Digital Certificates – From Concept to Implementation
Part 6 (Hands-on Lab)

Session FD8
June 20th 2011

Wai Choi, CISSP
IBM Corporation
RACF/PKI Development
Poughkeepsie, NY

e-mail: wchoi@us.ibm.com

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- CICS*
- DB2*
- IBM*
- IBM (logo)*
- OS/390*
- RACF*
- Websphere*
- z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Identrus is a trademark of Identrus, Inc

VeriSign is a trademark of VeriSign, Inc

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Objectives of this Lab

At the end of this lab, you will be able to

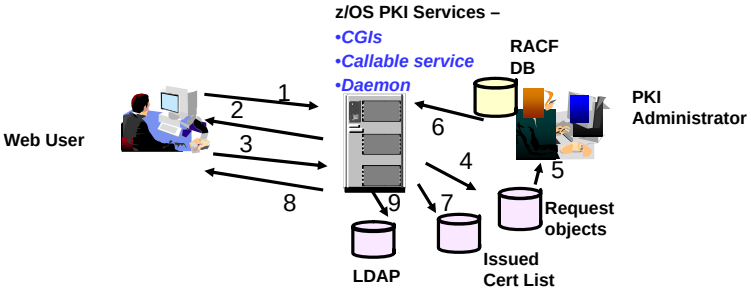
- Submit and approve a certificate request for
  - A certificate with key pair generated by the browser – EX 1
  - A certificate with key pair generated by PKI Services – EX 2
  - A certificate with key pair generated on a z/OS server – EX 3
- View the installed certificate from the IE broswer – EX 4
- Revoke/Suspend a certificate – EX 5
- Check the certificate status – EX 6
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)
- Customize PKI Services – EX 7
  - Configuration file – pkiserv.conf
  - Template file – pkiserv.tmpl

Background information

- PKI Services is an application to generate and manage certificates.

z/OS PKI Services Process Flow – a simplified sample view

1. User contacts PKI Services to request for certificate
2. CGI constructs a web page for user to input information
3. CGI packages all the info and send to the callable service
4. Callable service calls the daemon to generate the request object and put it in the Request objects DB
5. Administrator approves the request through the administrator web page
6. CGI calls callable service which in turn calls the daemon to create the certificate, sign with the CA key in the RACF DB
7. Certificate is placed in the Issued Cert List DB
8. User retrieves the certificate
9. Certificate is posted to LDAP



- Configuration is done through 3 files – pkiserv.envars, pkiserv.conf, pkiserv.tmpl.
- In z/OS V1R8, we support multiple instances of PKI Services running on the same LPAR. It is this feature that makes this lab possible since each of you can experiment with your own set up.
- Each user will have his own Certificate Authority (CA) Domain with its CA certificate issued by a Master CA with subject name ‘OU=Demo Customer Design Centre Certificate Authority,O=TEST,C=US’
- The users’ CA certificates are named ‘CN=Sharb01CA,OU=Test,O=The Sharb01 Firm’, ‘CN=Sharb02CA…’, ‘CN=Sharb03CA…’ etc.

- This is the partial content of a sample **pkiserv.envars** file
- It sets up the environment variables for the CA Domain name and the location of the PKI Services configuration file, pkiserv.conf

```
…
# When running as a CA Domain, set the CA Domain name by assigning
# desired value to the _PKISERV_CA_DOMAIN variable.
# Note: The first eight characters must be unique.
#
# example: _PKISERV_CA_DOMAIN=WebAppCA
_PKISERV_CA_DOMAIN=SHARB01
#
# Configuration File location and Message configuration Options
#
_PKISERV_CONFIG_PATH=/sharelab/sharb01/pkilab
_PKISERV_MSG_LOGGING=stdout_logging
_PKISERV_MSG_LEVEL=*.w
…
```

- This is the partial content of a sample **pkiserv.conf** file
- It specifies the names of the VSAM datasets used as the PKI Services databases
- It contains the time intervals for certain tasks to perform
- It has the global information needed to be in the certificates in all kinds of templates, eg. The CRL Distribution Point location
- **Re-starting PKI Services is needed for any changes to this file**

```
…
# Data set name of the VSAM request (object store) base CLUSTER
ObjectDSN='pkisrvd.vsam.ost'
# Data set name of the VSAM issued certificate list (ICL) base CLUSTER
ICLDSN='pkisrvd.vsam.icl'
# How often to turn approved requests into certificates
CreateInterval=1m
# How often to create the CRL
TimeBetweenCRLs=10m
# CRL distribution point name
CRLDistName=CRL
# CRL distribution point extension containing the location
CRLDistURI1=http://mvs1.centers.ihost.com:8041/Sharb01/crls/
# Is OCSP responder enabled?
OCSPType=basic
…
```

- This is the partial content of a sample **pkiserv.tmpl** file
- It contains HTML like tags
- There are different types of templates for certificates with certain usage
- The certificate information needed are customizable per template basis, verses those global information specified in pkiserv.conf
- Under the <CONTENT> section is a list of fields that you expect user to input when a request is made
- Under the <CONSTANT> section is a list of hard coded fields
- **The change to this file will be picked up dynamically**

```
<TEMPLATE NAME=1-Year PKI SSL Browser Certificate>
<CONTENT>
%%Requestor (optional)%%
%%NotifyEmail (optional)%%
%%PassPhrase%%
%%Mail (optional)%%
%%CommonName%%
…
</CONTENT>

<CONSTANT>
 %%OrgUnit=Class 1 Internet Certificate CA%%
 %%Org=The Sharbxx Firm%%
 %%KeyUsage=handshake%%
 %%ExtKeyUsage=clientauth%%
 %%AuthInfoAcc=OCSP,URL=http://mvs1.centers.ihost:8041/Sharb01/public-
   cgi/caocsp%%
 %%NotBefore=0%%
 %%NotAfter=365%%
 …
</CONSTANT>
…
</TEMPLATE>
```

Exercise Instructions:

Note 1: All the references of xx refer to the number part of your assigned id, eg. 01 if your assigned ID is sharb01)

Note 2: You will play both roles as an end user and as an administrator in the lab. The tasks performed by an end user and an administrator are indicated by a male  ***and female***  ***icon respectively.***

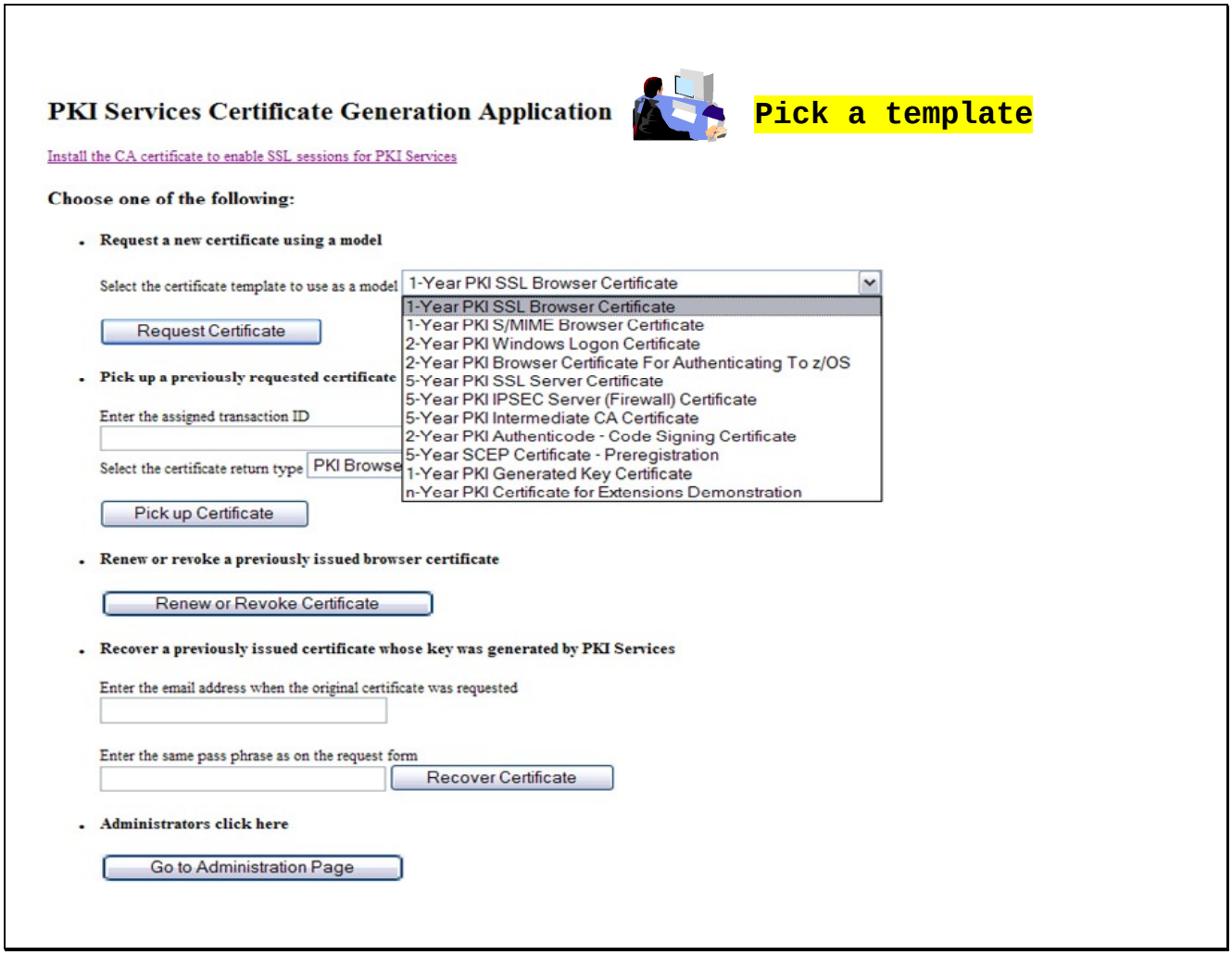
Note 3: If you are not familiar with the MVS/OMVS system, you may refer to Appendix 1 to get some hints.

Exercise 1 - Request a certificate with key pair generated from the browser

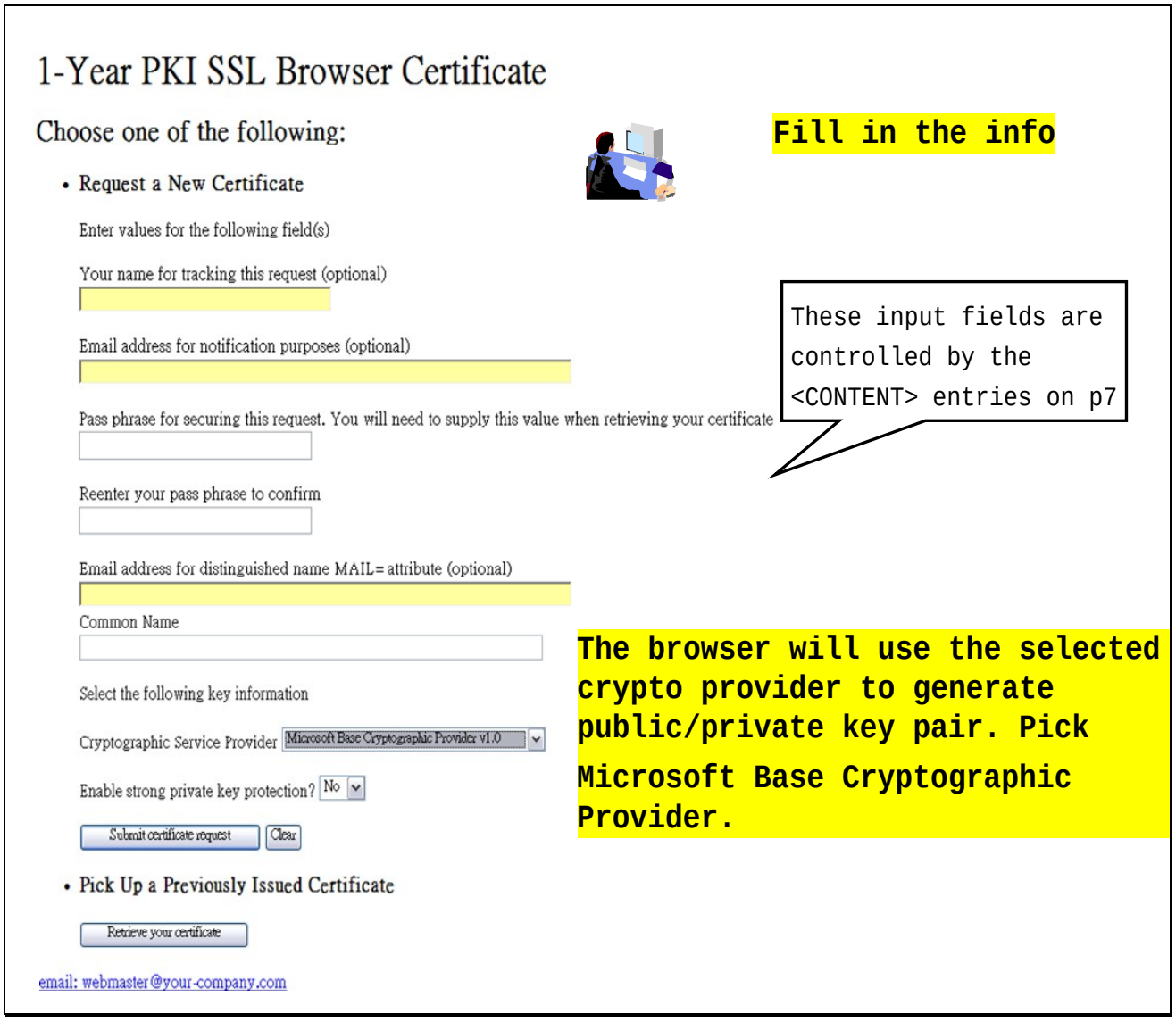
A. Submit a request

- Open an Internet Explorer browser to go to the url (change xx to the number part of your assigned id): http://mvs1.centers.ihost.com:8041/Sharbxx/public-cgi/camain.rexx
- Click on the “Install the CA certificate to enable SSL sessions for PKI Services’ link so that SSL can be performed for the subsequent actions

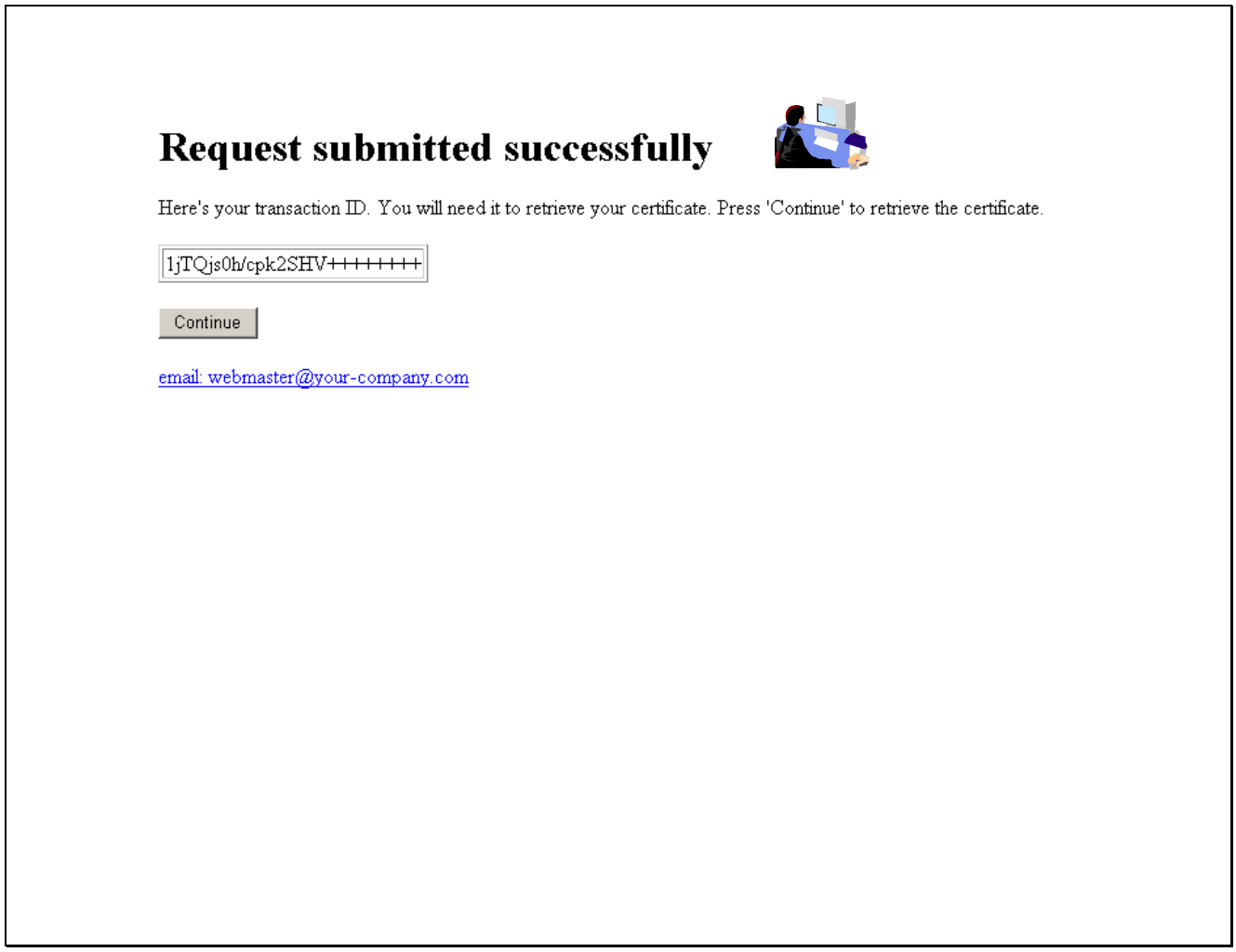
- Choose the ‘1 Year PKI SSL Browser Certificate’ template
- Click ‘Request Certificate’



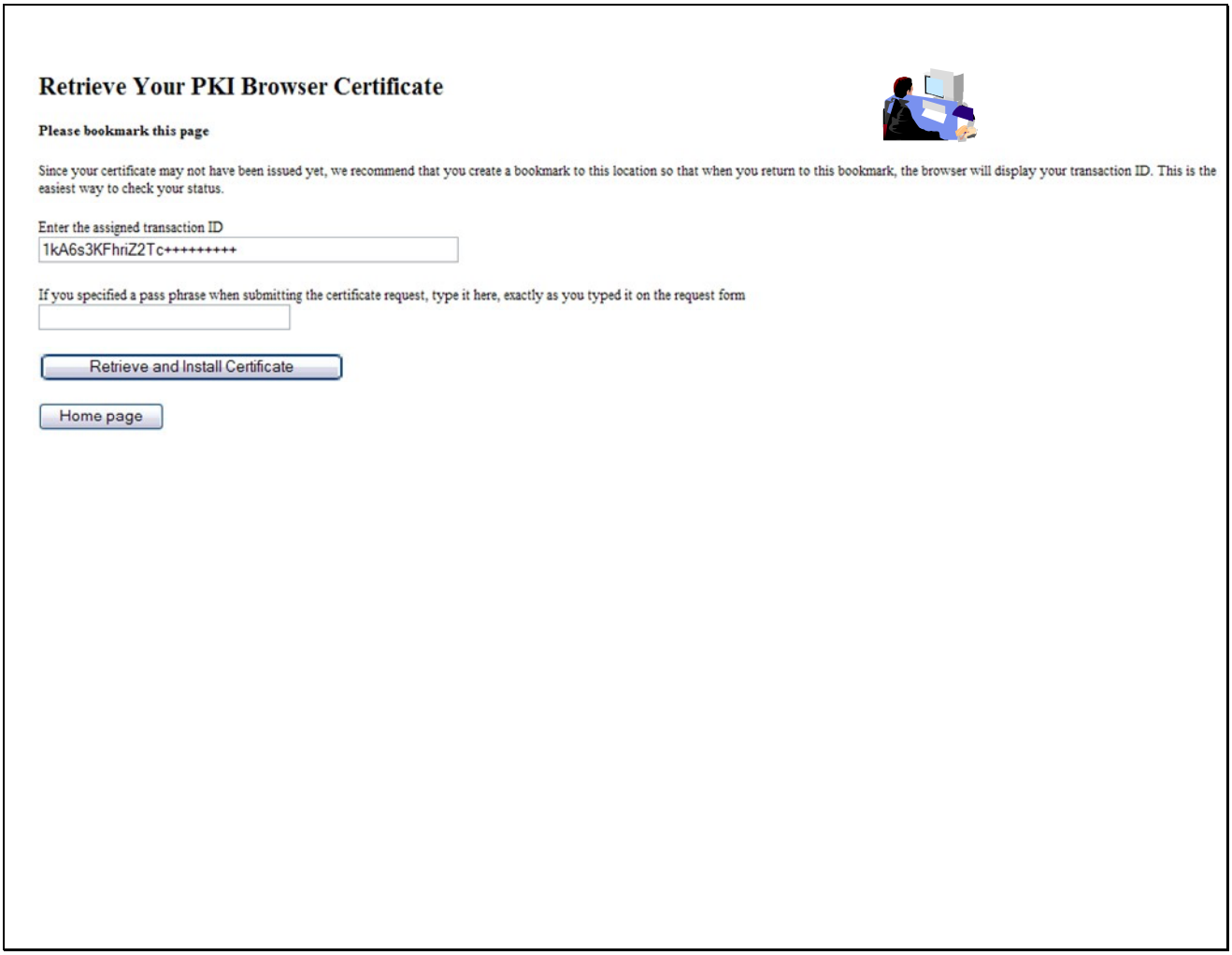
- Fill in the values for the certificate request information
- Select Microsoft Base Cryptographic Provider to generate key pair
- Click on ‘Submit certificate request’



- Save this transaction ID into some file (eg. Open notepad and paste it)
- Click ‘Continue’



- Enter the passphrase that you entered when you made the request
- Click on ‘Retrieve and Install Certificate’ (It will fail, see next page)



- You will find the request was not successful because it is waiting for the administrator to approve it

Request was not successful

Please correct the problem or report the error to your Web admin person

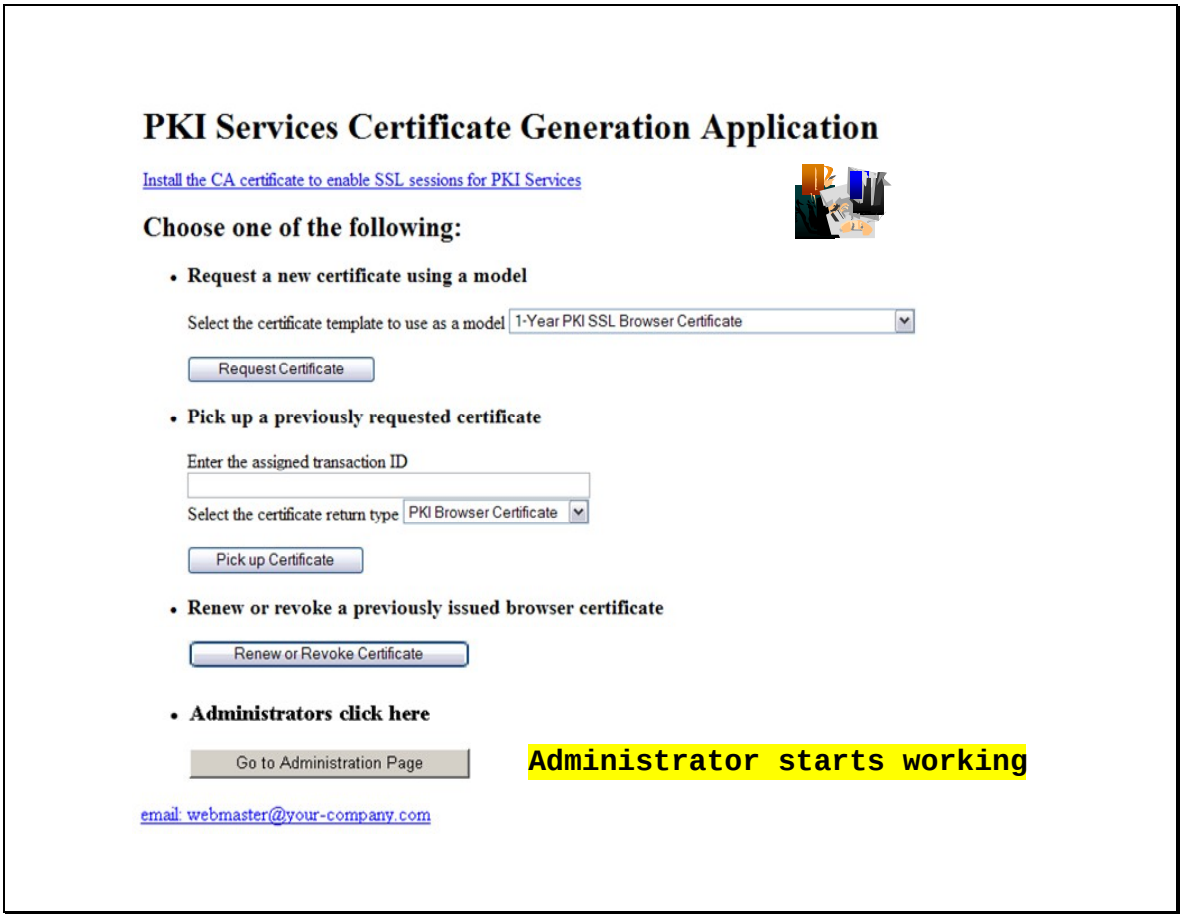
```
IKYI002I SAF Service IRRSPX00 Returned SAF RC = 8 RACF RC = 8 RACF RSN = 56
Request is still pending approval or yet to be issued
```

email: webmaster@your-company.com

Certificate not ready

B. Approve the certificate request

- Open another Internet Explorer browser to go to the same url (change xx to the number part of your assigned id): http://mvs1.centers.ihost.com:8041/Sharbxx/public-cgi/camain.rexx
- This time you act as an administrator, click on the 'Go to Administration Page'
- When prompted for userid and password, use your assigned sharbxx userid and password



- Choose ‘Show requests pending approval’ and click on ‘Find Certificates or Certificate Requests’

PKI Services Administration

Choose one of the following:

- **Work with a single certificate request**

  Enter the Transaction ID:

  [ ] Process Request

- **Work with a single issued certificate**

  Enter the Serial Number:

  [ ] Process Certificate

- **Specify search criteria for certificates and certificate requests**

Certificate Requests	Issued Certificates
○ Show all requests	○ Show all issued certificates
◉ Show requests pending approval	○ Show revoked certificates
○ Show approved requests	○ Show suspended certificates
○ Show completed requests	○ Show expired certificates
○ Show rejected requests	○ Show active certificates (not expired, not revoked, not suspended)
○ Show rejections in which the client has been notified	○ Show disabled certificates (suspended or revoked, not expired)
○ Show preregistered requests	○ Show active, automatic renewal enabled certificates
	○ Show active, automatic renewal disabled certificates
	○ Show active, not renewable certificates

Additional search criteria (Optional)

Requestor's name [ ]

Show recent activity only [(Not Selected) ▾]

Show certificates that will expire [(Not Selected) ▾] (Only applicable to active certificates when recent activity is not selected)

[Find Certificates or Certificate Requests]

- This shows the request summary
- Click on the Trans ID link to view the request details

Certificate Requests

Request summary info

The following certificate requests matched the search criteria specified:

All ☑	Requestor	Certificate Request Information	Status	Dates
☑	jan27a	**Trans ID:** 1kA$sDZcZjkZ2Tc+++++++++ **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Pending Approval	**Created:** 2011/01/27 **Modified:**2011/01/27

Choose one of the following:

- **Click on a transaction ID to see more information or to modify, approve, reject, or delete requests individually**
- **Select and take action against multiple requests at once**

Action Comment (Optional)

Approve - Approve without modification all requests selected above that are "Pending Approval"

Reject - Reject all requests selected above that are "Pending Approval"

Delete - Delete all requests selected above

Respecify Your Search Criteria

Home Page

- Notice that Subject name value has values coming from both the user input (the CN value) and the hard coded value in pkiserv.tmpl under the <CONSTANT> section (the OU and O values)
- Click on ‘Approve Request with Modifications’

- As an administrator, you can modify the info that the user input before you approve the request
- After the modification, if any, click on 'Approve with specified modifications'

Modify and Approve Request

Requestor	Request Information	Dates
jan27a	**Trans ID:**1kA8sDZcZjkZ2Tc+++++++++ **Template:**1-Year PKI SSL Browser Certificate **Subject:**CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	**Created:** 2011/01/27 **Modified:**2011/01/27

You may modify the following fields by providing new values. To remove a field simply blank it out or de-select it.

- **Subject Distinguished Name:**

Common Name (optional)
jan27a

Organizational Unit (optional)
Class 1 Internet Certificate CA

Organizational Unit (optional)

Organization (optional)
The Sharb01 Firm

Country
US

Page primed with requested info. Administrator can change them if necessary.

- **Extensions:**

Indicate the key usage for the certificate (optional)
Protocol handshaking, e.g. SSL (digitalSignature, keyEncipherment)
Certificate and CRL signing (keyCertSign, cRLSign)
Document signing (nonRepudiation)
Data encryption (dataEncipherment)

Indicate the extended key usage the certificate
Server side authentication (serverAuth)
Client side authentication (clientAuth)
Code signing (codeSigning)
Email protection (emailProtection)

HostIdMappings Extension value(s) in subject-id@host-name form (optional)

HostIdMappings Extension value(s) in subject-id@host-name form (optional)

HostIdMappings Extension value(s) in subject-id@host-name form (optional)

HostIdMappings Extension value(s) in subject-id@host-name form (optional)

- **Validity Period:**

Date certificate becomes valid	Date certificate expires (at end of day)
2011 1 27	2012 1 26

Automatic Renewal: Not set

Action Comment (Optional)

Approve with specified modifications

Reset Modified Fields

- You will get a confirmation that the request is approved
- Click on ‘Administration Home Page’ to take a look at the request status

- Choose ‘Show all requests’ and click on ‘Find Certificates or Certificate Requests’

To display all the requests

Choose one of the following:

- **Work with a single certificate request**

  Enter the Transaction ID:

  [ ] Process Request

- **Work with a single issued certificate**

  Enter the Serial Number:

  [ ] Process Certificate

- **Specify search criteria for certificates and certificate requests**

Certificate Requests	Issued Certificates
(•) Show all requests	( ) Show all issued certificates
( ) Show requests pending approval	( ) Show revoked certificates
( ) Show approved requests	( ) Show suspended certificates
( ) Show completed requests	( ) Show expired certificates
( ) Show rejected requests	( ) Show active certificates (not expired, not revoked, not suspended)
( ) Show rejections in which the client has been notified	( ) Show disabled certificates (suspended or revoked, not expired)
( ) Show preregistered requests	( ) Show active, automatic renewal enabled certificates
	( ) Show active, automatic renewal disabled certificates
	( ) Show active, not renewable certificates

Additional search criteria (Optional)

Requestor's name [ ]

Show recent activity only [(Not Selected) ▾]

Show certificates that will expire [(Not Selected) ▾] (Only applicable to active certificates when recent activity is not selected)

[Find Certificates or Certificate Requests]

- Notice that the status of the request became ‘Approved’. If the certificate has been created, a serial number will also be displayed.
- Click on ‘Re-specify Your Search Criteria’ to check on the certificate

Certificate Requests

The following certificate requests matched the search criteria specified:

All ☑	Requestor	Certificate Request Information	Status	Dates
☑	jan27a	**Trans ID:** 1kA8sDZcZjkZ2Tc+++++++++ **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Approved **Serial #:** 3	**Created:** 2011/01/27 **Modified:**2011/01/27

Choose one of the following:

- **Click on a transaction ID to see more information or to modify, approve, reject, or delete requests individually**
- **Select and take action against multiple requests at once**

Action Comment (Optional)

Delete - Delete all requests selected above

Respecify Your Search Criteria

Home Page

Request is approved. The presence of a serial number indicates the certificate is created.

- This time choose ‘Show all issued certificates’ and click on ‘Find Certificates or Certificate Requests’

Choose one of the following:

- **Work with a single certificate request**

Enter the Transaction ID:

[ ] Process Request

- **Work with a single issued certificate**

To display all the certificates

Enter the Serial Number:

[ ] Process Certificate

- **Specify search criteria for certificates and certificate requests**

Certificate Requests	Issued Certificates
○ Show all requests	◉ Show all issued certificates
○ Show requests pending approval	○ Show revoked certificates
○ Show approved requests	○ Show suspended certificates
○ Show completed requests	○ Show expired certificates
○ Show rejected requests	○ Show active certificates (not expired, not revoked, not suspended)
○ Show rejections in which the client has been notified	○ Show disabled certificates (suspended or revoked, not expired)
○ Show preregistered requests	○ Show active, automatic renewal enabled certificates
	○ Show active, automatic renewal disabled certificates
	○ Show active, not renewable certificates

Additional search criteria (Optional)

Requestor's name [ ]

Show recent activity only [(Not Selected) ▾]

Show certificates that will expire [(Not Selected) ▾] (Only applicable to active certificates when recent activity is not selected)

[Find Certificates or Certificate Requests]

- Similar info as in the request. The status of the certificate is ‘Active’ when it is created
- Click on the Serial # link to display certificate details

Issued Certificates

The following issued certificates matched the search criteria specified:

All ☑	Requestor	Certificate Information	Status	Key archived	Dates
☑	jan27a	**Serial #:** 3 **Template:**1-Year PKI SSL Browser Certificate **Subject:** CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Active	No	**Created:** 2011/01/27 **Modified:**2011/01/27

Choose one of the following:

Certificate summary info

- **Click on a serial number to see more information or to perform action on a single certificate**
- **Select and take action against multiple certificates at once**

Action Comment (Optional)

Revoke | No Reason | - Revoke all selected active certificates

Suspend - Suspend all selected active certificates

Delete - Delete all selected certificates

Respecify Your Search Criteria

Home Page

This page can also be reached from the Serial # link appeared on the Certificate Requests page (p. 22)

Where do the values of Validity, Usage, Extended Usage come from? User input, pkiserv.tmpl or pkiserv.conf?

Single Issued Certificate

Certificate detail info

Requestor:	jan27a	**Created:**	2011/01/27
Status:	Active	**Modified:**	2011/01/27
Template:	1-Year PKI SSL Browser Certificate	**PassPhrase:**	a
Serial #:	3		
Previous Action Comment:	Issued certificate		

Subject:	CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US
Issuer:	CN=Sharb01 CA,OU=Test,O=The Sharb01 Firm,C=US
Validity:	2011/01/27 00:00:00 - 2012/01/26 23:59:59
Usage:	handshake(digitalSignature, keyEncipherment)
Extended Usage:	clientauth

Action to take:

Action Comment (Optional)

Revoke Certificate | No Reason

Suspend Certificate

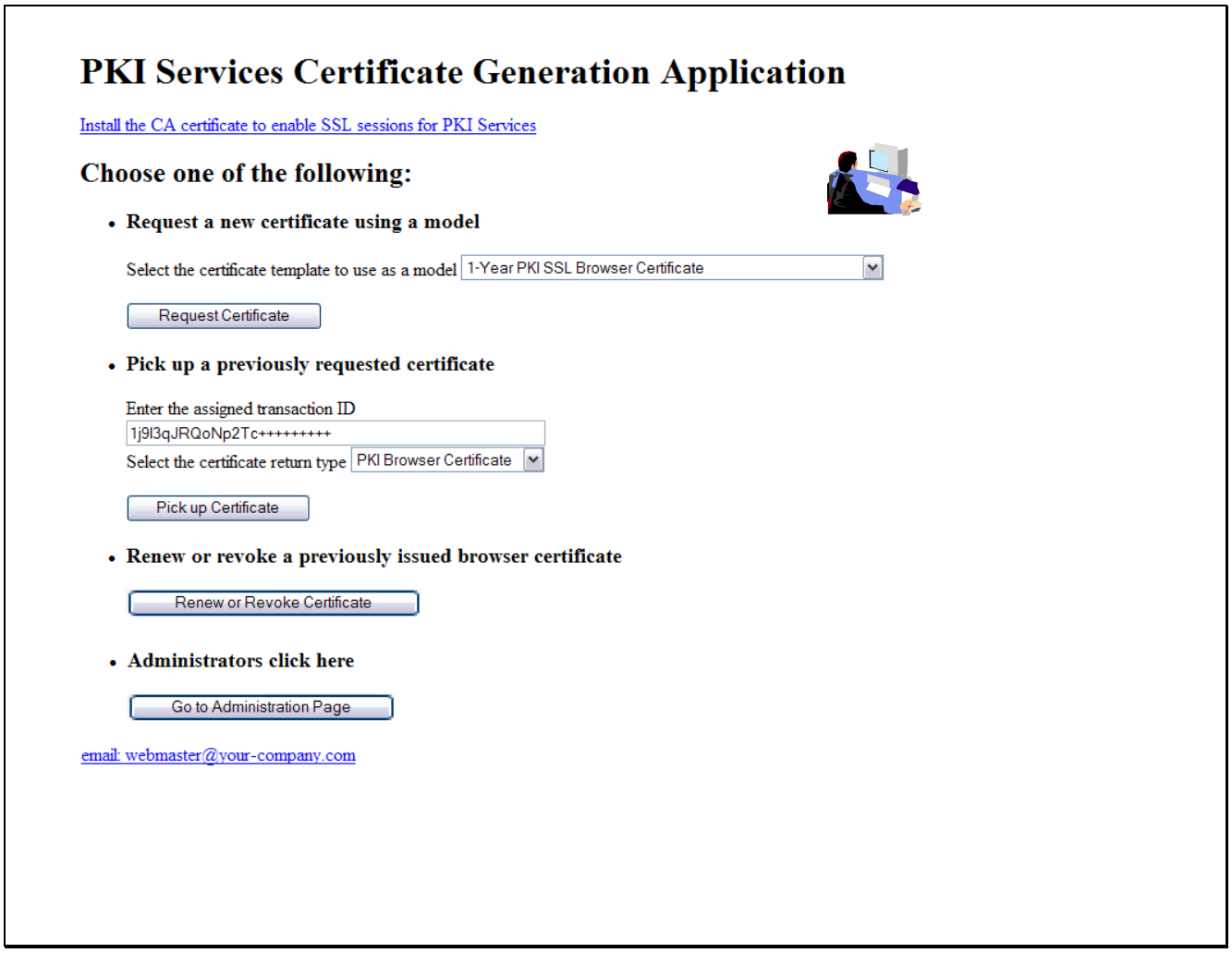
Disable Automatic Renewal

Enable Automatic Renewal

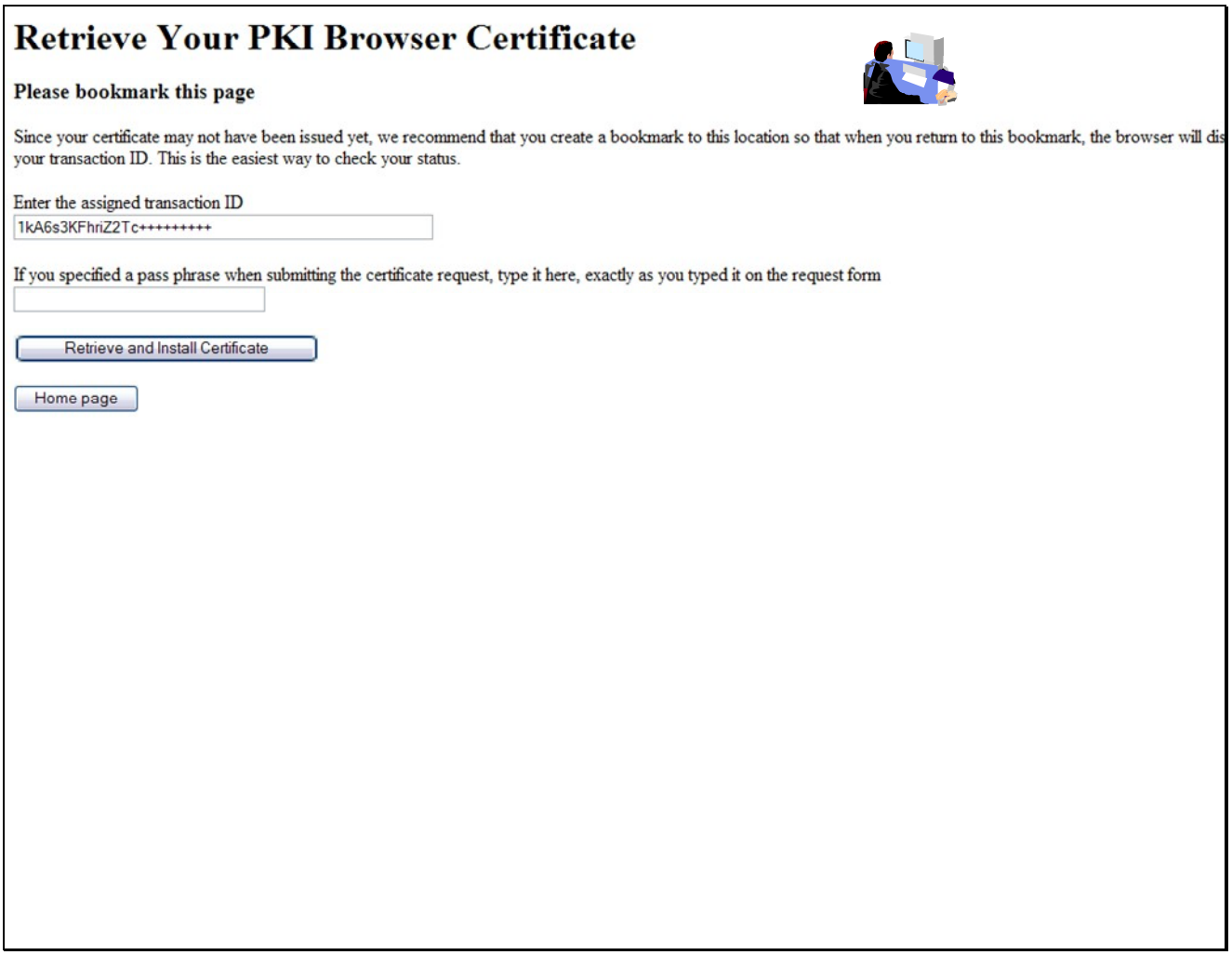
Delete Certificate

C. Pick up the certificate

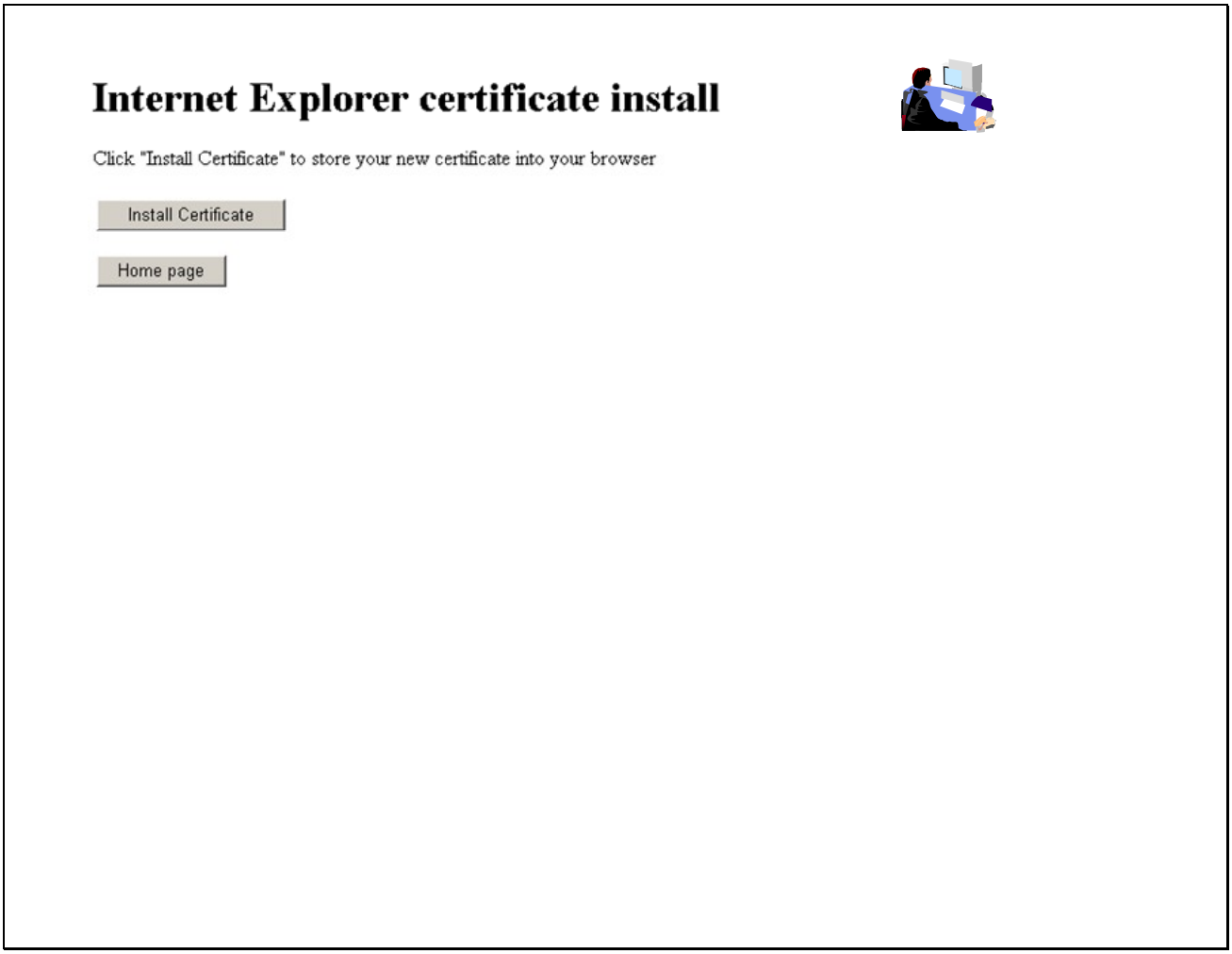
- Switch back to the user browser window and go to this page again (p.9)
- Enter the transaction ID, select ‘PKI Browser Certificate’ as the certificate return type and click on ‘Pick up Certificate’



- Enter the password that you entered when you made the request and click ‘Retrieve and Install Certificate’



- Click ‘Install Certificate’
- Answer ‘Yes’ when you are asked whether you want to install the certificate(s)

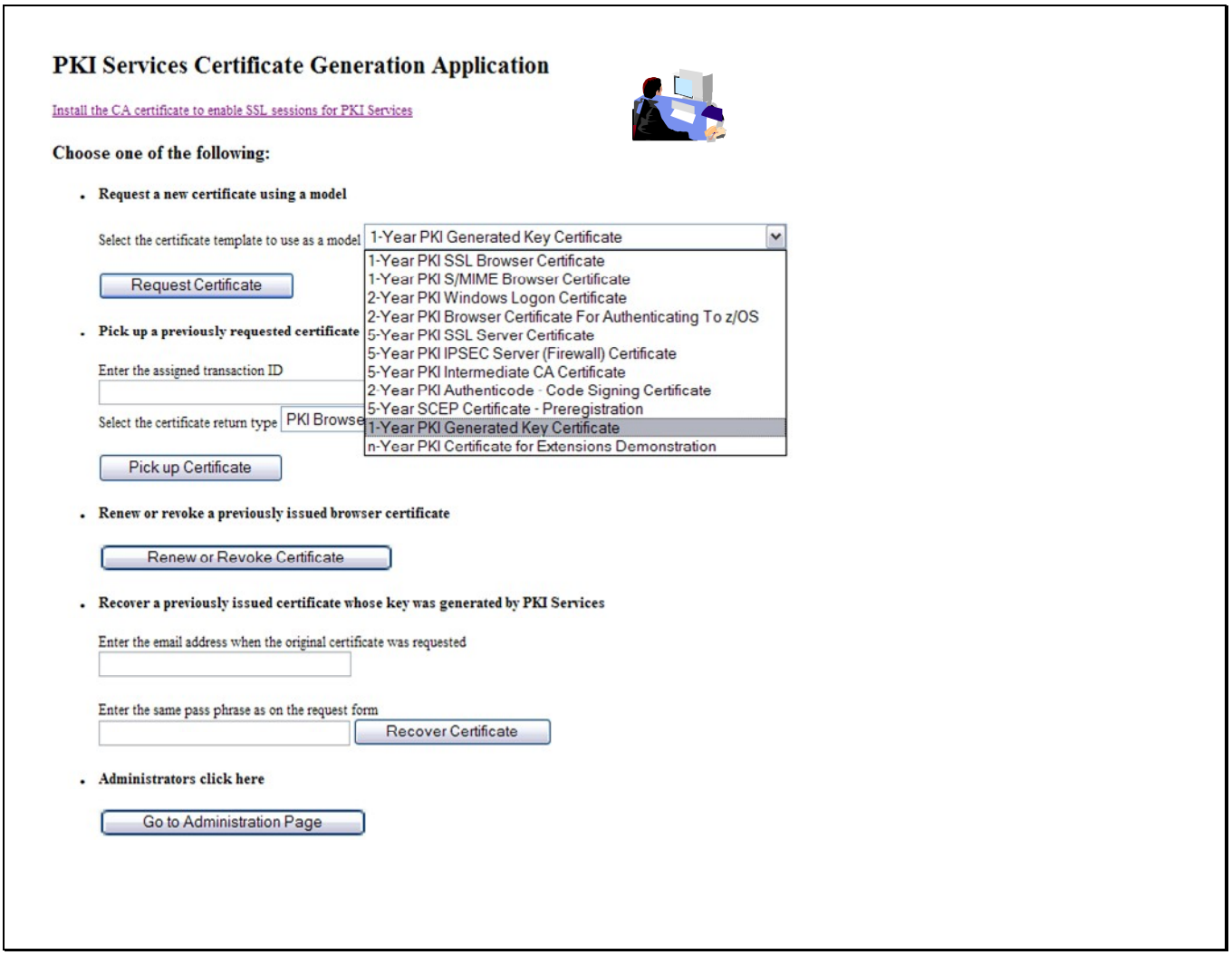


- You will look at the certificate you installed from the browser in Exercise 4.

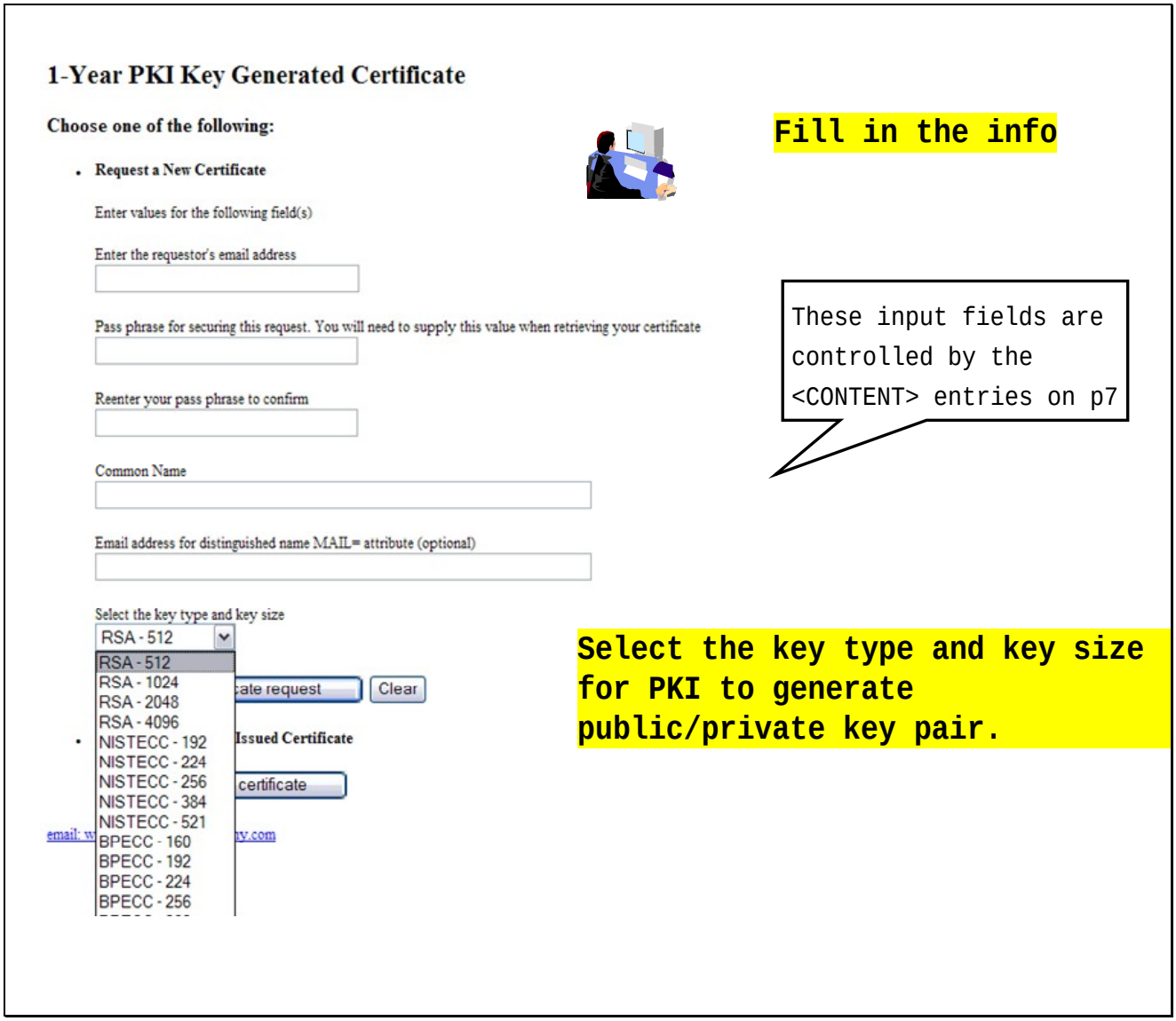
Exercise 2 - Request a certificate with key pair generated by PKI Services

A. Submit a request

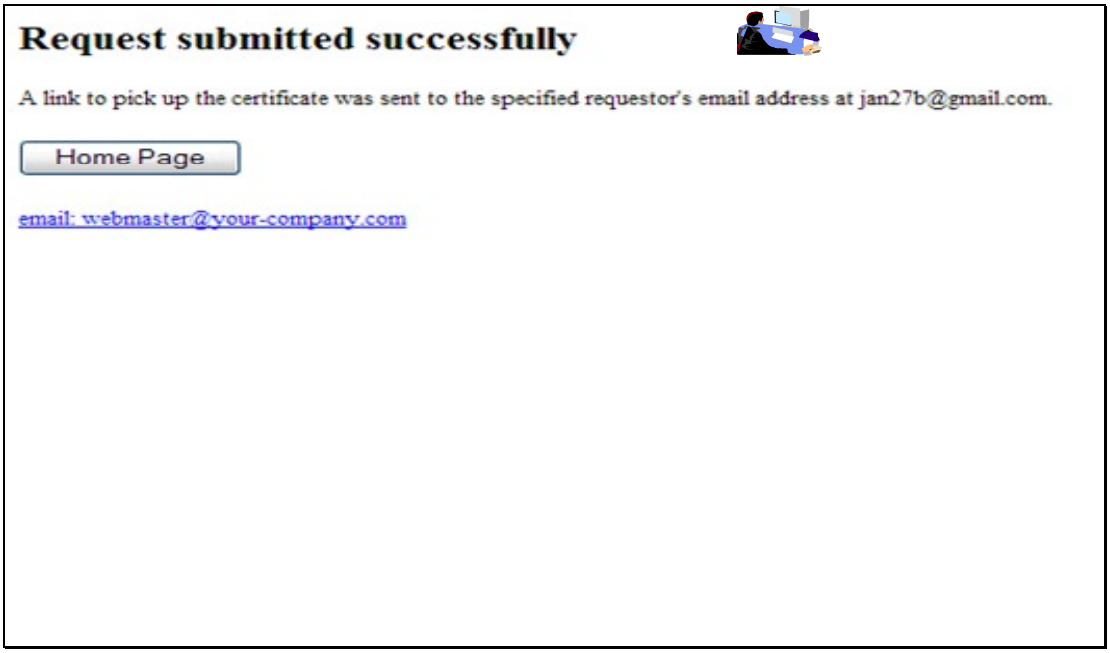
- Go to the main page again as in Exercise 1 (change xx to the number part of your assigned id): http://mvs1.centers.ihost.com:8041/Sharbxx/public-cgi/camain.rexx
- Choose the '1 Year PKI Generated Key Certificate' template
- Click 'Request Certificate'



- Fill in the values for the certificate request information
- Select the key type and key size for PKI to generate key pair
- Click on ‘Submit certificate request’



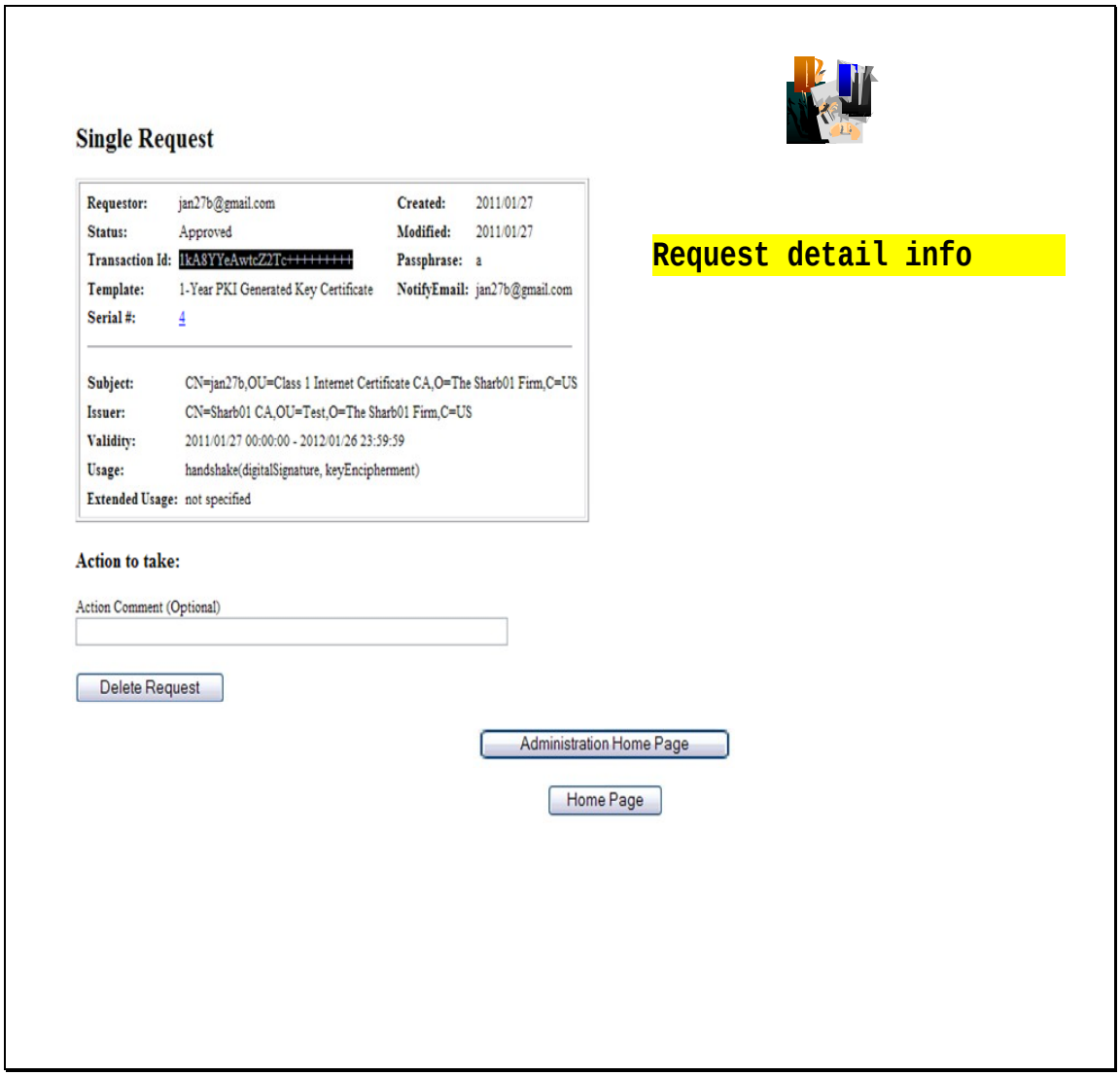
- Unlike the browser generated key certificate, you do not get back a transaction ID on this page



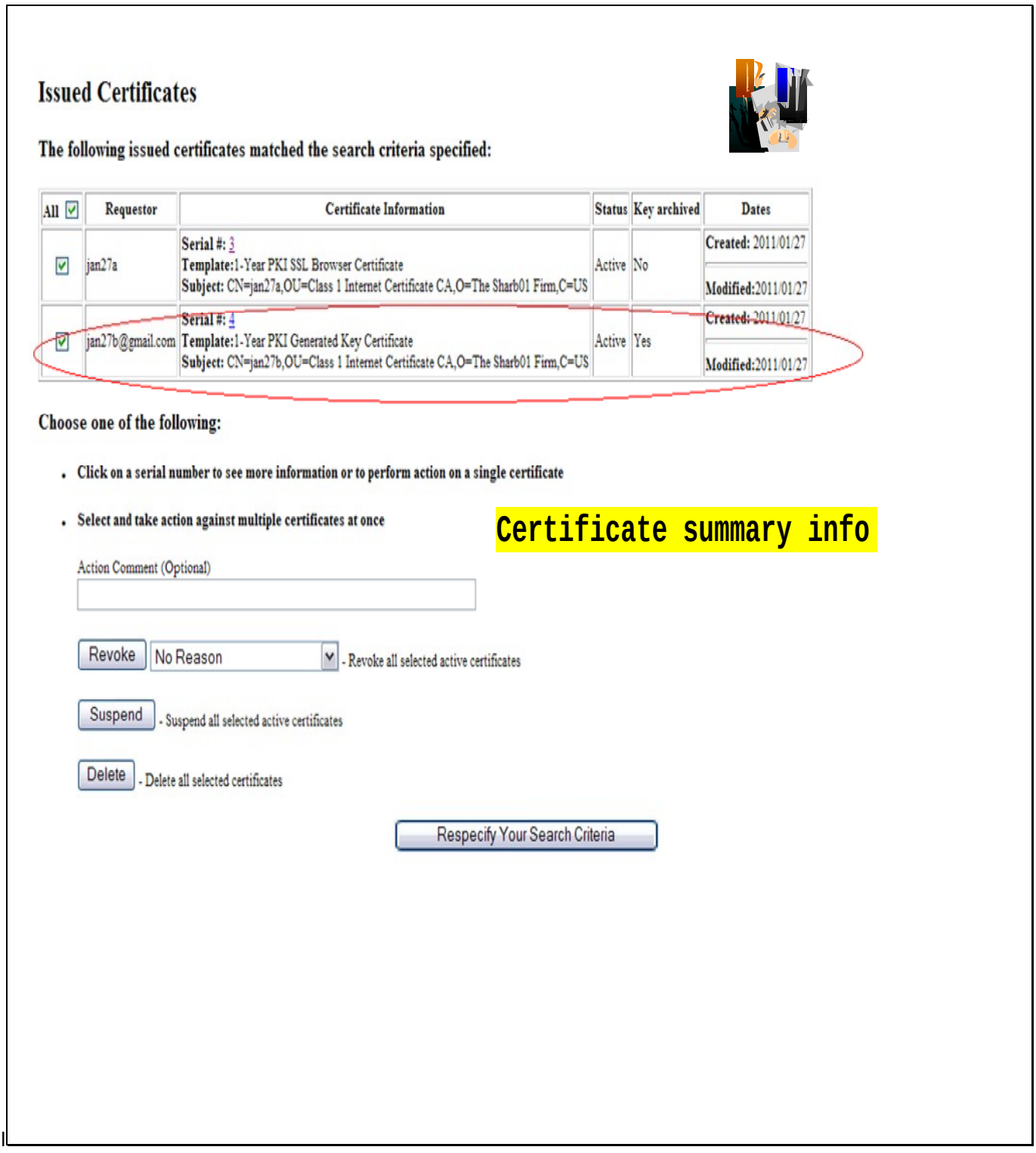
- Note: The lab system won't allow the sending out of email. We will use the administrator role to get the transaction ID to retrieve the certificate.

B. Approve the request

- Go to the administrator's page to approve the request the same way you just did as in Exercise 1
- Save the Transaction Id from the request detail page. (You will need it to retrieve the certificate in Step C later.)

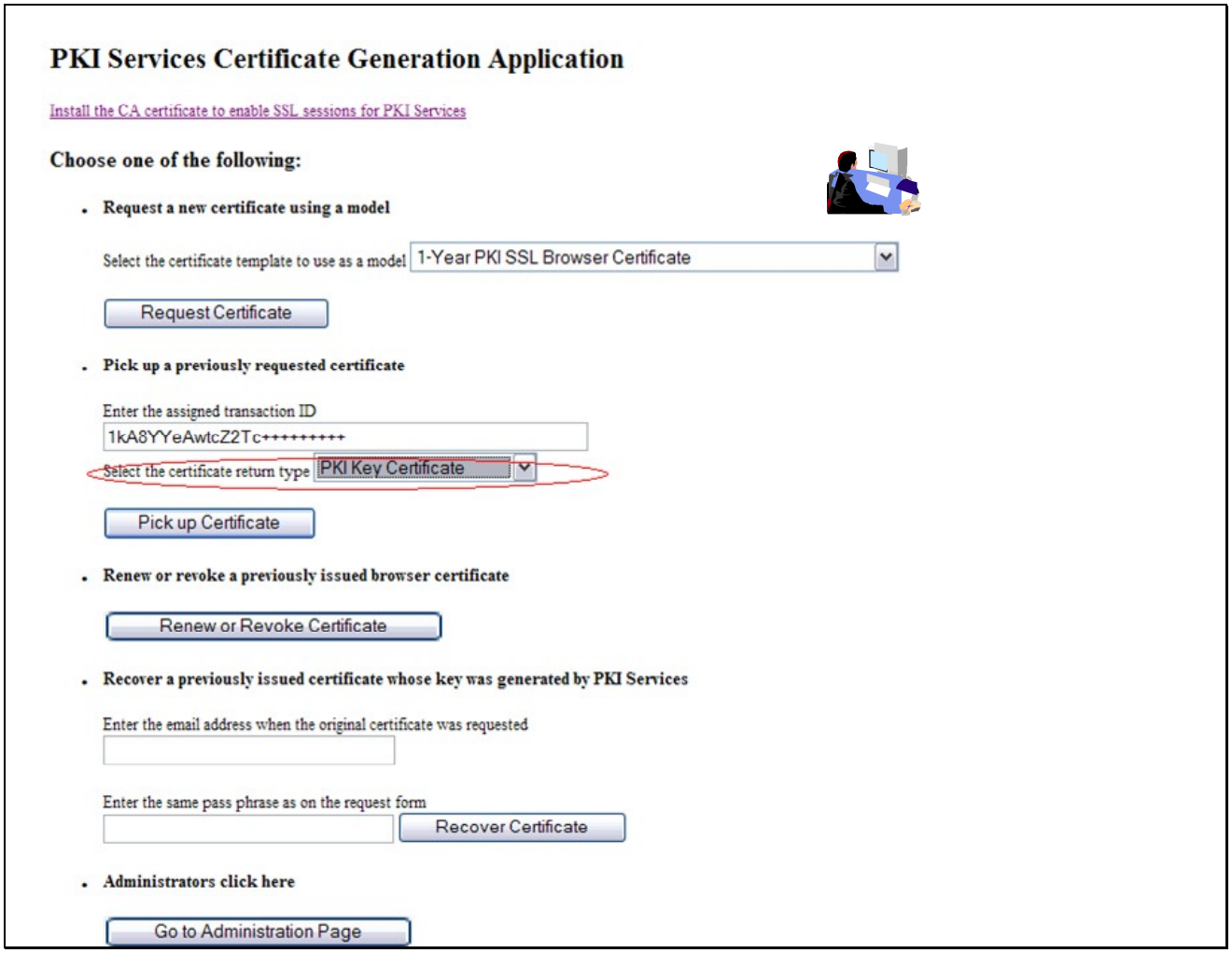


- Notice that the Key archived column for this certificate is Yes since the key pair was generated by PKI Services and PKI keeps a copy of it.

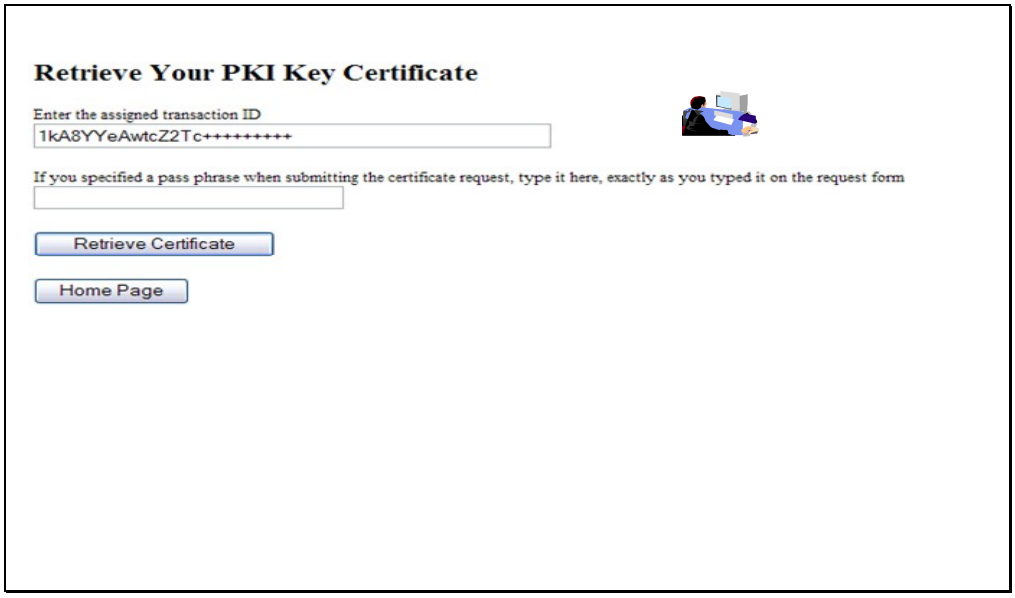


C. Pick up the certificate

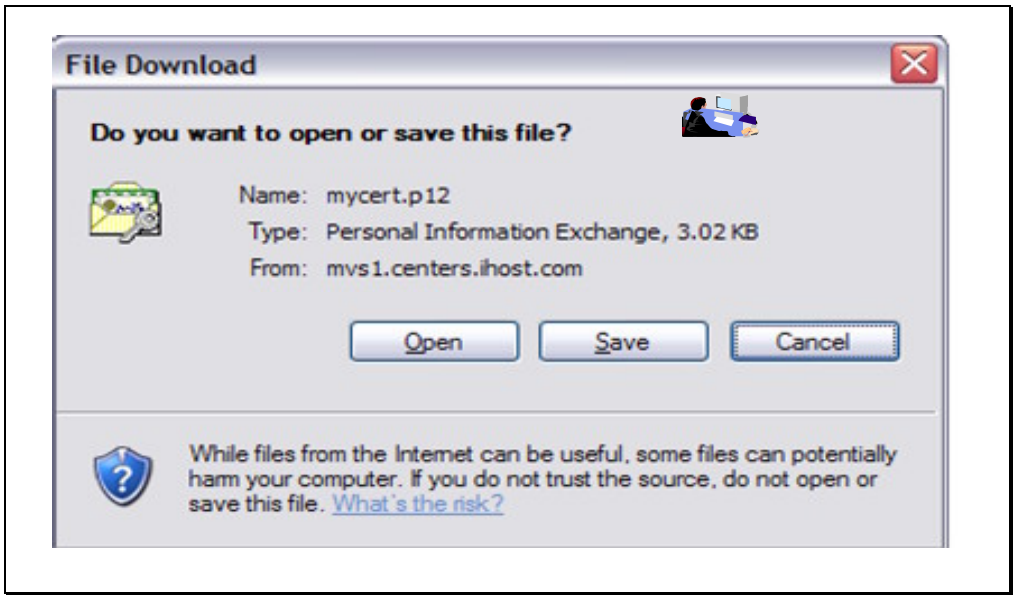
- Go back to the user home page to retrieve the PKI key generated certificate. Paste the Transaction ID and select ‘PKI Key Certificate’ as the certificate return type. Click on Pick up Certificate.



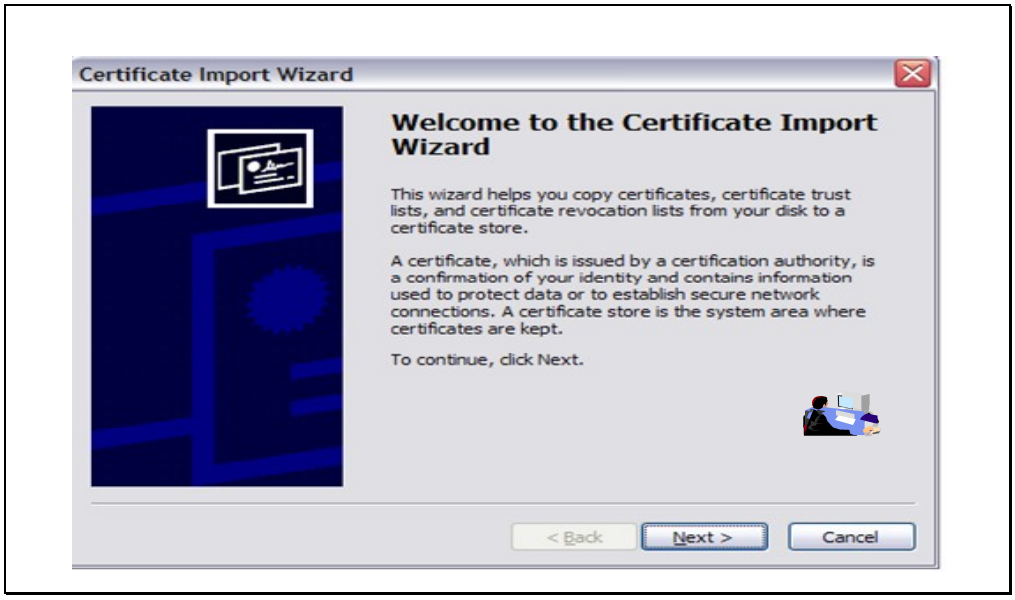
- Note: In real system, the end user will reach this page by clicking on the link sent to his email address
- Enter the pass phrase you entered when you made the request



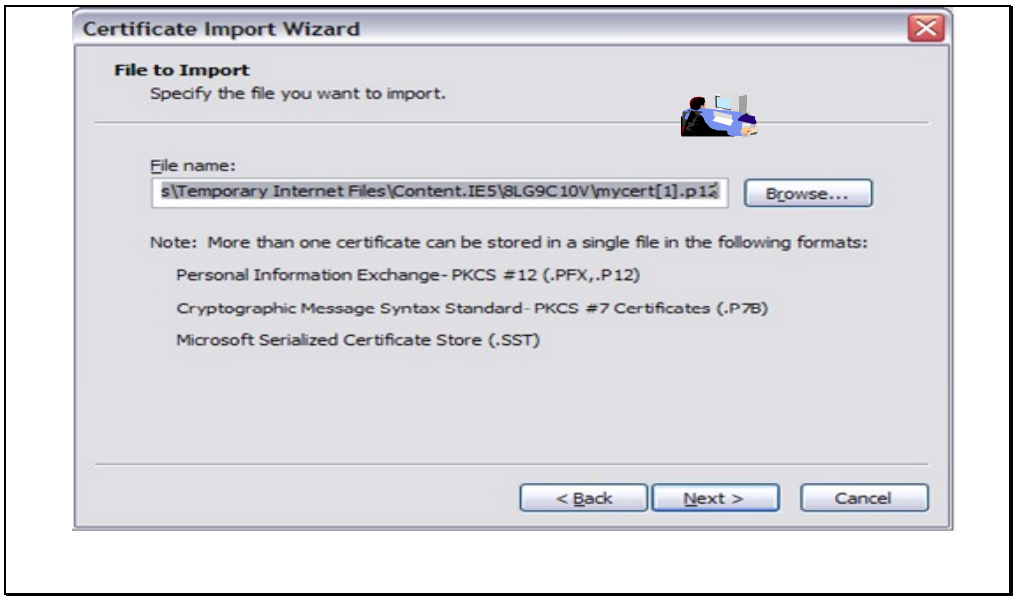
- Click Open.



- Click Next.

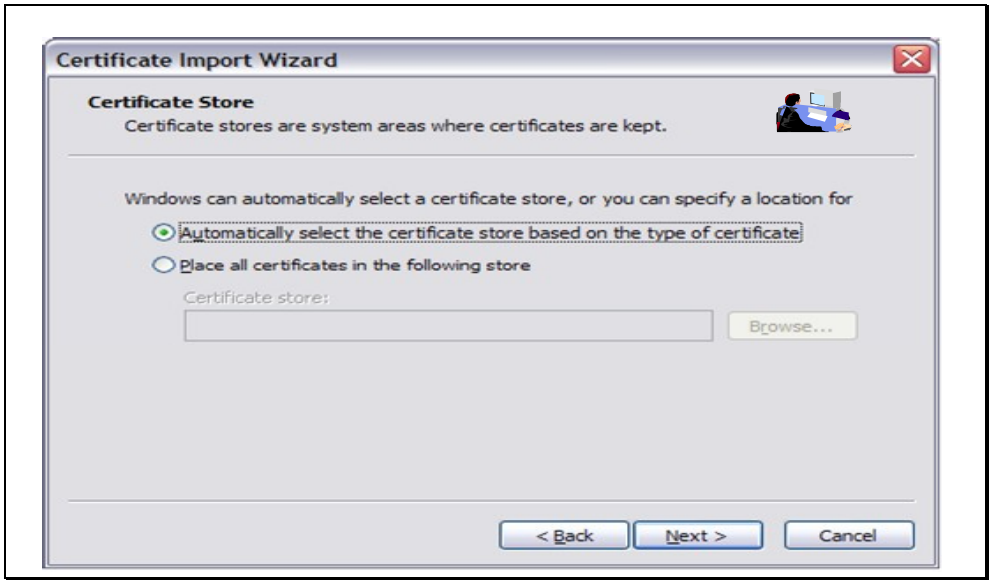


- Click Next.



- Enter the password and check the key as exportable.

- Click Next.



- Click Finish.

- You will look at the certificate you installed from the browser in Exercise 4.

Exercise 3 - Request a certificate with key pair generated on z/OS

A. Create a request 

- Log on the MVS system (See Appendix 1)
- Go to ISPF panel, enter option 6

```
File  Edit  View  Communication  Actions  Window  Help
------------ SHARE ISPF 5.9 SCROLLABLE PRIMARY OPTION MENU  ---------- S1
OPTION  ===> 6_

  D  Alternate Dialog ===> CMD(%????)
  D2 Alternate Dialog ===> PANEL(????)
                                                              More:
  The time is 12:30 p.m. on Tuesday, July 22, 2008 (2008.204)
  Your uid is SHARB01  dsn prefix is SHARB01   proc is SHARE    sys is S1

  0     SETTINGS     - Specify ISPF parameters
  1     VIEW         - View source data or output listing
  1P    VIEW-OE      - View/Browse files in the Open Edition file system
  2     EDIT         - Create or change source data
  2P    EDIT-OE      - Edit files in the Open Edition file system
  3     UTILITIES    - Perform utility functions
  3P    ISHELL-OE    - Open Edition ISPF shell
  4     FOREGROUND   - Invoke language processors in foreground
  5     BATCH        - Submit job for language processing
  6     COMMAND      - Enter TSO command, CLIST, or REXX exec
  7     DIALOG TEST  - Perform dialog testing
  8     LM UTILITIES - Perform library administrator utility functions
  9     IBM PRODUCTS - Additional IBM program development products
  10    SCLM         - Software Configuration and Library Manager
```

- From ISPF 6, enter the RACDCERT command to create a certificate request by 2 commands: (*Note: Values are case sensitive within quotes*)
    - RACDCERT id(Sharbxx) GENCERT SUBJECT(CN('MySSLCertxx')) WITHLABEL('MySSLCertxx')
    - RACDCERT id(Sharbxx) GENREQ(LABEL('MySSLCertxx')) DSN(myssl)

```
  Menu  List  Mode  Functions  Utilities  Help
 ------------------------------------------------------------------------
                              ISPF Command Shell
Enter TSO or Workstation commands below:

===> RACDCERT id(Sharbxx) GENCERT SUBJECT(CN('MySSLCertxx'))
   WITHLABEL('MySSLCertxx')
```

```
 Menu  List  Mode  Functions  Utilities  Help
                                ISPF Command Shell
Enter TSO or Workstation commands below:

===> RACDCERT id(Sharbxx) GENREQ(LABEL('MySSLCertxx')) DSN(myssl)
```

- PF3 to exit out option 6 and go to ISPF 3.4, hit enter

```
File  Edit  View  Communication  Actions  Window  Help
------------ SHARE ISPF 5.9 SCROLLABLE PRIMARY OPTION MENU  ---------- S1
OPTION  ===> 3.4

  D  Alternate Dialog ===> CMD(%????)
  D2 Alternate Dialog ===> PANEL(????)
                                                              More:      +
  The time is 12:45 p.m. on Tuesday, July 22, 2008 (2008.204)
  Your uid is SHARB01  dsn prefix is SHARB01   proc is SHARE    sys is S1

  0     SETTINGS     - Specify ISPF parameters
  1     VIEW         - View source data or output listing
  1P    VIEW-OE      - View/Browse files in the Open Edition file system
  2     EDIT         - Create or change source data
  2P    EDIT-OE      - Edit files in the Open Edition file system
  3     UTILITIES    - Perform utility functions
```

- enter ‘Sharbxx.myssl’ on the ‘Dsname Level’ input line and hit enter

```
 Menu  RefList  RefMode  Utilities  Help
                          Data Set List Utility
Option ===>
                                                              More:      +
   blank Display data set list            P Print data set list
       V Display VTOC information        PV Print VTOC information

Enter one or both of the parameters below:
   Dsname Level . . . SHARBxx.myssl
   Volume serial  . . ______
```

- Put letter ‘e’ next to ‘Sharbxx.myssl’
- Select its entire content by using the mouse. Click on Edit->Copy. This will be used to paste on the PKCS#10 Certificate Request box in the following steps.

- Don’t exit out of this file, leave it there.

B. Submit the request

- Go to the PKI Services Start page (p.9). This time choose the '5 Year PKI SSL Server Certificate' template and click on 'Request Certificate'.

- Fill in the information

5-Year PKI SSL Server Certificate

Choose one of the following:

- **Request a New Certificate**

Enter values for the following field(s)

Your name for tracking this request (Optional)

Email address for notification purposes (Optional)

Pass phrase for securing this request. You will need to supply this value when retrieving your certificate

Reenter your pass phrase to confirm

Email address for distinguished name MAIL= attribute (Optional)

Common Name (Optional)

Organizational Unit (Optional)

Street address (Optional)

Locality (Optional)

State or Province (Optional)

Zipcode or postal code (Optional)

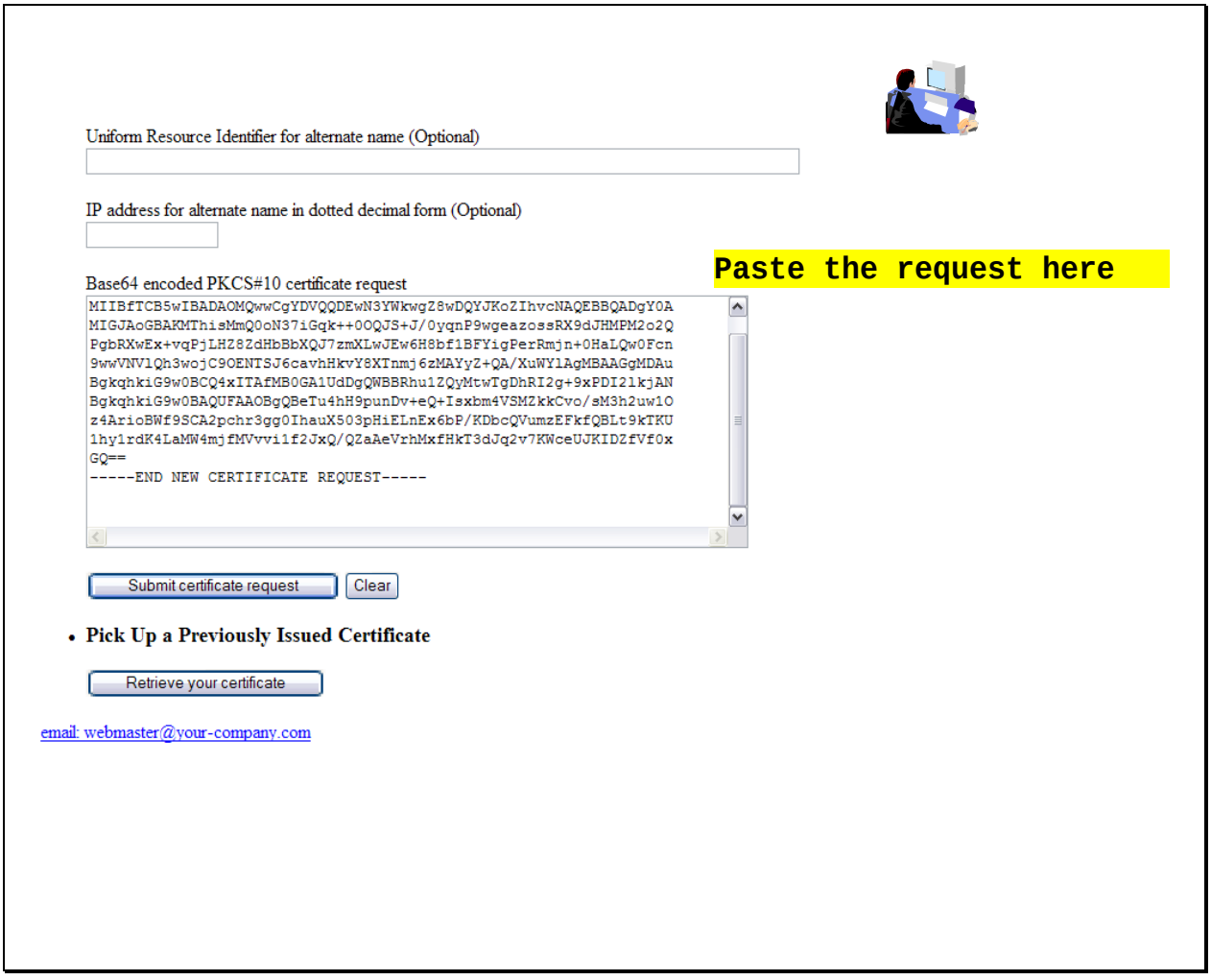
Country (Optional)

Email address for alternate name (Optional)

Domain name for alternate name (Optional)

Fill in info just like the browser cert case except…

- Paste the request from the ‘Sharbxx.myssl’ dataset
- Click on ‘Submit certificate request’ and save the transaction ID (see p.13)
- Go to the Administrator pages to approve this request in the same way you did in the browser certificate case



C. Approve the request

- Same steps as in the previous exercises

D. Pick up the certificate

- Retrieve the certificate in the same way shown on p. 26 and p. 27, except that this time you choose ‘PKI Server Certificate’ as the return type.
- Highlight the content to copy. (*You may need to copy the entire content in parts.)*

Here's your Certificate. Cut and paste it to a file

```
-----BEGIN CERTIFICATE-----
MIIGhwYJKoZIhvcNAQcCoIIGeDCCBnQCAQExADALBgkqhkiG9w0BBwGgggZcMIID
9TCCA16gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJVUzEMMAoG
A1UEChMDSUJNMRUwEwYDVQQLEwxIUiBDZXJOIEF1dGgwHhcNMDQxMDA2MDAwMDAw
WhcNMDkxMDA0MjM1OTU5WjBQMQswCQYDVQQGEwJVUzERMA8GA1UECBMITmV3IFlv
cmsxFTATBgNVBAoTDE51dyBZb3JrIFJVRzEXMBUGA1UEAxMOUlVHIFdlYiBTZXJ2
ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJQLBDRIAdlhnFYyQE/MOZ9S
eF+8zLv4AD6MyN1IP/Tr+Ij3T6c9mNYUB7fWqSpAIfmPt8W6KWLROMb3lHVuYYtB
oGaQ/FprcnHEkvP5QbOrvbxfqoZnrA1N4kGisGiBgv6evZ1fLAHpOJNLAaJfC2/h
EbBOsdQ4RL8VCfzrSo2BAgMBAAGjggH7MIIB9zApBgNVHREEIjAghhhodHRwOi8v
d3d3LnJ1Z3NlcnZlci5jb22HBAl7LUMwDgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQM
MAoGCCsGAQUFBwMBMIIBYwYDVR0fBIIBWjCCAVYwSaBHoEWkQzBBMQswCQYDVQQG
DAJVUzEMMAoGA1UECgwDSUJNMRUwEwYDVQQLDAxIUiBDZXJOIEF1dGgxDTALBgNV
BAMMBENSTDEwXaBboFmGV2xkYXA6Ly85LjU2LjUOLjEzMDozODkvQ049Q1JMMSxP
VT1IUiUyMENlcnQlMjBBdXRoLE89SUJNLEM9VVM/Y2VydGlmaWNhdGVSZXZvY2FO
aW9uTGlzdDBxoG+gbYZrbGRhcDovL215b3RoZXJsZGFwc2VydmVyLm15Y29tcGFu
eS5jb2O6Mzg5LONOPUNSTDEsT1U9SFIlMjBDZXJOJTIwQXVOaCxPPUlCTSxDPVVT
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwN6A1oDOGMWhOdHA6Ly93d3cubXlj
b21wYW55LmNvbS9QSOlTZXJ2L2NhY2VydHMvQ1JMMS5jcmwwHQYDVROOBBYEFFp6
TKC8zJOGNu/lvjWmjqx/S2+NMB8GA1UdIwQYMBaAFLdu6pMUI9gIBAPXMeK3zu1Z
M+arMAOGCSqGSIb3DQEBBQUAA4GBADpj6blOeBL+z2GQmd9EQGXyP5zrPYoALIJ8
LP3ugJ5sI1R55mtNsUm358JzYwtT/46uP6zmDnn3hxAt6cwMiWYHNpKzIQHfx+O2
lSL/fX/5u8QCFhR8E7a18Z+AeppcoOi6/YxHfHl+5qIcMv5/oekbH28foxSNwlRb
n/tKWewmMIICXzCCAcigAwIBAgIBADANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQG
EwJVUzEMMAoGA1UEChMDSUJNMRUwEwYDVQQLEwxIUiBDZXJOIEF1dGgwHhcNMDQx
MDA0MDQwMDAwWhcNMjAwMTAyMDM1OTU5WjAyMQswCQYDVQQGEwJVUzEMMAoGA1UE
ChMDSUJNMRUwEwYDVQQLEwxIUiBDZXJOIEF1dGgwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALAbZJJN/FEu/VDi+mRmuJzpwKl6V4ATqNHztjuEMbdzl3rtIpaR
OqIh61atRRsddACuH4vkxaNxg/WHOdzFp/kknDHmrh1EwlIwRLCEfU3LAiBg8URO
QiPhwV61cQUHSTW+uxnXJq56OKQAOo4weiFr+GRm6ISa3i1/Yt4oIeIDAgMBAAGj
gYQwgYEwPwYJYIZIAYb4QgENBDITMEdlbmVyYXRlZCBieSBOaGUgU2VjdXJpdHkg
U2VydmVyIGZvciB6LO9TIChSQUNGKTAOBgNVHQ8BAf8EBAMCAQYwDwYDVROTAQH/
BAUwAwEB/zAdBgNVHQ4EFgQUt27qkxQj2AgEA9cx4rfO7Vkz5qswDQYJKoZIhvcN
AQEFBQADgYEAqWTnhDcf7GUAww7hBk5XWbODsT5N/A/P2mVFs7mSpJpT3IldbE+I
Ipf4kRFruoN6bIFDwOyFnCp71BbWH8dF/OnMwBGMsFEhLrF6Fjw12ovObWVqCiAE
-----END CERTIFICATE-----
```

email: webmaster@your-company.com

The cert is returned in B64 format for you to cut and paste it to a file from the server side. You may not be able to paste the entire content into the server dataset. Do it in parts OR use a function provided by PCOMM: Edit->Paste, Paste Next.

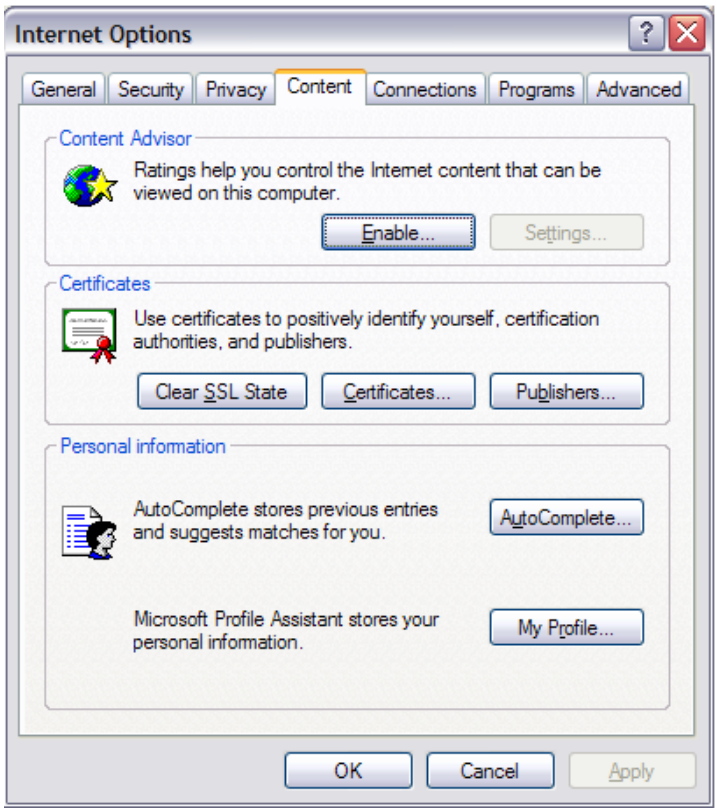
E. Install the certificate in the server 

- Go back to the MVS system, the content of the ‘Sharbxx.myssl’ should be still displaying. Replace the content of the ‘Sharbxx.myssl’ dataset with this copied content by deleting its original content and *paste the new content. (*This is a convenient way so that we don’t have to allocate another dataset for this.*)
    - ***A neat trick to paste multiple pages: Click on Edit->Paste, Edit->Paste Next***
- Save the file by hitting PF3
- Go to ISPF 6, enter the following command to replace the original self-signed certificate with this one issued by PKI Services
    - RACDCERT ID(Sharbxx) ADD(‘Sharbxx.myssl’)

(*You will get a warning message IRRD113I about incorrect range. That’s fine since the CA cert in this lab was set up to have a very short validity period*.)

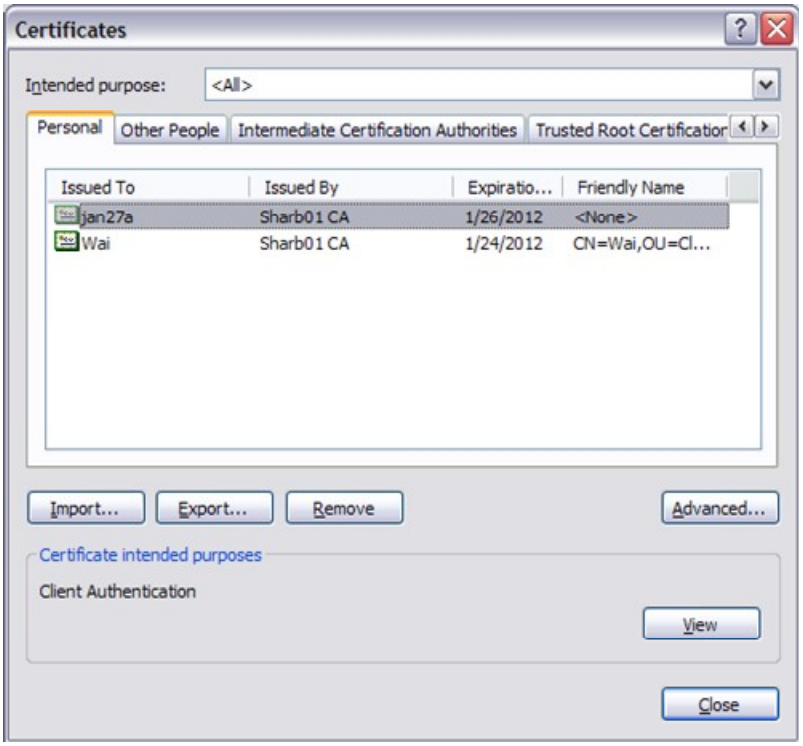
Exercise 4 - View the installed certificate from the IE browser

- From IE, click on Tools -> Internet Options…
- Go to the Content tab
- Click on ‘Certificates’



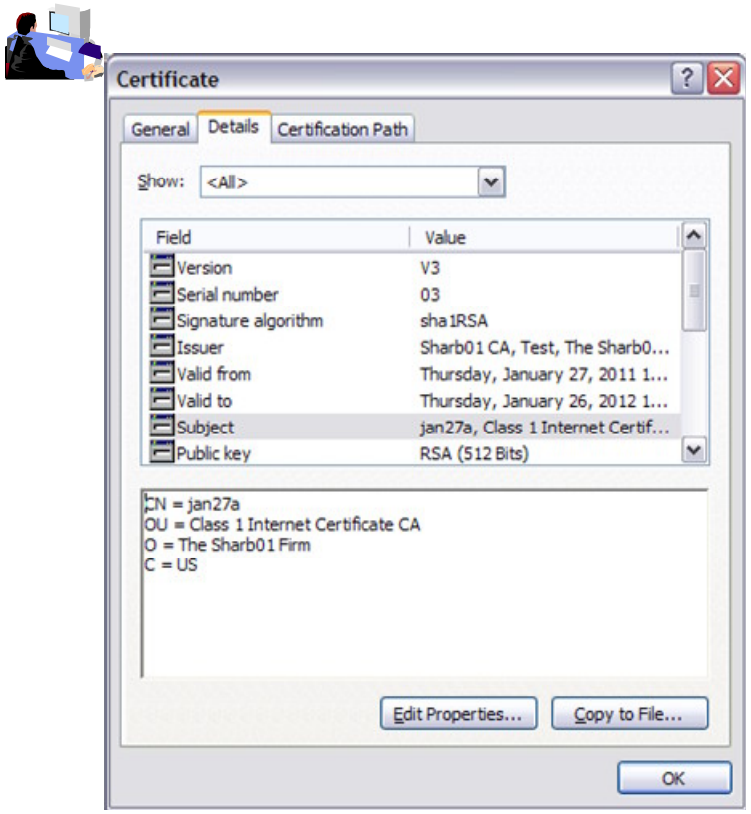
- Go to the ‘Personal’ tab and find the certificate you have just installed. Find it by the name you entered when you made the request
- Click on ‘View’ and go to the ‘Details’ tab’ to look at some certificate details

Certificate is installed in browser



- Highlight the entry you want to see, eg. When Subject is highlighted, you can see all the components of the certificate subject name

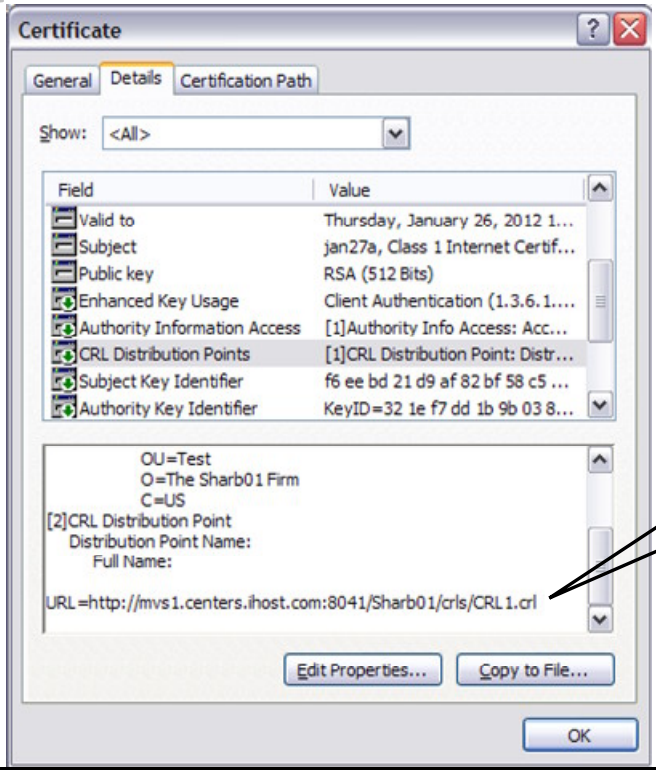
And look at the details of each field – Subject



Fields supplied by user or hardcoded by administrator in pkiserv.tmpl

- CRL Distribution Points shows the URL of the Certificate Revocation List (You will make use of it in Exercise 6)

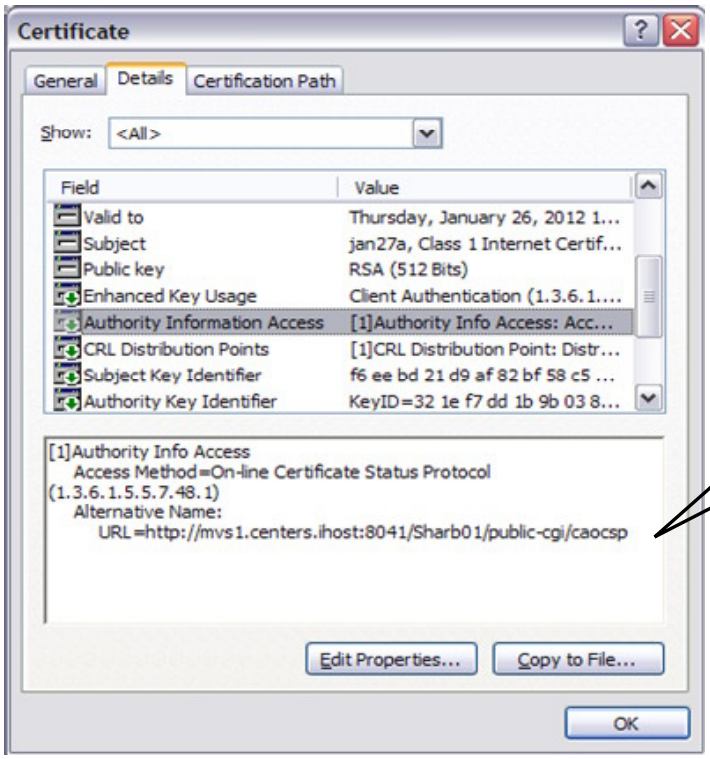
And look at the details of each field – CRL DP location



This is set up in pkiserv.conf

- Authority Information Access shows the URL of the Online Certificate Status Protocol responder (You will need this in Exercise 6)

And look at the details of each field – OCSP location



This is hardcoded by administrator in pkiserv.tmpl

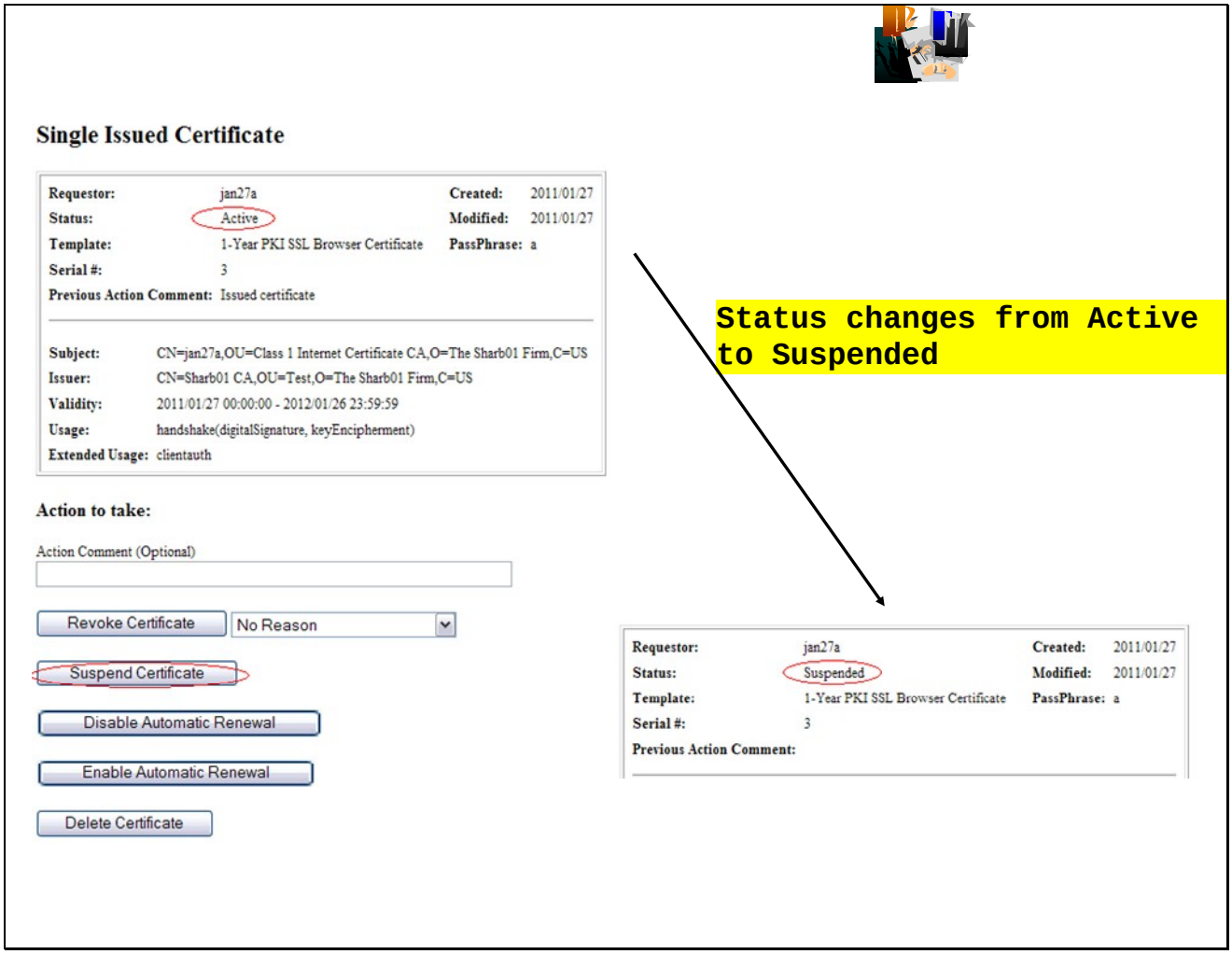
Exercise 5 - Suspend a certificate by the administrator

(*Both the end user and the administrator can revoke/suspend a certificate. The user can act on his own certificate while the administrator can act on any.*

***Both revoke and suspend will cause the certificate to be posted to a CRL. But the suspended one will not appear on the next CRL if the administrator resumes it.*)**

- This shows the administrator path. Go to the page to display the certificate details and click on 'Suspend Certificate' (p. 23 – 25)

  (*If the user wants to suspend his own certificate, he can go to 'Home page' (p.9) and click on 'Renew or Revoke Certificate' and go through the subsequent pages*)
- You may check the result. Click on 'Administration Home Page' which will bring you to p.16. Choose 'Show all issued certificates'. You will see that the status is now displayed as 'Suspended' instead of 'Active'



Exercise 6 - Check the status of a certificate outside PKI Services 

- *through Certificate Revocation List (CRL)*
    - *this is a snap shot of all the revoked/suspended certificates at the time of the query. Depending on the time the CRL is refreshed, a revoked certificate may not appear on the list*
- *through Online Certificate Status Protocol (OCSP)*
    - *this provides the live status of a certificate at the time of the query*

Note**: **In this lab, in addition to the roles of the certificate owner and the PKI Services administrator, you also play the role of any third party who wants to verify your certificate's status. In this lab setup, you can export the certificate you've just created, and its issuers' chain in the way described below. But in the real world, the third party needs to get all the related certificates in different ways, eg. get them from some public directory like LDAP.

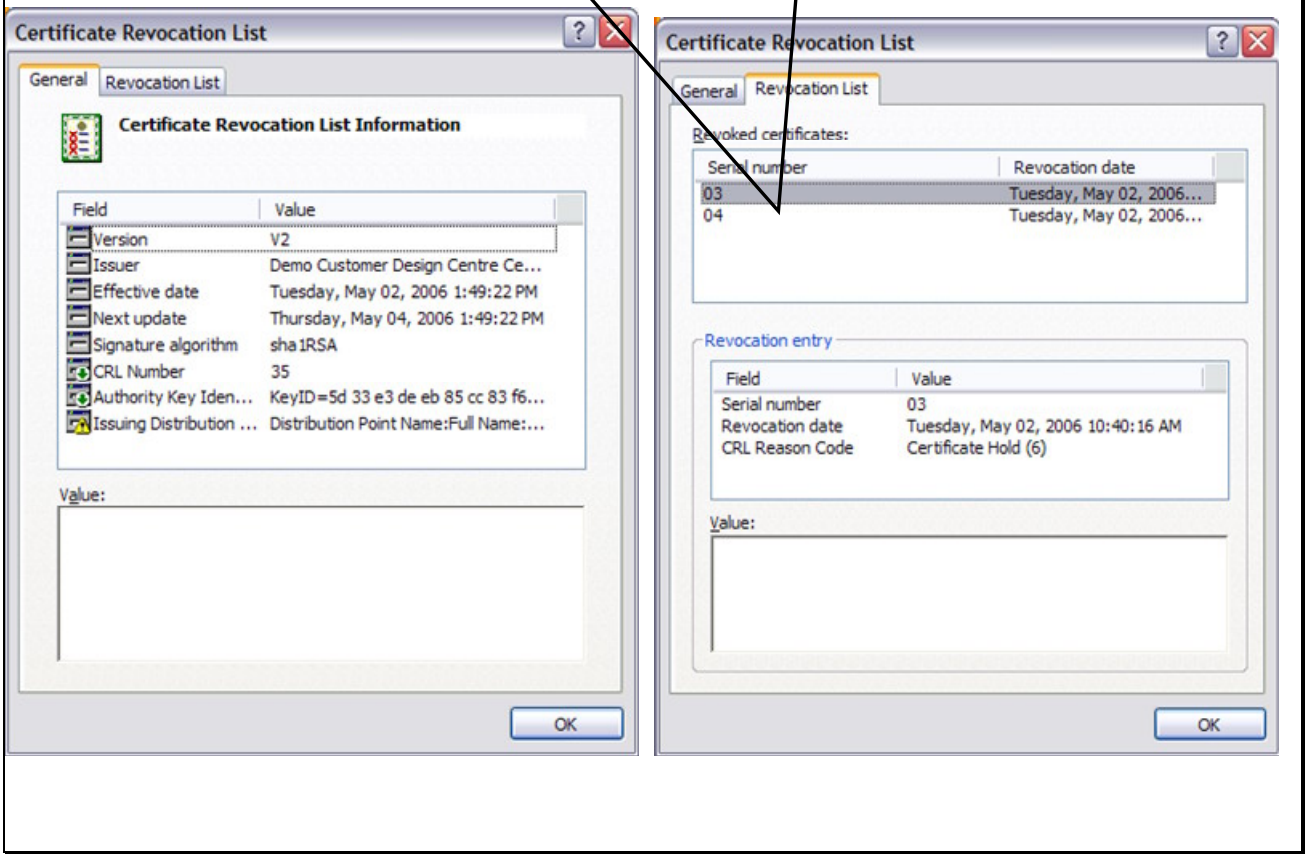
Method 1: Check the certificate status through CRL

- Open an IE browser and enter the url displayed in the CRL Distribution Point field in the certificate you have installed (p.29, 30, 32) in Exercise 1 and click Open when prompted
- Click on the 'Revocation List' tab to look at the list of serial numbers of revoked/suspended certificates

(*If you don't find the certificate you just revoked, wait for a few minutes and try again. You need to wait until the next CRL is posted. Where is the posting interval of CRL set? pkiserv.tmpl or pkiserv.conf?*)

Go to http://mvs1.centers.ihost.com:8041/Sharbxx/crls/CRL1.crl

Cert with serial no. 3 and 4 are revoked or suspended



Method 2: Check the certificate status through OCSP

- Export the **user certificate** from Exercise 1 (do not export the private key) from the browser. Click on 'Export' on p. 48 under the 'Personal' tab. Save it to **c:\temp\mycert.cer** in Base-64 format (click the 2nd radio button when you are asked on the export format).
- Export its **signer certificate** from the browser. Click on 'Export' on p. 48 under the 'Intermediate Certification Authorities' tab. Its name should be Sharbxx CA (xx is the number part of your assigned id). Save it to **c:\temp\mycacert.cer** in Base-64 format also.
- Export the **root certificate**. Click on 'Export' on p. 48 under the 'Trusted Root Certification Authorities' tab. Its name should be 'Demo Customer Design Centre Certificate Authority'. Save it to **c:\temp\cacert.cer** in Base-64 format too.

(*We will use the openssl command to send a status request to the PKI Services responder.*
***To save the typing, a batch file named 'statusof' that contains the command which expects 2 parameters (file contains the user cert and part of URL identifying your system) is placed under \openssl\bin. (The openssl command syntax is in the Appendix 2).*)**

- Open a Windows Command processor window,
    - enter 'cd \openssl\bin'
    - enter 'statusof c:\temp\mycert.cer xx' (xx is the number part of your assigned id)

- Look at the Serial Number, Cert Status and Revocation Reason
- The first box shows the status after the certificate is suspended – revoked status with reason 6 means suspension

- The second box shows the status of the same certificate after it is resumed (Go to the Single Issued Certificate page to click on the 'Resume Certificate' button)

Get the status from OCSP using openSSL…

```
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: O = The Share03 Firm, OU = Test, CN = Share03 CA
    Produced At: Dec  7 03:13:46 2006 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 1BA48167FFFD2EC4D90BB2E1F66B109E055C34BE
      Issuer Key Hash: ACDDB2434055FF87FFB8790B3F09AED8A3EB0816
      Serial Number: 01
    Cert Status: revoked
    Revocation Time: Dec  6 22:36:04 2006 GMT
    Revocation Reason: certificateHold (0x6)
    This Update: Dec  7 03:13:46 2006 GMT
```

Cert 01 is suspended (from reason 0x6)

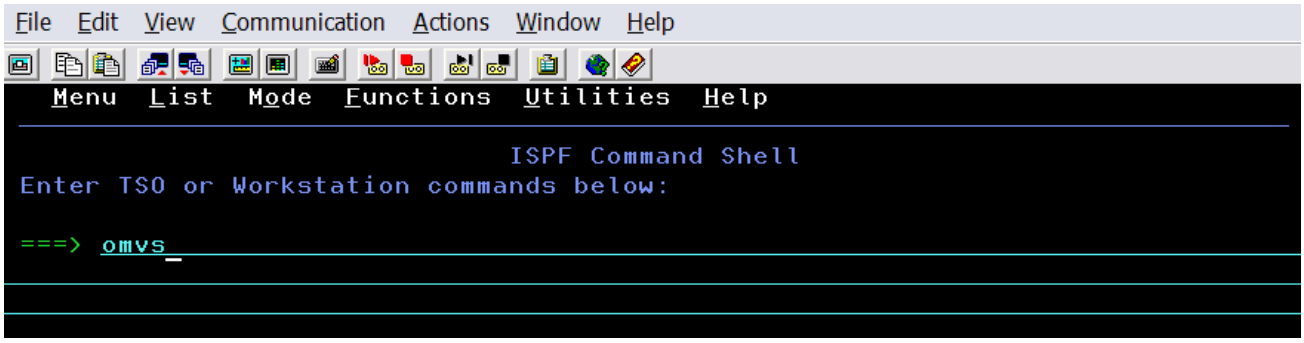
```
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: O = The Share03 Firm, OU = Test, CN = Share03 CA
    Produced At: Dec  7 03:27:54 2006 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 1BA48167FFFD2EC4D90BB2E1F66B109E055C34BE
      Issuer Key Hash: ACDDB2434055FF87FFB8790B3F09AED8A3EB0816
      Serial Number: 01
    Cert Status: good
    This Update: Dec  7 03:27:54 2006 GMT
```

Cert 01 is not revoked or suspended

Exercise 7 – Customization 

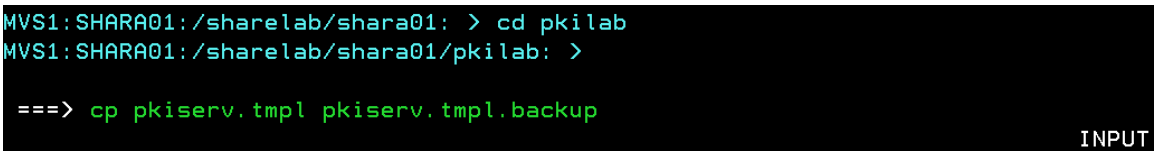
A. Customize a template in pkiserv.tmpl

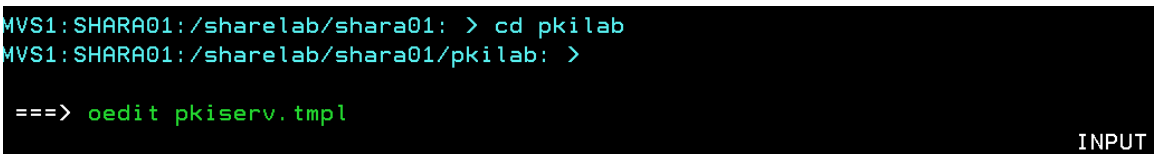
- Choose the 'n-Year PKI Certificate for Extensions Demonstration' template from the Home page (p. 9) and take a look at all the input fields for that template. There are a lot of them. Don't fill in anything yet.
- Go to the MVS system's OMVS session



- Edit the pkiserv.tmpl file under /sharelab/sharbxx/pkilab in a similar way shown below.

(Note: Save a copy before you make any changes – cp pkiserv.tmpl pkiserv.tmpl.backup)





You want to

1) change input field(s) to hard coded field(s),

Here are the steps:

- Find the <TEMPLATE NAME= n-Year PKI Certificate for Extensions Demonstration> section, under **<CONTENT>**

  Delete : **ValidStateProv(frm) &&**

  Delete: **ValidCountry(frm) &&**

  Delete: **%%StateProv (optional)%%**

  Delete: **%%Country (optional)%%**

Under **<CONSTANT>**,

Add: **%%StateProv=New York%%**

Add: **%%Country=US%%**

2) change optional field(s) to required field(s)

Here is the step:

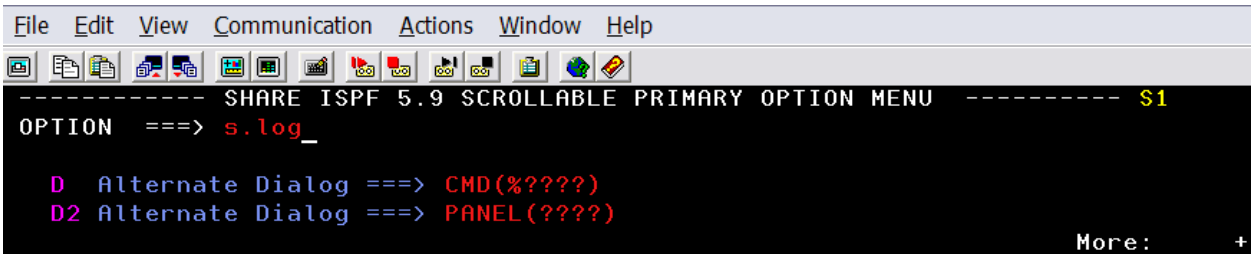
under **<CONTENT>**

Change: **%%PostalCode (optional)%%** to **%%PostalCode%%**

- Save the changes
- Open **another** IE window to go to the '**n-Year PKI Certificate for Extensions Demonstration**' template again. Compare this page with the previous one. You will see:
  - the input fields for 'State of Province' and 'Country' are no longer there.
  - the 'Postal Code' field becomes a required field.
- You can fill in the info to make a request and check for the information in the certificate created using the steps you have learnt.

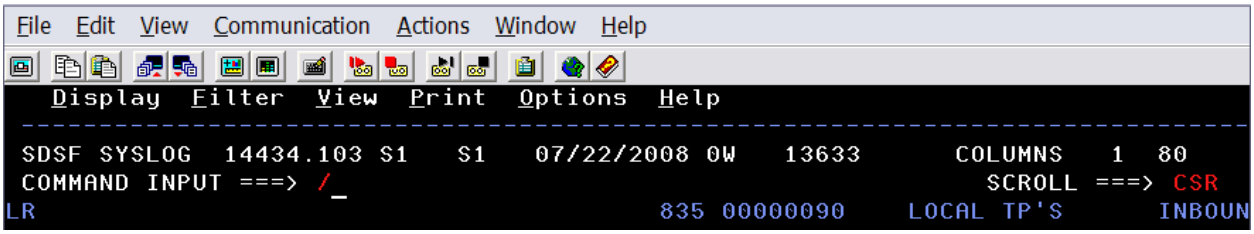
B. Customize pkiserv.conf

- Go to the MVS system's OMVS session to edit the pkiserv.conf file under /sharelab/sharbxx/pkilab as follows.
  (Note: Save a copy before you make any changes – cp pkiserv.conf pkiserv.conf.backup)
  You want to change the time interval to turn an approved request into a certificate.
  - Change: CreateInterval=1m to CreateInterval=5m
- PF3 to save the change
- Restart PKI Services (Any changes to pkiserv.conf need re-starting the daemon to pick up the changes)
  - Go to MVS system, ISPF S.LOG

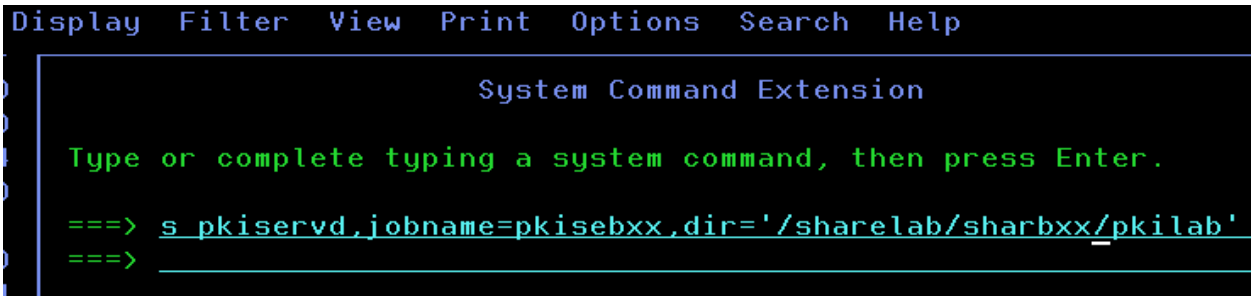


  - On COMMAND INPUT ===>, enter '/p pkisebxx' to stop the daemon first

  - Then restart PKI Services, enter '/', hit enter



  - Enter 's pkiservd,jobname=pkiseaxx,dir='/sharelab/sharbxx/pkilab'



- Go to the PKI Service web page to request a certificate and check if you have to wait longer to get back a certificate after it has been approved (See how long you will see a serial number displayed under the request status when you display the requests, p.22. You need to refresh the page to see the change if any.)

Appendix 1

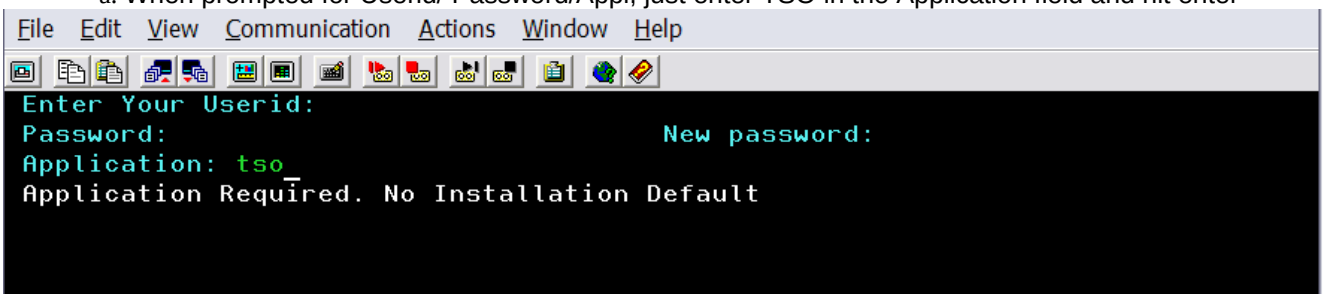
Some commands for the TSO session (3270 interface)

Start emulator

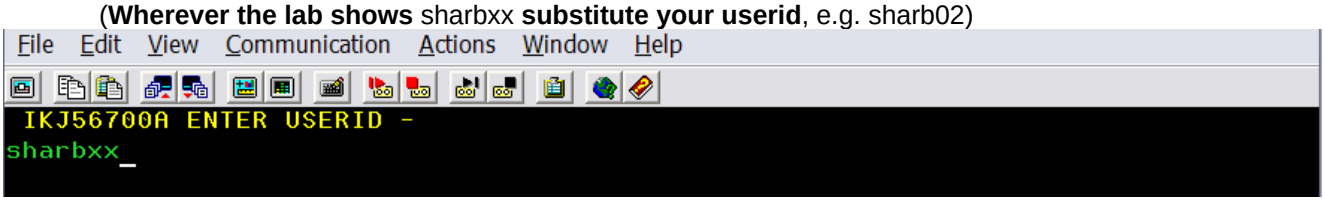
a. Double Click on the provided icon provided
This starts a Pcomm 3270 session using **mvs1.centers.ihost.com**.
***Note**: The **Enter** key is the right **Ctrl** key*

Logon to MVS system

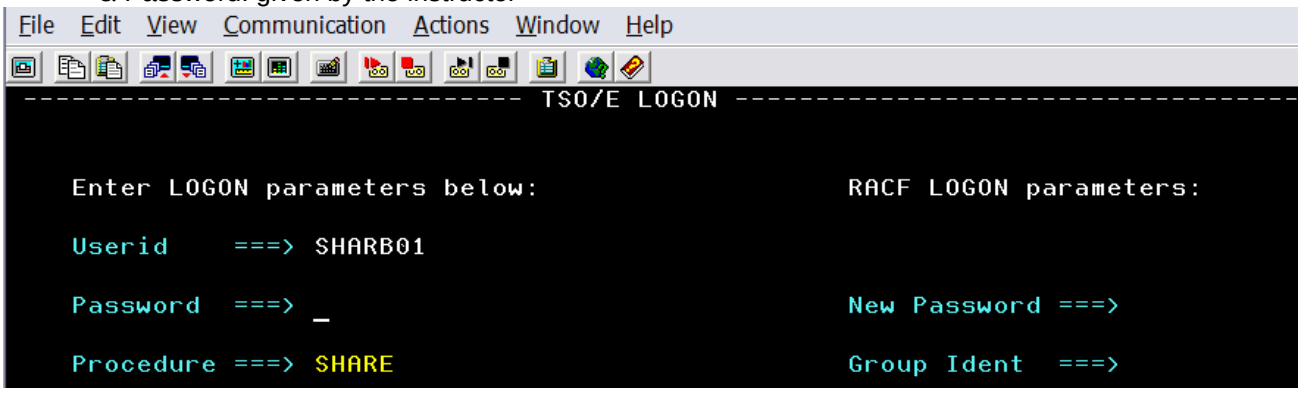
a. When prompted for Userid/ Password/Appl, just enter TSO in the Application field and hit enter



b. Enter Userid: sharbxx
(**Wherever the lab shows** sharbxx **substitute your userid**, e.g. sharb02)



c. Password: given by the instructor



d. Hit enter when you see ***, you will be in the ISPF main panel

Logoff from MVS system

a. Keep hitting PF3 until you are presented with this panel

```
Log Data Set (SHARBxx.SPFLOG1.LIST) Disposition:
Process Option . . . .    1. Print data set and delete
                          2. Delete data set without printing
                          3. Keep data set - Same
                             (allocate same data set in next session)
                          4. Keep data set - New
                             (allocate new data set in next session)
```

b. Enter option 2
c. Enter logoff

Open a OMVS session

a. From ISPF main panel, enter option 6
b. Enter: **omvs**

Exit a OMVS session

a. From OMVS shell, type ‘exit’

Using the oedit editor / ISPF editor

a. From OMVS shell, type ‘oedit <filename>
b. From the line numbers columns (on the left side):
    i – insert a line (i 20 – insert 20 lines)
    c – copy a line
    m – move a line
    a – paste a line that you’ve copied using ‘c’ or moved using ‘m’ after the current line
    d – delete a line (d 20 – delete 20 lines)
c. From Command ===>
    f xx – find the occurrences of xx
    c xx yy – change the occurrence of xx to yy (PF6 to repeat the change to the other occurrences)
d. PF3 to save the file and exit (If you want to exit without saving, type ‘cancel’ on Command===> line)

Appendix 2

A sample openssl command to send a request to an OCSP responder

issuer: file contains the issuer cert of the target cert in Base-64 format

cert: file contains the target cert in Base-64 format, the one you want to check the status

url: location of the responder, in our case, it is PKI Services itself. (The CA and the responder can be different)

resp_text: indicates the print out of the response text

respout: file contains the DER encoded response

CAfile: file contains the root certificate in Base-64 format

Get the status from OCSP using openSSL…

Send a request to the responder:

```
openssl ocsp
-issuer \temp\mycacert.cer
-cert \temp\mycert.cer
-url http://mvs1.centers.ihost.com:8041/Sharbxx/public-
  cgi/caocsp
-resp_text -respout \temp\resp.der
-CAfile \temp\cacert.cer

(Note: In the provided batch file, two input parameters
  are used:
-cert %1
-url http://mvs1.centers.ihost.com:8041/Sharb%2/public-
  cgi/caocsp)
```

Here is the link to install openSSL in windows:

http://www.slproweb.com/products/Win32OpenSSL.html

The document:

http://www.openssl.org/docs/apps/openssl.html

References

- **PKI Services web site:**
  - http://www.ibm.com/servers/eserver/zseries/zos/pki
- **PKI Services Red Book:**
  - http://www.redbooks.ibm.com/abstracts/sg246968.html
- **RACF web site:**
  - http://www.ibm.com/servers/eserver/zseries/zos/racf
- **IBM Education Assistant:**
  - http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp
- **Cryptographic Services**
  - PKI Services Guide and Reference (SA22-7693)
  - OCSF Service Provider Developer's Guide and Reference (SC24-5900)
  - ICSF Administrator's Guide (SA22-7521)
  - System SSL Programming (SC24-5901)
- **Security Server Manuals:**
  - RACF Command Language Reference (SC28-1919)
  - RACF Security Administrator's Guide (SC28-1915)
  - RACF Callable Services Guide (SC28-1921)
  - LDAP Administration and Use (SC24-5923)
- **IBM HTTP Server Manuals:**
  - Planning, Installing, and Using (SC31-8690)
- **Other Sources:**
  - PKIX - http://www.ietf.org/html.charters/pkix-charter.html

Disclaimer

- The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.
- In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.
- It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.
- IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.