

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

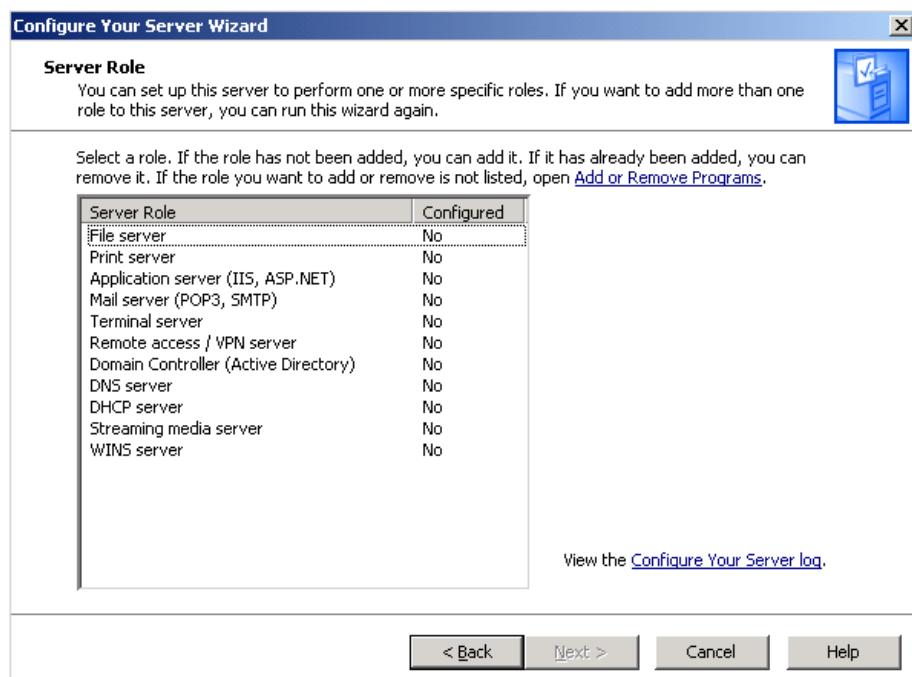
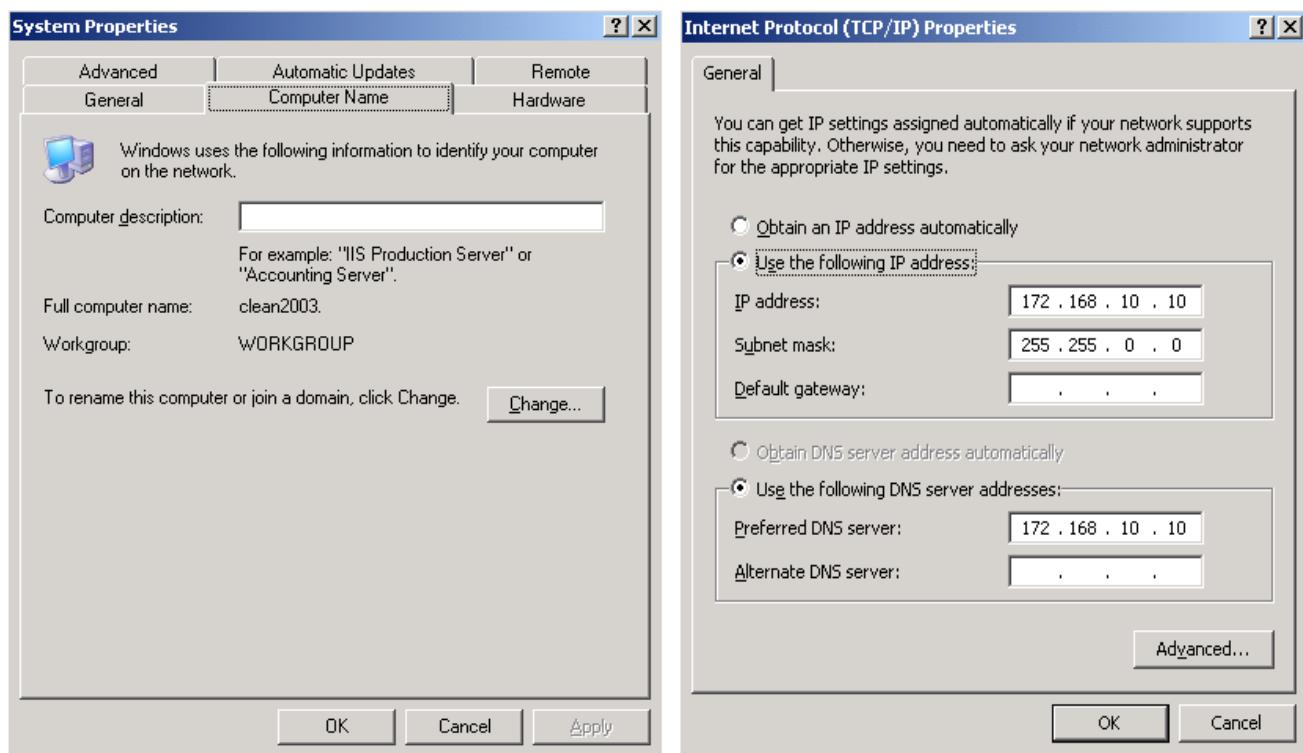
Table of Content

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

- Start\Manage Your Server\Add or remove a role\click “Next”

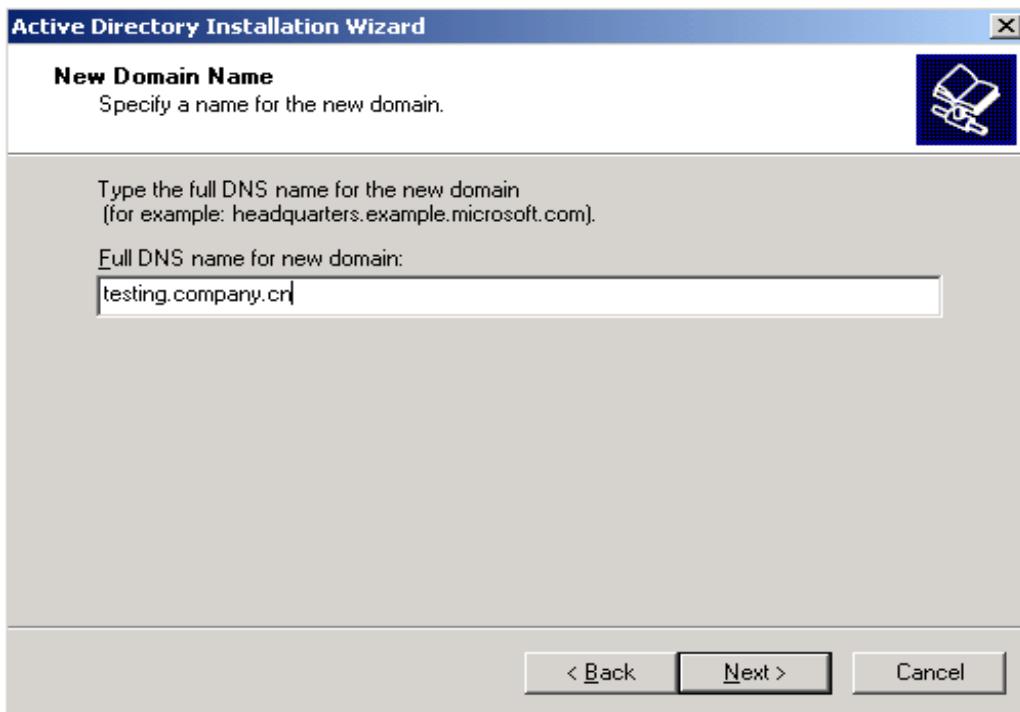
The screenshot shows the 'Manage Your Server' interface with the title 'Manage Your Server' and 'Server: CLEAN2003'. On the left, there's a sidebar with icons for server management. The main content area has a heading 'Adding Roles to Your Server' with a sub-section about adding roles for specific tasks like file sharing. Below it is another section titled 'Managing Your Server Roles' with a note about returning to this page for administrative tasks. A message indicates no roles have been added yet. On the right, there are two panels: 'Tools and Updates' listing links like Administrative Tools, More Tools, Windows Update, etc., and 'See Also' listing links such as Help and Support, Microsoft TechNet, Deployment and Resource Kits, etc. At the bottom left is a checkbox for 'Don't display this page at logon'.

- Choose “Domain Controller (Active Directory)”

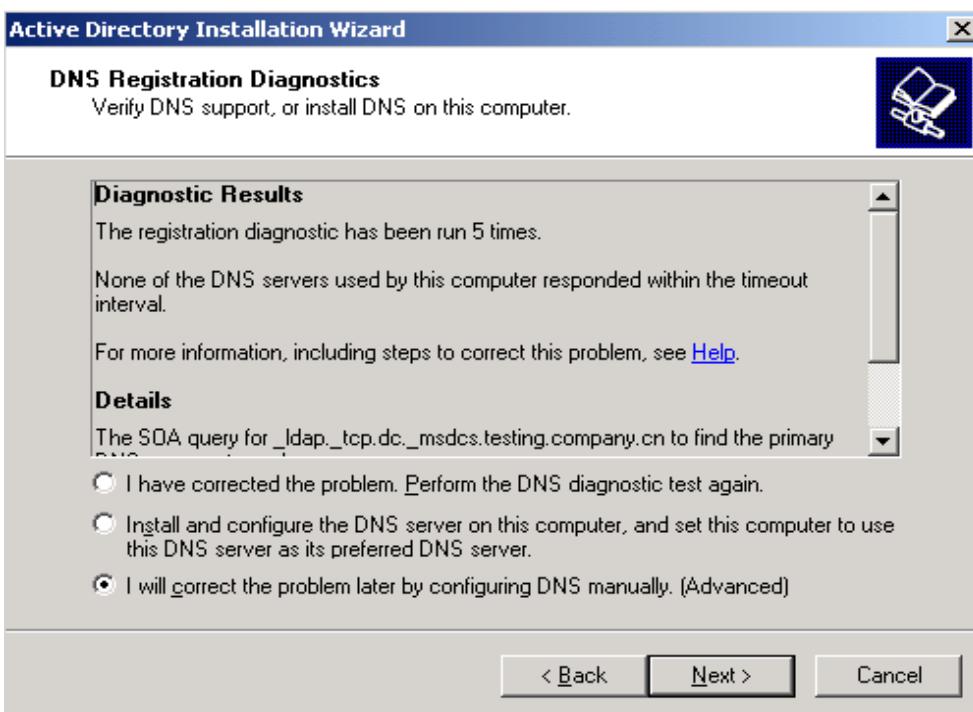
The screenshot shows the 'Configure Your Server Wizard' with the title 'Configure Your Server Wizard'. The current step is 'Server Role'. It includes a note that you can set up the server for one or more roles. The main area shows a table of server roles with a column for 'Configured' status. The 'Domain Controller (Active Directory)' role is selected and highlighted. To the right, there's a detailed description of what domain controllers do, a link to 'Read about domain controllers', and a link to view the 'Configure Your Server log'. At the bottom are navigation buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Server Role	Configured
File server	No
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	No
DNS server	No
DHCP server	No
Streaming media server	No
WINS server	No

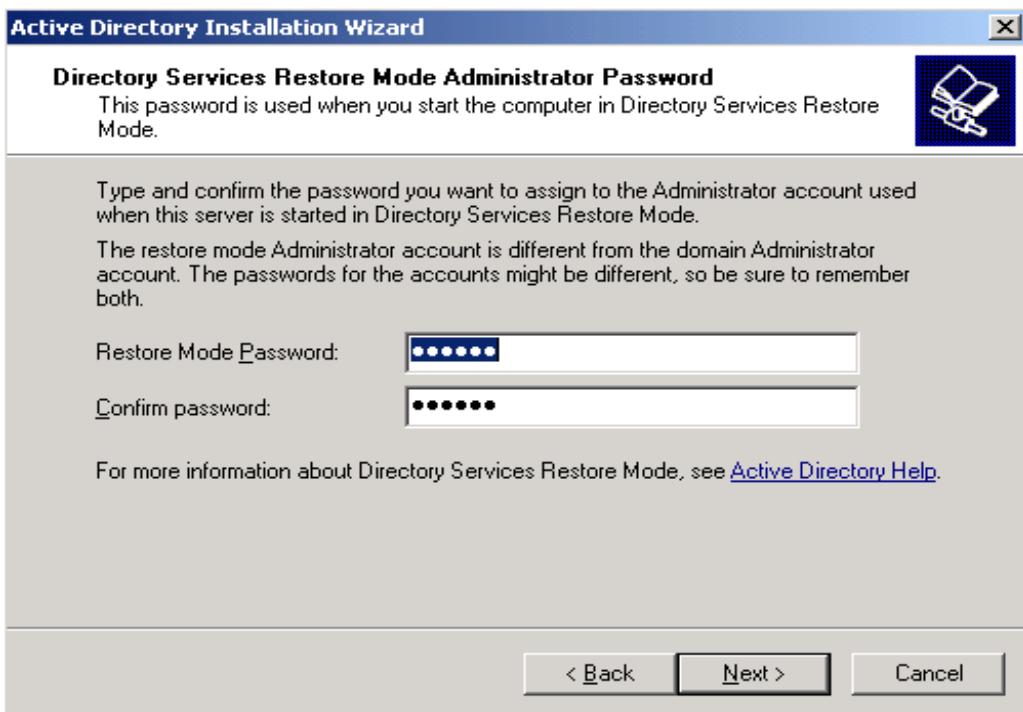
3. Click “Next” 6 times
4. At “Full DNS name for new domain:” input “testing.company.cn”



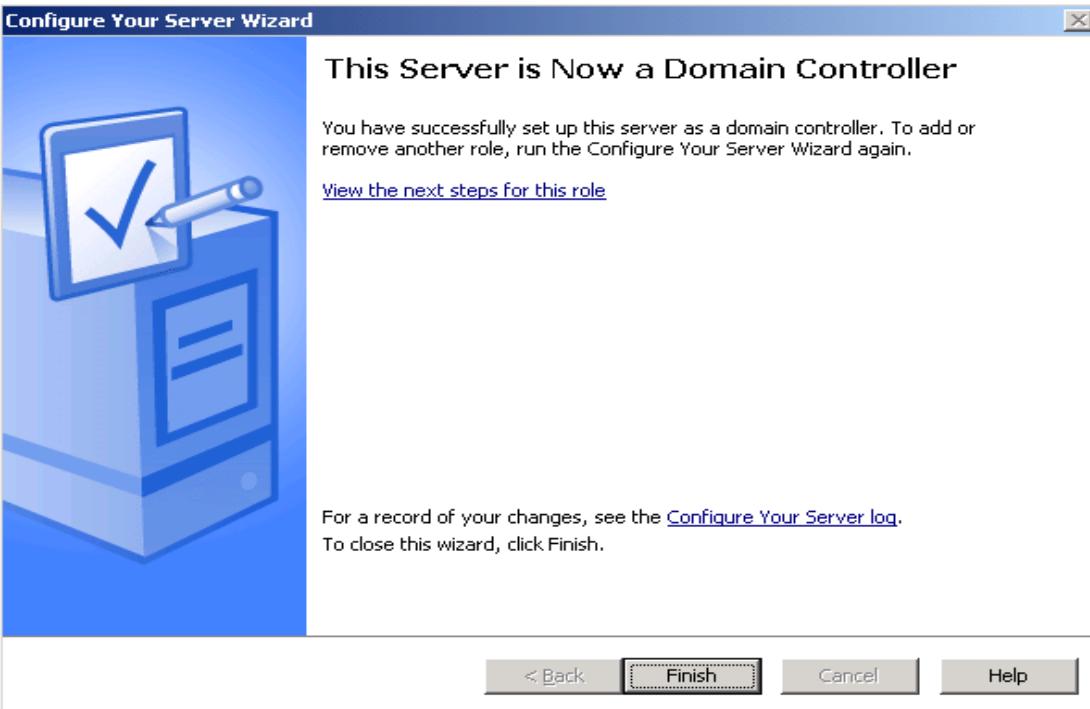
5. Click “Next” 4 times



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”



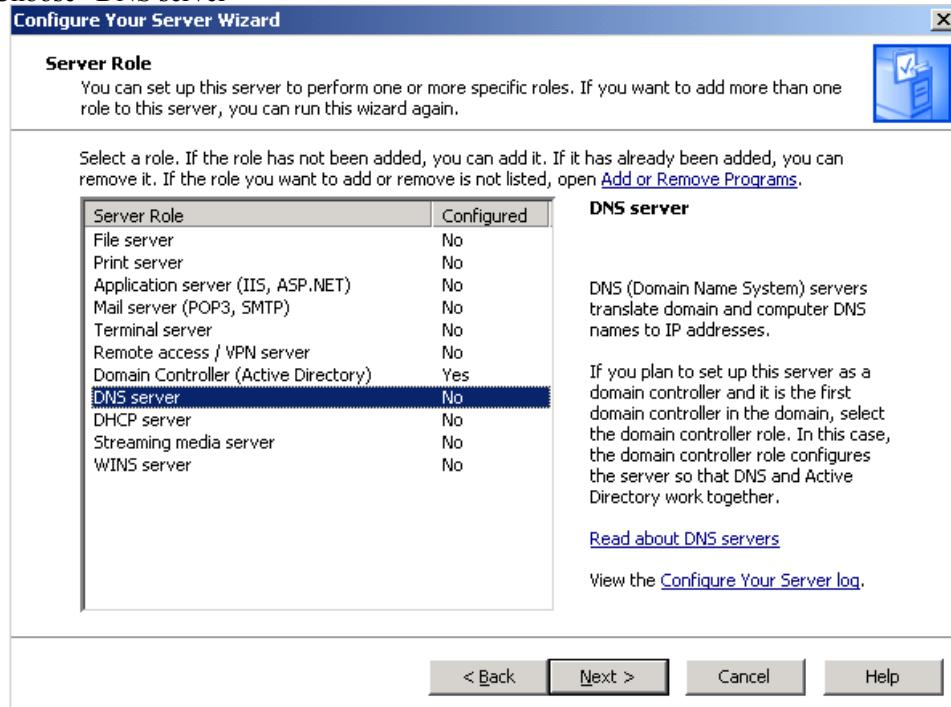
10. Click "Next" 2 times
11. Click "Finish"
12. Click "Restart Now"



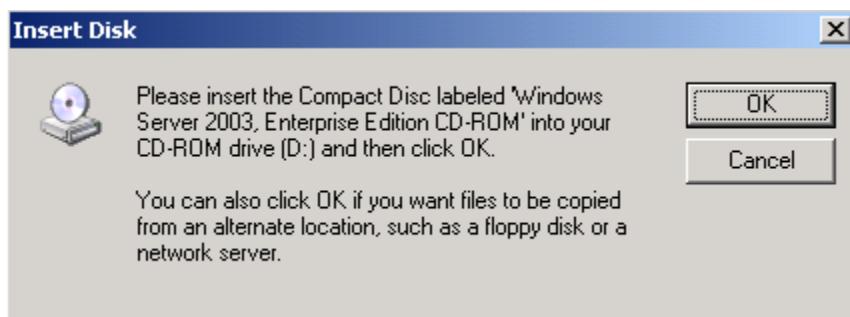
13. When the computer is restarted click "Finish"

1.2 -- Create a DNS Server

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



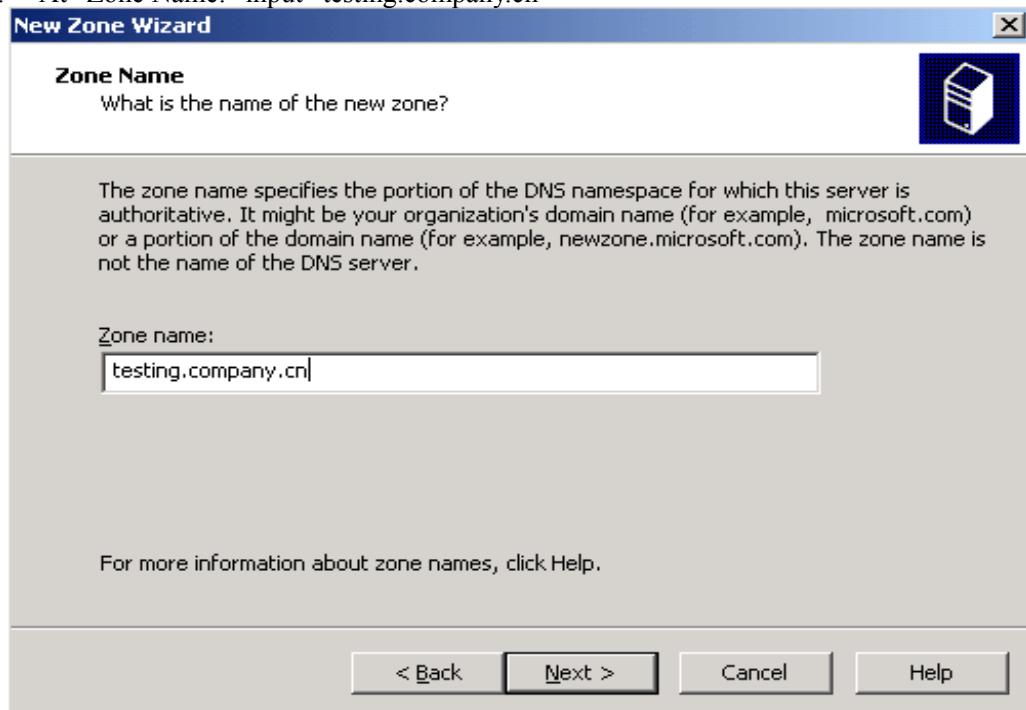
3. Click “Next” 2 times



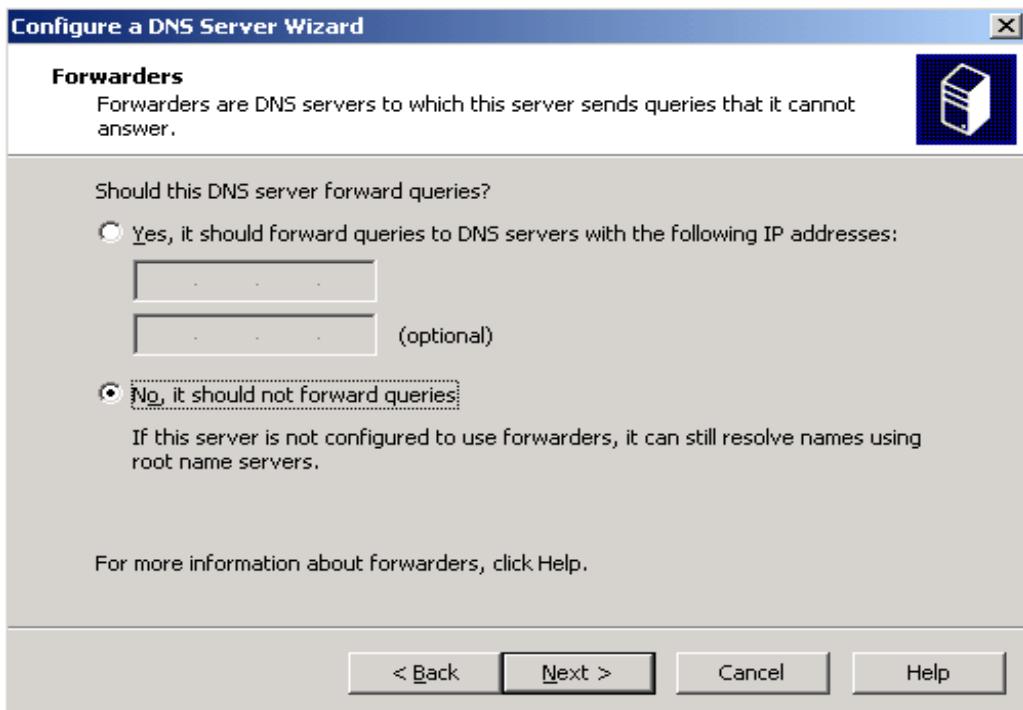
4. Click “OK”
5. Browse to Windows Server 2003 Enterprise CD/ENGLISH/WIN2003_VLP/ENT/I386/DNSMGR.DL_
6. Click “Open”



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"



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



14. Click "Finish"

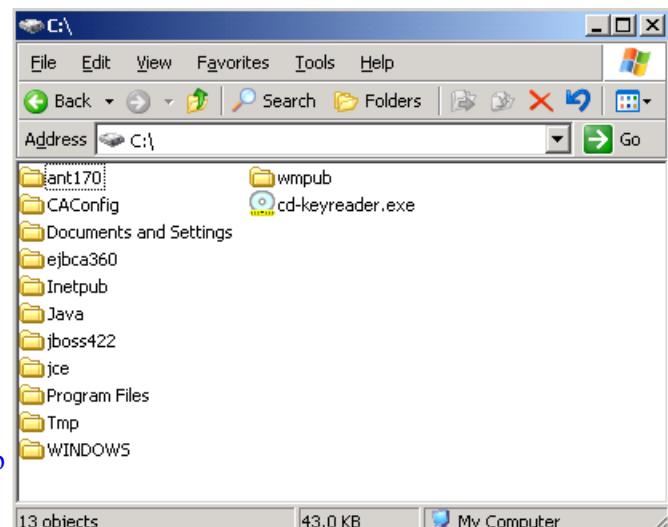
2 -- Install EJBCA Components

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

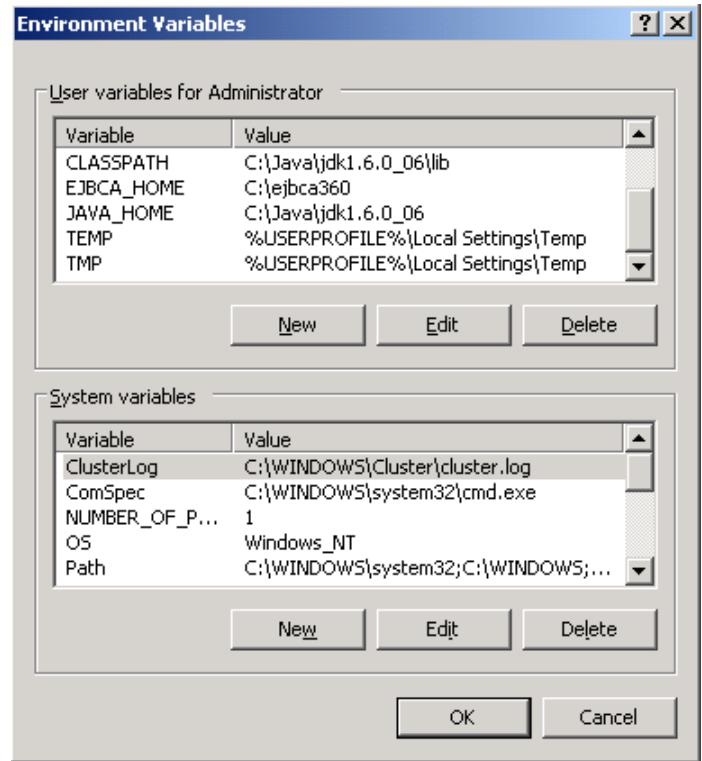
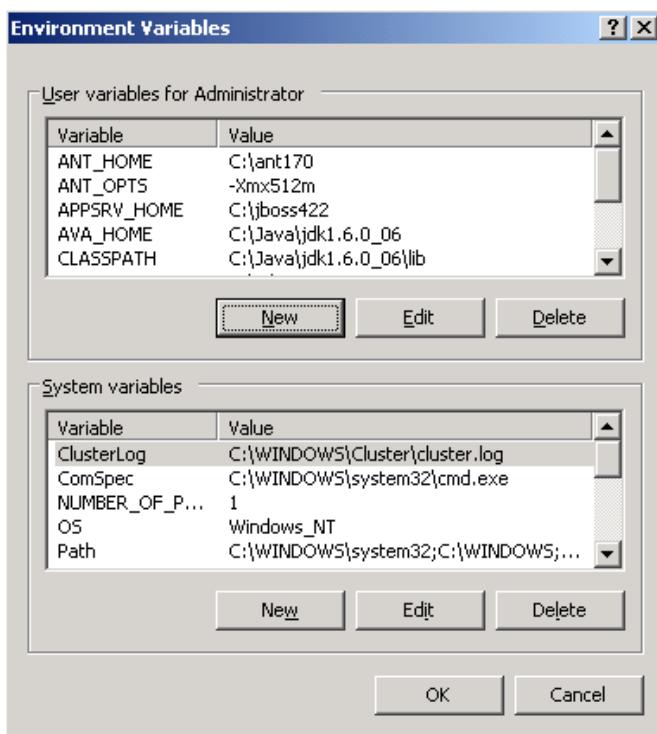


Overwrite	using
C:\Java\jre1.6.0_06\lib\security\local_policy.jar	C:\jce\local_policy.jar
C:\Java\jdk1.6.0_06\jre\lib\security\local_policy.jar	C:\jce\local_policy.jar
C:\Java\jre1.6.0_06\lib\security\US_export_policy.jar	C:\jce\US_export_policy.jar
C:\Java\jdk1.6.0_06\jre\lib\security\US_export_policy.jar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

3. Add user variables

- Right click "My Computer"\Properties\Advanced\Environment Variables\User variable for Administrator\New
- Add user variable one by one

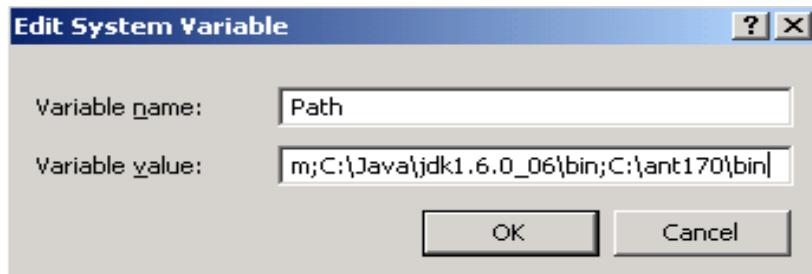
User variables	value
ANT_HOME	C:\ant170
ANT_OPTS	-Xmx512m
APPSRV_HOME	C:\jboss422
CLASSPATH	C:\Java\jdk1.6.0_06\lib
EJBCA_HOME	C:\ejbcas360
JAVA_HOME	C:\Java\jdk1.6.0_06



4. Edit system variable "Path"

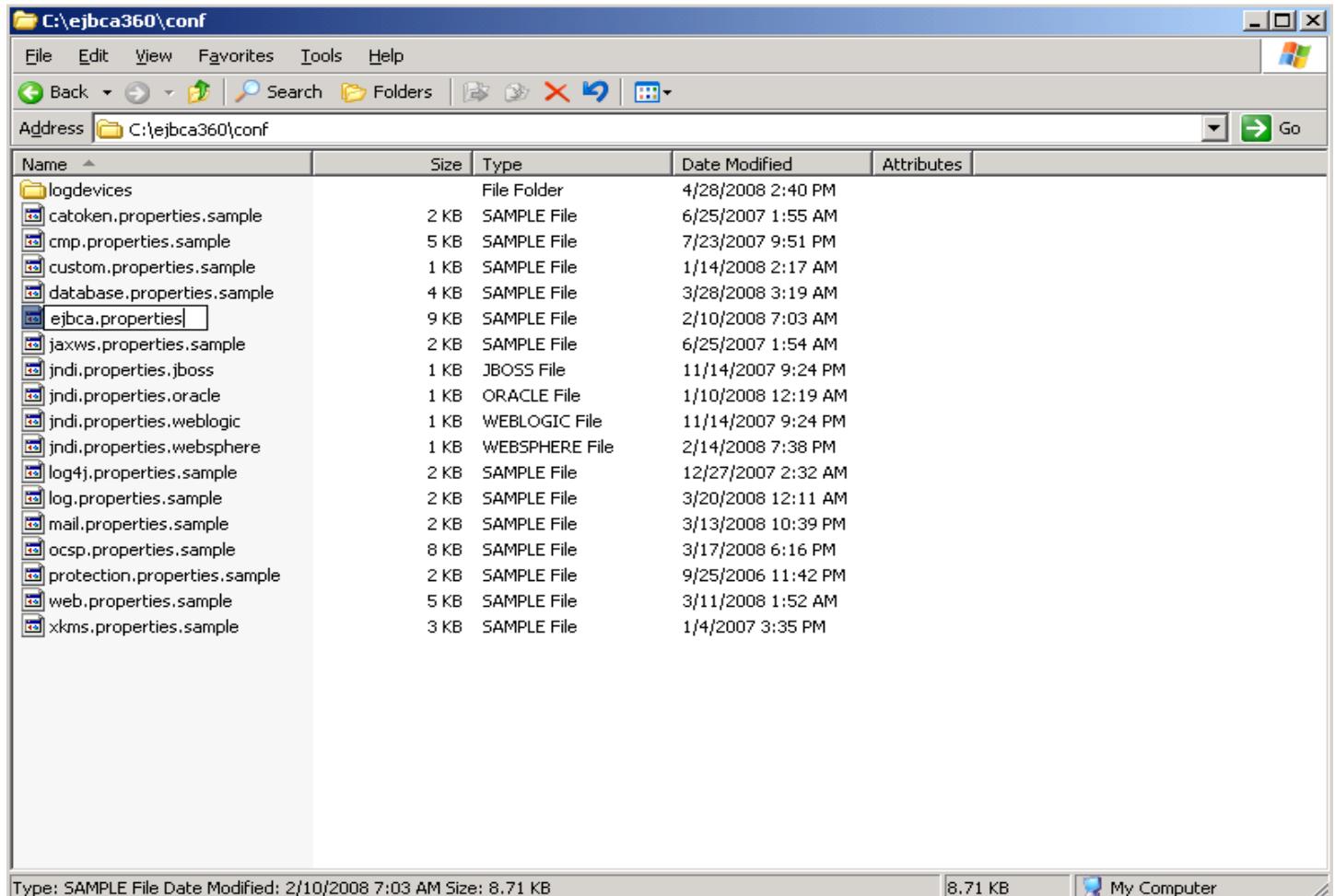
- Choose "Path"\Click "Edit"
- Add ":" at the end of the value
- Add the new directory to the value

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 ejbc3 directory, type “cd\”\enter\cd ejbc360\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 ejbc360
C:\ejbc360>ant bootstrap
```

```
C:\ Command Prompt
buildwithcmptcpservice:
deploy:
[echo] Merging available external modifications from C:\ejbc360\ejbc360-custom.
[copy] Warning: C:\ejbc360\ejbc360-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

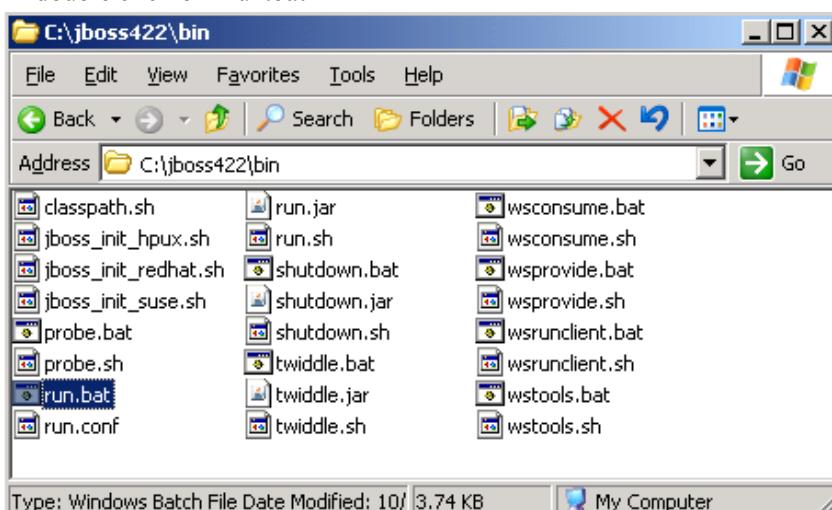
j2ee:web-configure:

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:\ejbc360>
```

4. If build successfully in previous step, start JBoss service by going to “C:\jboss422\bin” and double click on “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: WSSERLET12: 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 processWsdlLocation
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: WSSERLET14: 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: SVNTag=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

```

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

```

[input] Please enter the server dn <default: CN=localhost,O=EJBCA Sample,C=SE> ?
[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.keytype        : soft
[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] httpsserver.hostname : localhost
[echo] httpsserver.dn   : CN=localhost,O=EJBCA Sample,C=SE
[echo] httpsserver.password : serverpwd
[echo] superadmin.password : ejbca
[echo] superadmin.batch  : true
[echo] java.trustpassword : changeit
[echo] appserver.home    : C:\jboss422

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'
[exec] 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=.../deplo
y/http-invoker.sar/invoker.war/
12:07:37,593 INFO [TomcatDeployer] undeploy, ctxPath=/jbossws, warUrl=.../deplo
y/jbossws.sar/jbossws-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

```

```

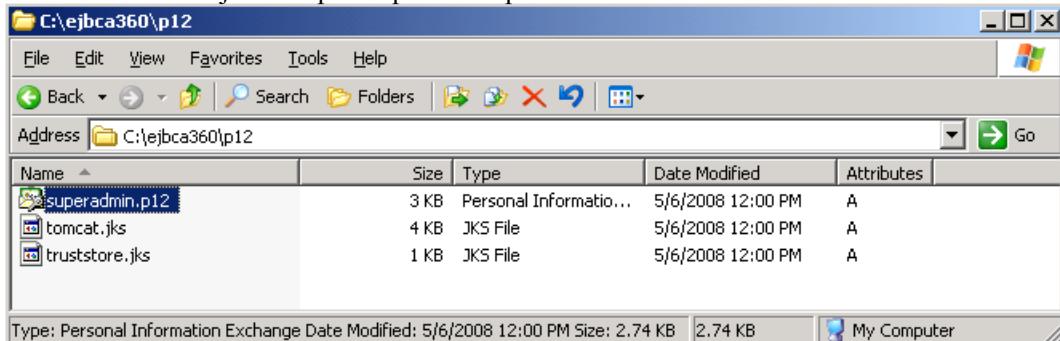
C:\ Command Prompt
j2ee:configure:
j2ee:deployBase:
[copy] Copying 2 files to C:\jboss422\server\default\deploy
[copy] Copying 1 file to C:\jboss422\server\default\deploy
j2ee:deploy:

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\



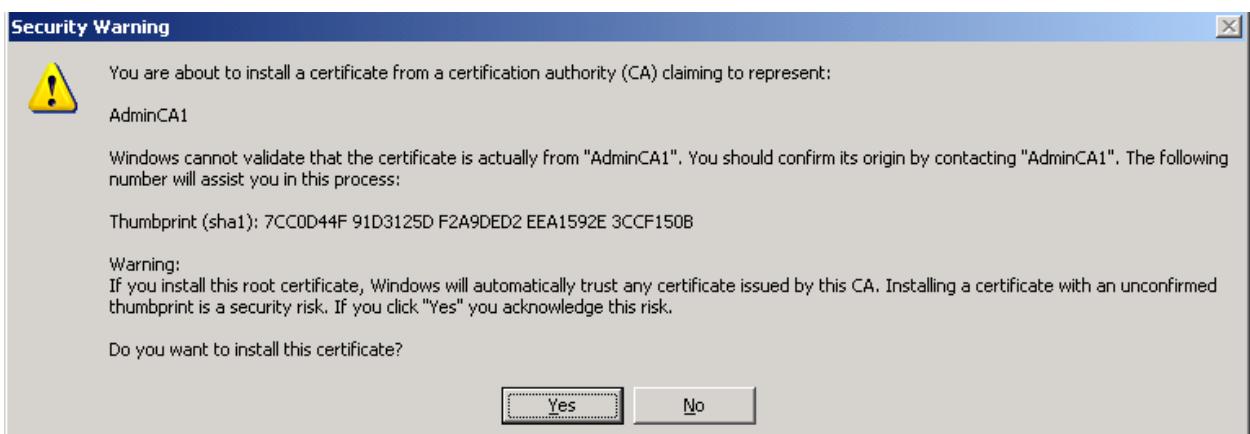
- ii. Click "Next" 2 times



- 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.

Welcome to the public EJBCA pages

Enroll

- Create Browser Certificate
- Create Server Certificate
- Create Keystore

Retrieve

- Fetch CA & OCSP Certificates
- Fetch CA CRLs
- Fetch User's Latest Certificate

Miscellaneous

- List User's Certificates
- Check Certificate Status
- Administration

EJBCA Administration

Welcome SuperAdmin to EJBCA Administration.

CA Functions

- [Basic Functions](#)
- [Edit Certificate Profiles](#)
- [Edit Publishers](#)
- [Edit Certificate Authorities](#)

RA Functions

- [Edit User Data Sources](#)
- [Edit End Entity Profiles](#)
- [Add End Entity](#)
- [List/Edit End Entities](#)

Supervision Functions

- [Approve Actions](#)
- [View Log](#)
- [Log Configuration](#)
- [Reports](#)

System Functions

- [System Configuration](#)
- [Edit Services](#)
- [Edit Administrator Privileges](#)

EJBCA is a fully functional Certificate Authority. Based on J2EE technology it constitutes a robust, high performance and component based CA. Both flexible and platform independent, EJBCA can be used standalone or integrated in any J2EE application.

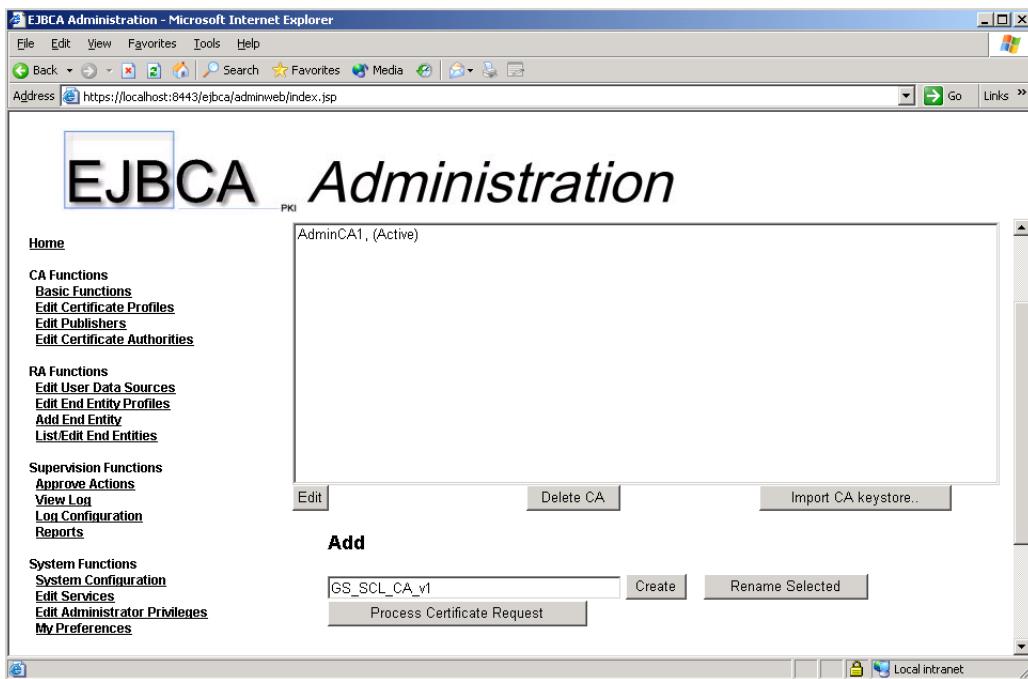
Written exclusively in Java, EJBCA can be run on any platform where a J2EE server is used and it has been tested on Linux and Windows platforms.

Made by PrimeKey Solutions AB, 2002-2008.

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

Authentication
Code

(leave empty for
system default)

Enable auto-
activation of CA
token

Signing Algorithm

RSA key size

ECDSA key spec

Subject DN

Signed By

Certificate Profile

Validity (Days)

Description

Use Subject Alternative Name

Policy Id
Leave policy id blank to use default certificate profile values.

Use UTF8 in policy text

Use PrintableString encoding in DN

Use LDAP DN
order
(experimental to
switch off)

CRL Specific
Data

Use Authority
Key Id
Authority Key Id
Critical

Use CRL
Number
CRL Number
Critical

Use CRL
Distribution
Point on CRLs
CRL Distribution
Point on CRLs
Critical

CRL Expire
Period (h)

CRL Issue
Interval (h)

CRL Overlap
Time (min)

Delta CRL
Period (h)
(0 if no delta
CRLs are
issued)

CRL Publishers

Default CRL
Dist. Point
(Used as default
value in
certificateprofiles
using this CA.)
<http://clean2003.testing.company.cn:8080/ejbca/publicweb/webdist/certdist?cmd=crl8>

Default CRL
Issuer

CA Defined
FreshestCRL
extension
(Used as default
value in
certificateprofiles
using this CA.)

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

Finish User

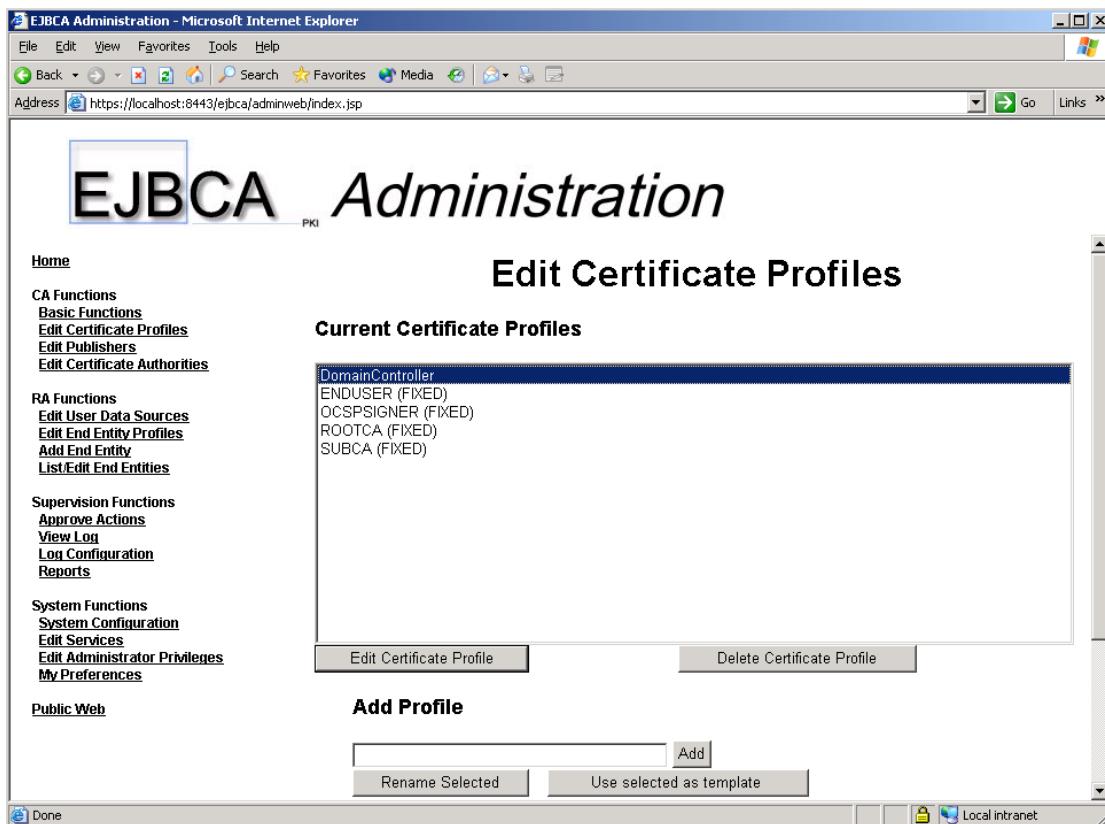
Create Cancel

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 checked="" 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"/>
Use CRL Distribution Point	<input checked="" 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 checked="" 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 checked="" type="checkbox"/>
OCSP Service Locator URI	<input type="text"/>
Add	<input type="button" value="Add"/>
CA issuer URI	<input type="text"/>
Use Certificate Policies	<input type="checkbox"/>
Certificate Policies Critical	<input checked="" type="checkbox"/>

<input type="button" value="Add"/>	Certificate Policy Id <input type="text"/> User Notice Text <input type="text"/> CPS <input type="text"/>
Use Qualified Certificate Statement <input type="checkbox"/>	
Qualified Certificate Statement <input checked="" type="checkbox"/> Critical	
Use PKIX QCSyntax-v2 <input checked="" type="checkbox"/>	
Semantics Id <input type="text"/>	
RA Name <input type="text"/>	
Use ETSI QC Compliance <input checked="" type="checkbox"/>	
Use ETSI Secure Signature <input checked="" type="checkbox"/> Creation Device	
Use ETSI transaction value limit <input checked="" 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 checked="" type="checkbox"/>	
Retention Period (in years) <input type="text"/>	
Use Custom QC-statement String <input checked="" type="checkbox"/>	
Custom QC-statement OID <input type="text"/>	
Custom QC-statement Text <input type="text"/>	
<div style="border: 1px solid black; padding: 5px; display: inline-block;"> Digital Signature Non-repudiation Key encipherment Data encipherment Key agreement Key certificate sign CRL sign Encipher only Decipher only </div>	
Key usage <input type="checkbox"/>	
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

Any Extended Key Usage
Server Authentication
Client Authentication
Code Signing
Email Protection
Time Stamping
MS Smart Card Logon
OCSigner
MS Encrypted File System
MS EFS Recovery
Internet Key Exchange for IPsec
SCVP Server Certificate Validation
SCVP Request Authentication

Use MS Template Value

Microsoft Template Value
(Only the value not the actual template)

Use CN Postfix

CN Postfix
Text appended after first CN field

Use a Subset of Subject DN

Subset of SubjectDN

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

Use a Subset of Subject Alt. Name

Subset of Subject Alt. Name

Other Name
RFC822 Name (email address)
DNS Name
IP Address
X400 Address
DirectoryName, Distinguished Name (DN)

Available bit lengths

0 Bits
192 Bits
239 Bits
256 Bits
384 Bits

Available CAs

Any CA
AdminCA1
GS_SCL_CA_v1

Publishers

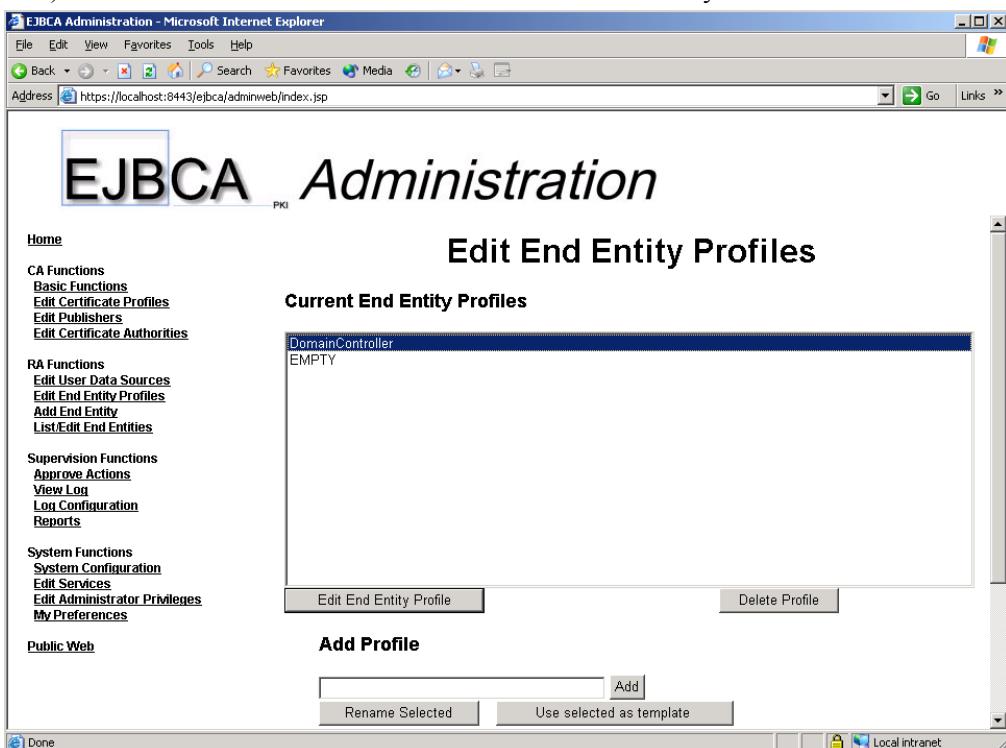
--

Type

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](#)

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

days:hours:minutes)

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

Notification Message

Printing of user data Use Default Required

Printer Name

Printed Copies

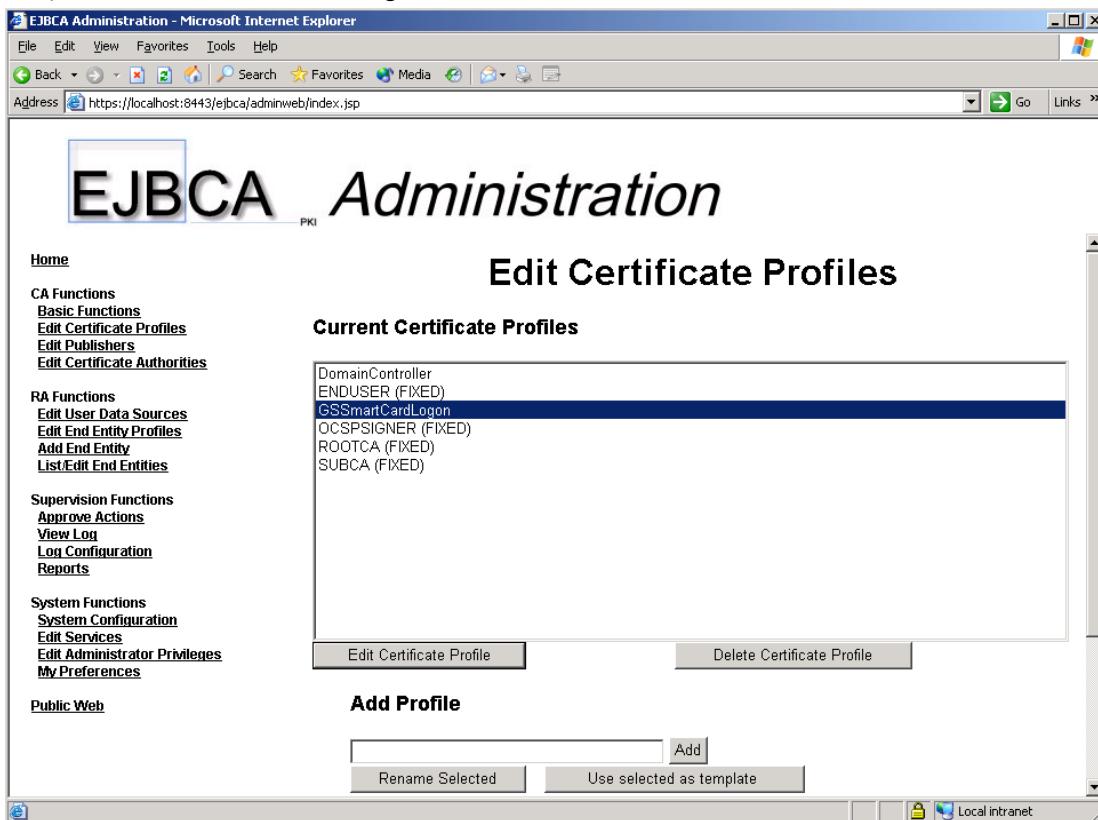
Current Template No Printing template is uploaded.

Upload Template

Made by PrimeKey Solutions AB, 2002-2008.

3.4 -- 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 checked="" 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"/>
Use CRL Distribution Point	<input checked="" 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 checked="" 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 checked="" type="checkbox"/>
OCSP Service Locator URI	<input type="text"/>
Add	<input type="button" value="CA issuer URI"/>
CA issuer URI	<input type="text"/>
Use Certificate Policies	<input type="checkbox"/>
Certificate Policies Critical	<input checked="" type="checkbox"/>

<input type="button" value="Add"/>	Certificate Policy Id <input type="text"/> User Notice Text <input type="text"/> CPS <input type="text"/>
Use Qualified Certificate Statement <input type="checkbox"/>	
Qualified Certificate Statement <input checked="" type="checkbox"/> Critical	
Use PKIX QCSyntax-v2 <input checked="" type="checkbox"/>	
Semantics Id <input type="text"/>	
RA Name <input type="text"/>	
Use ETSI QC Compliance <input checked="" type="checkbox"/>	
Use ETSI Secure Signature <input checked="" type="checkbox"/> Creation Device	
Use ETSI transaction value limit <input checked="" 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 checked="" type="checkbox"/>	
Retention Period (in years) <input type="text"/>	
Use Custom QC-statement String <input checked="" type="checkbox"/>	
Custom QC-statement OID <input type="text"/>	
Custom QC-statement Text <input type="text"/>	
<div style="border: 1px solid black; padding: 5px; display: inline-block;"> Digital Signature Non-repudiation Key encipherment Data encipherment Key agreement Key certificate sign CRL sign Encipher only Decipher only </div>	
Key usage <input checked="" type="checkbox"/>	
Allow Key Usage Override <input checked="" type="checkbox"/>	
Use Extended Key Usage <input checked="" type="checkbox"/> Extended Key Usage Critical <input type="checkbox"/>	

<p>Extended Key Usage</p> <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;"> 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>	<p>Use MS Template Value <input type="checkbox"/></p> <p>Microsoft Template Value (Only the value not the actual template) <input type="text" value="DomainController"/></p> <p>Use CN Postfix <input type="checkbox"/></p> <p>CN Postfix <input type="text"/></p> <p>Text appended after first CN field</p>
<p>Use a Subset of Subject DN <input type="checkbox"/></p> <p>Subset of SubjectDN</p> <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;"> 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>	
<p>Use a Subset of Subject Alt. Name <input type="checkbox"/></p> <p>Subset of Subject Alt. Name</p> <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;"> Other Name RFC822 Name (email address) DNS Name IP Address X400 Address DirectoryName, Distinguished Name (DN) </div>	
<p>Available bit lengths</p> <div style="border: 1px solid black; padding: 5px; background-color: #f0f0f0;"> 0 Bits 192 Bits 239 Bits 256 Bits 384 Bits </div>	

Available CAs

Any CA
AdminCA1
GS_SCL_CA_v1

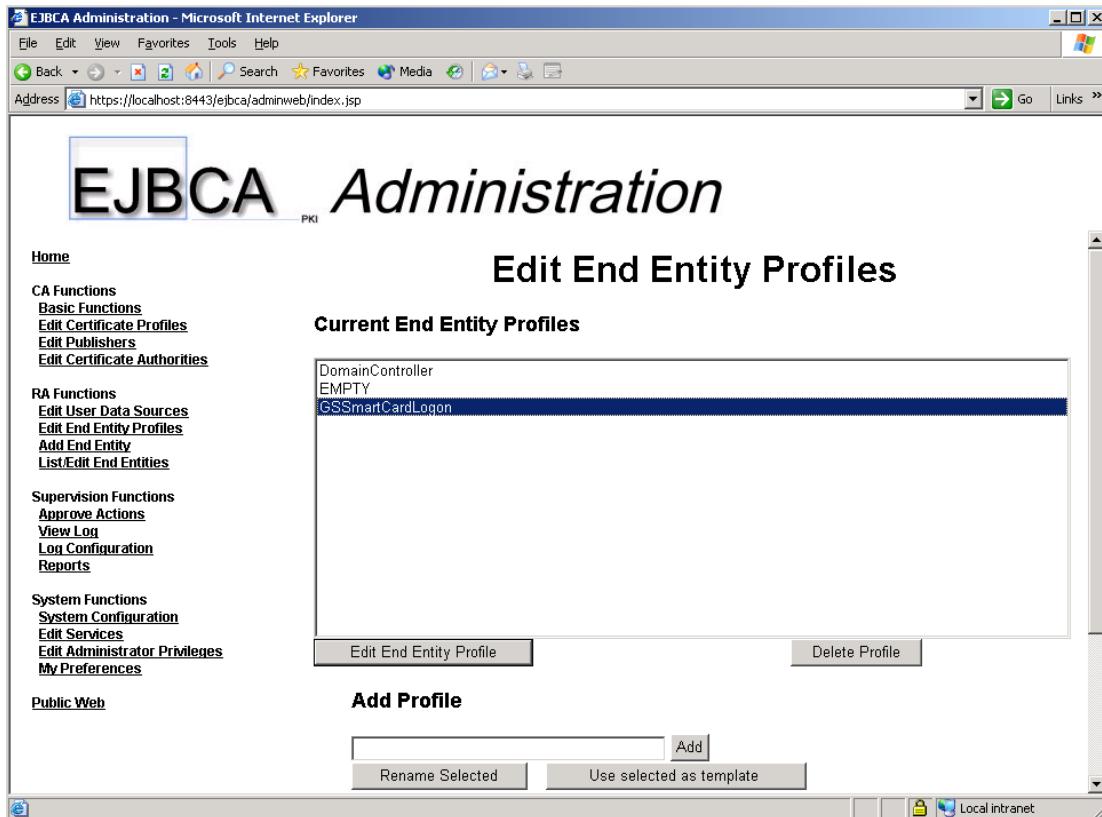
Publishers

Type

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](#)

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

Default Certificate Profile

Available Certificate Profiles

Default CA

Available CAs

Default Token

Available Tokens

Number of allowed requests

Types:

Administrator	<input type="checkbox" value="Use"/>	<input type="checkbox" value="Default"/>	<input type="checkbox" value="Required"/>
Send Notification	<input type="checkbox" value="Use"/>	<input type="checkbox" value="Default"/>	<input type="checkbox" value="Required"/>

Notification Sender

Notification Recipient

Notification Events

Notification Subject

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

The screenshot shows the EJBCA Administration interface in Microsoft Internet Explorer. The title bar reads "EJBCA Administration - Microsoft Internet Explorer". The main content area has a header "Add End Entity". On the left, there's a sidebar with navigation links like "Home", "CA Functions", "Basic Functions", "Edit Certificate Profiles", etc. The main form fields are as follows:

End Entity Profile	DomainController	Required
Username	DomainController-001	<input checked="" type="checkbox"/>
Password	*****	<input checked="" type="checkbox"/>
Confirm Password	*****	
Subject DN Fields		
CN, Common Name	DomainController-001	<input checked="" type="checkbox"/>
Subject Alternative Name Fields		
DNS Name	clean2003.testing.company.cn	<input type="checkbox"/>
MS GUID, Globally Unique Identifier	5210ac15e5152d429bce750038443a68	<input type="checkbox"/>
Certificate Profile	DomainController	<input checked="" type="checkbox"/>
CA	GS_SCL_CA_v1	<input checked="" type="checkbox"/>
Token	User Generated	<input checked="" type="checkbox"/>
<input type="button" value="Add End Entity"/> <input type="button" value="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")

The screenshot shows the EJBCA Administration interface in Microsoft Internet Explorer. The title bar reads "EJBCA Administration - Microsoft Internet Explorer". The main content area is titled "Add End Entity". On the left, there's a sidebar with navigation links under categories like CA Functions, RA Functions, Supervision Functions, and System Functions. The main form has several input fields:

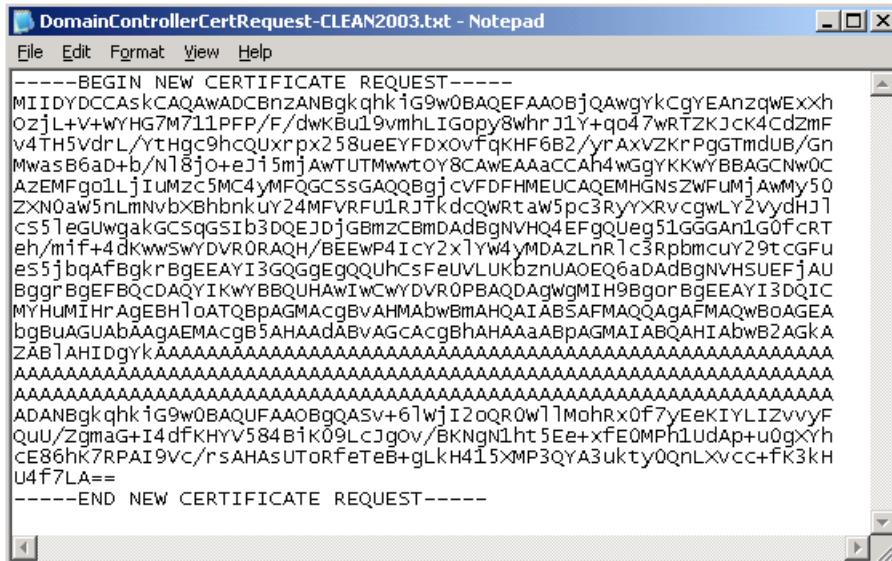
- "End Entity Profile": A dropdown menu set to "GSSmartCardLogon". To its right is a "Required" checkbox.
- "Username": An input field containing "AdministratorGSSCL-001". To its right is a checked checkbox.
- "Password": An input field containing "*****". To its right is a checked checkbox.
- "Confirm Password": An input field containing "*****". To its right is a checked checkbox.
- "Subject DN Fields": An input field containing "CN, Common Name". To its right is a checked checkbox.
- "Subject Alternative Name Fields": An input field containing "MS UPN, User Principal". To its right is a checked checkbox.
- "Name": An input field containing "testing.company.cn". To its right is a checked checkbox.
- "Certificate Profile": A dropdown menu set to "GSSmartCardLogon". To its right is a checked checkbox.
- "CA": A dropdown menu set to "GS_SCL_CA_v1". To its right is a checked checkbox.
- "Token": A dropdown menu set to "User Generated". To its right is a checked checkbox.

At the bottom right of the form are "Add End Entity" and "Reset" buttons. The status bar at the bottom of the browser window shows "Done" and "Local intranet".

- 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"

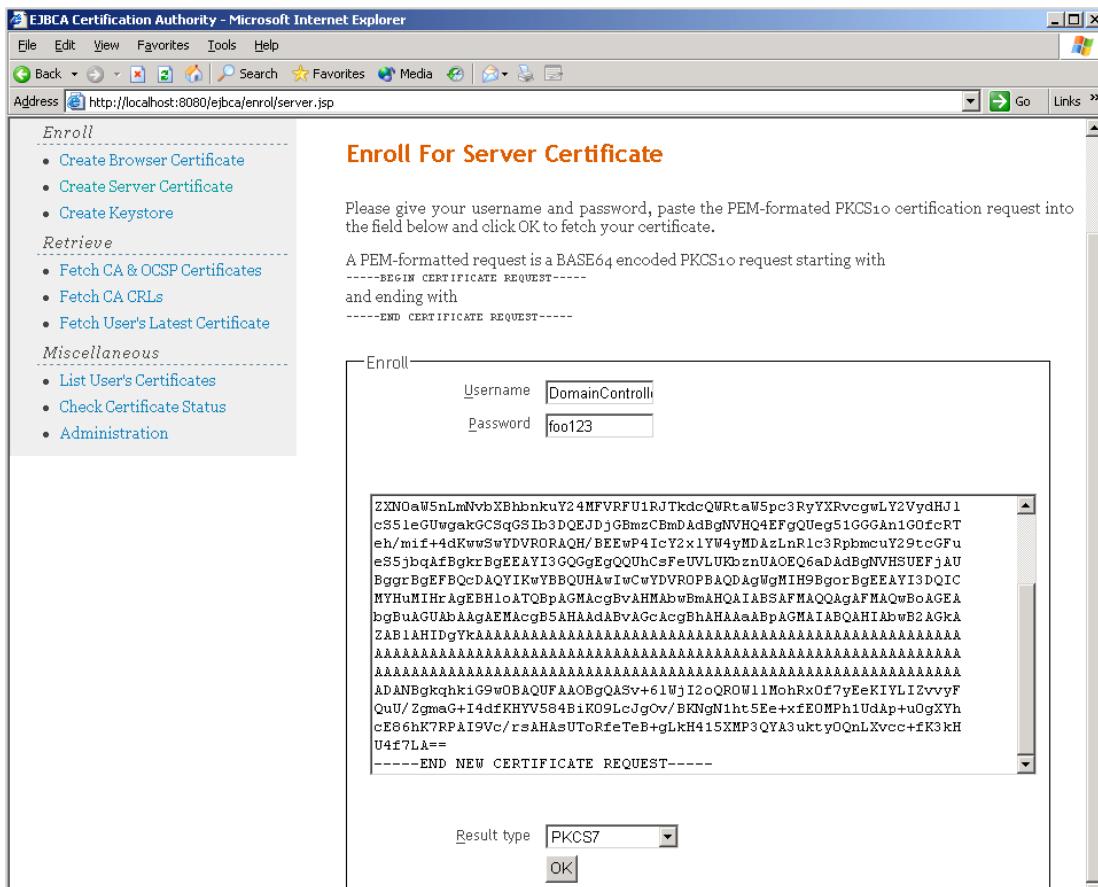


```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYDCCASkCAQAwADCBrnZBqkqhk1G9w0BAQEFAAOBjQAWgYkCgYEAnzqwExh
OzjL+v+wYHG7M711PFP/F/dwKBu19vmlIGopy8Whrj1Y+qo47wRTZKjck4CdZmF
v4TH5VdrL/yTHgc9hcQuxrpx258ueEYFDxovfQKHFB2, /yRAxZKrpPgGTmdUB/Gn
MwasB6aD+b/N18jo+eJ15mjAwUTMmwTOY8CAwEEaaCCAh4wgYKKWYBBAGCNw0C
AZEMFgo1l_j1uMzc5MC4yMFQGCSsGAQQBgjcvFDfHEMUCAQEMHGNsZWFUUmjAmy50
ZXNoaw5nLmNvbxBhbnkuY24MFVRFU1RJTkdQWRtaW5pc3RyYXRvcgwLY2VydHJ1
cs51eGUwqakGCSqGSIB3DQEJDjGBmzCbmDAdBgnVHQ4EFgQUeg51GGGAN1GOfcRT
eh/mif+4dKwvSwYDVRORAQH/BEEwP4Icy2x1Yw4yMDAzLnR1c3RpbcuY29tcGfu
es5jbqAFBqkrBgeEAYI3GQGgEgQQQuCsFeUVLUkbznuAOE6adAdBgnVHSUEfjAU
BggRbgEFBQcdAQYIKwYBBQUHAWiwcwYDVR0PBAQDAgwgMI9BgorBgeEAYI3DQIC
MYHuMIHrAgEBH1oATQBpAGMACgBvAHMAdwBmAHQAIABSAFMQAQQAgAFMAQwB0AGEA
bgBuAGUAbAgAEAMAcgB5AHAAdABvAGCACgBhAHAAaABpAGMAIABQAHIAbwB2AGKA
ZAB1AHIDgYkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBqQASv+61wjI2oQR0w11MohRxOf7yEeKIYLIZvvF
QuU/ZgmaG+I4dfKHV584B1k09lcJgov/BKNGn1ht5Ee+xFE0MPh1UdAp+u0gXyh
cE86hK7RPAI9Vc/rsAHAsUToRfeTeB+gLkH415XMP3QYA3uktyQOnLXvcc+fK3kH
U4f7LA==
-----END NEW CERTIFICATE REQUEST-----

```

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



EJBCA Certification Authority - Microsoft Internet Explorer

Enroll

- Create Browser Certificate
- Create Server Certificate
- Create Keystore

Retrieve

- Fetch CA & OCSP Certificates
- Fetch CA CRLs
- Fetch User's Latest Certificate

Miscellaneous

- List User's Certificates
- Check Certificate Status
- Administration

Enroll For Server Certificate

Please give your username and password, paste the PEM-formatted PKCS10 certification request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded PKCS10 request starting with
-----BEGIN CERTIFICATE REQUEST-----
and ending with
-----END CERTIFICATE REQUEST-----

Enroll

Username	DomainController-001
Password	foo123

-----BEGIN CERTIFICATE REQUEST-----

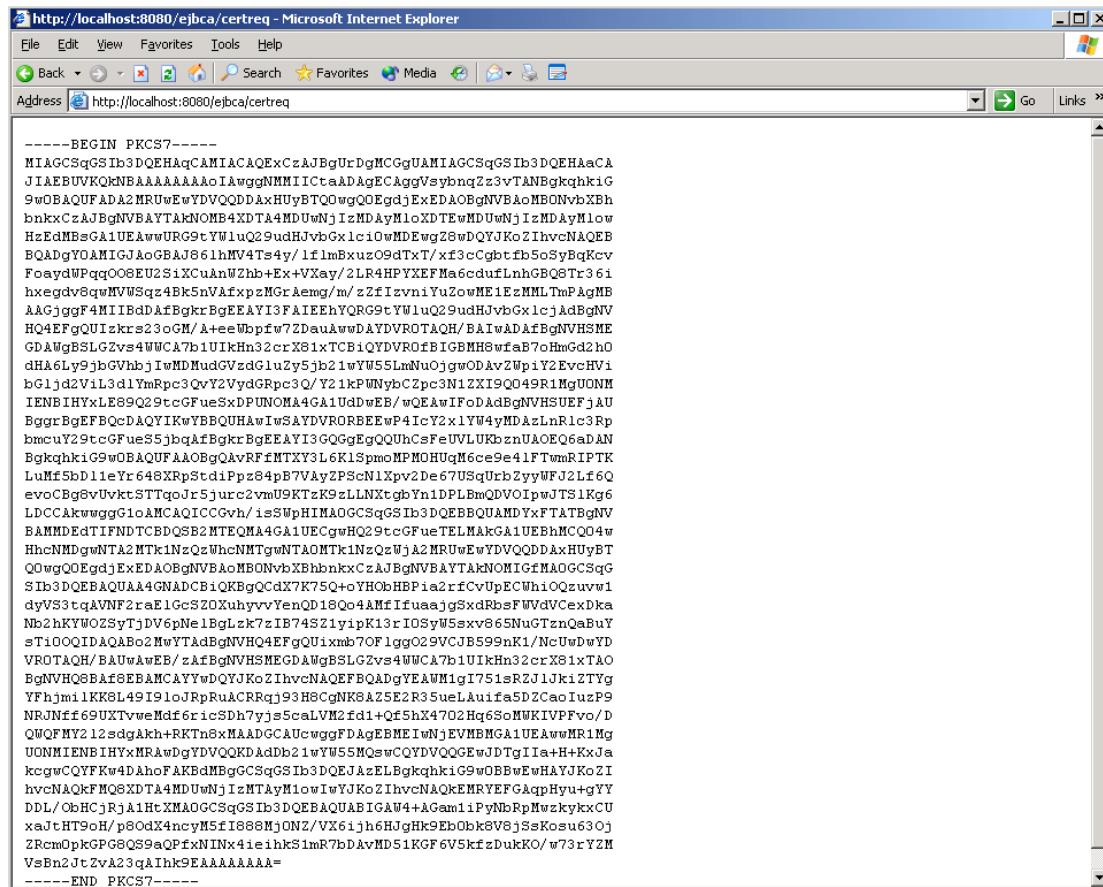
```

ZXNoaw5nLmNvbXBhbnkuY24MFVRFU1RJTkdQWRtaW5pc3RyYXRvcgwLY2VydHJ1
cs51eGUwqakGCSqGSIB3DQEJDjGBmzCbmDAdBgnVHQ4EFgQUeg51GGGAN1GOfcRT
eh/mif+4dKwvSwYDVRORAQH/BEEwP4Icy2x1Yw4yMDAzLnR1c3RpbcuY29tcGfu
es5jbqAFBqkrBgeEAYI3GQGgEgQQQuCsFeUVLUkbznuAOE6adAdBgnVHSUEfjAU
BggRbgEFBQcdAQYIKwYBBQUHAWiwcwYDVR0PBAQDAgwgMI9BgorBgeEAYI3DQIC
MYHuMIHrAgEBH1oATQBpAGMACgBvAHMAdwBmAHQAIABSAFMQAQQAgAFMAQwB0AGEA
bgBuAGUAbAgAEAMAcgB5AHAAdABvAGCACgBhAHAAaABpAGMAIABQAHIAbwB2AGKA
ZAB1AHIDgYkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ADANBgkqhkiG9w0BAQUFAAOBqQASv+61wjI2oQR0w11MohRxOf7yEeKIYLIZvvF
QuU/ZgmaG+I4dfKHV584B1k09lcJgov/BKNGn1ht5Ee+xFE0MPh1UdAp+u0gXyh
cE86hK7RPAI9Vc/rsAHAsUToRfeTeB+gLkH415XMP3QYA3uktyQOnLXvcc+fK3kH
U4f7LA==
-----END NEW CERTIFICATE REQUEST-----

```

Result type **OK**

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



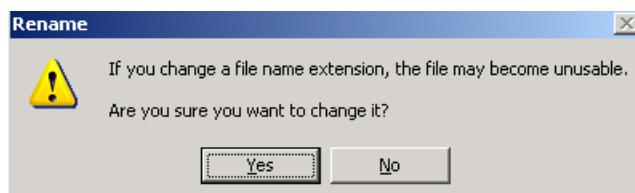
The screenshot shows a Microsoft Internet Explorer window with the URL <http://localhost:8080/ejbca/certreq>. The page content displays a large block of PKCS7 encoded data, starting with "-----BEGIN PKCS7-----" and ending with "-----END PKCS7-----". The data is a base64 encoded string representing a certificate request.

```

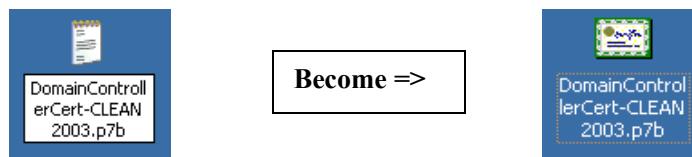
-----BEGIN PKCS7-----
MIAGCSqGSIb3DQEHAaCAMIACQExCzAJBgUrDgMCggUANIAQCSqGSIB3DQEHAaCA
JIAEBUVKQKNsAAAAAAoIAwggNMMIICtaADAgECaggVsybnqZz3vTANBgkqhkiG
9wOBAQUFAD2MRUwEwYDVQDDAxHuYBTQ0wgQOEgjExEDAOBgNvBaoMBONvbXBh
bnkxCcAJBgNVBAYTAKNOMB4XDTA4MDUwNjIzMDAyMloXDTEwMDUwNjIzMDAyMlw
HzEdMBsGA1UEAwURG9tYWluQz9udHJvbGx1c1owMDAwgZ8wDQYJKoZIhvcNAQEB
BQAdYQAMIGJaoGBAJ861hMV4Ts4y/lfimBxuzo9dTxT/x3fcCgbtfb5oSyBqKcv
FoaydWPqqO6EU2rXcV2VydGQpc3Q/Y21kPWNybCzpc3NzX19Q049R1mGUONM
IENBIEHyLE89Q29tcFueSxDPUOMA4GA1UdDwEB/wQEAvIfoDadBgnVHSUEFjAU
BggRgEFBPccDAQYIKwYBBQUHawIwSAyDVORBEEwP41cY2xLYW4yMDAsLnRic3Rp
bmCuY29tcFueSS5jbgqAfBgkrBgkEAYI3CQGgEgQQUhCseUVLURbznuAeQ6aDAN
BgkchkiG9wOBAQUBAOBgQAvRFEMTXY3L6KLSpmoMPMOHQm6ce9e41FTmRIPTK
LuMf5bd11eYz648XRpStd1Ppz84pB7VAYzPScNLKpv2De67USqUrbzyyWFJ2Lf6Q
eveCBg8vUvktSTKTqoJr5juc2vnU9KTzK9zLLNxtgbYn1DPLBmQDVOIpwJTS1Kg6
LDCCAkwwggGioAMCAQICCvbu/isUpHIMAOGCSqGS1b3DQEBQUAMDYXTATBgNv
BAMMDEdTIFNDTCBDQS2MTEQMA4GA1UECgwHQB9tcFueTELMAKGA1UEBhMCQ04w
HhcNHDgwNTIA2MTK1NzQ2WhcNHTgwNTIAONTk1NzQzUjA2MRUwEwYDVQDDAxHuYBT
Q0wgQOEqdjExEDAOBgNvBaoMBONvbXhbnnkxCzAJBgNVBAYtANOMIGMAOGCSqG
S1b3DQEBQAUAAA4GNADCBiKbgQcdXTK75Q+oYHObHPiavrfCvUpECWhiOQzuvw1
dyVS3tqAVNF2raE1GcS2OXuhyyvYenQD18Qo4AMfIfuaeajgSxdRbsFVVdVCexDka
Nb2HKWYZsYJ3DV6pNe1bgLz7z1B74S21yipK13r10SyW5xv865NuGTznqaBuY
sT10OQIDACABo2MwYTAdbgNVHQ4EFgQU1xbm7Of1ggO29VCJB599n1/McUwDwYD
VR0TAQH/BAUwAEB/zafBgNVHSMEGDAGbSLG2zv4WWCA7b1UIkHm32crX81xTAO
BgNVHQ8BAf8EBAMCAYYwPQYJKoZIhvCNQAEFBQDgYEAMhI75isZJUJk1ZTyg
YFHjm1K8L49I91oJRpRuACCRqj93H8CgNk8A25E2R35sueLAuifa5DZCaoIuzP9
NRJNif69UtvweMdf6ricSDh7yjs5caLMv2fd1+Qf5hX4702Hg5SoNUK1VPvvo/D
QWQFMY21zsdgAkh+RKTn8xMAADGCAuCwggFDAgEBMEIwNjEVMBMG1aUEAwMR1Mg
UONMIENBIEHyMRAwDgYDVQQRKAdb21wYU55MQuwCQYDVQGCEwJDtgIIa+h+KxJa
kgcwQYFV4Bh0FAKbdMBgGCsgGS1b3DQEJAzELBqkqhk1c9wOBBeWwHAYUKoZI
hvcNAQkFQ8XTD4MDUwNjIzMTAytWJKoZIhvCNQkEMRYERGQpHyu+gYY
DDL/OBHCjRja1HeXMAOGCSqGS1b3DQEBAQUABIGAU4+AQam1iPyNDRpHwzkykxCU
xaJtHT9oH/p8od4ncyMSfI888Mj0NZ/VX61jh6HJgHk9SEbOkhBV8jSsKosu63oj
ZRcmOpkGPGBQS9aQPfxNINx4ie1hkSimR7bDavHD51KGf6V5kfzduK0/w73rYZM
VsBn2JtZvA23qA1hk5EAAAAAAA=
```

-----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"

EJBCA Certificate/CRL Retrieval - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Stop Search Media

Address http://localhost:8080/ejbca/retrieve/ca_certs.jsp Links >

EJBCA Fetch CA Certificate

CA: AdminCA1

In PEM format:
[CN=AdminCA1,O=EJBCA Sample,C=SE,OCSPResponder certificate](#)

For Netscape / Mozilla:
[CN=AdminCA1,O=EJBCA Sample,C=SE,OCSPResponder certificate](#)

For Internet Explorer:
[CN=AdminCA1,O=EJBCA Sample,C=SE,OCSPResponder certificate](#)

CA: GS_SCL_CA_v1

In PEM format:
[CN=GS SCL CA v1,O=Company,C=CN](#)

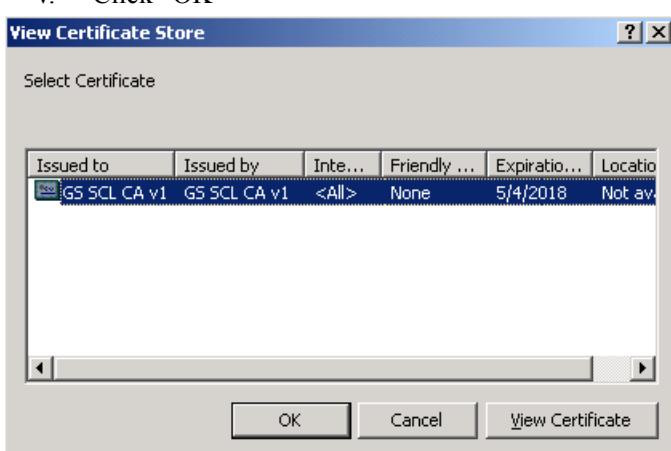
For Netscape / Mozilla:
[CN=GS SCL CA v1,O=Company,C=CN](#)

For Internet Explorer:
[CN=GS SCL CA v1,O=Company,C=CN](#)

- 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 desktop
 - 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

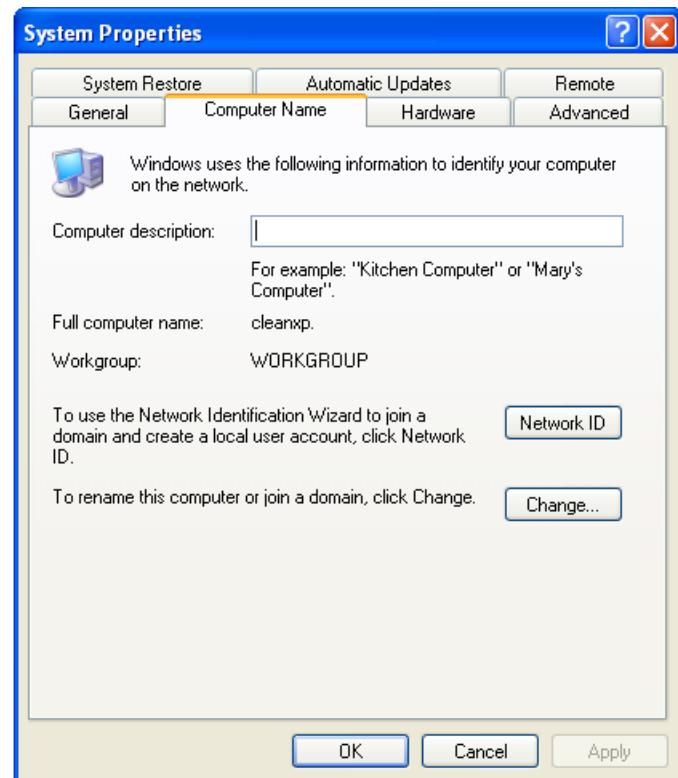
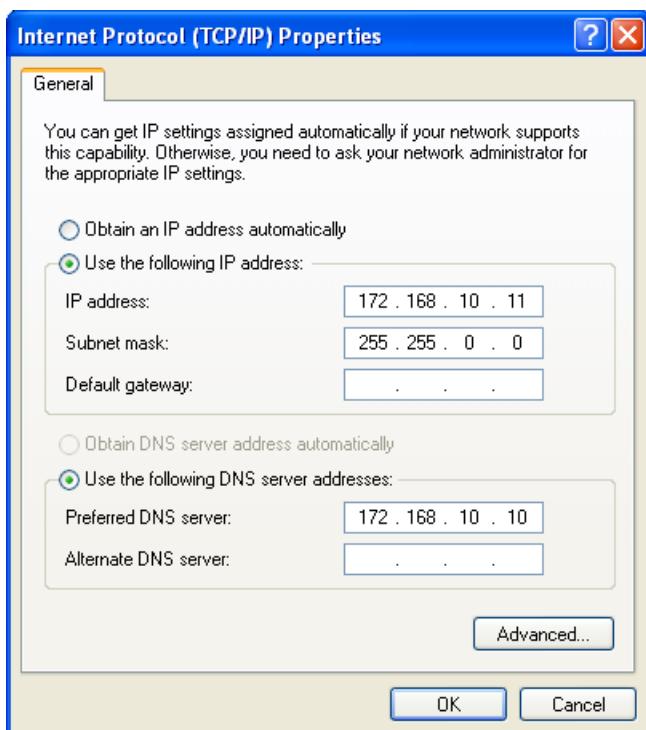
10. Import the CA certificate to "Enterprise NTAuth store"
 - i. Double click the "3. ImportCACertToNTAuthStore.vbs" on desktop
 - ii. Click "OK"
 - iii. Select "GS SCL CA v1.cer" and click "Open"
 - iv. Click "OK"
 - v. Click "OK"



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



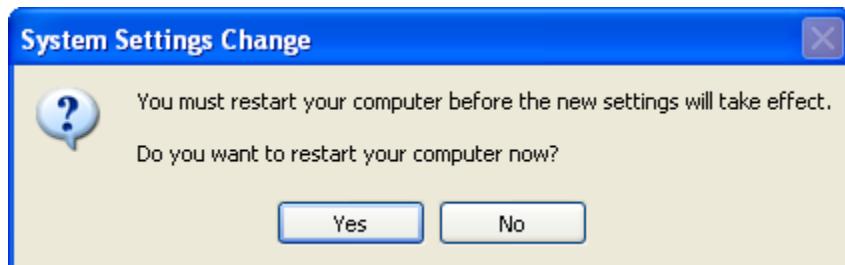
1. Add client into domain "testing.company.cn"
 - i. Right click "My Computer"\Computer Name\Change...



- ii. Select “Domain.”\input “testing.company.cn”
- iii. Click “OK”



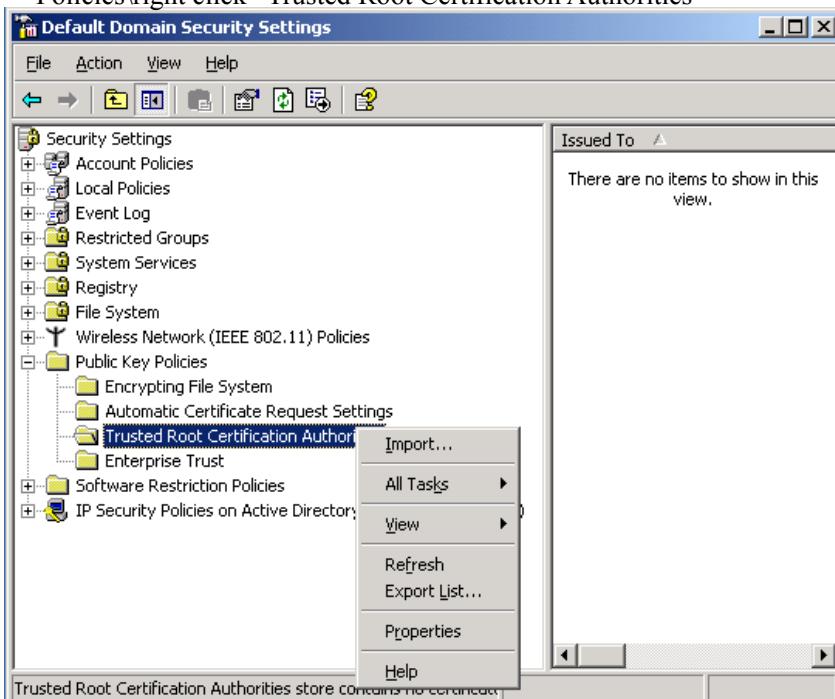
- iv. Input “administrator” as “User name.”
- v. Input the server’s password as “Password”
- vi. Click “OK” 4 times



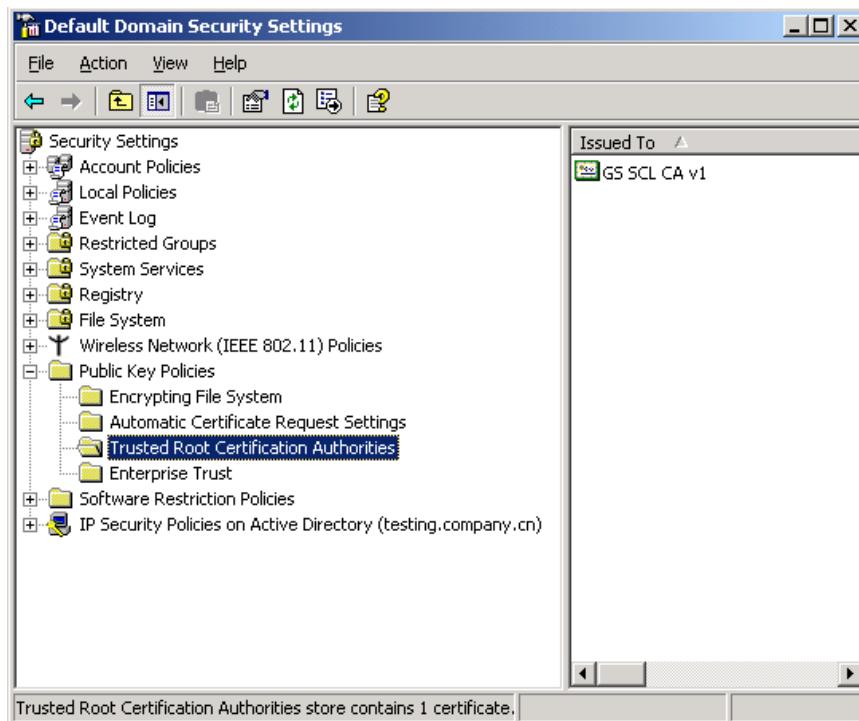
- vii. Click “Yes” to restart workstation

4.1 -- Add CA Certificate to Domain Security Policy

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

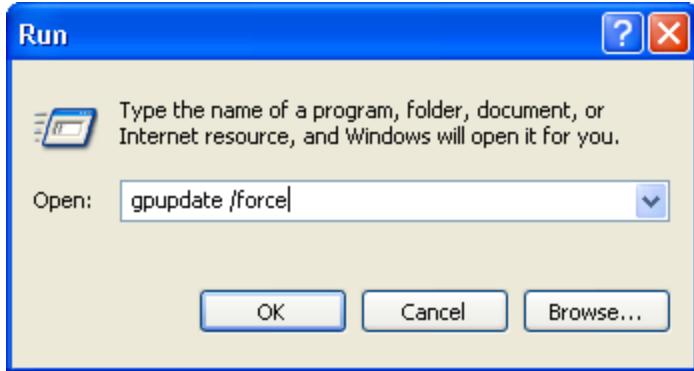


- Choose “Import...”
- Click “Next”
- Browse to the “GS SCL CA v1.cer”
- Click “Open”
- Click “Next” 2 times
- Click Finish
- Click “OK”



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 “/”)



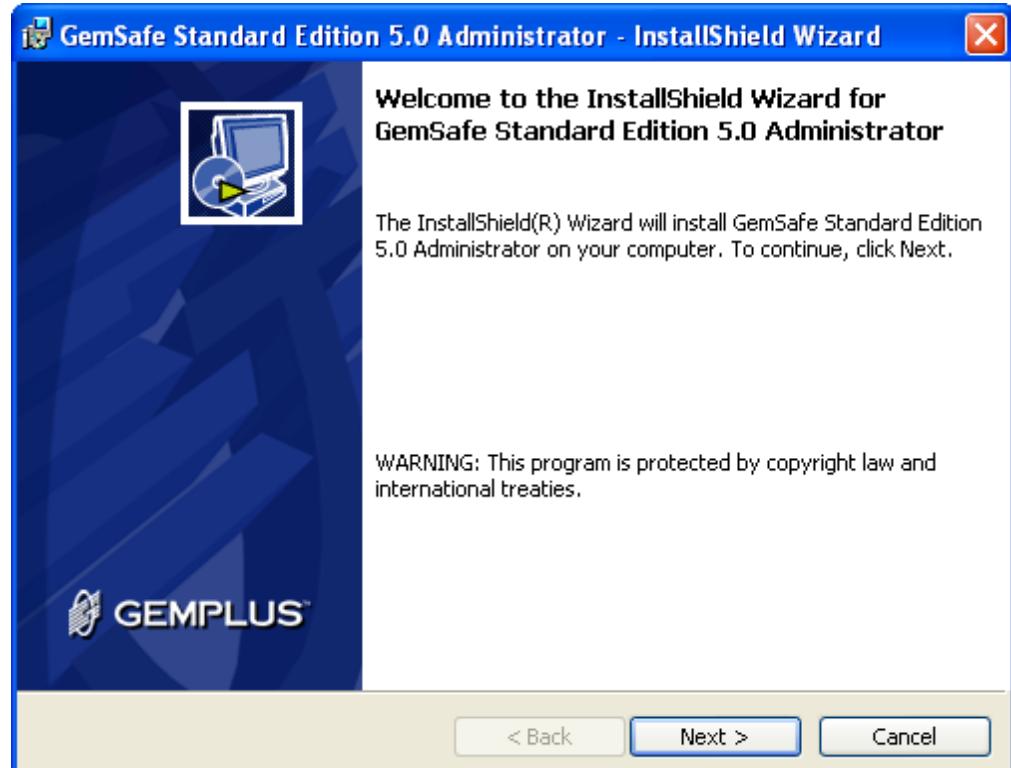
4. Click “OK”

4.3 -- Install GemSAFE Toolbox on Workstation

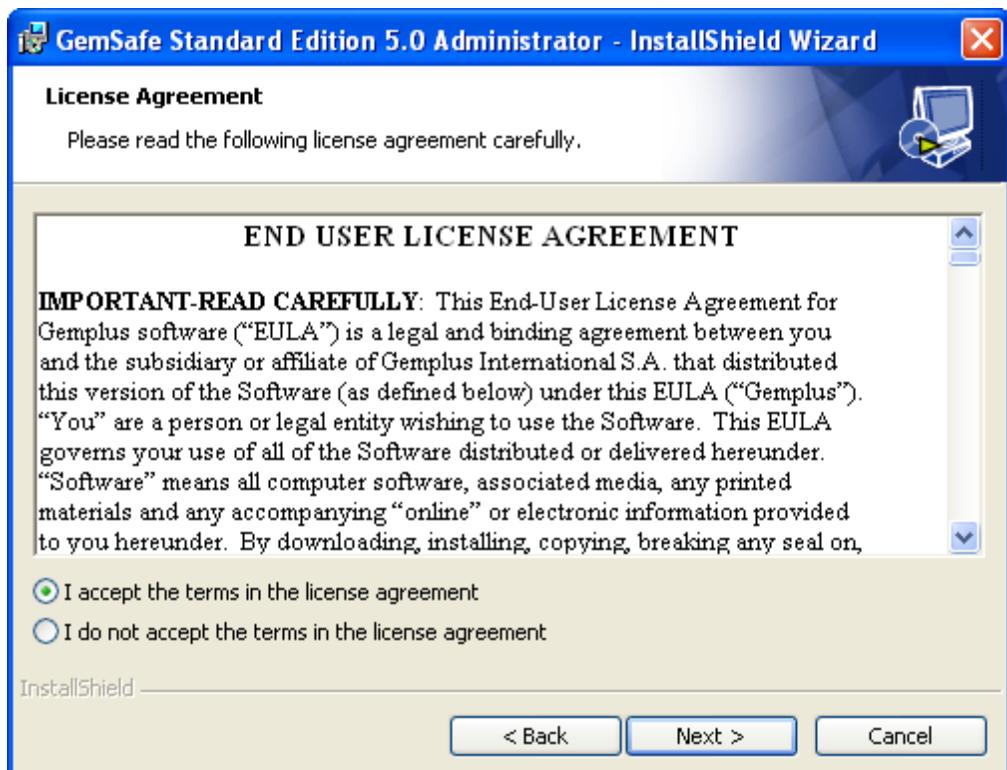
1. Run GemSAFE toolbox on Workstation



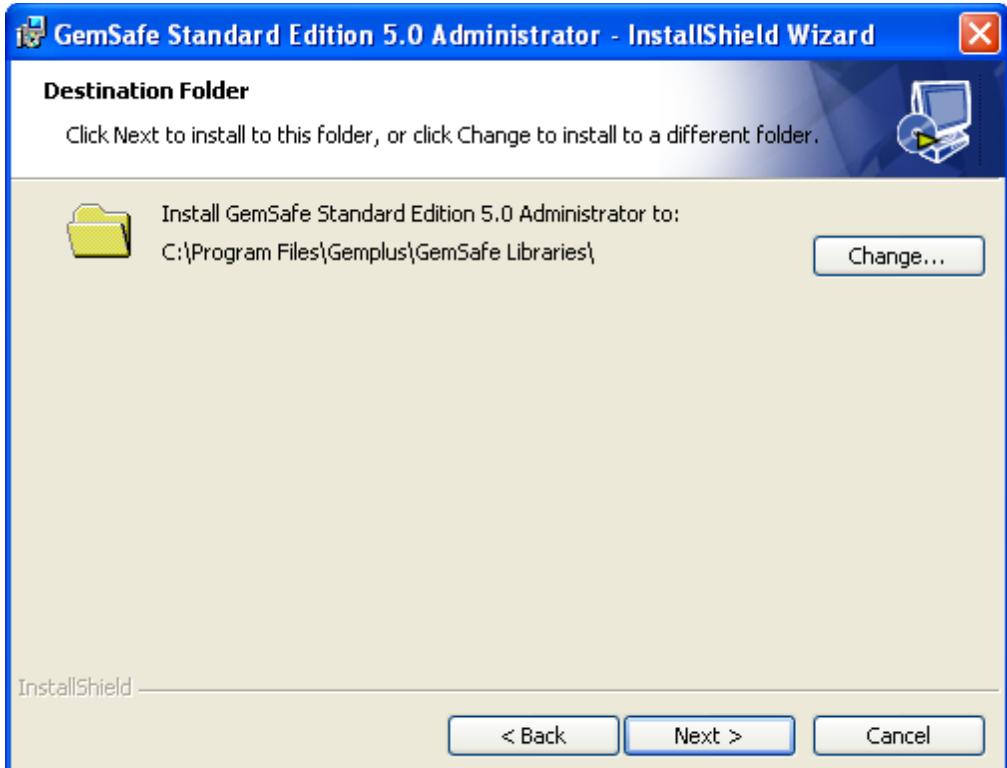
2. Click "OK"



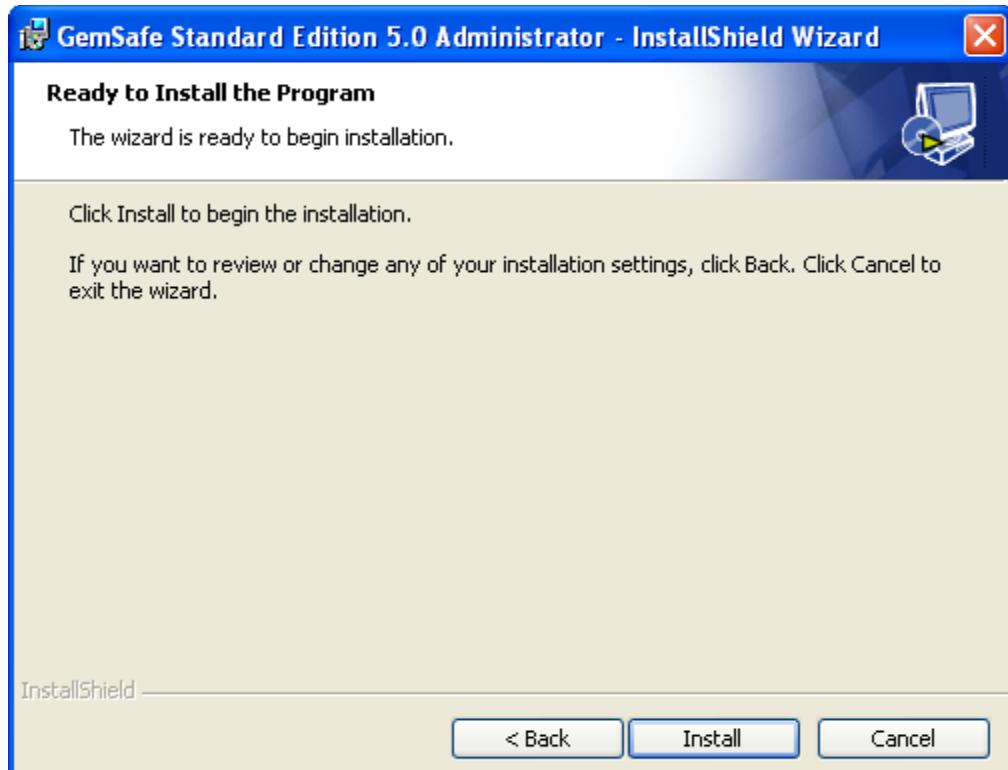
3. Click "Next>"



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



6. Click "Next>"



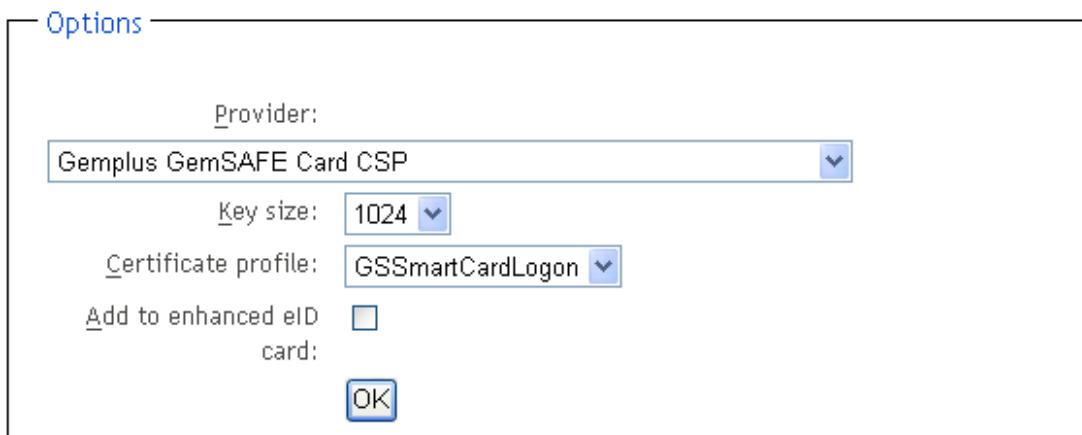
7. Click "Install"



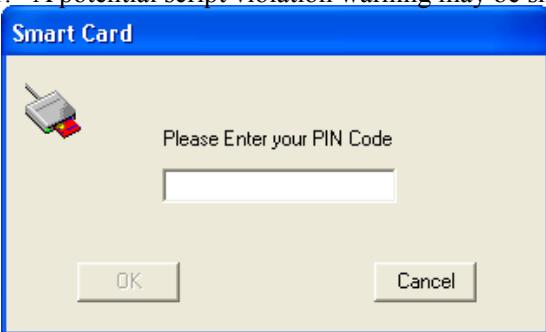
8. Click "Finish":

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”



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



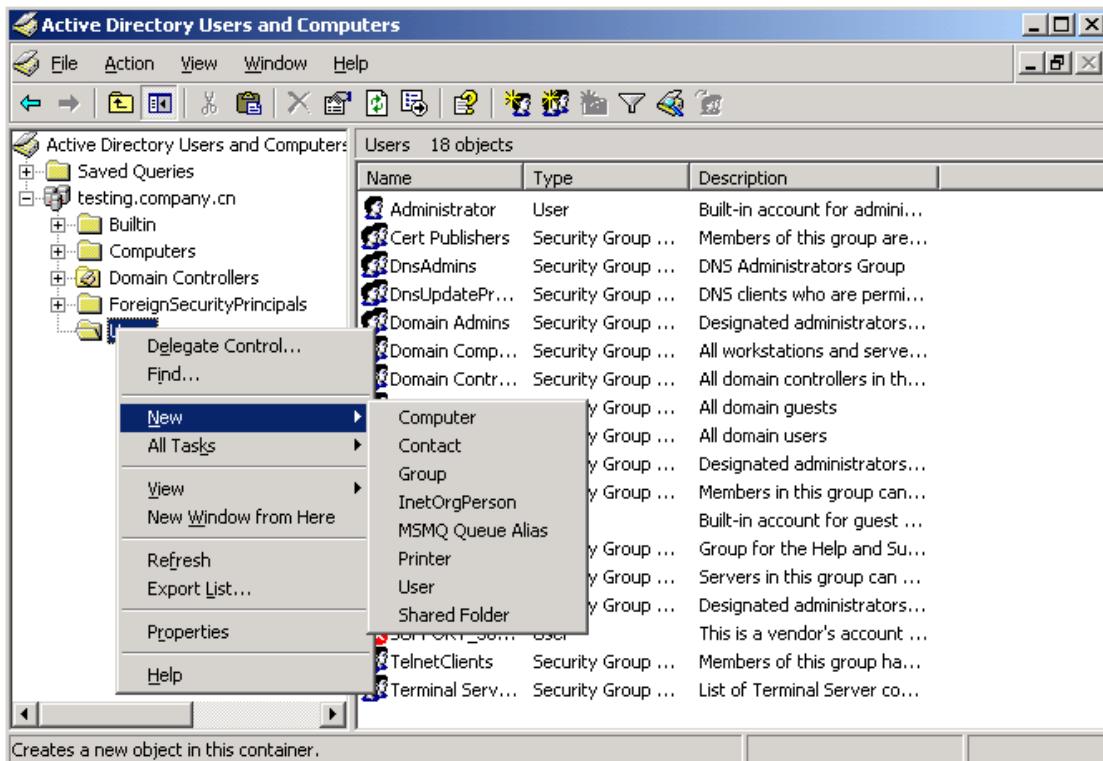
6. Enter the token's pin number and click "OK"
7. You will be logged on to the workstation under administrator account

5 -- Logon Workstation Using another Account

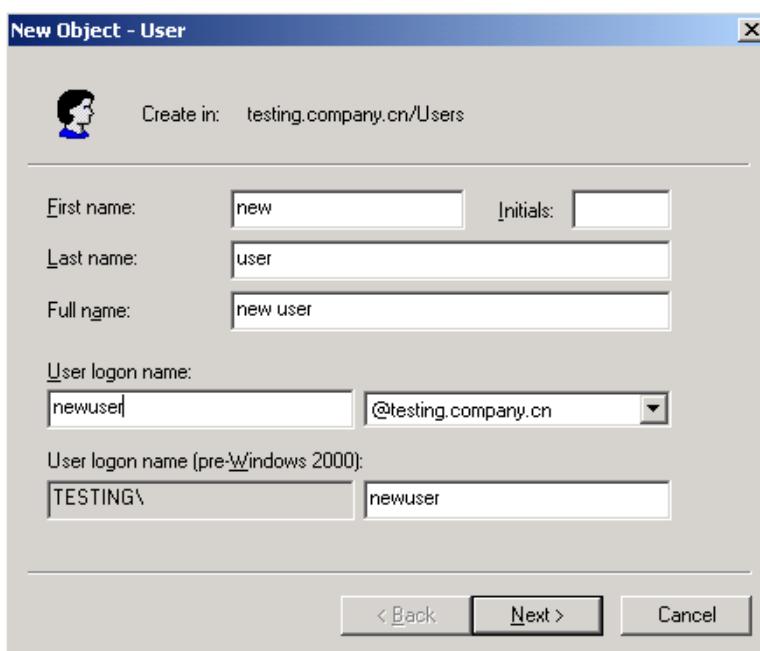
If you want to logon to other user account, you must know your account username, which is stored under domain controller's database

5.1 -- Create a New User Account

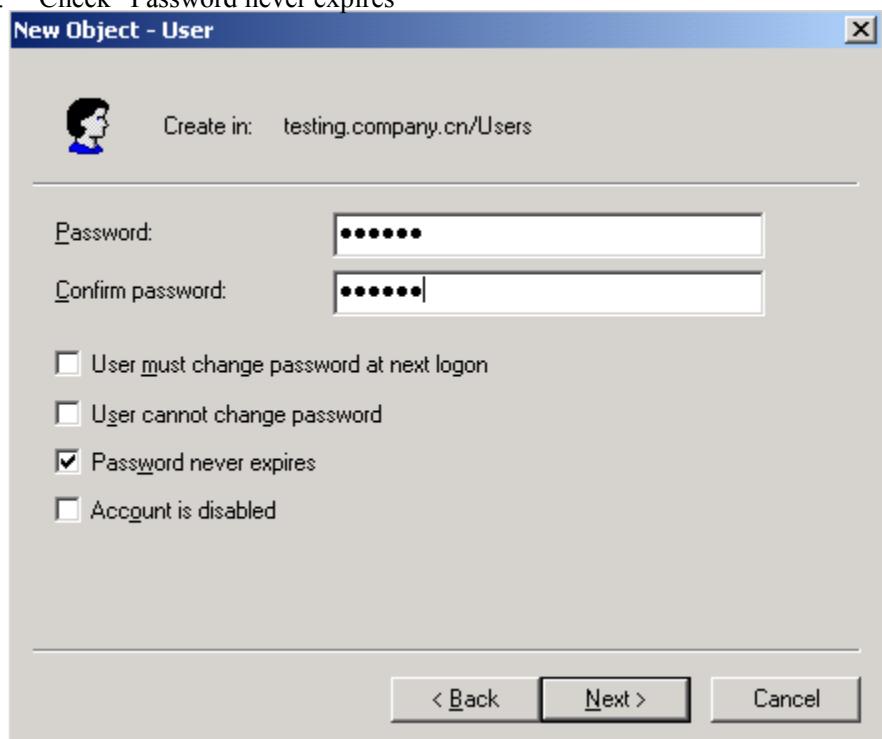
1. Go to domain controller\Start\Administrative Tools\Active Directory Users and Computers
2. Click to expand the node “testing.company.cn”\right click “Users”\New\User



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



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



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 ▾

Add End Entity 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:	<input type="text" value="newuser"/>
Password:	<input type="password" value="*****"/>
<input type="button" value="OK"/>	

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:	<input type="text" value="Gemplus GemSAFE Card CSP"/>
Key size:	<input type="text" value="1024"/>
Certificate profile:	<input type="text" value="GSSmartCardLogon"/>
Add to enhanced eID card:	<input type="checkbox"/>
<input type="button" value="OK"/>	

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