

EJBCA with GemSAFE Toolbox Part2 Sign and Encrypt Email

Introduction

This document introduces the process of using EJBCA together with GemSAFE toolbox to encrypt and sign email. In short, there are 4 compulsory settings for signing and encryption email.

1. The end entity's email must same with the email account you are going to use
2. In certificate profile, Digital Signature and Key Encipherment must be chosen in key usage; Email Protection must be chosen in Extended Key usage.
3. In end entity profile, "EMail, EmailAddress in DN" must be added.
4. CA's certificate must be imported to local machine

This document is a continuation form a document call EJBCA "with GemSAFE Toolbox Part1 workstation logon". The forth setting, "importing CA's certificate to local machine" had been done in previous document. If you want to skip the previous document and directly get started from this, don't forget to import the CA's certificate to local machine yourselves.

Table of Content

EJBCA with GemSAFE Toolbox Part2 Sign and Encrypt Email.....	1
Introduction.....	2
Table of Content.....	3
1 -- Configure EJBCA.....	4
1.1 -- Create Certificate Profile "Email".....	5
1.2 -- Create End Entity Profile "Email".....	10
1.3 -- Add "EmailSender" End Entity.....	14
1.4 -- Enroll Certificate to GemSAFE Smartcard.....	15
2 -- Configure Server.....	16
2.1. -- Add Server as a Email Server.....	17
2.2. -- Add a New Email Account.....	19
3 -- Configure Microsoft Outlook 2003 for Sending Encrypted and Signed Emails.....	20

1 -- Configure EJBCA

1.1 -- Create Certificate Profile “Email”

1. On server, go to EJBCA Administration GUI
2. Click “Edit Certificate Profiles”
3. Type "Email" in the text box under “Add Profile”. Click “Add”
 - a) Choose “Email” under “Current Certificate Profiles”
 - b) Click “Edit Certificate Profile”
 - c) Set “Email” certificate profile’s parameters
 - i. Under "Key Usage" select "Digital Signatures" and “Key Encipherment”
 - ii. Check "Use Extended Key Usage"
 - iii. Under "Extended Key Usage" select " Email Protection "
 - iv. Under "Available CAs" select only "GS_SCL_CA_v1"
4. Leave all other setting by default, click “save”
5. The following is the screen capture of the settings

Edit Certificate Profile

Certificate Profile : Email

[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 type="checkbox"/>
Use CRL Distribution Point	<input type="checkbox"/>
CRL Distribution Point Critical	<input 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.

1.2 -- Create End Entity Profile "Email"

1. On server, go to EJBCA Administration GUI
2. Click "Edit End Entity Profiles"
3. Type "Email" in the text box under "Add Profile". Click "Add"
 - a) Choose "Email" under "Current End Entity Profiles"
 - b) Click "Edit End Entity Profile"
 - c) Set "email" end entity profile's parameters
 - i. Under "Subject DN" fields, add "Email, EmailAddress in DN"
 - ii. Under "Email, EmailAddress in DN", check "Required"
 - iii. Under "Default certificate profile" select "Email"
 - iv. Under "Available certificate profiles" select "Email"
 - v. Under "Default CA" select "GS_SCL_CA_v1"
 - vi. Under "Available CAs" select only "GS_SCL_CA_v1"
4. Leave all other setting by default, click "save"
5. The following is the screen capture of the settings

Edit End Entity Profile

Profile : Email

[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"/> Email, EmailAddress in DN	Required <input checked="" type="checkbox"/> See also configuration of Email field.	
<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="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 checked="" type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable <input checked="" 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. 5/11/08 8:39 PM or days:hours:minutes)	<input type="text"/>	
		Use <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>	
	Certificate Validity End Time (e.g. 5/11/08 8:39 PM or days:hours:minutes)	<input type="text"/>	
		Use <input type="checkbox"/> Modifiable <input checked="" type="checkbox"/>	
	Default Certificate Profile	<input type="text" value="Email"/>	

Available Certificate Profiles	<div>DomainController ENDUSER Email 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

Bullzip PDF Printer

Printed Copies

1

Current Template No Printing template is uploaded.

Upload Template

Upload Template

Save

Cancel

Made by PrimeKey Solutions AB, 2002-2008.

1.3 -- Add "EmailSender" End Entity

1. On server, go to EJBCA Administration GUI
2. Click "Add End Entity"
3. Under "End Entity Profile" choose "GS SmartCardLogon"
4. User Name= "EmailSender01"
5. Password="foo123"
6. Confirm Password="foo123"
7. CN, Common Name= "EmailSender01"
8. MS UPN, User Principal Name = emailsender01@testing.company.cn
9. The following is the screen capture of the settings

Add End Entity

End Entity Profile	Email	Required
Username	EmailSender01	<input checked="" type="checkbox"/>
Password	••••••	<input checked="" type="checkbox"/>
Confirm Password	••••••	
Email	emailsender01@testing.company.cn	<input checked="" type="checkbox"/>
Subject DN Fields		
Email, EmailAddress in DN Use data from Email field :	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CN, Common Name	EmailSender01	<input checked="" type="checkbox"/>
Certificate Profile	Email	<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"/>		

Previously added end entities

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

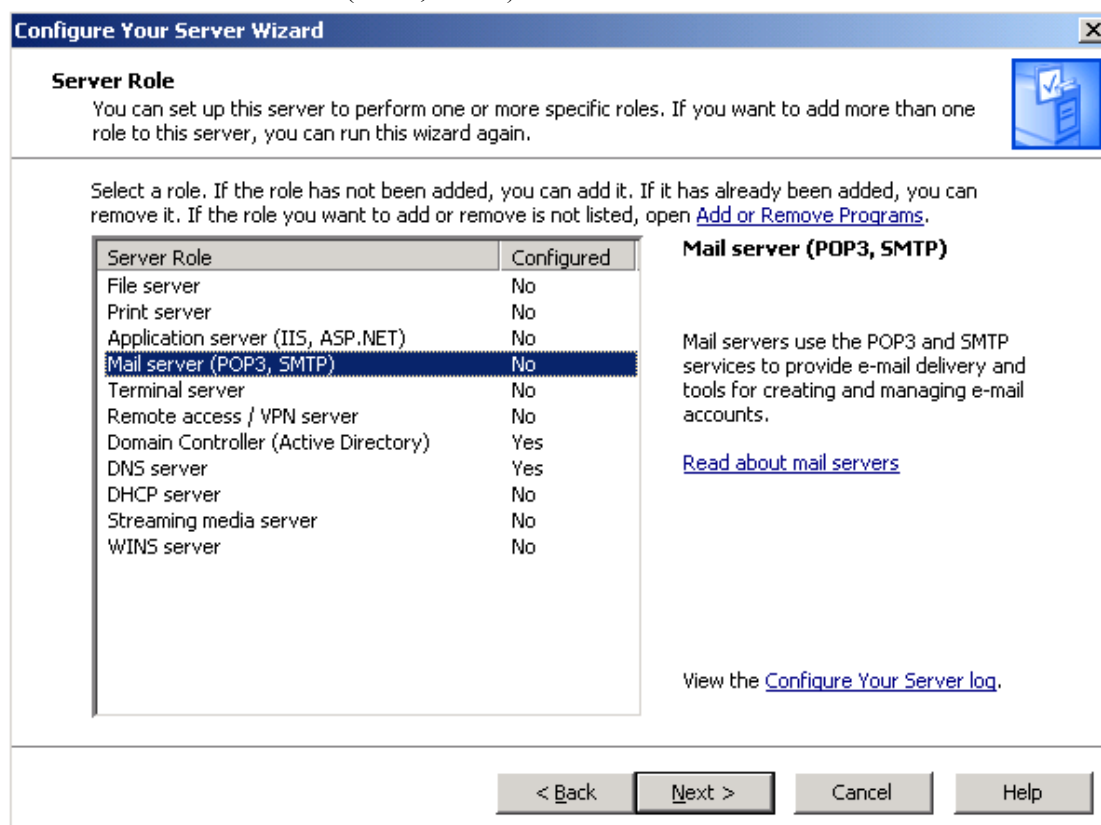
1.4 -- Enroll Certificate to GemSAFE Smartcard

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:"=EmailSender01
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"

2 -- Configure Server

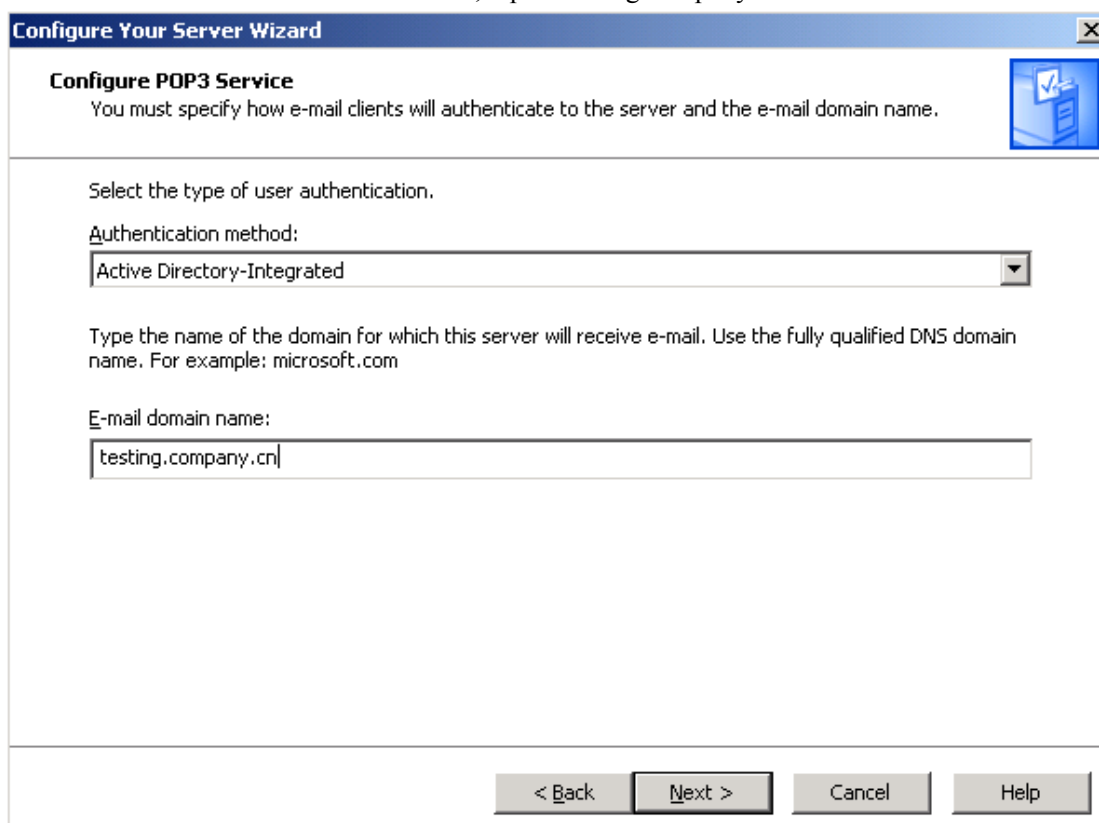
2.1. -- Add Server as a Email Server

1. Go to Domain Controller\start\Manage Your Server\Add or Remove a Role\Click “Next”\
2. Chose “Mail server (POP3, SMTP)”



3. Click “Next”

4. In “E-mail domain name:” field, input “testing.company.cn”



The screenshot shows the 'Configure Your Server Wizard' window with the title bar 'Configure Your Server Wizard'. The main heading is 'Configure POP3 Service'. Below it, a sub-heading says 'You must specify how e-mail clients will authenticate to the server and the e-mail domain name.' To the right is a blue icon of a server with a checkmark. The text 'Select the type of user authentication.' is followed by 'Authentication method:' and a dropdown menu showing 'Active Directory-Integrated'. Below this, it says 'Type the name of the domain for which this server will receive e-mail. Use the fully qualified DNS domain name. For example: microsoft.com'. The 'E-mail domain name:' field contains 'testing.company.cn'. At the bottom are buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

5. Click “Next” 2 times
6. You may be prompted to locate the Windows Server 2003 image or CD location

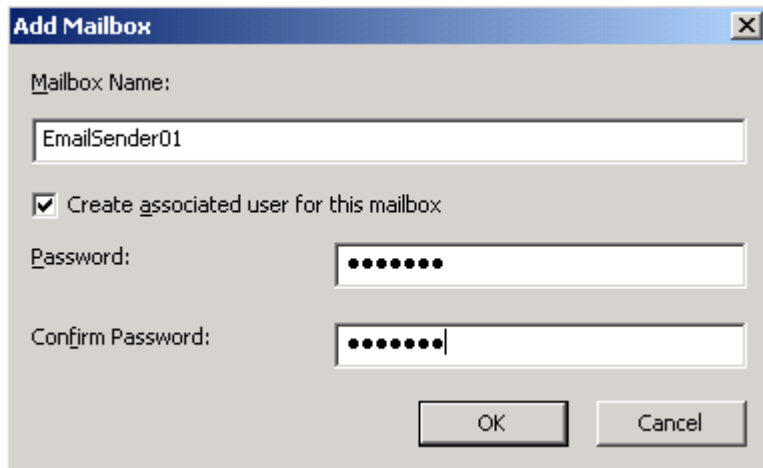


The screenshot shows the 'Configure Your Server Wizard' window with the title bar 'Configure Your Server Wizard'. The main heading is 'This Server is Now a Mail Server'. To the left is a large blue icon of a server with a checkmark. The text says 'You have successfully set up this server as a mail server. To add or remove another role, run the Configure Your Server Wizard again.' Below this is a link: 'View the next steps for this role'. At the bottom, it says 'For a record of your changes, see the [Configure Your Server log](#). To close this wizard, click Finish.' At the bottom are buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

7. Click “Finish”

2.2. -- Add a New Email Account

1. At server, go to Start\Administrative Tools\POP3 Service
2. Click "CLEAN2003" node\Click "testing.company.cn"\ Add MailBox
3. Mailbox Name: EmailSender01
4. Password: foo123@
5. Confirm Password: foo123@



Add Mailbox

Mailbox Name: EmailSender01

☒ Create associated user for this mailbox

Password:

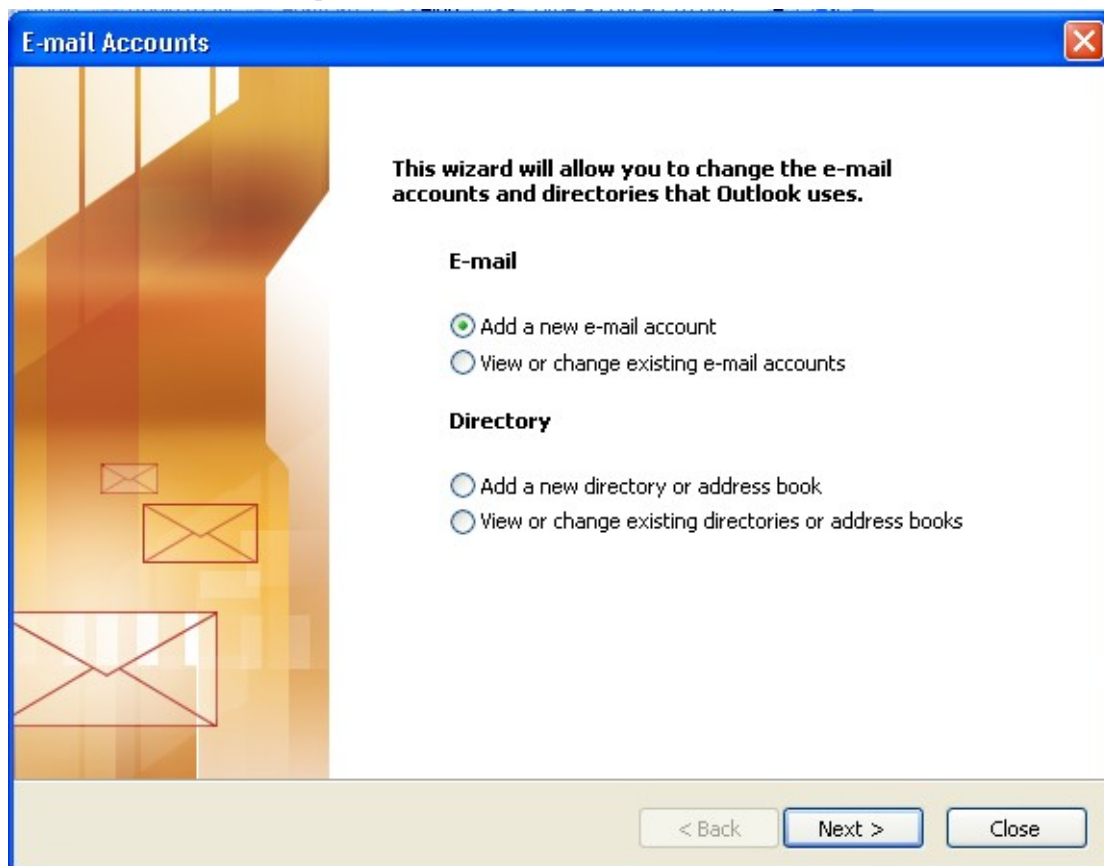
Confirm Password:

OK Cancel

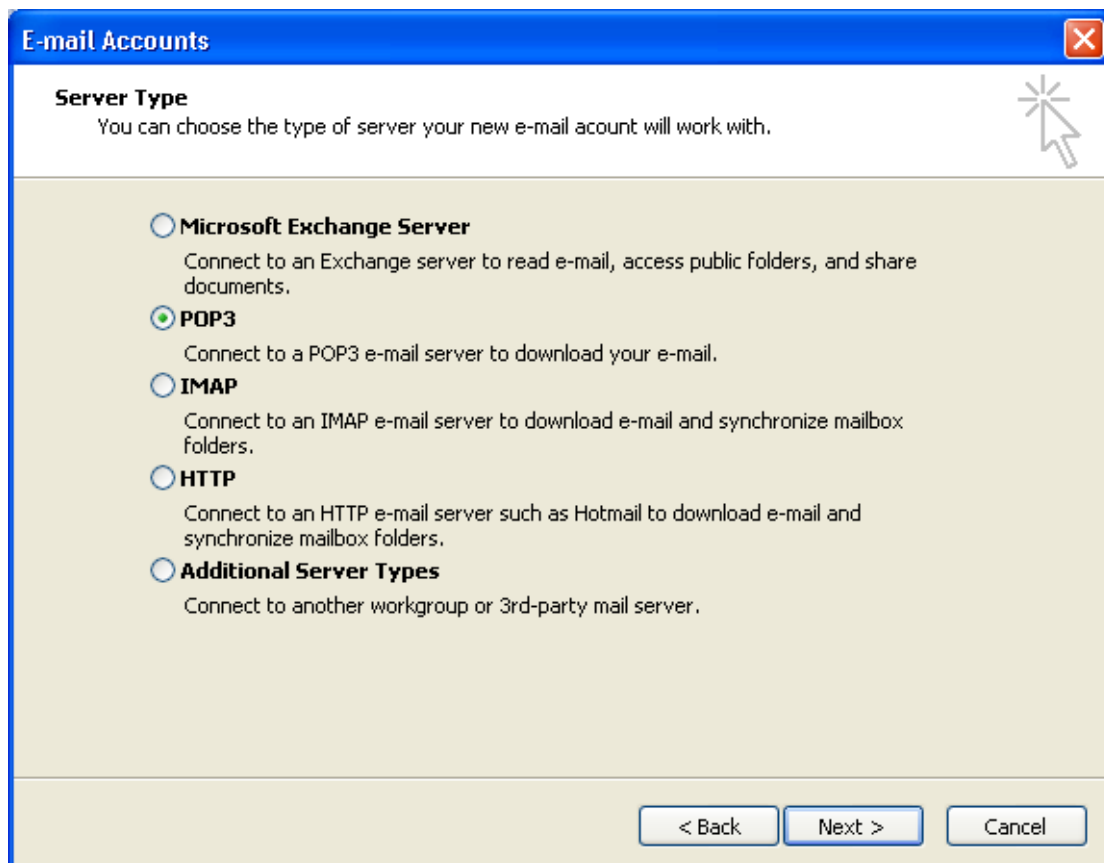
6. Click "OK"
7. Click "OK"

3 -- Configure Microsoft Outlook 2003 for Sending Encrypted and Signed Emails

1. Install Microsoft Outlook 2003 on Workstation
2. Add email account—"EmailSender01", to Microsoft Outlook 2003
 - a) At workstation, open Microsoft Outlook 2003\ tools\E-mail Accounts...



- b) Click "Next"



- c) Choose "POP3" \ Click "Next >"
- d) Your Name = EmailSender01
- e) E-mail Address = emailsender01@testing.company.cn
- f) Incoming mail Server (POP3): = testing.company.cn
- g) Outgoing mail Serve (SMTP): = testing.company.cn
- h) Username= emailsender01
- i) Password = foo123@
- j) Check "logon using Secure Password Authentication (SPA)"

E-mail Accounts

Internet E-mail Settings (POP3)
Each of these settings are required to get your e-mail account working.

User Information
Your Name:
E-mail Address:

Server Information
Incoming mail server (POP3):
Outgoing mail server (SMTP):

Logon Information
User Name:
Password:
☒ Remember password
☒ Log on using Secure Password Authentication (SPA)

Test Settings
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

k) Click "Test Account Settings..."

Test Account Settings

Congratulations! All tests completed successfully. Click Close to continue.

Tasks **Errors**

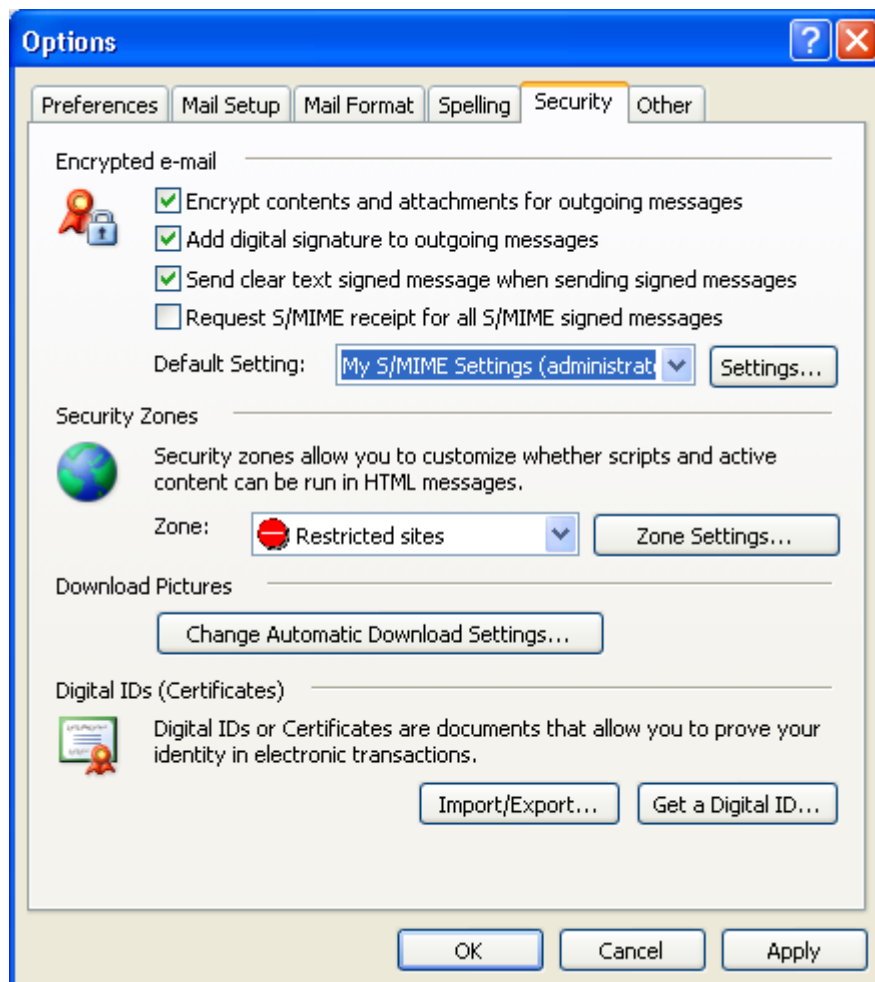
Tasks	Status
✓ Establish network connection	Completed
✓ Find outgoing mail server (SMTP)	Completed
✓ Find incoming mail server (POP3)	Completed
✓ Log onto incoming mail server (PO...	Completed
✓ Send test e-mail message	Completed

l) Click "Close"

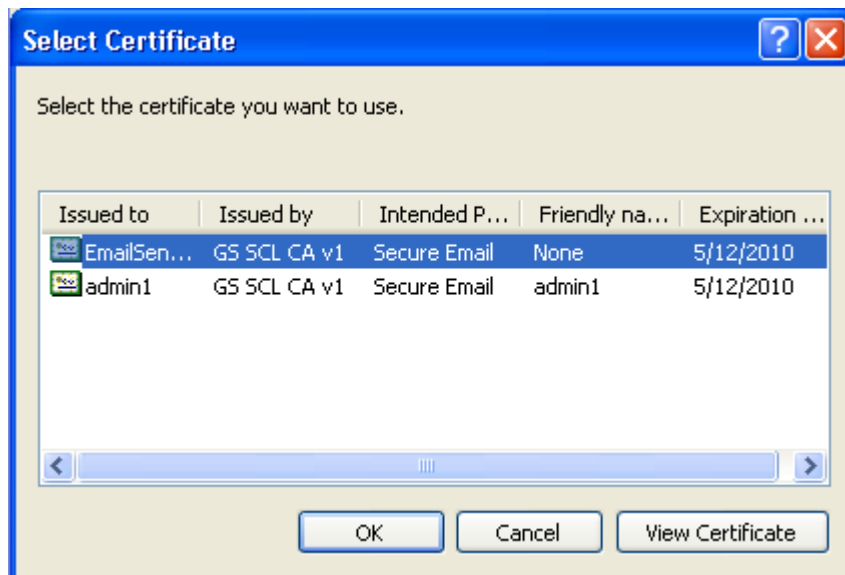
m) Click "Next >"

n) Click "Finish"

- a) In Microsoft Outlook 2003, Tools\ Options...\ Security
- b) Check “Encrypt contents and attachments for outgoing messages”
- c) Check “Add digital signature to outgoing messages”



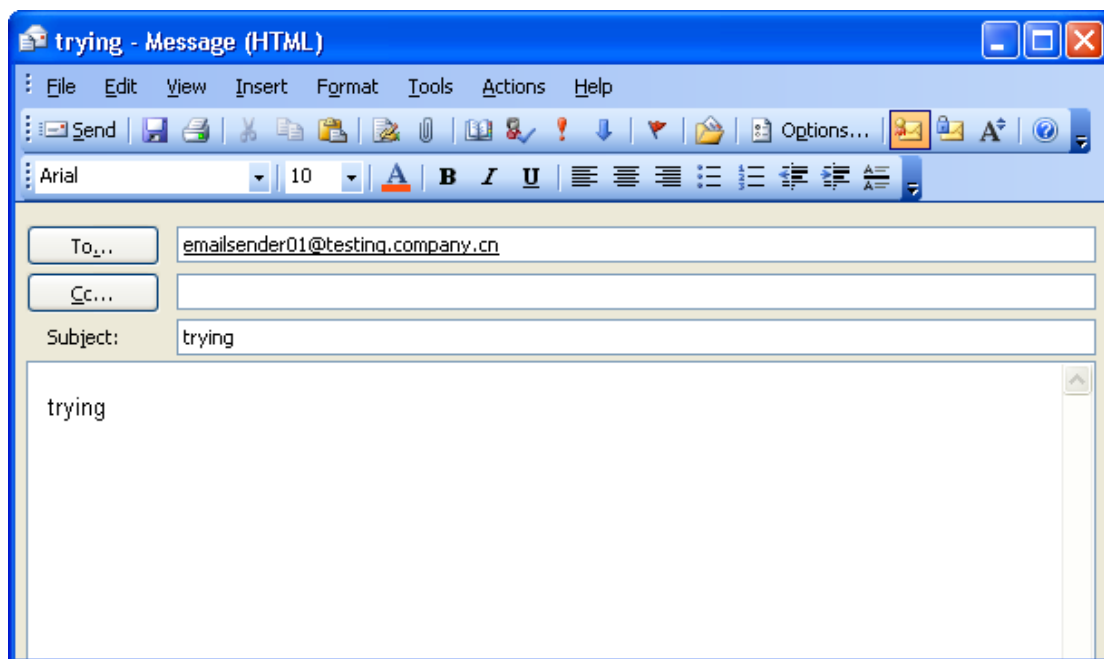
- d) Click “Setting...”
- e) Click “Choose”
- f) Select the EmailSender01’s certificate



- g) Click "OK"
- h) Select "Hash Algorithm:" as "MD5"



- i) Click "OK"
 - j) Click "Apply"
 - k) Click "OK"
3. Now you can use Microsoft Outlook 2003 to send a signed email to yourself (for illustration purpose)



4. When you received a signed email, you can reply with a signed and encrypted email