Workstation Logon

Introduction

This document describes installation of EJBCA3.6.0, starting from a clean Windows Server 2003 and a clean Window XP Professional.

In this document, EJBCA 3.6.0 is used together with:

1. GemSAFE toolbox
2. GemSAFE PCSC token
3. ApacheAnt1.7.0
4. Jboss4.2.2
5. JDK 6 Update 6
6. JCE6

for **workstation smart card logon**.

The procedures to use EJBCA for **email signing, email encryption and SSL service** will be described in another document in series

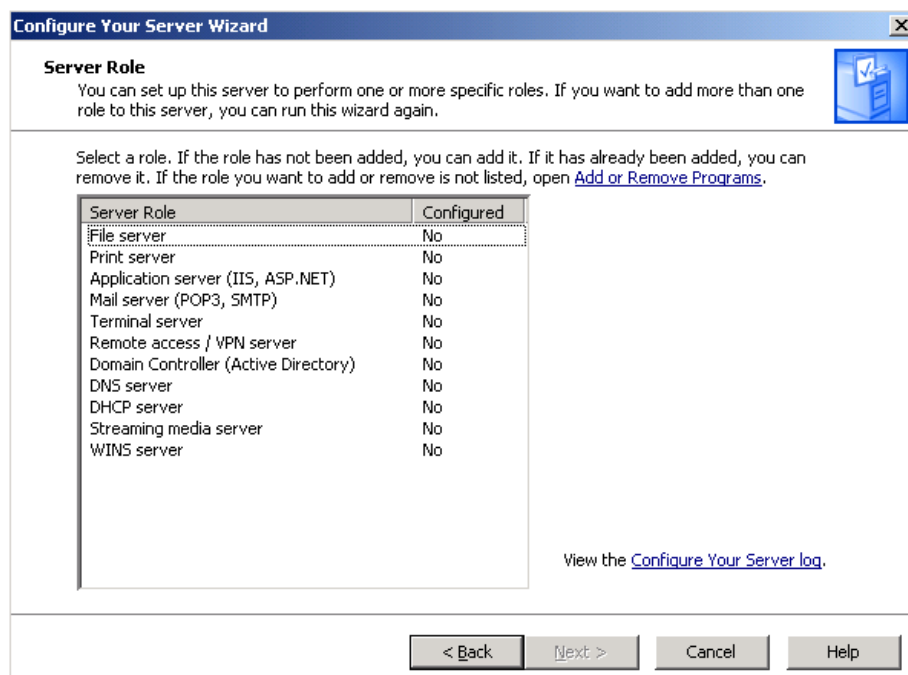
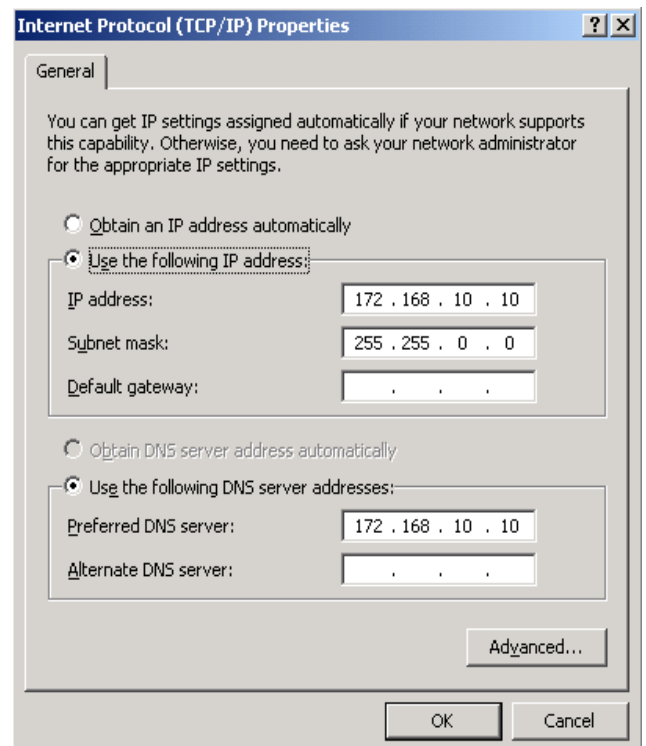
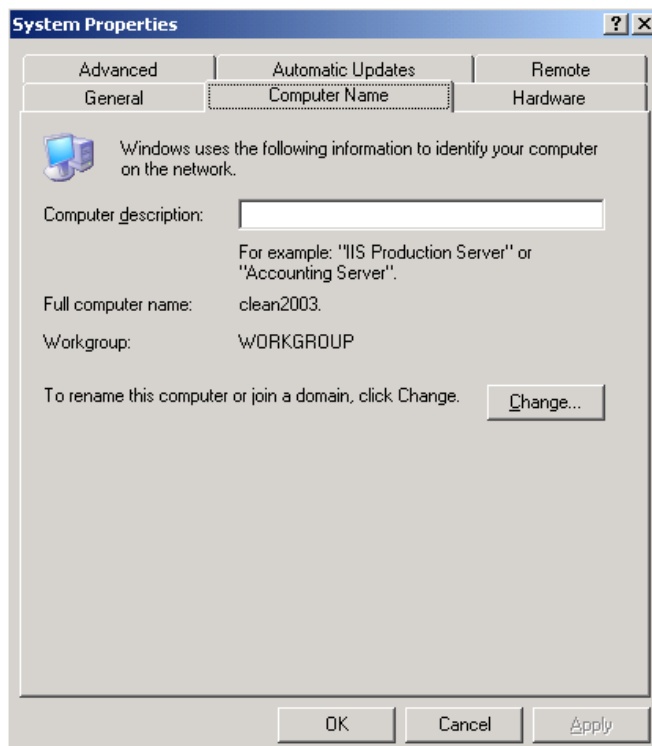
Table of Content

EJBCA with GemSAFE Toolbox Part1 Workstation Logon.....	1
Introduction.....	2
Table of Content.....	3
1 -- Configure Server.....	4
1.1 -- Create a Domain Controller.....	6
1.2 -- Create a DNS Server.....	9
2 -- Install EJBCA Components.....	12
2.1 -- Deploy EJBCA and Supplementary Components.....	16
3 -- Configure EJBCA.....	21
3.1 -- Create CA.....	22
3.2 -- Create Certificate Profile "DomainController".....	26
3.3 -- Create End Entity Profile "DomainController".....	31
3.4 -- Create New Certificate Profile "GSSmartCardLogon".....	35
3.5 -- Create New End Entity Profile "GSSmartCardLogon".....	40
3.6 -- Fetch Domain Controller & Certificate Authority Certificate.....	44
4 -- Logon to Workstation.....	50
4.1 -- Add CA Certificate to Domain Security Policy.....	53
4.2 -- Install Certificate on Workstation.....	54
4.3 -- Install GemSAFE Toolbox on Workstation.....	55
4.4 -- Enroll Certificate to GemSAFE Smartcard.....	58
4.5 -- Use Smart Card to Logon Workstation.....	59
5 -- Logon Workstation Using another Account	60
5.1 -- Create a New User Account.....	61
5.2 -- Add End Entity for New User.....	63
5.3 -- Enroll New User's Certificate to Token.....	64

1 -- Configure Server

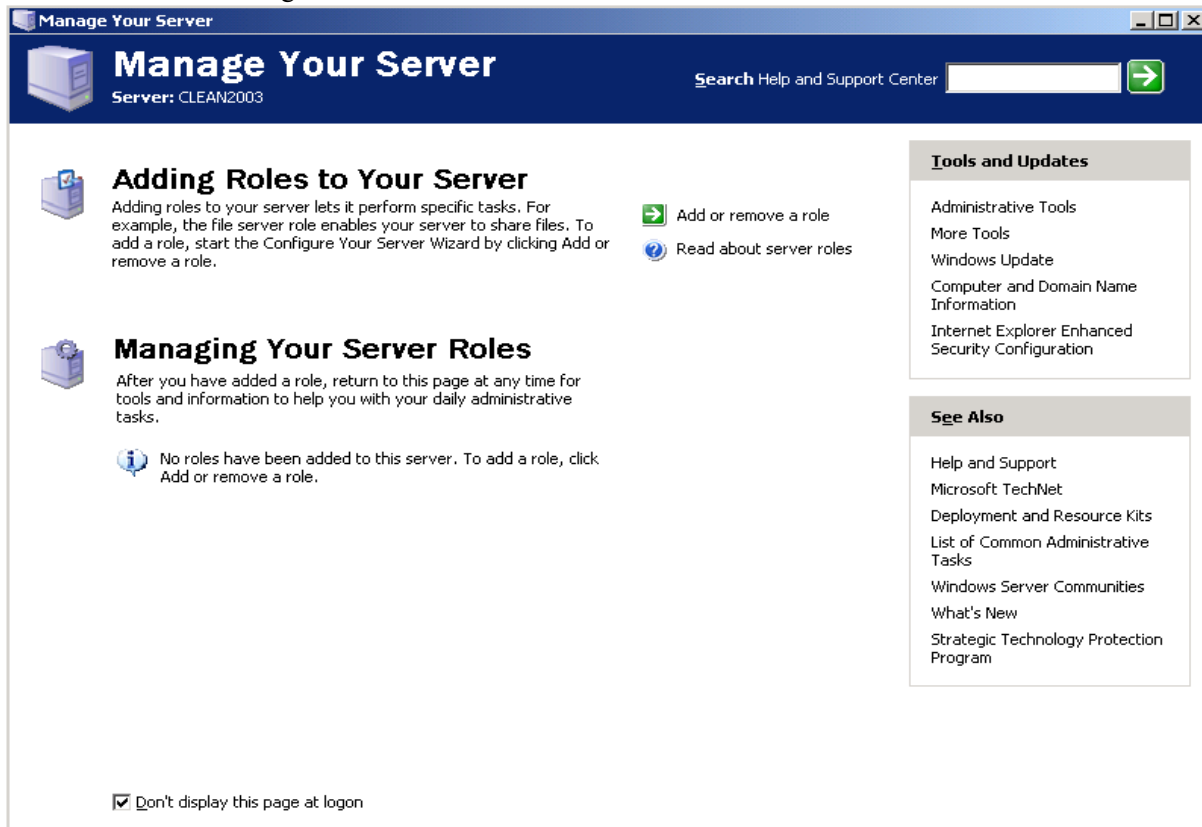
Initial server properties:

- Server OS: Windows Server 2003 Enterprise Edition
- Computer name: clean2003
- IP address: 172.168.10.10
- Subnet mask: 255.255.0.0
- Preferred DNS server: 172.168.10.10
- Workgroup: WORKGROUP
- Server role: nothing

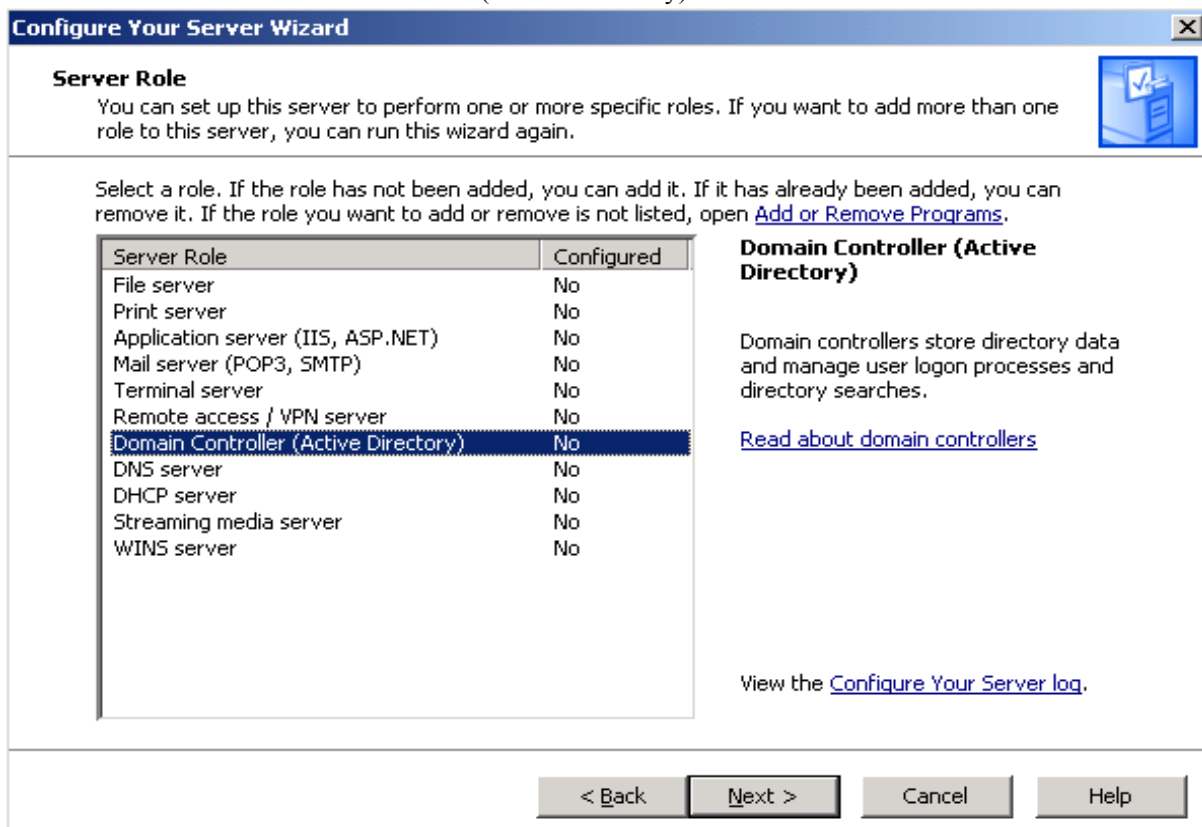


1.1 -- Create a Domain Controller

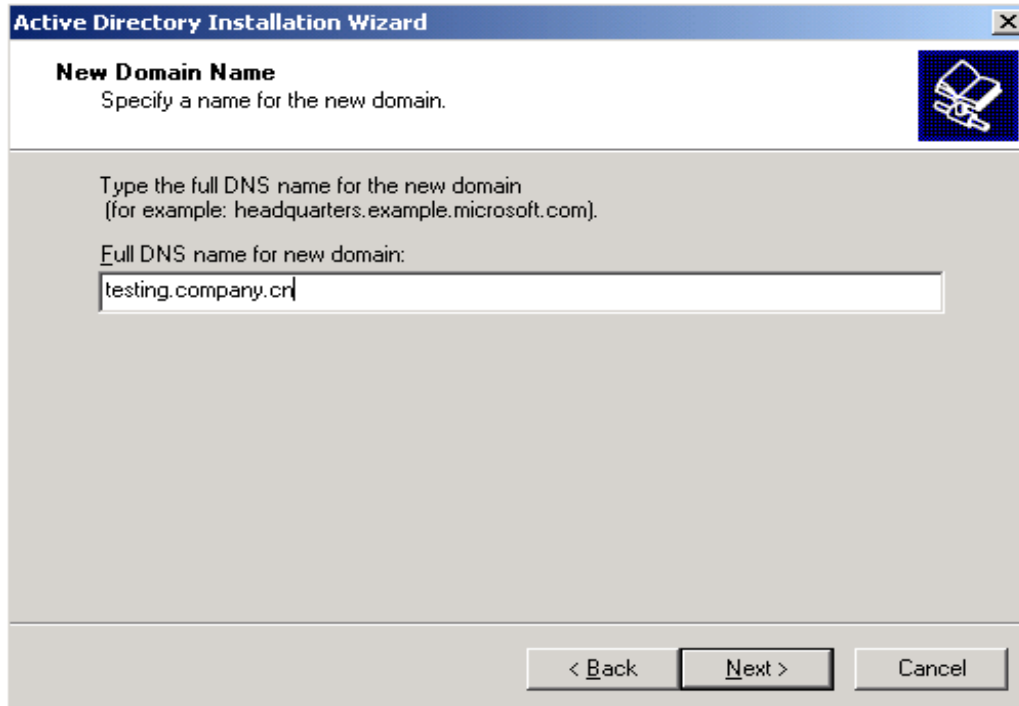
1. Start\Manage Your Server\Add or remove a role\click "Next"



2. Choose "Domain Controller (Active Directory)"

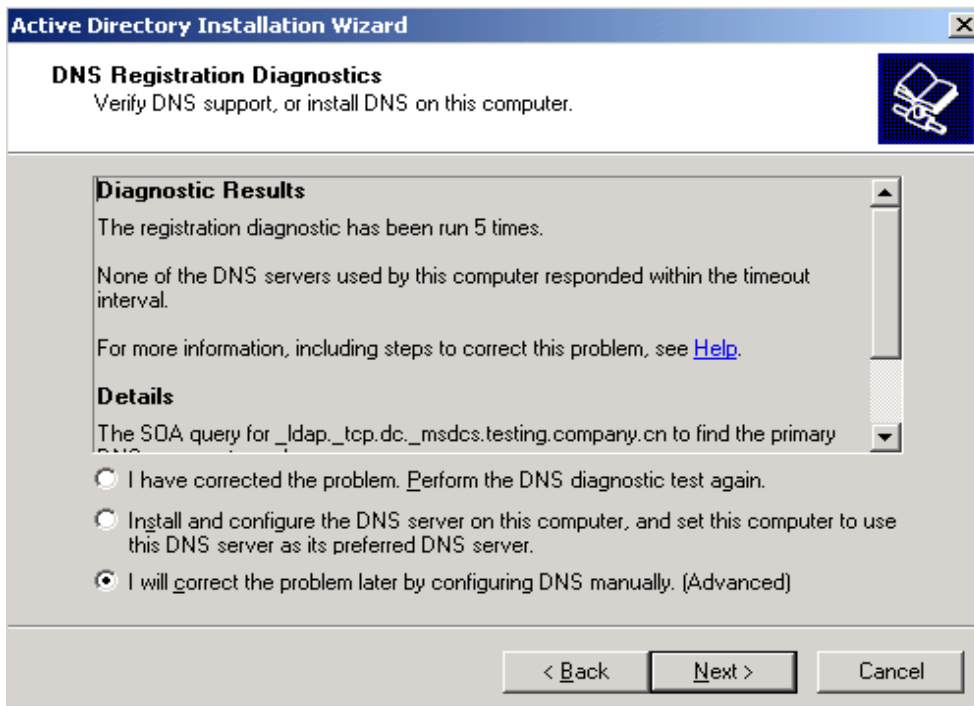


3. Click “Next” 6 times
4. At “Full DNS name for new domain:” input “testing.company.cn”



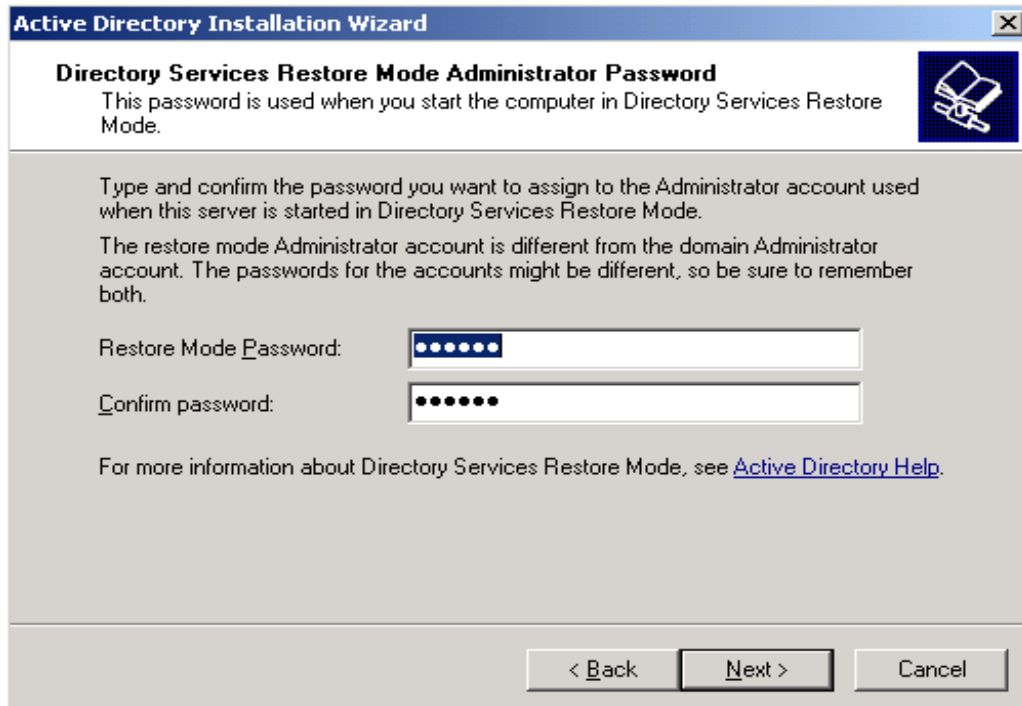
The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'New Domain Name' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'New Domain Name' with the instruction 'Specify a name for the new domain.' To the right of this text is a small icon of a computer with a hand. The main area contains the text 'Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).' followed by 'Full DNS name for new domain:' and a text input field containing 'testing.company.cn'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Click “Next” 4 times



The screenshot shows the 'Active Directory Installation Wizard' window, specifically the 'DNS Registration Diagnostics' step. The title bar reads 'Active Directory Installation Wizard'. Below the title bar, the section is titled 'DNS Registration Diagnostics' with the instruction 'Verify DNS support, or install DNS on this computer.' To the right of this text is a small icon of a computer with a hand. The main area contains a scrollable text box with the following content: 'Diagnostic Results', 'The registration diagnostic has been run 5 times.', 'None of the DNS servers used by this computer responded within the timeout interval.', 'For more information, including steps to correct this problem, see [Help](#).', 'Details', 'The SOA query for _ldap._tcp.dc._msdcs.testing.company.cn to find the primary DNS server failed.', and three radio button options: 'I have corrected the problem. Perform the DNS diagnostic test again.', 'Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server.', and 'I will correct the problem later by configuring DNS manually. (Advanced)'. The third option is selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Choose “I will correct the problem later by configure DNS manually. (Advanced)”
7. Click “Next” 2 times
8. At “Restore Mode Password:” input “foo123”
9. At “Confirm password:” input “foo123”



Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password
This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

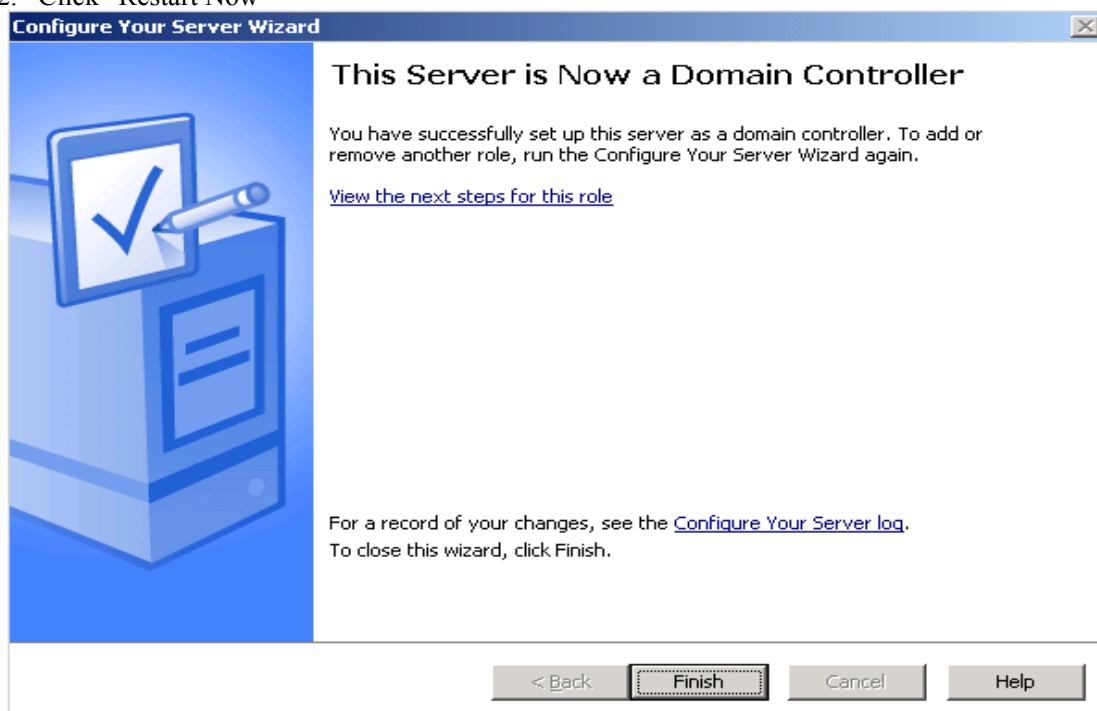
Restore Mode Password:

Confirm password:

For more information about Directory Services Restore Mode, see [Active Directory Help](#).

< Back Next > Cancel

10. Click "Next" 2 times
11. Click "Finish"
12. Click "Restart Now"



Configure Your Server Wizard

This Server is Now a Domain Controller

You have successfully set up this server as a domain controller. To add or remove another role, run the Configure Your Server Wizard again.
[View the next steps for this role](#)

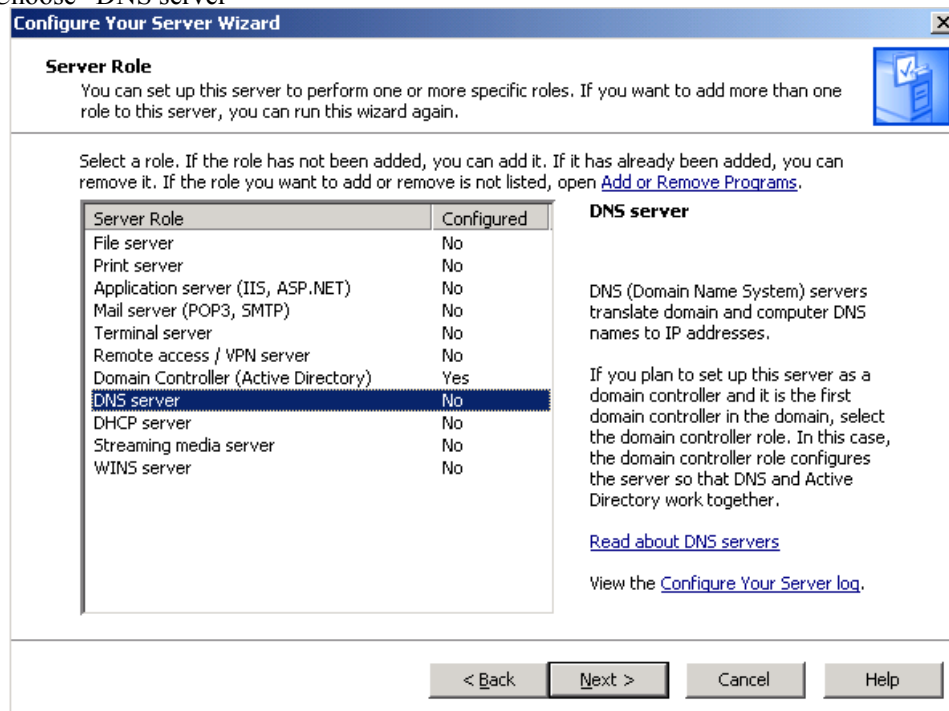
For a record of your changes, see the [Configure Your Server log](#).
To close this wizard, click Finish.

< Back Finish Cancel Help

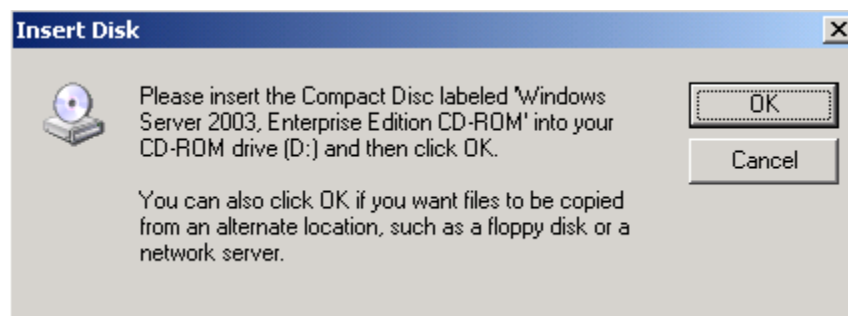
13. When the computer is restarted click "Finish"

1.2 -- Create a DNS Server

1. Start\Manage Your Server\Add or remove a role\click "Next"
2. Choose "DNS server"



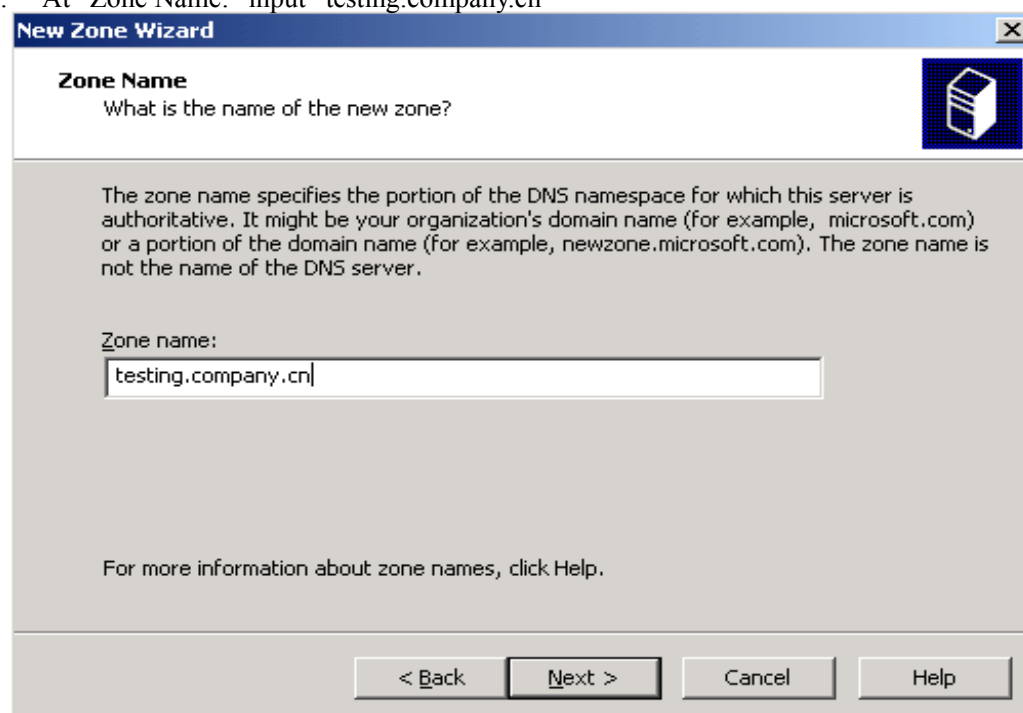
3. Click "Next" 2 times



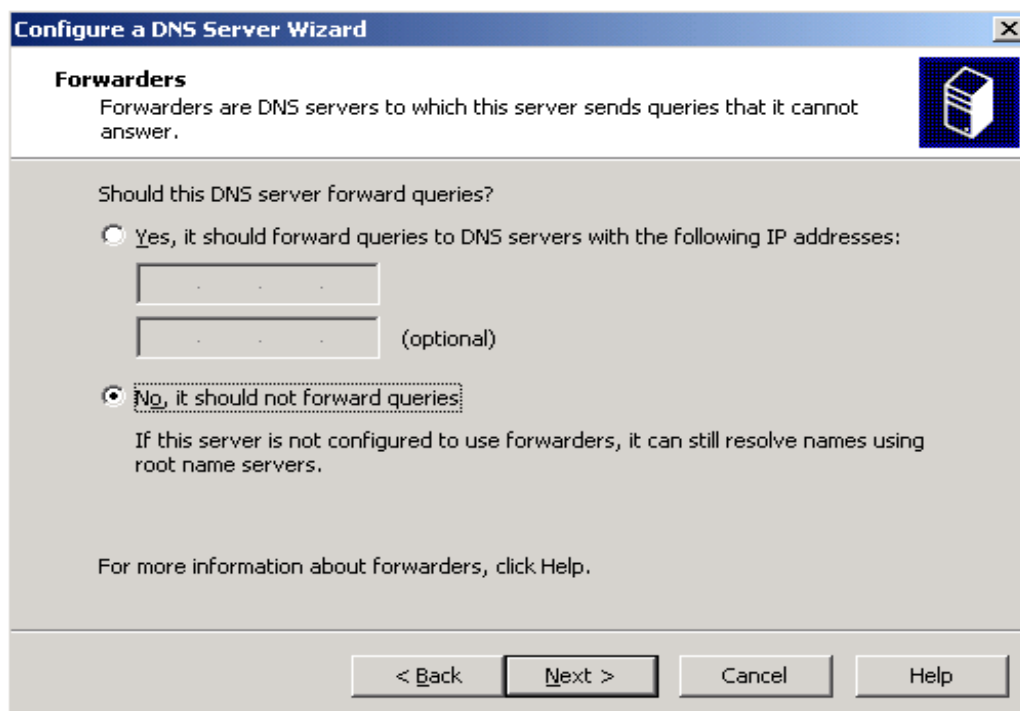
4. Click "OK"
5. Browse to Windows Server 2003 Enterprise CD/ENGLISH/WIN2003_VLP/ENT/I386/DNSMGR.DL_
6. Click "Open"



7. Click "Next" 3 times
8. At "Zone Name:" input "testing.company.cn"



9. Click "Next" 2 times
10. Choose "No, it should not forward queries"



Configure a DNS Server Wizard

Forwarders

Forwarders are DNS servers to which this server sends queries that it cannot answer.

Should this DNS server forward queries?

☐ Yes, it should forward queries to DNS servers with the following IP addresses:

(optional)

☒ No, it should not forward queries:

If this server is not configured to use forwarders, it can still resolve names using root name servers.

For more information about forwarders, click Help.

< Back Next > Cancel Help

11. Click "Next"
12. Click "Finish"
13. Ignore the error message



Configure Your Server Wizard

This Server is Now a DNS Server

You have successfully set up this server as a DNS server. To add or remove another role, run the Configure Your Server Wizard again.

[View the next steps for this role](#)

For a record of your changes, see the [Configure Your Server log](#).
To close this wizard, click Finish.

< Back Finish Cancel Help

14. Click "Finish"

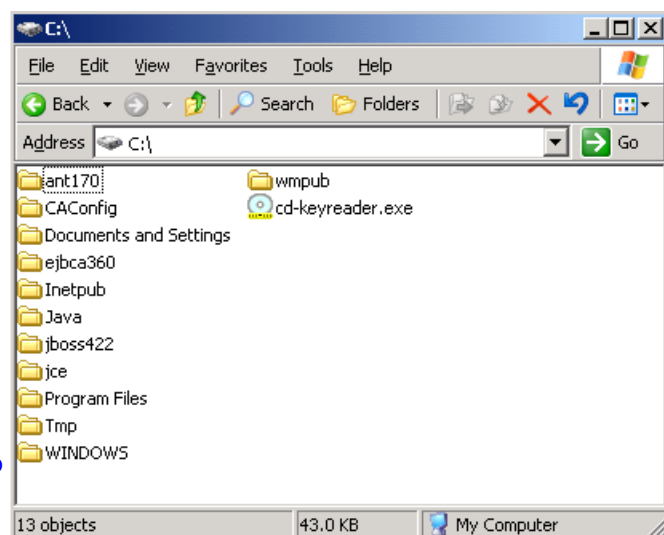
2 -- Install EJBCA Components

1. Download various installation files

Apache ant 1.7.0	http://apache.mirror.phpchina.com/ant/binaries/apache-ant-1.7.0-bin.zip
JBoss 4.2.2	http://downloads.sourceforge.net/jboss/jboss-4.2.2.GA.zip?modtime=1193094131&big_mirror=1
EJBCA 3.6.0	http://downloads.sourceforge.net/ejbca/ejbca_3_6_0.zip?modtime=1207510966&big_mirror=0
JDK 6 Update 6	http://java.sun.com/javase/downloads/index.jsp
Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6	http://java.sun.com/javase/downloads/index.jsp
1. GenerateDCCertRequest.vbs	http://download.primekey.se/ejbca/smartcardlogon/ReleasePackage/Scripts/1.%20GenerateDCCertRequest.vbs
2. InstallDomainControllerCert.vbs	http://download.primekey.se/ejbca/smartcardlogon/ReleasePackage/Scripts/2.%20InstallDomainControllerCert.vbs
3. ImportCACertToNTAuthStore.vbs	http://download.primekey.se/ejbca/smartcardlogon/ReleasePackage/Scripts/3.%20ImportCACertToNTAuthStore.vbs
ReqDCCert.vbs	http://download.primekey.se/ejbca/smartcardlogon/ReleasePackage/Scripts/ReqDCCert.vbs

2. Install various components

- i. JDK at [C:\Java\jdk1.6.0_06](#)
- ii. JRE at [C:\Java\jre1.6.0_06](#)
- iii. Ant 1.7.0 at [C:\ant170](#)
- iv. JBoss 4.2.2 at [C:\jboss422](#)
- v. EJBCA 3.6.0 at [C:\ejbca360](#)
- vi. Jce at [C:\jce](#)
- vii. 1. GenerateDCCertRequest.vbs at [desktop](#)
- viii. 2. InstallDomainControllerCert.vbs at [desktop](#)
- ix. 3. ImportCACertToNTAuthStore.vbs at [desktop](#)
- x. ReqDCCert.vbs at [desktop](#)
- xi. Overwrite Jce files

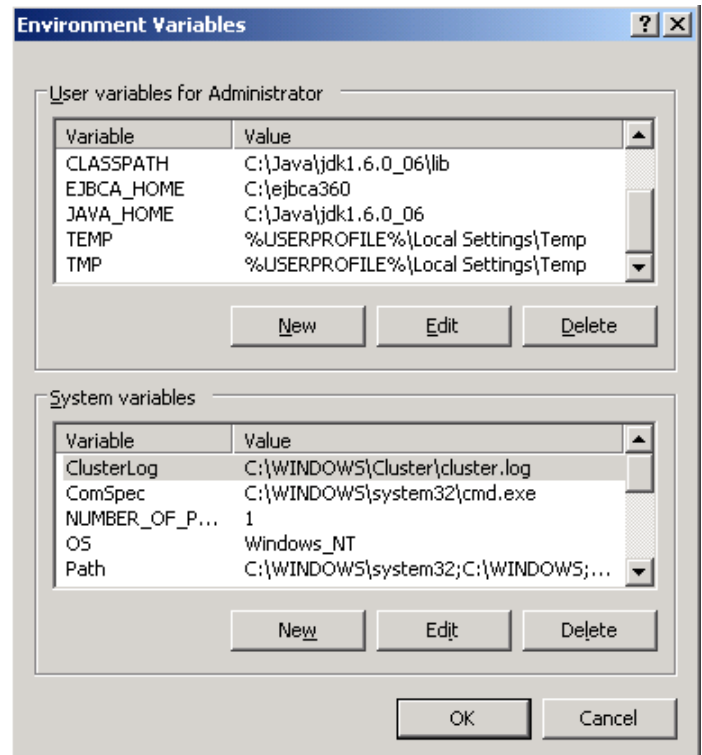
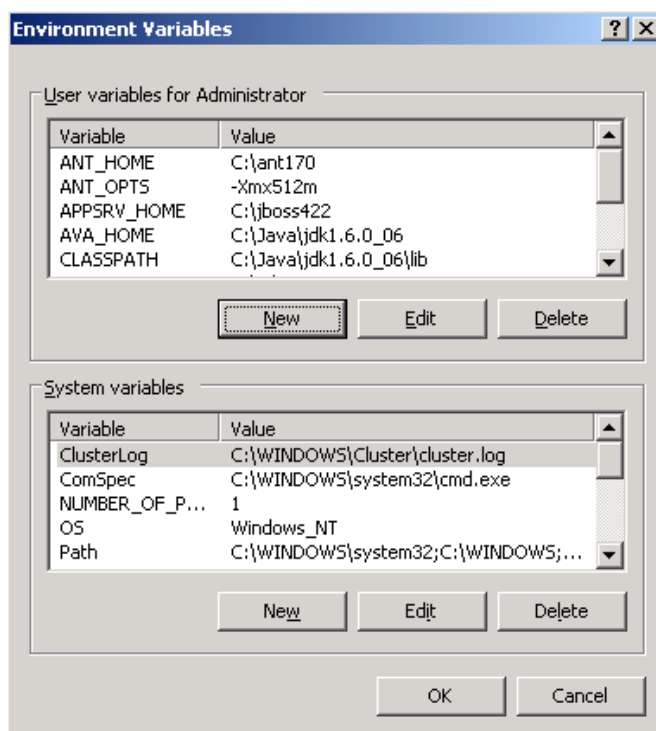


Overwrite	using
C:\Java\jre1.6.0_06\lib\security\local_policy.jar	C:\jce\local_policy.jar
C:\Java\jdk1.6.0_06\jre\lib\security\local_policy.jar	C:\jce\local_policy.jar
C:\Java\jre1.6.0_06\lib\security\US_export_policy.jar	C:\jce\US_export_policy.jar
C:\Java\jdk1.6.0_06\jre\lib\security\US_export_policy.jar	C:\jce\US_export_policy.jar

3. Add user variables

- i. Right click “My Computer”\Properties\Advanced\Environment Variables\User variable for Administrator\New
- ii. Add user variable one by one

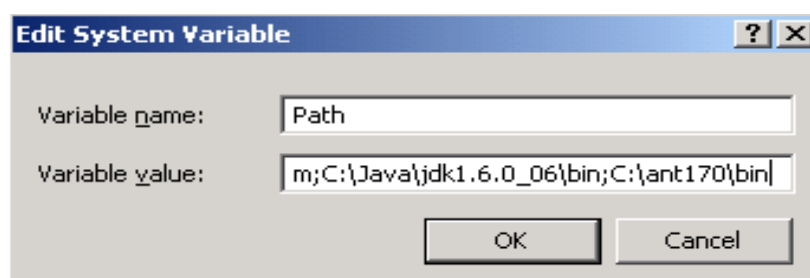
User variables	value
ANT_HOME	C:\ant170
ANT_OPTS	-Xmx512m
APPSRV_HOME	C:\jboss422
CLASSPATH	C:\Java\jdk1.6.0_06\lib
EJBCA_HOME	C:\ejbca360
JAVA_HOME	C:\Java\jdk1.6.0_06



4. Edit system variable “Path”

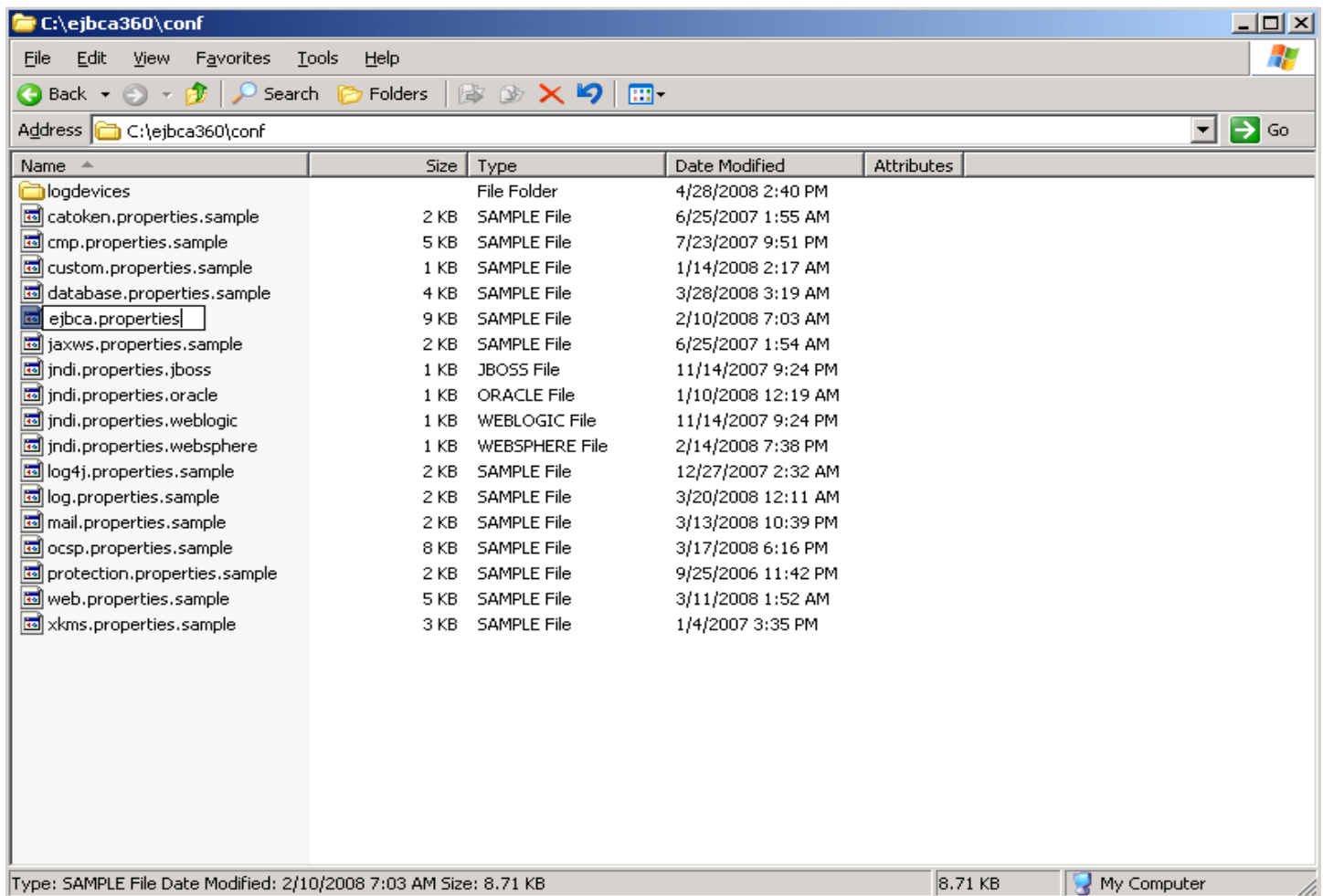
- i. Choose “Path”\Click “Edit”
- ii. Add “;” at the end of the value
- iii. Add the new directory to the value

System variables	value
Path	C:\Java\jdk1.6.0_06\bin;C:\ant170\bin



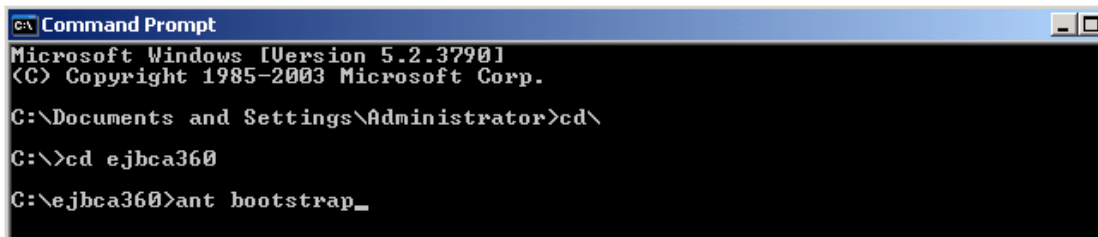
5. Rename

Rename	to
C:\ejbca360\conf\ejbca.properties.sample	C:\ejbca360\conf\ejbca.properties



2.1 -- Deploy EJBCA and Supplementary Components

1. Open a command prompt, start/run/type "cmd"\enter
2. Go to ejbca directory, type "cd"\enter/cd ejbca360\enter
3. type "ant bootstrap" and press enter



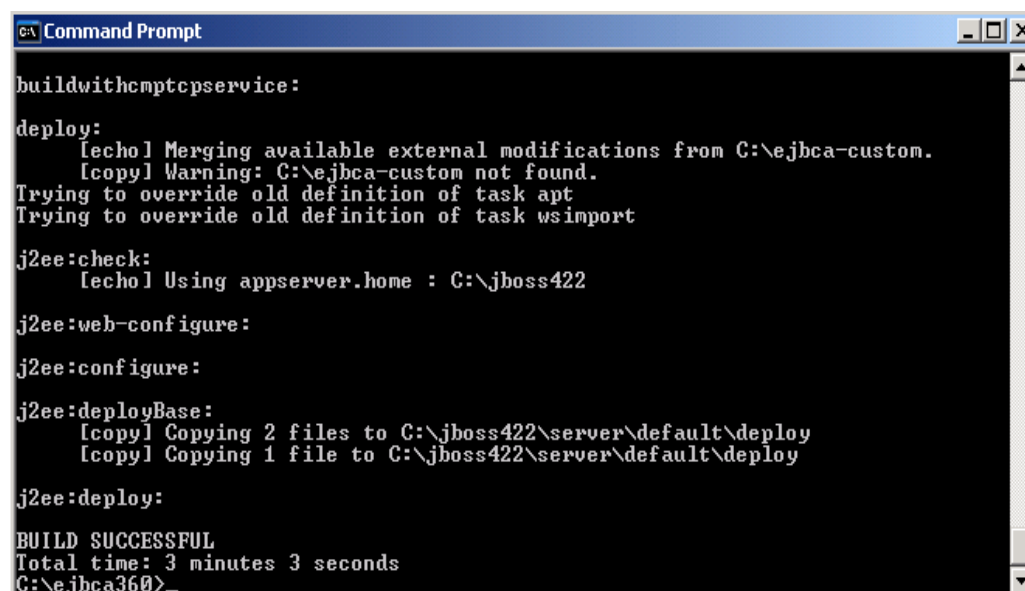
```

C:\>Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>cd ejbca360

C:\ejbca360>ant bootstrap_
  
```



```

C:\>Command Prompt

buildwithcmptcpservice:

deploy:
    [echo] Merging available external modifications from C:\ejbca-custom.
    [copy] Warning: C:\ejbca-custom not found.
    Trying to override old definition of task apt
    Trying to override old definition of task wsimport

j2ee:check:
    [echo] Using appserver.home : C:\jboss422

j2ee:web-configure:

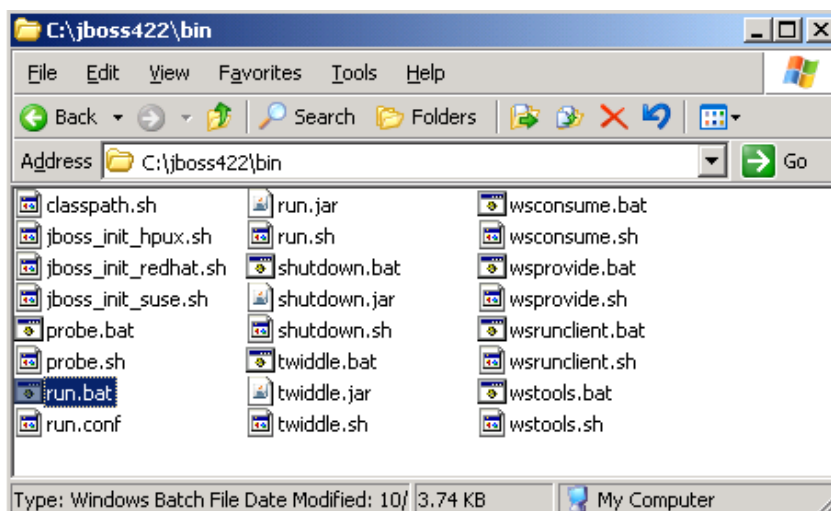
j2ee:configure:

j2ee:deployBase:
    [copy] Copying 2 files to C:\jboss422\server\default\deploy
    [copy] Copying 1 file to C:\jboss422\server\default\deploy

j2ee:deploy:

BUILD SUCCESSFUL
Total time: 3 minutes 3 seconds
C:\ejbca360>
  
```

4. If build successfully in previous step, start JBoss service by going to "C:\jboss422\bin" and double click on "run.bat"




```

C:\ Shortcut to run.bat
parameters.
11:50:39,656 INFO [OCSPServletBase] ExtensionClass not defined in initialization parameters.
11:50:39,718 INFO [TomcatDeployer] deploy, ctxPath=/ejbca/publicweb/webdist, warUrl=.../tmp/deploy/tmp51816ejbca.ear-contents/webdist-exp.war/
11:50:39,875 INFO [TomcatDeployer] deploy, ctxPath=/ejbca/xkms, warUrl=.../tmp/deploy/tmp51816ejbca.ear-contents/xkms-exp.war/
11:50:40,140 ERROR [STDERR] May 6, 2008 11:50:40 AM com.sun.xml.ws.transport.http.servlet.WSServletContextListener contextInitialized
INFO: WSSERULET12: JAX-WS context listener initializing
11:50:41,937 ERROR [STDERR] May 6, 2008 11:50:41 AM com.sun.xml.ws.transport.http.servlet.RuntimeEndpointInfoParser processWsdLocation
INFO: wsdl cannot be found from DD or annotation. Will generate and publish a new WSDL for SEI endpoints.
11:50:41,984 ERROR [STDERR] May 6, 2008 11:50:41 AM com.sun.xml.ws.transport.http.servlet.WSServletDelegate init
INFO: WSSERULET14: JAX-WS servlet initializing
11:50:42,015 INFO [EARDeployer] Started J2EE application: file:/C:/jboss422/server/default/deploy/ejbca.ear
11:50:42,218 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-127.0.0.1-8080
11:50:42,250 INFO [AjpProtocol] Starting Coyote AJP/1.3 on ajp-127.0.0.1-8009
11:50:42,312 INFO [Server] JBoss (MX MicroKernel) [4.2.2.GA (build: SUNTag=JBoss_4_2_2_GA date=200710221139)] Started in 1m:15s:125ms

```

5. After starting JBoss service, type “ant install” in the first command prompt and press enter

```

C:\ Command Prompt
buildwithcmptcpservice:
deploy:
[echo] Merging available external modifications from C:\ejbca-custom.
[copy] Warning: C:\ejbca-custom not found.
Trying to override old definition of task apt
Trying to override old definition of task wsimport
j2ee:check:
[echo] Using appserver.home : C:\jboss422
j2ee:web-configure:
j2ee:configure:
j2ee:deployBase:
[copy] Copying 2 files to C:\jboss422\server\default\deploy
[copy] Copying 1 file to C:\jboss422\server\default\deploy
j2ee:deploy:
BUILD SUCCESSFUL
Total time: 3 minutes 3 seconds
C:\ejbca360>ant install

```

6. To use default setting for super admin certificate, just press “Enter” when command prompt prompts you to input anything

```

C:\ Command Prompt
[Input] Please enter the server dn (default: CN=localhost,O=EJBCA Sample,C=SE)
E) ? [CN=localhost,O=EJBCA Sample,C=SE]

[Input] Please enter the superadmin password (default: ejbca) ? [ejbca]

[Input] Please enter the if superadmin keystore should be batched (default: true) ? [true]

[Input] skipping input as property java.trustpassword has already been set.

ejbca:init:
[echo]
[echo] ----- CA Properties -----
[echo] ca.name : AdminCA1
[echo] ca.dn : CN=AdminCA1,O=EJBCA Sample,C=SE
[echo] ca.tokenpassword : null
[echo] ca.tokenpassword : null
[echo] ca.keyspec : 2048
[echo] ca.keytype : RSA
[echo] ca.signaturealgorithm : SHA1WithRSA
[echo] ca.validity : 3650
[echo] ca.policy : null
[echo] ca.tokenproperties : conf/catoken.properties
[echo] httpserver.hostname : localhost
[echo] httpserver.dn : CN=localhost,O=EJBCA Sample,C=SE
[echo] httpserver.password : serverpwd
[echo] superadmin.password : ejbca
[echo] superadmin.batch : true
[echo] java.trustpassword : changeit
[echo] appserver.home : C:\jboss422
[echo]

ejbca:install:
[echo] Initializing CA with AdminCA1 'CN=AdminCA1,O=EJBCA Sample,C=SE' soft
null 2048 RSA 3650 null SHA1WithRSA conf/catoken.properties...
[echo] ca init AdminCA1 "CN=AdminCA1,O=EJBCA Sample,C=SE" soft null 2048 RS

```

```

C:\ Command Prompt
otca.der'
[echo] Adding to or creating keystore: C:\ejbca360\p12\truststore.jks
[exec] keytool error: java.lang.Exception: Keystore file does not exist: C:\
\ejbca360\p12\truststore.jks
[exec] java.lang.Exception: Keystore file does not exist: C:\ejbca360\p12\t
ruststore.jks
[exec] at sun.security.tools.KeyTool.doCommands(KeyTool.java:569)
[exec] at sun.security.tools.KeyTool.run(KeyTool.java:172)
[exec] at sun.security.tools.KeyTool.main(KeyTool.java:166)
[exec] Result: 1
[exec] keytool error: java.lang.Exception: Keystore file does not exist: C:\
\ejbca360\p12\truststore.jks
[exec] java.lang.Exception: Keystore file does not exist: C:\ejbca360\p12\t
ruststore.jks
[exec] at sun.security.tools.KeyTool.doCommands(KeyTool.java:569)
[exec] at sun.security.tools.KeyTool.run(KeyTool.java:172)
[exec] at sun.security.tools.KeyTool.main(KeyTool.java:166)
[exec] Result: 1
[exec] Certificate was added to keystore
[exec] [Storing C:\ejbca360\p12\truststore.jks]
[delete] Deleting: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\rootca.der

BUILD SUCCESSFUL
Total time: 4 minutes 48 seconds
C:\ejbca360>

```

7. If build successfully in previous step, stop the JBoss service by press “Ctrl + C” in the second command prompt, which is the command prompt appeared after JBoss service was started

```

C:\ Shortcut to run.bat
12:07:36,109 INFO [MailService] Mail service 'java:/Mail' removed from JNDI
12:07:36,109 INFO [TomcatDeployer] undeploy, ctxPath=/web-console, warUrl=.../d
eploy/management/console-mgr.sar/web-console.war/
12:07:36,562 INFO [Http11Protocol] Pausing Coyote HTTP/1.1 on http-127.0.0.1-80
80
12:07:36,562 INFO [AjpProtocol] Pausing Coyote AJP/1.3 on ajp-127.0.0.1-8009
12:07:37,562 INFO [StandardService] Stopping service jboss.web
12:07:37,578 INFO [Http11Protocol] Stopping Coyote HTTP/1.1 on http-127.0.0.1-8
080
12:07:37,593 INFO [AjpProtocol] Stopping Coyote AJP/1.3 on ajp-127.0.0.1-8009
12:07:37,593 INFO [TomcatDeployer] undeploy, ctxPath=/, warUrl=.../deploy/jboss
-web.deployer/ROOT.war/
12:07:37,593 INFO [TomcatDeployer] undeploy, ctxPath=/invoker, warUrl=.../depl
oy/http-invoker.sar/invoker.war/
12:07:37,593 INFO [TomcatDeployer] undeploy, ctxPath=/jbossweb, warUrl=.../depl
oy/jbossweb.sar/jbossweb-context.war/
12:07:37,609 INFO [TomcatDeployer] undeploy, ctxPath=/jbossmq-httpil, warUrl=..
./deploy/jms/jbossmq-httpil.sar/jbossmq-httpil.war/
12:07:37,656 INFO [MailService] Mail service 'java:/EjbcaMail' removed from JND
I
12:07:37,906 INFO [TransactionManagerService] Stopping recovery manager
12:07:38,796 INFO [Server] Shutdown complete
Shutdown complete
Halting VM
Terminate batch job (Y/N)? y_

```

8. Type “y” and press enter
9. After closing JBoss, type “ant deploy” in the first command prompt and press enter

```

C:\ Command Prompt
ruststore.jks
[exec] at sun.security.tools.KeyTool.doCommands(KeyTool.java:569)
[exec] at sun.security.tools.KeyTool.run(KeyTool.java:172)
[exec] at sun.security.tools.KeyTool.main(KeyTool.java:166)
[exec] Result: 1
[exec] Certificate was added to keystore
[exec] [Storing C:\ejbca360\p12\truststore.jks]
[delete] Deleting: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\rootca.der

BUILD SUCCESSFUL
Total time: 4 minutes 48 seconds
C:\ejbca360>ant deploy_

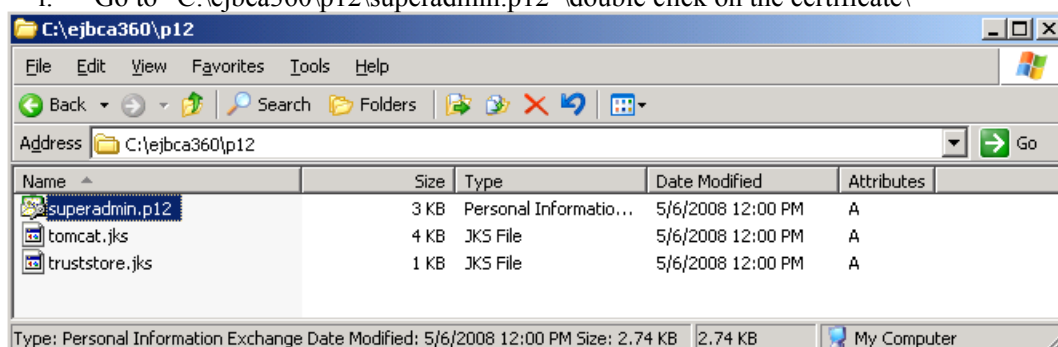
C:\ Command Prompt
j2ee:configure:
j2ee:deployBase:
[copy] Copying 2 files to C:\jboss422\server\default\deploy
[copy] Copying 1 file to C:\jboss422\server\default\deploy
j2ee:deploy:

BUILD SUCCESSFUL
Total time: 52 seconds
C:\ejbca360>

```

10. If build successfully in previous step, Import super administrator's certificate from C:\ejbca360\p12\superadmin.p12,

i. Go to "C:\ejbca360\p12\superadmin.p12" double click on the certificate\



ii. Click "Next" 2 times

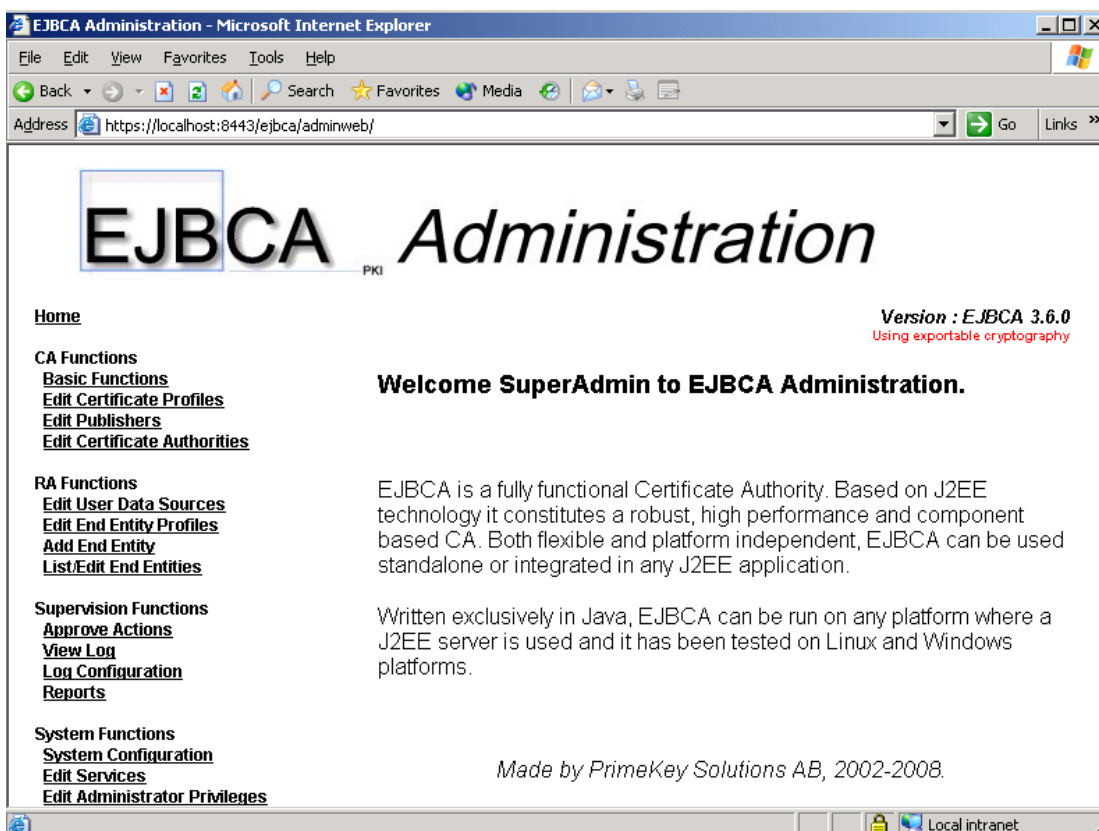
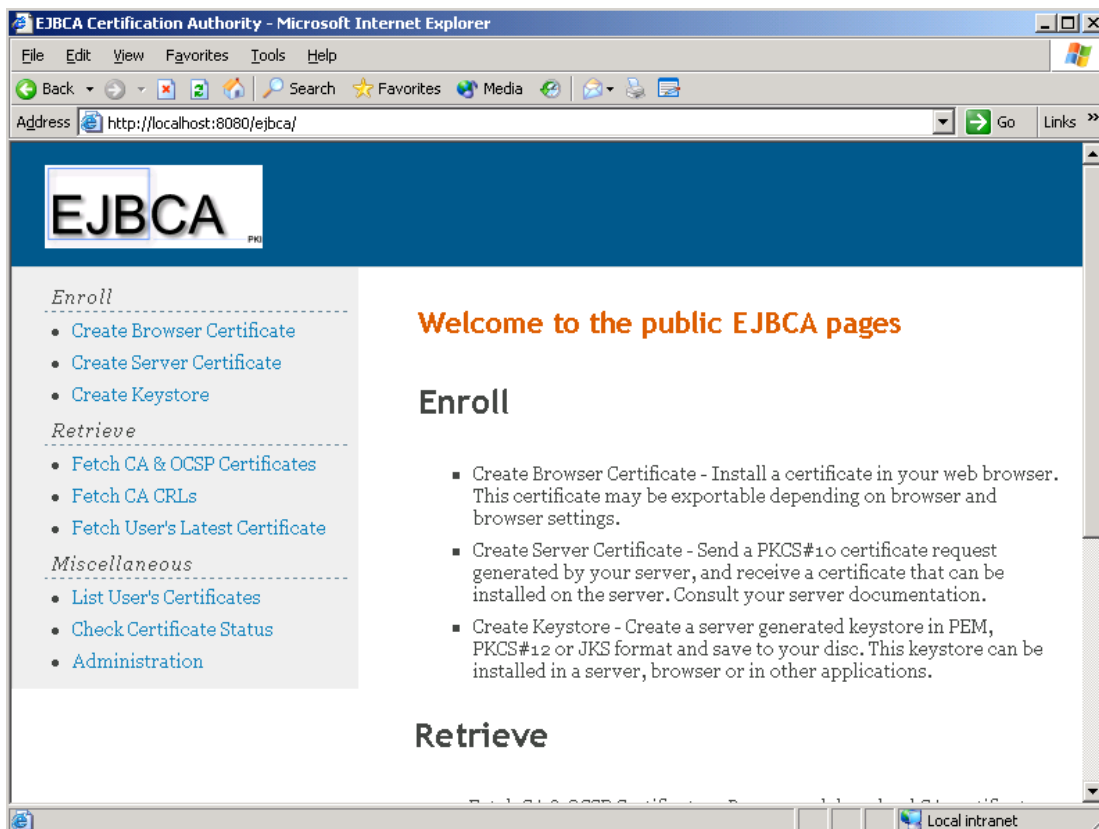


- iii. Input "ejbca" as password
- iv. Click "Next" 2 times
- v. Click "Finish"



- vi. Select "Yes" for the warning
- vii. Click "OK"

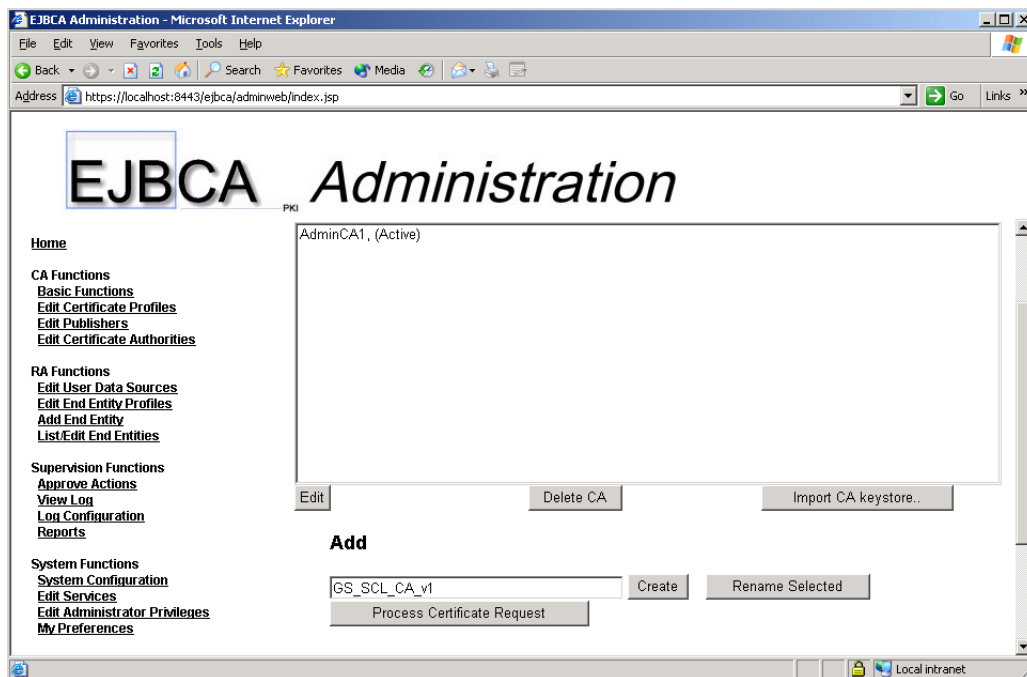
11. Start JBoss service again by going to “C:\jboss422\bin” and double click on “run.bat”
12. when JBoss service is started again, verify that you are able to access <https://localhost:8443/ejbca/> for EJBCA admin-GUI, and <https://localhost:8443/ejbca/adminweb/> for EJBCA public pages
13. If you see the 2 following web pages, EJBCA, ant and JBoss are successfully installed and deployed.



3 -- Configure EJBCA

3.1 -- Create CA

- 1) Go to EJBCA Administration GUI
- 2) Click “Edit Certificate Authorities”



- 3) Type "GS_SCL_CA_v1" in the text box under “Add”. Click “create”
- 4) Set CA’s parameters
 - i. “Subject DN”= CN=GS SCL CA v1,O=Company,C=CN
 - ii. “Validity (Days)”= 3650
 - iii. “Default CRL Dist. Point (Used as default value in certificate profiles using this CA.)”= http://clean2003.testing.company.cn:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=GS SCL CA v1,O=Company,C=CN
- 5) Leave all other setting by default, click “Create”
- 6) The following is the screen capture of the settings

Create CA

CA Name : GS_SCL_CA_v1

[Back to Certificate Authorities](#)

Type of CA	X509
CA Token Type	<input type="text" value="Soft"/>
Authentication Code (leave empty for system default)	<input type="text"/>
Enable auto-activation of CA token	<input checked="" type="checkbox"/>
Signing Algorithm	<input type="text" value="SHA1WithRSA"/>
RSA key size	<input type="text" value="1024"/>
ECDSA key spec	<input type="text"/>
Subject DN	<input type="text" value="CN=GS_SCL_CA_v1,O=Company,C=CN"/>
Signed By	<input type="text" value="Self Signed"/>
Certificate Profile	<input type="text" value="ROOTCA"/>
Validity (Days)	<input type="text" value="3650"/>
Description	<input type="text"/>
Use Subject Alternative Name	<input type="text"/>
Policy Id <i>Leave policy id blank to use default certificate profile values.</i>	<input type="text"/>
Use UTF8 in policy text	<input type="checkbox"/>
Use PrintableString encoding in DN	<input type="checkbox"/>

Use LDAP DN order (experimental to switch off)	<input checked="" type="checkbox"/>
CRL Specific Data	
Use Authority Key Id	<input checked="" type="checkbox"/>
Authority Key Id Critical	<input type="checkbox"/>
Use CRL Number	<input checked="" type="checkbox"/>
CRL Number Critical	<input type="checkbox"/>
Use CRL Distribution Point on CRLs	<input checked="" type="checkbox"/>
CRL Distribution Point on CRLs Critical	<input type="checkbox"/>
CRL Expire Period (h)	<input type="text" value="24"/>
CRL Issue Interval (h)	<input type="text" value="0"/>
CRL Overlap Time (min)	<input type="text" value="10"/>
Delta CRL Period (h) (0 if no delta CRLs are issued)	<input type="text" value="0"/>
CRL Publishers	<input type="text"/>
Default CRL Dist. Point (Used as default value in certificateprofiles using this CA.)	<input type="text" value="http://clean2003.testing.company.cn:8080/ejbca/publicweb/webdist/certdist?cmd=crl&"/> <input type="button" value="Generate"/>
Default CRL Issuer	<input type="text"/>
CA Defined FreshestCRL extension (Used as default value in certificateprofiles using this CA.)	<input type="text"/>
Default OCSP	

Service Locator
(Used as default
value in
certificateprofiles
using this CA.)

Generate

Other Data

OCSPService Active ☒

XKMS Service Active ☐

CMS Service Active ☐

Approval
Settings

Add/Edit End Entity
Key Recovery
Revocation
Activate CA Token

Number of
Required
Approvals

1

Finish User ☒

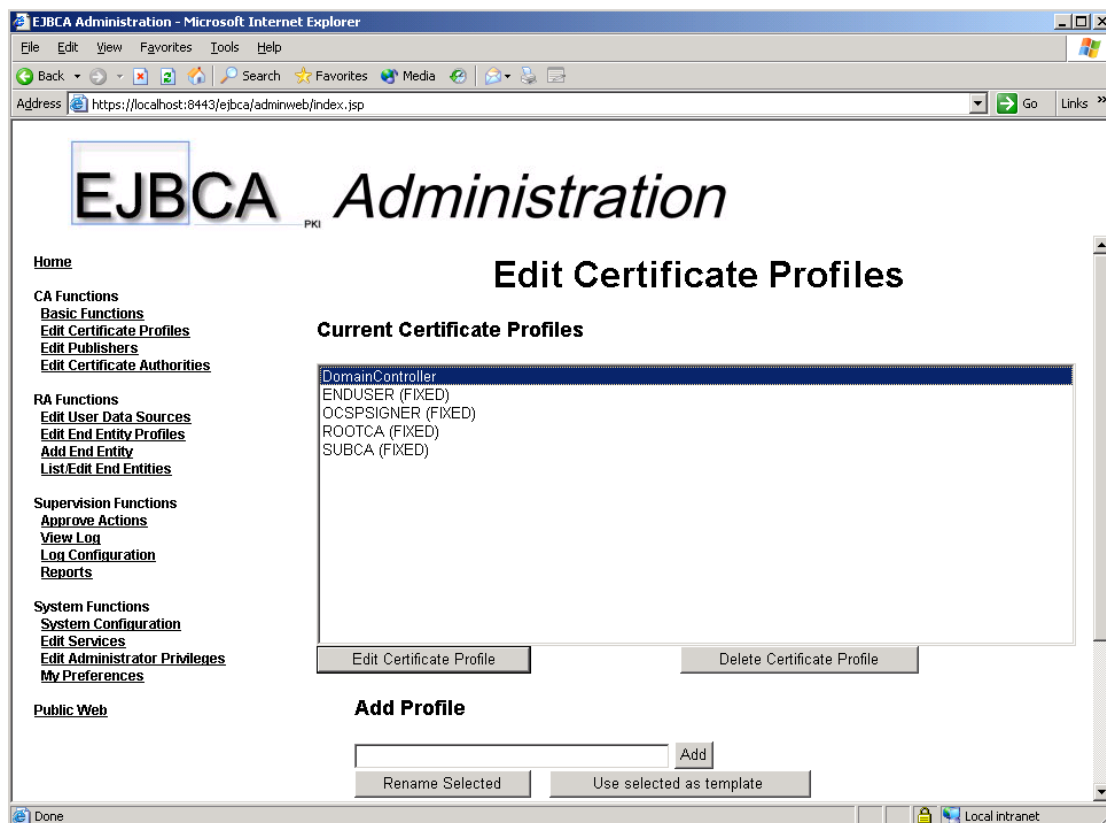
Create Cancel

Make Certificate Request

Made by PrimeKey Solutions AB, 2002-2008.

3.2 -- Create Certificate Profile "DomainController"

- 1) Go to EJBCA Administration GUI
- 2) Click "Edit Certificate Profiles"
- 3) Type "DomainController" in the text box under "Add Profile". Click "Add"
- 4) Choose "DomainController" under "Current Certificate Profiles"



- 5) Click "Edit Certificate Profile"
- 6) Set domain controller certificate's parameters
 - i. Check "Use CRL Distribution Point"
 - ii. Under "Key Usage" select "Digital Signatures" and "Key encipherment"
 - iii. Check "Use Extended Key Usage"
 - iv. Under "Extended Key Usage" select "Server Authentication" and "Client Authentication"
 - v. Check "Use MS Template Value"
 - vi. Check "Use a Subset of Subject Alt. Name"
 - vii. Select "Subset of Subject Alt. Name" "DNS Name" and "MS GUID, Global Unique Identifier"
 - viii. Under "Available CAs" select only "GS_SCL_CA_v1"
- 7) Leave all other setting by default, click "save"
- 8) The following is the screen capture of the settings

Edit Certificate Profile

Certificate Profile : DomainController

[Back to Certificate Profiles](#)

Validity (Days)	<input type="text" value="730"/>
Allow validity override	<input type="checkbox"/>
Allow extension override	<input type="checkbox"/>
Use Basic Constraints	<input checked="" type="checkbox"/>
Basic Constraints Critical	<input checked="" type="checkbox"/>
Use Path Length Constraint	<input type="checkbox"/>
Path Length Constraint	<input type="text"/>
Use Key Usage	<input checked="" type="checkbox"/>
Key Usage Critical	<input checked="" type="checkbox"/>
Use Subject Key ID	<input checked="" type="checkbox"/>
Use Authority Key Id	<input checked="" type="checkbox"/>
Use Subject Alternative Name	<input checked="" type="checkbox"/>
Subject Alternate Name Critical	<input type="checkbox"/>
Use Subject Directory Attributes	<input type="checkbox"/>
	<input checked="" type="checkbox"/>
Use CRL Distribution Point	<input type="checkbox"/>
CRL Distribution Point Critical	<input checked="" type="checkbox"/>
Use CA defined CRL Dist. Point	<input type="checkbox"/>
CRL Distribution Point URI	<input type="text"/>
CRL issuer	<input type="text"/>
Use FreshestCRL extension	<input type="checkbox"/>
Use CA Defined FreshestCRL extension	<input type="checkbox"/>
FreshestCRL extension URI	<input type="text"/>
Use OCSP No Check	<input type="checkbox"/>
Use Authority Information Access	<input type="checkbox"/>
Use CA defined OCSP locator	<input type="checkbox"/>
OCSP Service Locator URI	<input type="text"/>
<input type="button" value="Add"/> CA issuer URI	<input type="text"/>
Use Certificate Policies	<input type="checkbox"/>
Certificate Policies Critical	<input type="checkbox"/>

	Certificate Policy Id	<input type="text"/>
<input type="button" value="Add"/>	User Notice Text	<input type="text"/>
	CPS	<input type="text"/>
Use Qualified Certificate Statement <input type="checkbox"/>		
	Qualified Certificate Statement Critical	<input type="checkbox"/>
	Use PKIX QCSyntax-v2	<input type="checkbox"/>
	Semantics Id	<input type="text"/>
	RA Name	<input type="text"/>
	Use ETSI QC Compliance	<input type="checkbox"/>
	Use ETSI Secure Signature Creation Device	<input type="checkbox"/>
	Use ETSI transaction value limit	<input type="checkbox"/>
	Value Limit Currency	<input type="text"/>
	Value Limit Amount	<input type="text"/>
	Value Limit Exponent	<input type="text"/>
	Use ETSI retention period	<input type="checkbox"/>
	Retention Period (in years)	<input type="text"/>
	Use Custom QC-statement String	<input type="checkbox"/>
	Custom QC-statement OID	<input type="text"/>
	Custom QC-statement Text	<input type="text"/>
	Key usage	<div><div>Digital Signature</div><div>Non-repudiation</div><div>Key encipherment</div><div>Data encipherment</div><div>Key agreement</div><div>Key certificate sign</div><div>CRL sign</div><div>Encipher only</div><div>Decipher only</div></div>
	Allow Key Usage Override	<input checked="" type="checkbox"/>
	Use Extended Key Usage	<input checked="" type="checkbox"/>
	Extended Key Usage Critical	<input type="checkbox"/>

Extended Key Usage	<div>Any Extended Key Usage Server Authentication Client Authentication Code Signing Email Protection Time Stamping MS Smart Card Logon OCSPSigner MS Encrypted File System MS EFS Recovery Internet Key Exchange for IPsec SCVP Server Certificate Validation SCVP Request Authentication</div>
Use MS Template Value	<input checked="" type="checkbox"/>
Microsoft Template Value (Only the value not the actual template)	<div>DomainController</div>
Use CN Postfix	<input type="checkbox"/>
CN Postfix Text appended after first CN field	<div></div>
Use a Subset of Subject DN	<input type="checkbox"/>
Subset of SubjectDN	<div>Email, EmailAddress in DN UID, Unique Id CN, Common Name SerialNumber, Serial Number GivenName, Given Name Initials SurName, family name Title OU, Organization Unit O, Organization L, Location ST, State or Province: DC, Domain Component C, Country (ISO 3166) Unstructured Address, IP address</div>
Use a Subset of Subject Alt. Name	<input checked="" type="checkbox"/>
Subset of Subject Alt. Name	<div>Other Name RFC822 Name (email address) DNS Name IP Address X400 Address DirectoryName, Distinguished Name (DN)</div>
Available bit lengths	<div>0 Bits 192 Bits 239 Bits 256 Bits 384 Bits</div>

Available CAs

Any CA
AdminCA1
GS_SCL_CA_v1

Publishers

Type

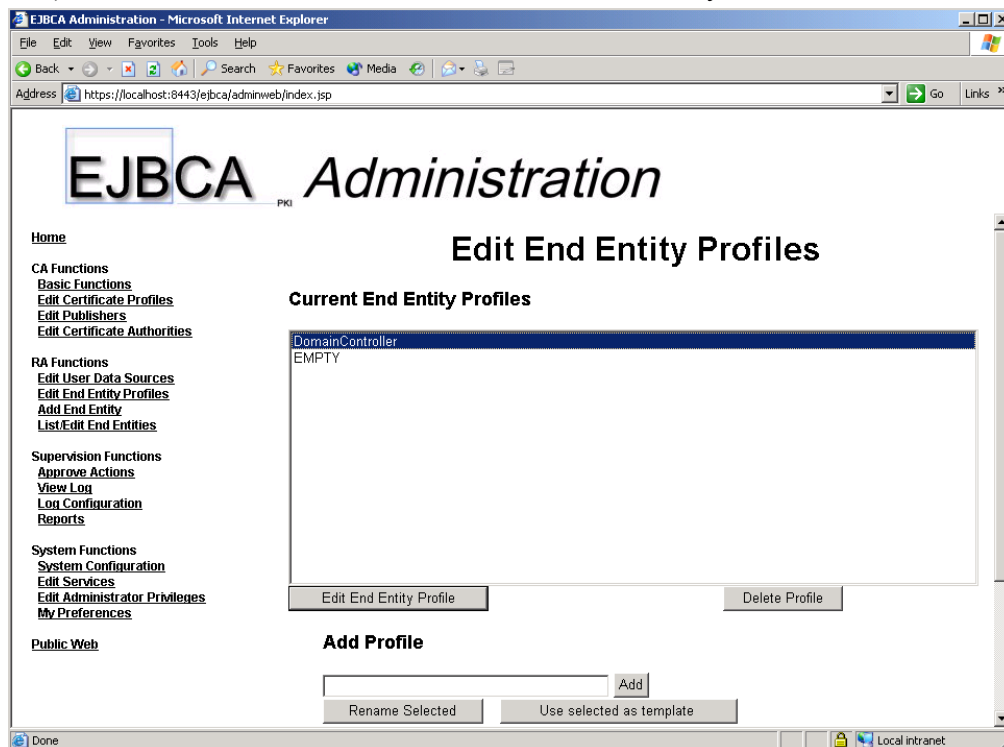
End Entity

Save Cancel

Made by PrimeKey Solutions AB, 2002-2008.

3.3 -- Create End Entity Profile "DomainController"

- 1) Go to EJBCA Administration GUI
- 2) Click "Edit End Entity Profiles"
- 3) Type "DomainController" in the text box under "Add Profile". Click "Add"
- 4) Choose "DomainController" under "Current End Entity Profiles"



- 5) Click "Edit End Entity Profile"
- 6) Set domain controller end entity profile's parameters
 - i. In the "Subject Alternative Name Fields" add "DNS Name" and "MS GUID, Global Unique Identifier"
 - ii. Under "Email Domain (Use only the domain part of the address, without the '@' char)" uncheck "use"
 - iii. Under "Default Certificate Profile" choose "DomainController"
 - iv. Under "Available Certificate Profiles" select "DomainController"
 - v. Under "Default CA" select "GS_SCL_CA_v1"
 - vi. Under "Available CAs" select only "GS_SCL_CA_v1"
- 7) Leave all other setting by default, click "save"
- 8) The following is the screen capture of the settings

Edit End Entity Profile

Profile : DomainController

[Back to End Entity Profiles](#)

	Username	<input type="text"/>	Required <input checked="" type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
	Password	<input type="password"/>	Autogenerated <input type="checkbox"/> Required <input checked="" type="checkbox"/>
	Batch generation (clear text pwd storage)	Use <input type="checkbox"/>	Default <input type="checkbox"/> Required <input type="checkbox"/>
Select for Removal	Subject DN Fields	<input type="text" value="Email, EmailAddress in DN"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	CN, Common Name	<input type="text"/>	Required <input checked="" type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
<input type="button" value="Remove"/>			
Select for Removal	Subject Alternative Name Fields	<input type="text" value="Other Name"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	DNS Name	<input type="text"/>	Required <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
<input type="checkbox"/>	MS GUID, Globally Unique Identifier	<input type="text"/>	Required <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
<input type="button" value="Remove"/>			
	Reverse Subject DN and Subject Alt Name Checks	<input type="checkbox"/>	
	Email Domain (Use only the domain part of the address, without the '@' char)	<input type="text"/>	Use <input type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/>
Select for Removal	Subject Directory Attribute Fields	<input type="text" value="Date of birth (yyyyMMdd)"/>	<input type="button" value="Add"/>
<input type="button" value="Remove"/>			
	Certificate Validity Start Time (e.g. 5/3/08 8:53 PM or days:hours:minutes)	<input type="text"/>	Use <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
	Certificate Validity End Time (e.g. 5/3/08 8:53 PM or	<input type="text"/>	Use <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>

days:hours:minutes)

Default Certificate Profile

Available Certificate Profiles

DomainController

ENDUSER

OCSPSIGNER

Default CA

Available CAs

AdminCA1

GS_SCL_CA_v1

Default Token

Available Tokens

User Generated

P12 file

JKS file

PEM file

Number of allowed requests Use ☐ Default

Types:

Administrator Use ☐ Default ☐ Required ☐

Send Notification Use ☐ Default ☐ Required ☐

Add

Delete all

Notification Sender (Email Address)

Notification Recipient

Notification Events

STATUSNEW

STATUSFAILED

STATUSINITIALIZED

STATUSINPROCESS

STATUSGENERATED

STATUSREVOKED

STATUSHISTORICAL

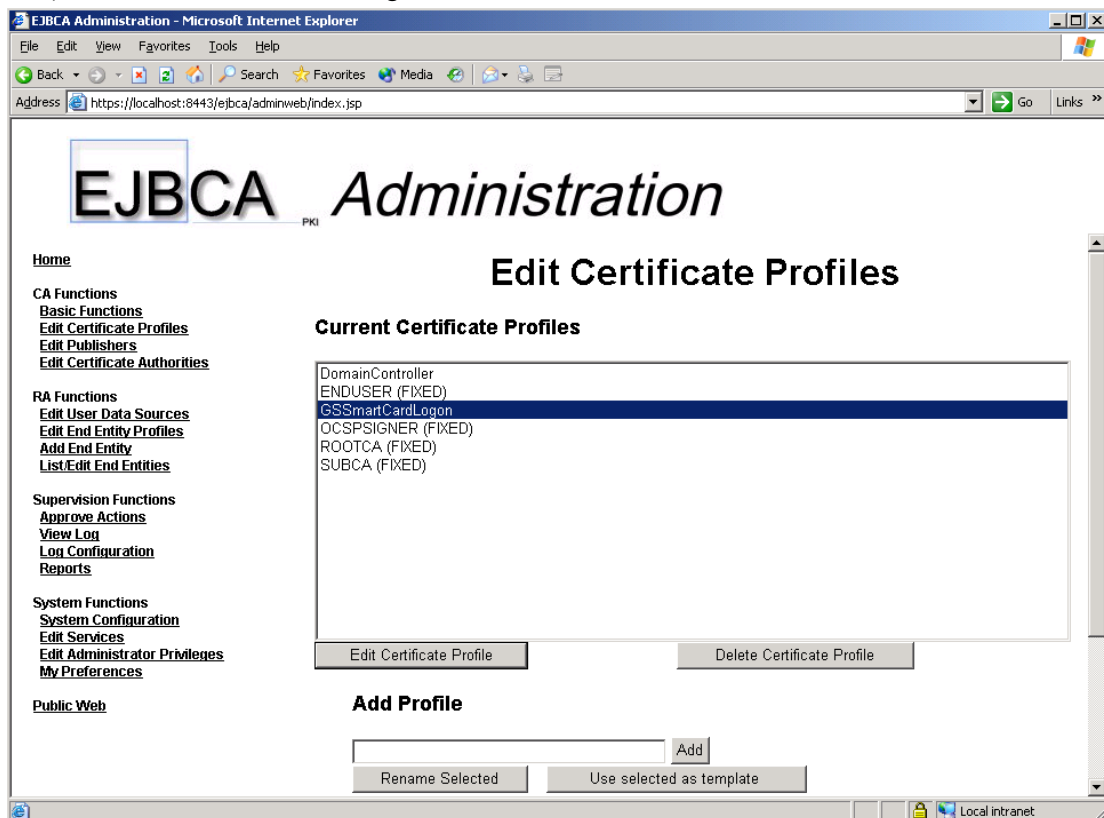
Notification Subject

	<input type="text"/>
Notification Message	<div><div></div><div></div></div>
Printing of user data	Use <input type="checkbox"/> Default <input type="checkbox"/> Required <input type="checkbox"/>
Printer Name	<div>Bullzip PDF Printer</div>
Printed Copies	<div>1</div>
Current Template	No Printing template is uploaded.
Upload Template	<div>Upload Template</div>
	<div>Save</div> <div>Cancel</div>

Made by PrimeKey Solutions AB, 2002-2008.

3.4 -- Create New Certificate Profile "GSSmartCardLogon"

- 1) Go to EJBCA Administration GUI
- 2) Click "Edit Certificate Profiles"
- 3) Type "GSSmartCardLogon" in the text box under "Add Profile". Click "Add"
- 4) Choose "GSSmartCardLogon" under "Current Certificate Profiles"



- 5) Click "Edit Certificate Profile"
- 6) Set GSSmartCardLogon certificate profile's parameters
 - i. Check "Use CRL Distribution Point"
 - ii. Under "Key Usage" select "Digital Signatures"
 - iii. Check "Use Extended Key Usage"
 - iv. Under "Extended Key Usage" select "Client Authentication" and "MS Smart Card Logon"
 - v. Under "Available CAs" select only "GS_SCL_CA_v1"
- 7) Leave all other setting by default, click "save"
- 8) The following is the screen capture of the settings

Edit Certificate Profile

Certificate Profile : GSSmartCardLogon

[Back to Certificate Profiles](#)

Validity (Days)	<input type="text" value="730"/>
Allow validity override	<input type="checkbox"/>
Allow extension override	<input type="checkbox"/>
Use Basic Constraints	<input checked="" type="checkbox"/>
Basic Constraints Critical	<input checked="" type="checkbox"/>
Use Path Length Constraint	<input type="checkbox"/>
Path Length Constraint	<input type="text"/>
Use Key Usage	<input checked="" type="checkbox"/>
Key Usage Critical	<input checked="" type="checkbox"/>
Use Subject Key ID	<input checked="" type="checkbox"/>
Use Authority Key Id	<input checked="" type="checkbox"/>
Use Subject Alternative Name	<input checked="" type="checkbox"/>
Subject Alternate Name Critical	<input type="checkbox"/>
Use Subject Directory Attributes	<input type="checkbox"/>
	<input checked="" type="checkbox"/>
Use CRL Distribution Point	<input type="checkbox"/>
CRL Distribution Point Critical	<input checked="" type="checkbox"/>
Use CA defined CRL Dist. Point	<input type="checkbox"/>
CRL Distribution Point URI	<input type="text"/>
CRL issuer	<input type="text"/>
Use FreshestCRL extension	<input type="checkbox"/>
Use CA Defined FreshestCRL extension	<input type="checkbox"/>
FreshestCRL extension URI	<input type="text"/>
Use OCSP No Check	<input type="checkbox"/>
Use Authority Information Access	<input type="checkbox"/>
Use CA defined OCSP locator	<input type="checkbox"/>
OCSP Service Locator URI	<input type="text"/>
<input type="button" value="Add"/> CA issuer URI	<input type="text"/>
Use Certificate Policies	<input type="checkbox"/>
Certificate Policies Critical	<input type="checkbox"/>

	Certificate Policy Id	<input type="text"/>
<input type="button" value="Add"/>	User Notice Text	<input type="text"/>
	CPS	<input type="text"/>
Use Qualified Certificate Statement <input type="checkbox"/>		
	Qualified Certificate Statement Critical	<input type="checkbox"/>
	Use PKIX QCSyntax-v2	<input type="checkbox"/>
	Semantics Id	<input type="text"/>
	RA Name	<input type="text"/>
	Use ETSI QC Compliance	<input type="checkbox"/>
	Use ETSI Secure Signature Creation Device	<input type="checkbox"/>
	Use ETSI transaction value limit	<input type="checkbox"/>
	Value Limit Currency	<input type="text"/>
	Value Limit Amount	<input type="text"/>
	Value Limit Exponent	<input type="text"/>
	Use ETSI retention period	<input type="checkbox"/>
	Retention Period (in years)	<input type="text"/>
	Use Custom QC-statement String	<input type="checkbox"/>
	Custom QC-statement OID	<input type="text"/>
	Custom QC-statement Text	<input type="text"/>
	Key usage	<div><div>Digital Signature</div><div>Non-repudiation</div><div>Key encipherment</div><div>Data encipherment</div><div>Key agreement</div><div>Key certificate sign</div><div>CRL sign</div><div>Encipher only</div><div>Decipher only</div></div>
	Allow Key Usage Override	<input checked="" type="checkbox"/>
	Use Extended Key Usage	<input checked="" type="checkbox"/>
	Extended Key Usage Critical	<input type="checkbox"/>

Extended Key Usage	<div>Any Extended Key Usage Server Authentication Client Authentication Code Signing Email Protection Time Stamping MS Smart Card Logon OCSPSigner MS Encrypted File System MS EFS Recovery Internet Key Exchange for IPsec SCVP Server Certificate Validation SCVP Request Authentication</div>
Use MS Template Value	<input type="checkbox"/>
Microsoft Template Value (Only the value not the actual template)	<div>DomainController</div>
Use CN Postfix	<input type="checkbox"/>
CN Postfix Text appended after first CN field	<div></div>
Use a Subset of Subject DN	<input type="checkbox"/>
Subset of SubjectDN	<div>Email, EmailAddress in DN UID, Unique Id CN, Common Name SerialNumber, Serial Number GivenName, Given Name Initials SurName, family name Title OU, Organization Unit O, Organization L, Location ST, State or Province: DC, Domain Component C, Country (ISO 3166) Unstructured Address, IP address</div>
Use a Subset of Subject Alt. Name	<input type="checkbox"/>
Subset of Subject Alt. Name	<div>Other Name RFC822 Name (email address) DNS Name IP Address X400 Address DirectoryName, Distinguished Name (DN)</div>
Available bit lengths	<div>0 Bits 192 Bits 239 Bits 256 Bits 384 Bits</div>

Available CAs

Any CA
AdminCA1
GS_SCL_CA_v1

Publishers

Type

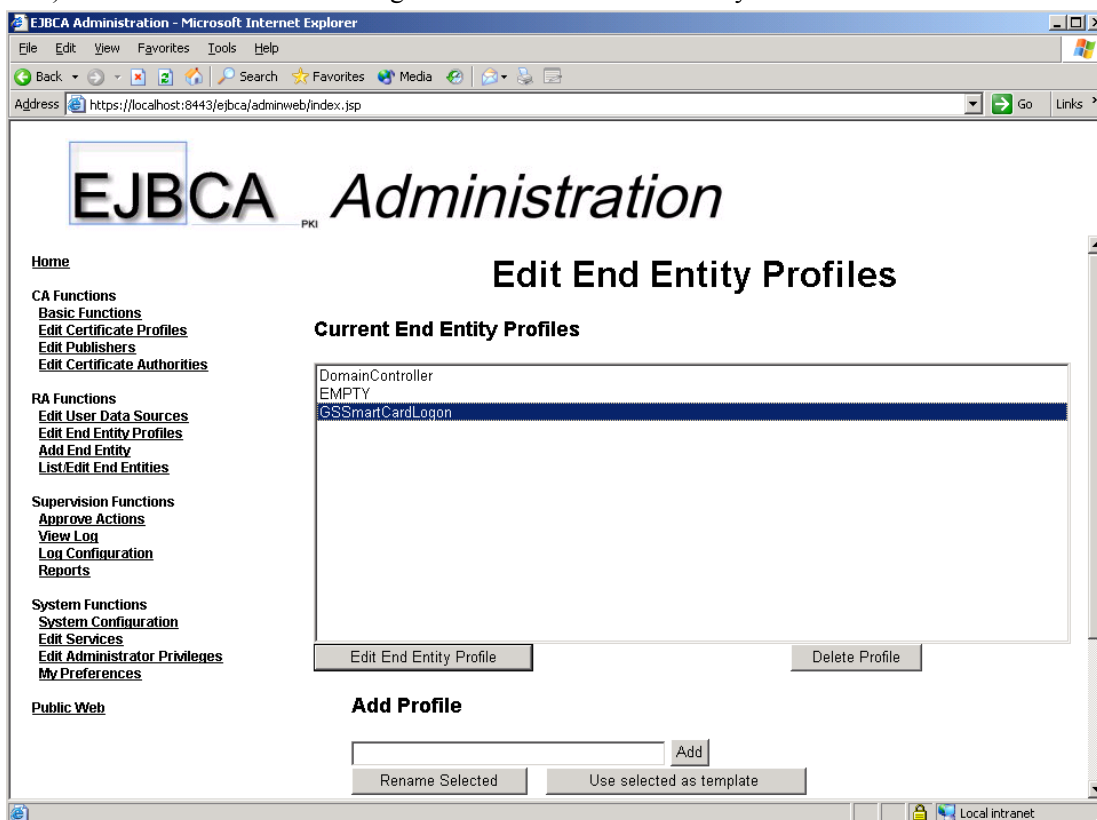
End Entity

Save Cancel

Made by PrimeKey Solutions AB, 2002-2008.

3.5 -- Create New End Entity Profile "GSSmartCardLogon"

- 1) Go to EJBCA Administration GUI
- 2) Click "Edit End Entity Profiles"
- 3) Type "GSSmartCardLogon" in the text box under "Add Profile". Click "Add"
- 4) Choose "MSSmartCardLogon" under "Current End Entity Profiles"



- 5) Click "Edit End Entity Profile"
- 6) Set GSSmartCardLogon end entity profile's parameters
 - i. Under "Subject Alternative Name Fields" add "MS UPN, User Principal Name"
 - ii. Check the "Required" box under "MS UPN, User Principal Name (Use only the domain part of the name, without the '@' char)"
 - iii. Under "Email Domain (Use only the domain part of the address, without the '@' char)" uncheck "use"
 - iv. Under "Default Certificate Profile" choose "GSSmartCardLogon"
 - v. Under "Available Certificate Profiles" choose "GSSmartCardLogon"
 - vi. Under "Default CA" choose "GS_SCL_CA_v1"
 - vii. Under "Available CAs" choose only "GS_SCL_CA_v1"
- 7) Leave all other setting by default, click "save"
- 8) The following is the screen capture of the settings

Edit End Entity Profile

Profile : GSSmartCardLogon

[Back to End Entity Profiles](#)

	Username	<input type="text"/>	Required <input checked="" type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
	Password	<input type="password"/>	Autogenerated <input type="checkbox"/> Required <input checked="" type="checkbox"/>
	Batch generation (clear text pwd storage)	Use <input type="checkbox"/>	Default <input type="checkbox"/> Required <input type="checkbox"/>
Select for Removal	Subject DN Fields	<input type="text" value="Email, EmailAddress in DN"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	CN, Common Name	<input type="text"/>	Required <input checked="" type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
<input type="button" value="Remove"/>			
Select for Removal	Subject Alternative Name Fields	<input type="text" value="Other Name"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	MS UPN, User Principal Name (Use only the domain part of the name, without the '@' char)	<input type="text"/>	Required <input checked="" type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
<input type="button" value="Remove"/>			
	Reverse Subject DN and Subject Alt Name Checks	<input type="checkbox"/>	
	Email Domain (Use only the domain part of the address, without the '@' char)	<input type="text"/>	Use <input type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/>
Select for Removal	Subject Directory Attribute Fields	<input type="text" value="Date of birth (yyyyMMdd)"/>	<input type="button" value="Add"/>
<input type="button" value="Remove"/>			
	Certificate Validity Start Time (e.g. 5/6/08 3:46 PM or days:hours:minutes)	<input type="text"/>	Use <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>
	Certificate Validity End Time (e.g. 5/6/08 3:46 PM or days:hours:minutes)	<input type="text"/>	Use <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>

Default Certificate Profile	<div>GSSmartCardLogon</div>
Available Certificate Profiles	<div>DomainController ENDUSER GSSmartCardLogon OCSPSIGNER</div>
Default CA	<div>GS_SCL_CA_v1</div>
Available CAs	<div>AdminCA1 GS_SCL_CA_v1</div>
Default Token	<div>User Generated</div>
Available Tokens	<div>User Generated P12 file JKS file PEM file</div>
Number of allowed requests	Use <input type="checkbox"/> Default <div>1</div>
Types:	
Administrator	Use <input type="checkbox"/> Default <input type="checkbox"/> Required <input type="checkbox"/>
Send Notification	Use <input type="checkbox"/> Default <input type="checkbox"/> Required <input type="checkbox"/>
<div>Add Delete all</div>	Notification Sender (Email Address) <input type="text"/>
	Notification Recipient <div>USER</div>
	Notification Events <div>STATUSNEW STATUSFAILED STATUSINITIALIZED STATUSINPROCESS STATUSGENERATED STATUSREVOKED STATUSHISTORICAL</div>
	Notification Subject <input type="text"/>

Notification Message

Printing of user data Use ☐
Default ☐ Required ☐

Printer Name

Printed Copies

Current Template No Printing template is uploaded.

Upload Template

Made by PrimeKey Solutions AB, 2002-2008.

3.6 -- Fetch Domain Controller & Certificate Authority Certificate

1. Go to domain controller\desktop\double click on "1. GenerateDCCertRequest.vbs"
2. A visual confirmation--"Done!" will be shown
3. Click "OK"
4. This script produces the following files on desktop

DomainControllerCertRequest-CLEAN2003.req
DomainControllerInfo-CLEAN2003.txt

5. Add end entity "DomainController-001"
 - i. Go to EJBCA Administration GUI
 - ii. Click "Add End Entity"
 - iii. Under "End Entity Profile" choose "DomainController"
 - iv. User Name= "DomainController-001"
 - v. Password="foo123"
 - vi. Confirm Password="foo123"
 - vii. CN, Common Name="DomainController-001"
 - viii. DNS Name=copy from " DomainControllerInfo-CLEAN2003.txt " at desktop
 - ix. MS GUID, Globally Unique Identifier= copy from " DomainControllerInfo-CLEAN2003.txt " at desktop

EJBCA Administration

Add End Entity

End Entity Profile: DomainController

Username: DomainController-001

Password: Required

Confirm Password: Required

Subject DN Fields

CN, Common Name: DomainController-001 Required

Subject Alternative Name Fields

DNS Name: clean2003.testing.company.cn

MS GUID, Globally Unique Identifier: 5210ac15e5152d429bce750038443a68

Certificate Profile: DomainController Required

CA: GS_SCL_CA_v1 Required

Token: User Generated Required

Add End Entity Reset

- x. Leave all other setting by default, click "Add End Entity"

6. Add a "GS SmartCardLogon" end entity
 - i. Go to EJBCA Administration GUI
 - ii. Click "Add End Entity"
 - iii. Under "End Entity Profile" choose "GS SmartCardLogon"
 - iv. User Name= "AdministratorGSSCL-001"
 - v. Password="foo123"
 - vi. Confirm Password="foo123"
 - vii. CN, Common Name= "AdministratorGSSCL-001"
 - viii. MS UPN, User Principal Name="Administrator@ testing.company.cn" (the field in front of "@" is the user name which supposed to logon to workstation later, in this case it is "Administrator")

EJBCA Administration

Add End Entity

End Entity Profile: Required

Username: Required

Password: Required

Confirm Password: Required

Subject DN Fields

CN, Common Name: Required

Subject Alternative Name Fields

MS UPN, User Principal Name: Required

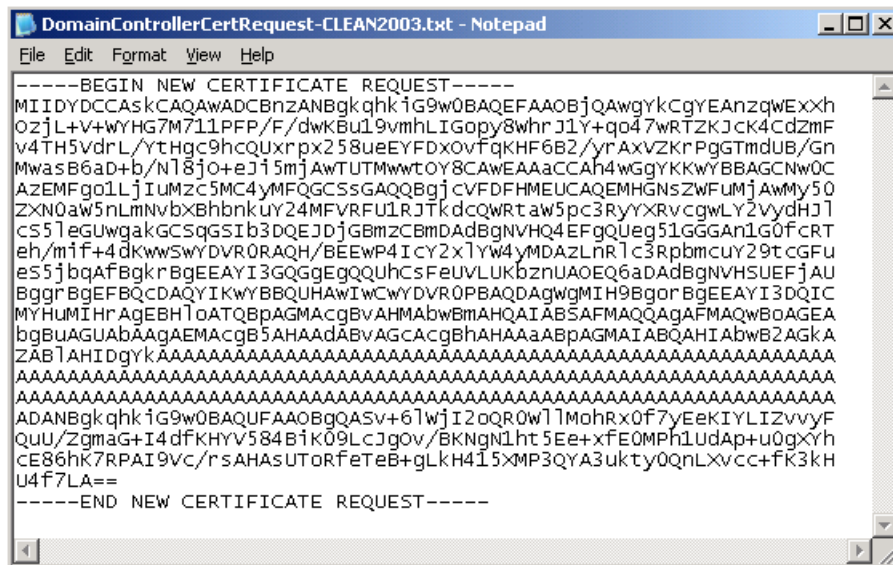
Certificate Profile: Required

CA: Required

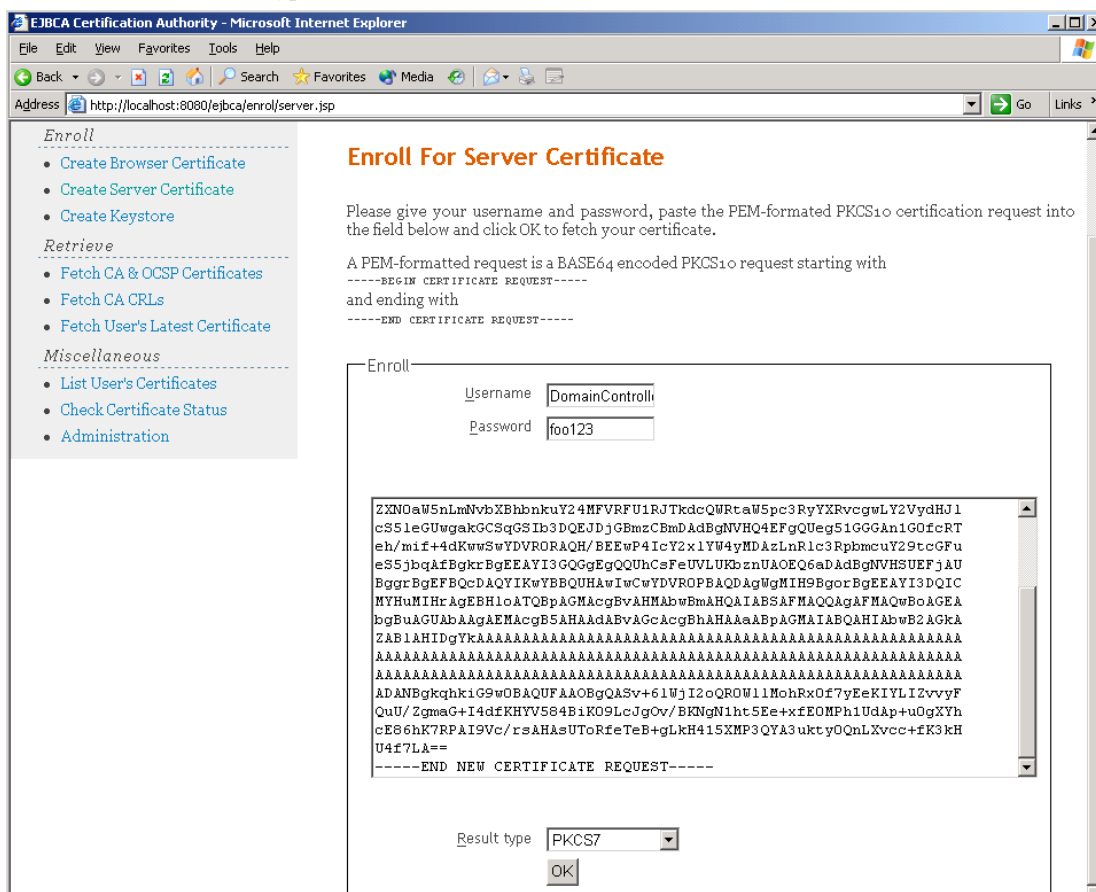
Token: Required

- ix. Leave all other setting by default, click "Add End Entity"

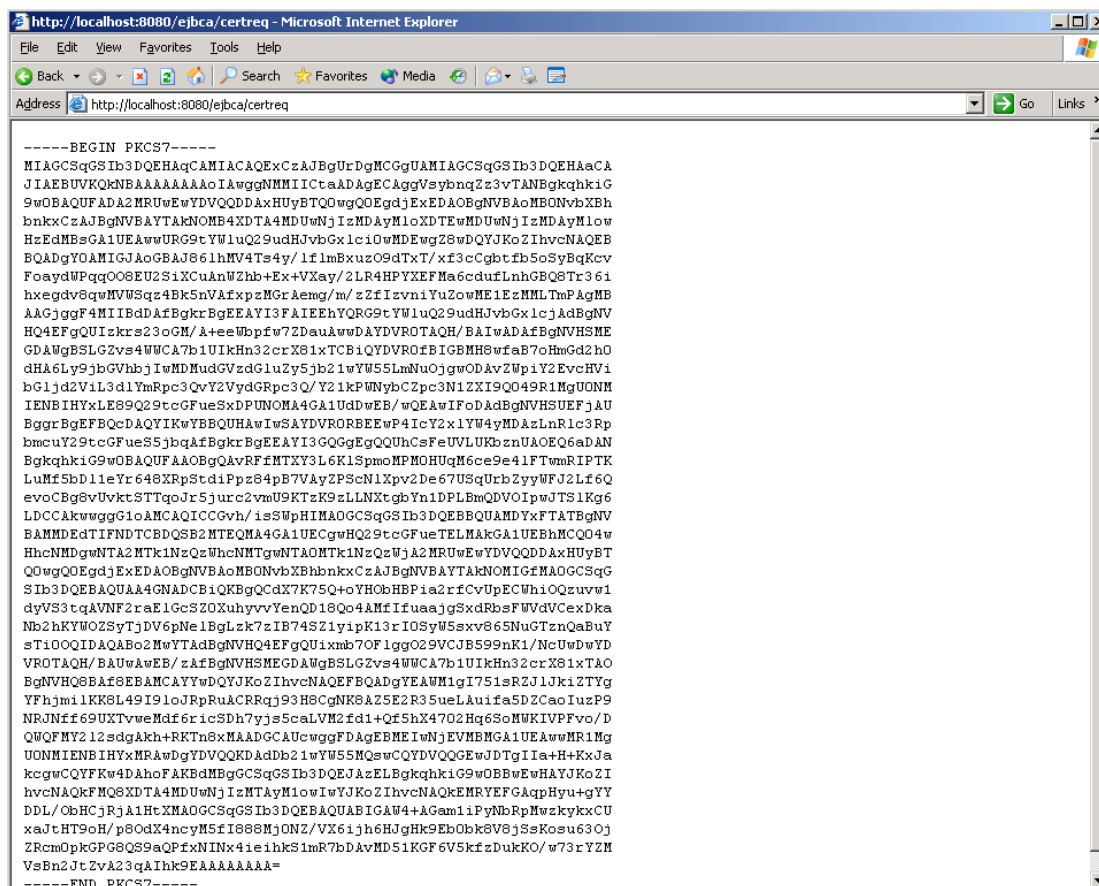
7. Fetch DC certificate
 - i. Go to EJBCA's Public Web Pages
 - ii. Click "Create Server Certificate"
 - iii. Enter username "DomainController-001"
 - iv. Enter password "foo123"
 - v. Rename the "DomainControllerCertRequest-CLEAN2003.req", which is at desktop, to "DomainControllerCertRequest-CLEAN2003.txt"
 - vi. Open the "DomainControllerCertRequest-CLEAN2003.txt"



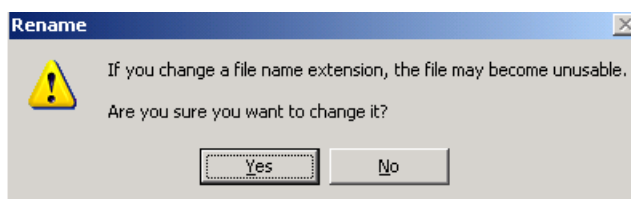
- vii. copy the content and paste it to text area in certificate creation web page
- viii. Under "Result Type" Choose "PKCS7"



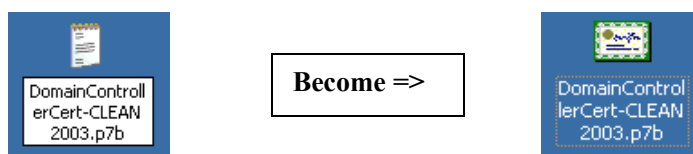
- ix. Click “OK”
- x. A page of code will be generated, starting by “-----BEGIN PKCS7-----” and ending by “-----END PKCS7-----”



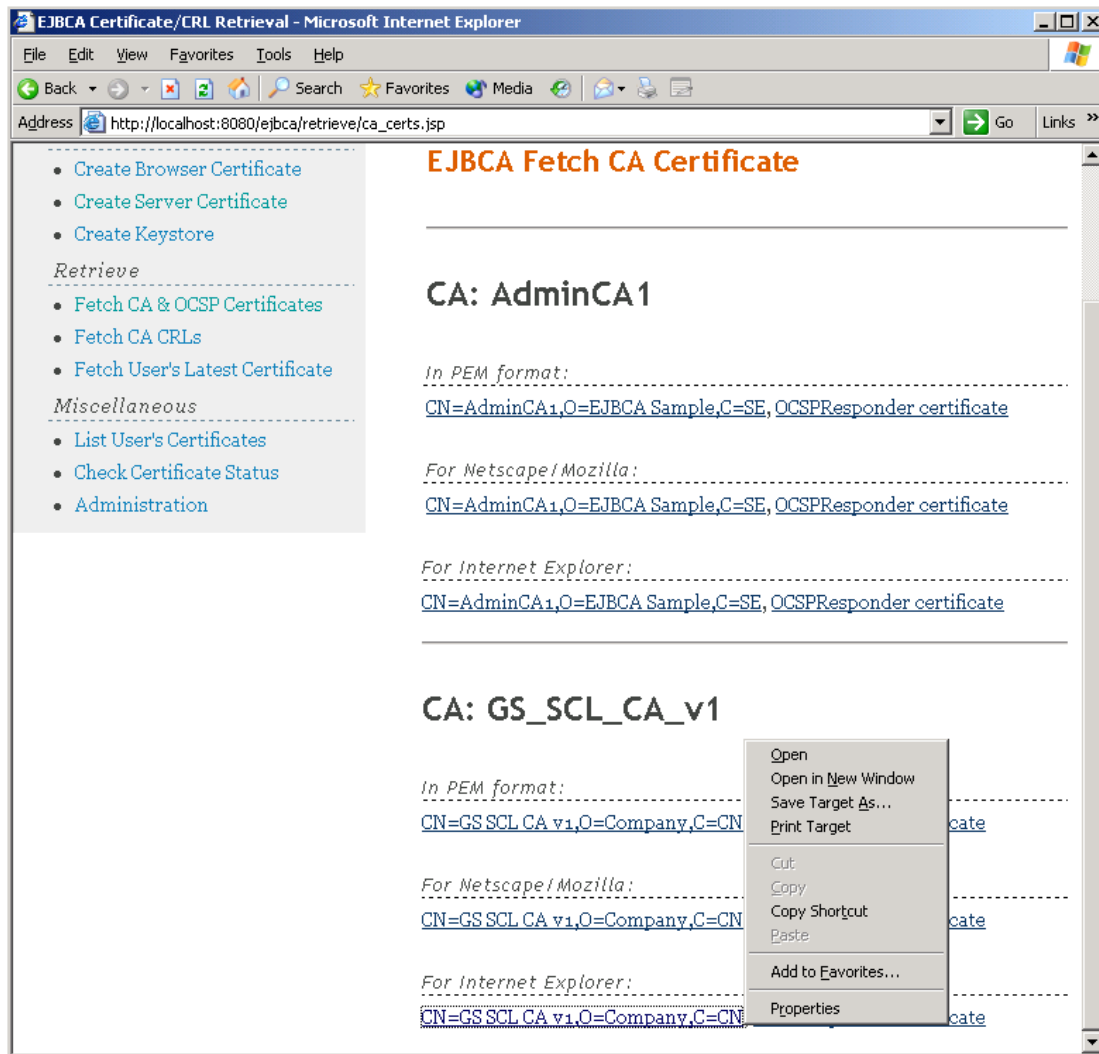
- xi. Copy it to a blank text file, save it, then rename the text file to “DomainControllerCert-CLEAN2003.p7b
- xii. Ignore the warning message



- xiii. Click “Yes”

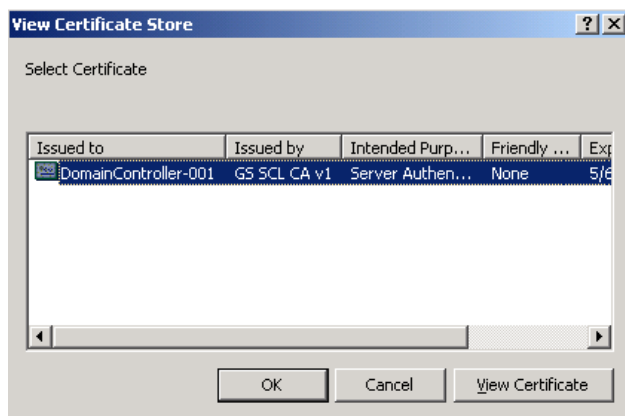


8. Fetch CA certificate
 - i. Go to EJBCA's Public Web Pages
 - ii. Click “Fetch CA & OCSP Certificates”

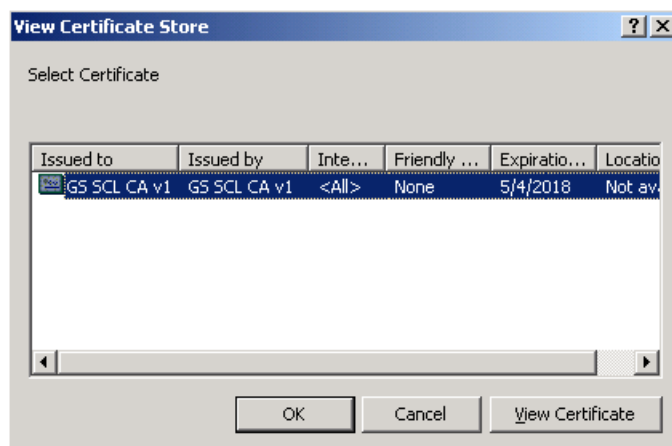


- iii. Under “CA: GS_SCL_CA_v1\For internet Explorer”, right click “CN=GS_SCL CA v1,O=Company,C=CN”\Save Target As...
 - iv. Save the certificate as “GS_SCL CA v1.cer” on desktop

9. Install and publish certificate on each Domain Controller
 - i. Double click the “2. InstallDomainControllerCert.vbs” on edesktop
 - ii. Click “OK”
 - iii. Select “DomainControllerCert-CLEAN2003.p7b” and click “Open”.
 - iv. Click “OK”



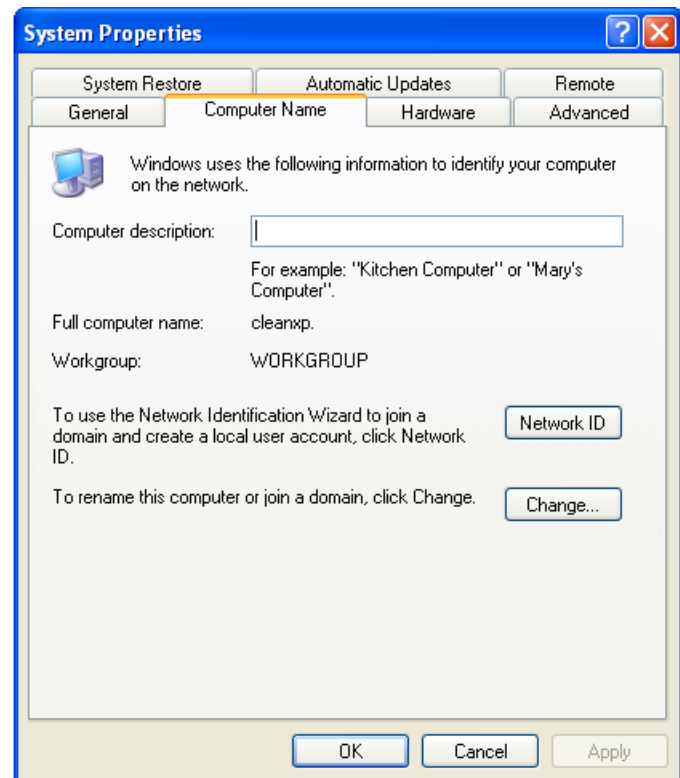
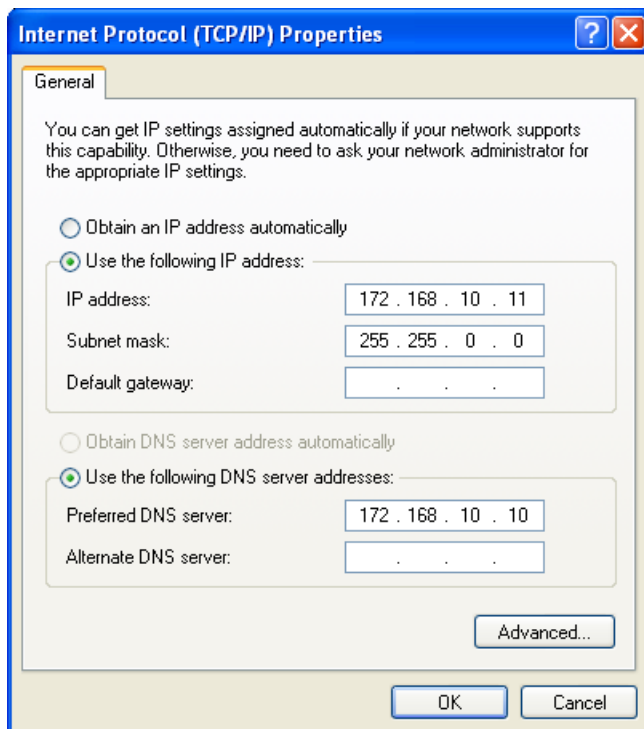
- v. Click “OK”
 - vi. A file “2. InstallDomainControllerCert.log” will be generated at desktop
10. Import the CA certificate to "Enterprise NTAAuth store"
 - i. Double click the “3. ImportCACertToNTAuthStore.vbs” on desktop
 - ii. Click “OK”
 - iii. Select “GS SCL CA v1.cer” and click “Open”
 - iv. Click “OK”
 - v. Click “OK”



4 -- Logon to Workstation

Initial workstation properties:

- Workstation OS: Windows XP Professional SP2
- Computer name: cleanxp
- IP address: 172.168.10.11
- Subnet mask: 255.255.0.0
- Preferred DNS server: 172.168.10.10
- Workgroup: WORKGROUP



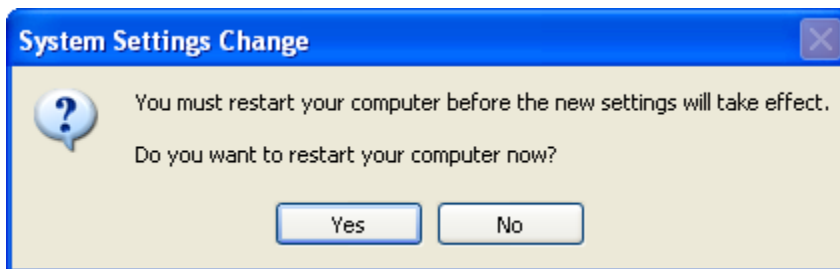
1. Add client into domain "testing.company.cn"
 - i. Right click "My Computer" \ Computer Name \ Change...



- ii. Select "Domain:"\input "testing.company.cn"
- iii. Click "OK"



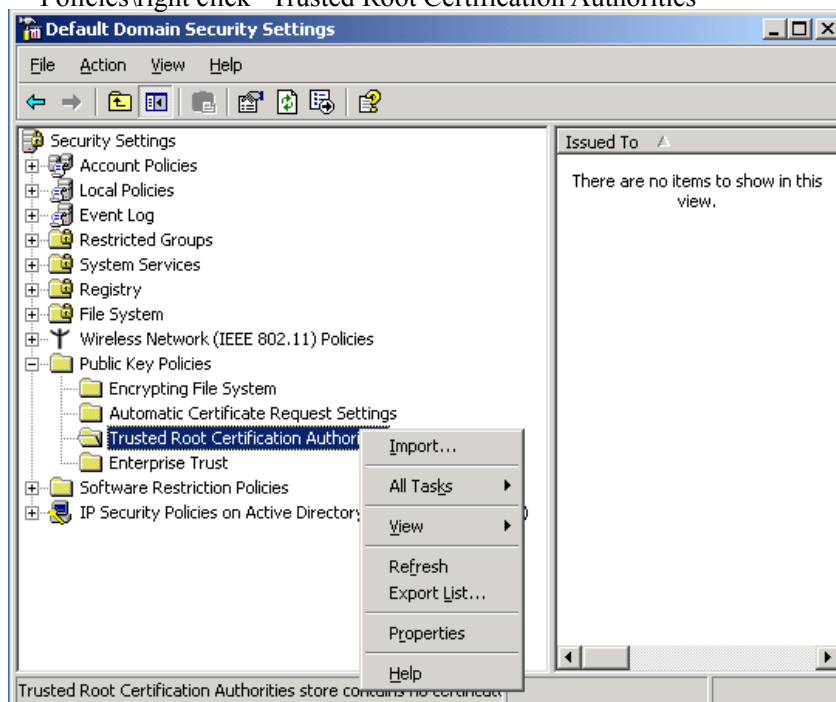
- iv. Input "administrator" as "User name:"
- v. Input the server's password as "Password"
- vi. Click "OK" 4 times



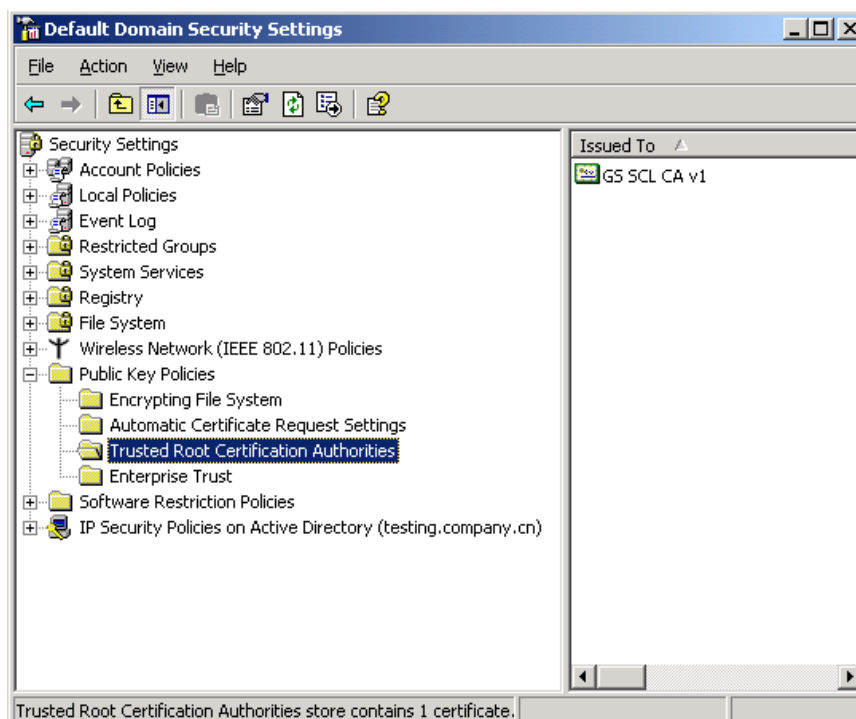
- vii. Click "Yes" to restart workstation

4.1 -- Add CA Certificate to Domain Security Policy

1. At Domain Controller, Start\Administrative Tools\Domain Security Policy\Public Key Policies\right click “Trusted Root Certification Authorities”

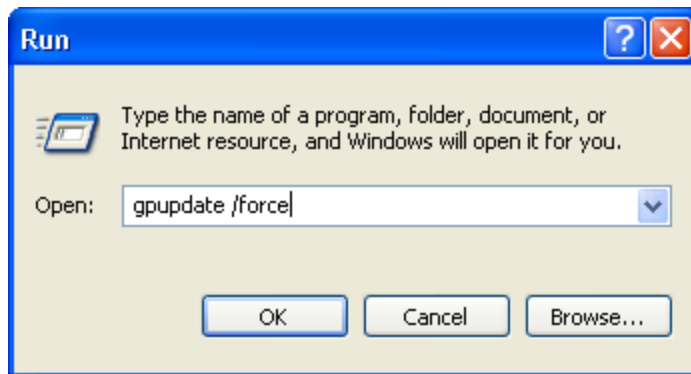


2. Choose “Import...”
3. Click “Next”
4. Browse to the “GS SCL CA v1.cer”
5. Click “Open”
6. Click “Next” 2 times
7. Click Finish
8. Click “OK”



4.2 -- Install Certificate on Workstation

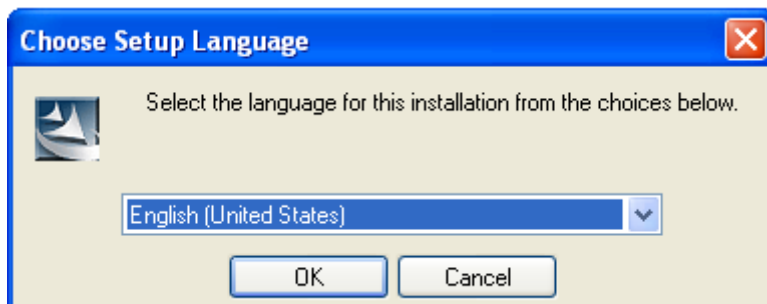
1. Logon workstation to domain “testing” using administrator account
2. Start\run...\
3. Input\ gpupdate /force (note that there is a space between “e” and “/”)



4. Click “OK”

4.3 -- Install GemSAFE Toolbox on Workstation

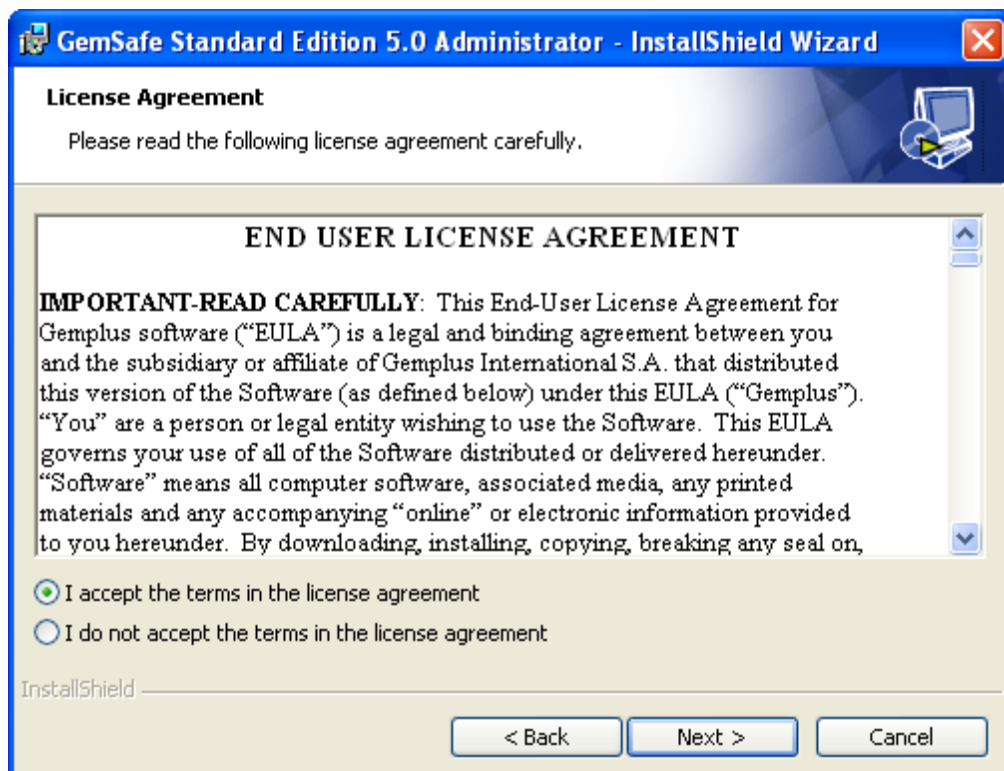
1. Run GemSAFE toolbox on Workstation



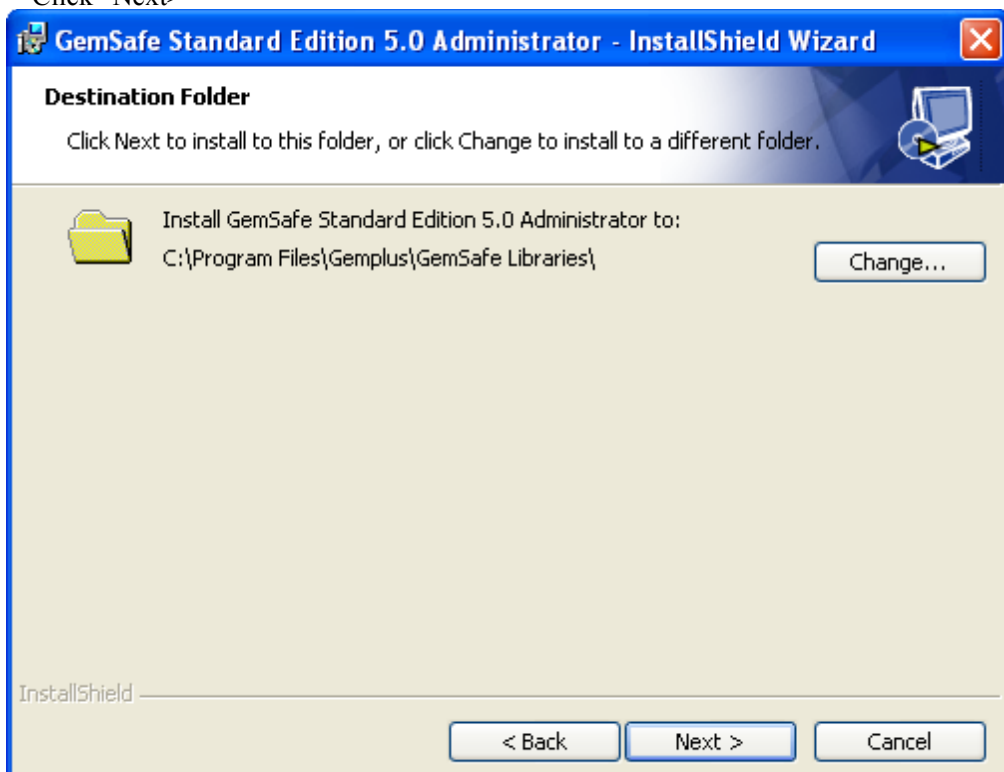
2. Click "OK"



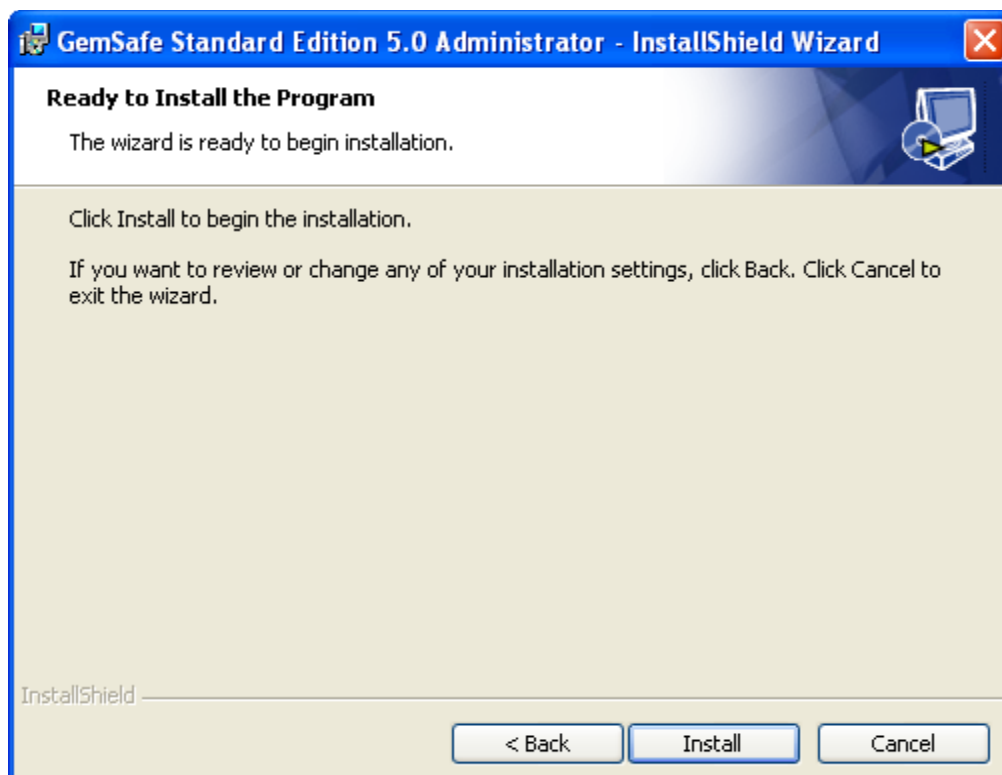
3. Click "Next>"



4. Choose "I accept the terms in the license agreement"
5. Click "Next>"



6. Click "Next>"



7. Click "Install"



8. Click "Finish":

4.4 -- Enroll Certificate to GemSAFE Smartcard

1. On work station, open Internet Explorer
2. Go to EJBCA's Public Web Pages, <http://testing.company.cn:8080/ejbca/>
3. plug in GemSAFE token
4. Click "Create Browser Certificate"
5. "Username:"= AdministratorGSSCL-001
6. "Password:"=foo123
7. Click "OK"
8. Another webpage will be shown
9. Under "Options", choose "Provider" as "Gemplus GemSAFE Card CSP"

Options

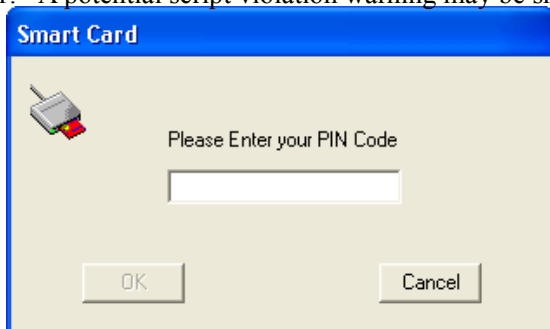
Provider:

Key size:

Certificate profile:

Add to enhanced eID card: ☐

10. Click "OK"
11. A potential script violation warning may be shown, Click "Yes"



12. Enter smart card's PIN
13. Click "OK"
14. A potential script violation warning may be shown, Click "Yes"



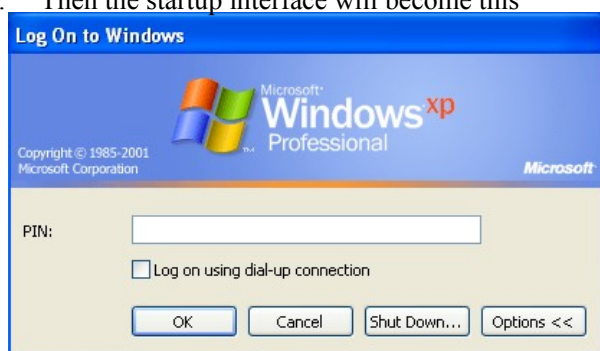
15. Click "OK"

4.5 -- Use Smart Card to Logon Workstation

1. Restart the server
2. Start JBoss service
3. Restart the client
4. When the workstation is started and the following screen is shown, plug in the token, which contains the certificate for workstation logon.



5. Then the startup interface will become this



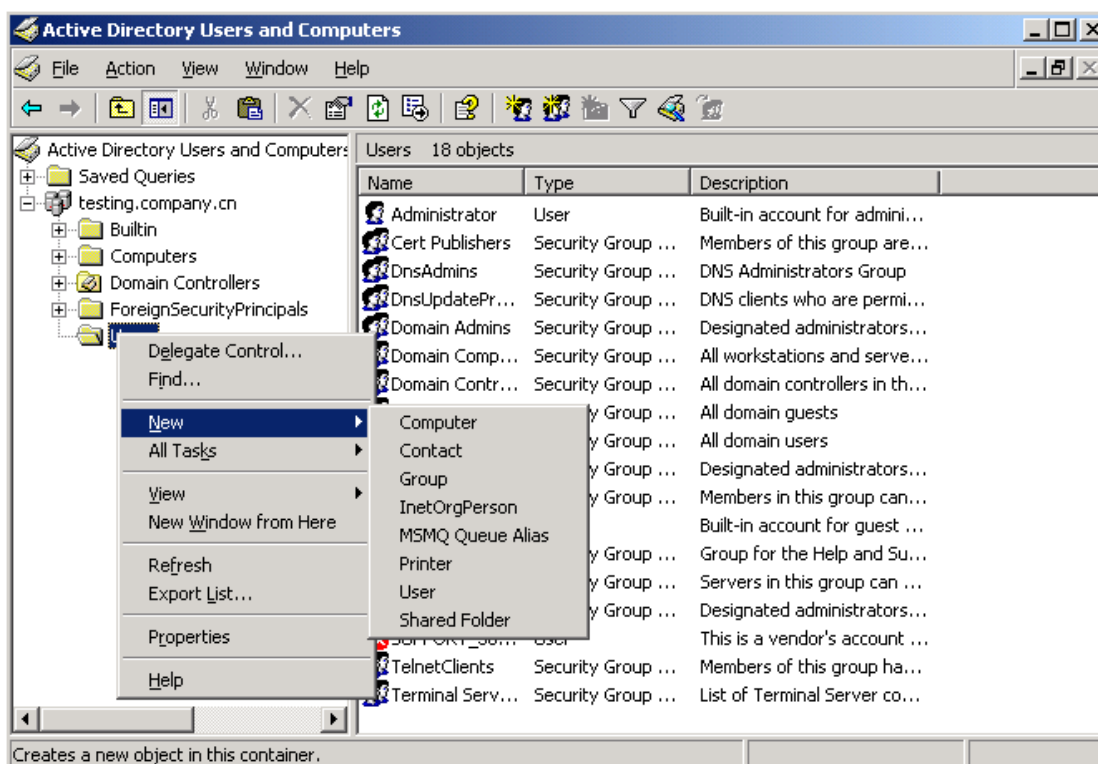
6. Enter the token's pin number and click "OK"
7. You will be logged on to the workstation under administrator account

5 -- Logon Workstation Using another Account

If you want to logon to other user account, you must know your account username, which is stored under domain controller's database

5.1 -- Create a New User Account

1. Go to domain controller\Start\Administrative Tools\Active Directory Users and Computers
2. Click to expand the node "testing.company.cn" right click "Users" \New\User



3. Input "First name" as "new"
4. Input "last name" as "user"
5. Input "User logon name" as "newuser"

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'testing.company.cn/Users'. The 'First name' field contains 'new', the 'Last name' field contains 'user', and the 'Full name' field contains 'new user'. The 'User logon name' field contains 'newuser' and the domain dropdown is set to '@testing.company.cn'. The 'User logon name (pre-Windows 2000)' field contains 'TESTING\' and 'newuser'.

Create in: testing.company.cn/Users

First name: new Initials:

Last name: user

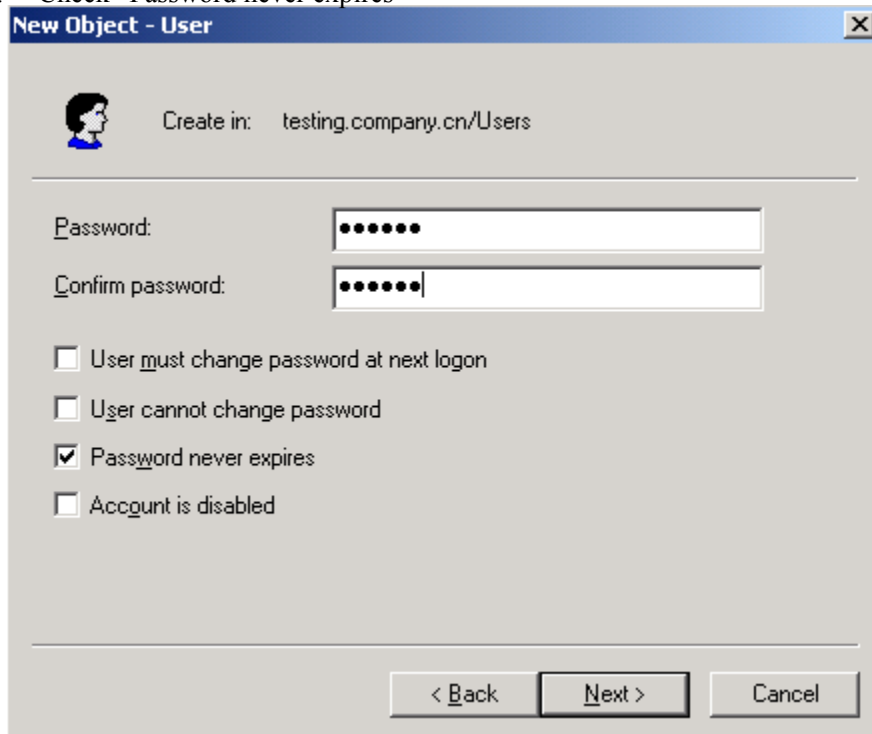
Full name: new user

User logon name: newuser @testing.company.cn

User logon name (pre-Windows 2000): TESTING\ newuser

< Back Next > Cancel

6. Click "Next>"
7. Input both "Password" and "Confirm password" as "foo123@"
8. Check "Password never expires"



New Object - User

Create in: testing.company.cn/Users

Password: [foo123@]

Confirm password: [foo123@]

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

9. Click "Next>"
10. Click "Finish"

5.2 -- Add End Entity for New User

1. Go to EJBCA Administration GUI
2. Click “Add End Entity”
3. Under “End Entity Profile” choose “GS SmartCardLogon”
4. User Name= “newuser
5. Password=“foo123”
6. Confirm Password=“foo123”
7. CN, Common Name= “newuser”
8. MS UPN, User Principal Name=“newuser@ testing.company.cn”

End Entity Profile	GSSmartCardLogon ▼
Username	newuser
Password	••••••
Confirm Password	••••••
Subject DN Fields	
CN, Common Name	newuser
Subject Alternative Name Fields	
MS UPN, User Principal Name	newuser @ testing.company.cn
Certificate Profile	GSSmartCardLogon ▼
CA	GS_SCL_CA_v1 ▼
Token	User Generated ▼
<input type="button" value="Add End Entity"/> <input type="button" value="Reset"/>	

9. Leave all other setting by default, click “Add End Entity”

5.3 -- Enroll New User's Certificate to Token

1. Go to workstation\open internet explorer\go to EJBCA public GUI\Create Browser Certificate\
2. Input "User Name" as "newuser", "Password" as "foo123"

Authentication

Username:

Password:

3. Click "OK"
4. Another webpage will be shown
5. plug in GemSAFE token
6. Under "Options", choose "Provider" as "Gemplus GemSAFE Card CSP"

Options

Provider:

Key size:

Certificate profile:

Add to enhanced eID card: ☐

7. Click "OK"
8. A potential script violation warning may be shown, Click "Yes"
9. Enter smart card's PIN
10. Click "OK"
11. A potential script violation warning may be shown, Click "Yes"
12. Click "OK"
13. Log off workstation (no need to restart workstation and server)
14. Now you can logon the "newuser" account using the token with new enrolled certificate