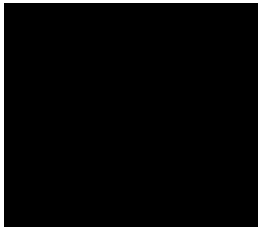


Digital Certificates – From Concept to Implementation Part 6 (Hands-on Lab)

**Session FD3
June 23rd 2014**

**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.

Background information

- PKI Services is an application to generate and manage certificates

z/OS PKI Services Process simplified sample

1. User contacts PKI Services
2. CGI constructs a web page
3. CGI packages all the information
4. Callable service creates the certificate object and puts it in the database
5. Administrator generates the certificate administrative data
6. CGI calls the callable service to create the certificate and puts it in the database
7. Certificate is available in the List Database
8. User can view the certificate
9. User can delete the certificate

- This is the partial content of a sample **pkiserv.envvars** 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

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)

This is the start page

Choose one of the following:

- **Request a new certificate using a model**
Select the certificate template to use as a model: 1-Year PKI SSL Browser Certificate
- **Pick up a previously requested certificate**
Enter the assigned transaction ID:
Select the certificate return type: PKI Browser Certificate
- **Renew or Revoke Certificate**

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

Click 'Install Certificate' and select 'Trusted Root Certification Authorities' as the Certificate Store

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

Pick a template

[Install the CA certificate to enable SSL sessions for PKI Services](#)

Choose one of the following:

- **Request a new certificate using a model**
Select the certificate template to use as a model: 1-Year PKI SSL Browser Certificate
- **Pick up a previously requested certificate**
 - 2-Year PKI Windows Logon Certificate
 - 2-Year PKI Browser Certificate For Authenticating To z/OS
 - 5-Year PKI SSL Server Certificate
- **Renew or revoke a previously issued browser certificate**
[Renew or Revoke Certificate](#)
- **Recover a previously issued certificate whose key was generated by PKI Services**
Enter the email address when the original certificate was requested
- **Administrators click here**
[Go to Administration Page](#)

- Fill in the values for the certificate request information
- Select Microsoft Enhanced Cryptographic Provider to generate key pair – 1024 bits
- Click on 'Submit certificate request'

1-Year PKI SSL Browser Certificate

Choose one of the following:



Fill in the info

- Request a New Certificate

Enter values for the following field(s)

[Redacted input field]

These input fields are controlled by the [Redacted] on p7

Email address for notification purposes (optional)

[Redacted input field]

Reenter your pass phrase to confirm

[Redacted input field]

Email address for distinguished name MAIL attribute (optional)

[Redacted input field]

Common Name

[Redacted input field]

Select the following key information

[Redacted key information selection area]

The browser will use the selected crypto provider to generate public/private key pair. Pick Microsoft Enhanced Cryptographic Provider.

- Pick Up a Previously Issued Certificate

Retrieve your certificate

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

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

Request submitted successfully



Here's your transaction ID. You will need it to retrieve your certificate. Press 'Continue' to retrieve the certificate.


1jTQjs0h/cpk2SHV+++++++

Continue

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

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

Retrieve Your PKI Browser Certificate



Please bookmark this page

Since your certificate may not have been issued yet, we recommend that you create a bookmark to this location so that when you return to this bookmark, the browser will display your transaction ID. This is the easiest way to check your status.

Enter the assigned transaction ID

- 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](mailto: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

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)



Choose one of the following:


- **Request a new certificate using a model**
Select the certificate template to use as a model
- **Pick up a previously requested certificate**
Enter the assigned transaction ID

Select the certificate return type
- **Renew or revoke a previously issued browser certificate**
- **Administrators click here**
 Administrator starts working

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

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

PKI Services Administration



Work with a single certificate request

Enter the Transaction ID:

Work with a single issued certificate

Enter the Serial Number:

~~Specify search criteria for certificates and certificate requests~~

Certificate Requests	Issued Certificates
<input type="radio"/> Show all requests	<input type="radio"/> Show all issued certificates

Show active, automatic renewal disabled certificates

Show active, not renewable certificates

Additional search criteria (Optional)

Requestor's name

Show recent activity only ▼

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



Certificate Requests

Request summary info

All <input checked="" type="checkbox"/>	Requestor	Certificate Request Information	Status	Dates
<input checked="" type="checkbox"/>	jan27a	Template: I-Real PKI SSL Browser Certificate Subject: CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Pending Approval	Modified: 2011/01/27

Choose one of the following:

- Select and take action against multiple requests at once

Action Comment (Optional)

Approve

Reject

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

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'



Single Request

Requestor:	jan27a	Created:	2011/01/27
Status:	Pending Approval	Modified:	2011/01/27
Template:	1 Year 1 Year SSL Browser Certificate		
Validity:	2011/01/27 00:00:00 - 2012/01/26 23:59:59		
Usage:	handshake(digitalSignature, keyEncipherment)		
Extended Usage:	clientauth		
Fingerprints:	<p>11:55:CD:7B:3B:9B:71:F7C:4B:E0:0A:60:BB:0F:36:DC:B8:6B:D6:BF:49:FF:07:5C:61:08:B3:11:E5:C6:00:27</p>		

The Subject's name value
 user input
 value in
 pkiserv.tmpl

Request detail info

Action to take:

Action Comment (Optional)

Approve Request As It is

Reject Request

Delete Request

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



• Subject Distinguished Name:

Common Name (optional)

Organizational Unit (optional)

Organizational Unit (optional)

Organization (optional)

Country

• Extensions:

Document signing (nonRepudiation)

Email protection (emailProtection)

Extended key usage (extendedKeyUsage)

Validity Period

2011 1 27

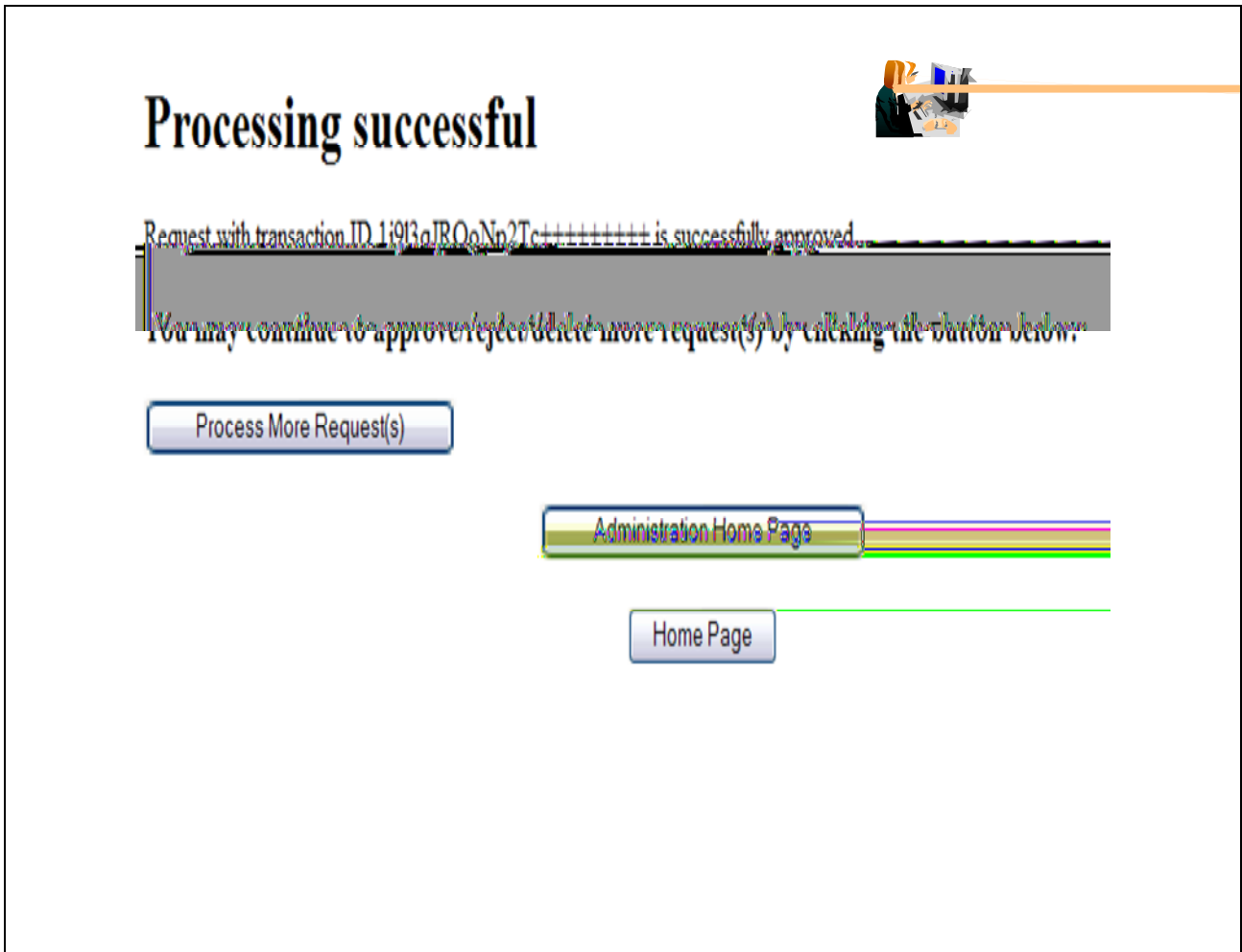
2012 1 26

Automatic Renewal: Not set

Action Comment (Optional)

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

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



The screenshot displays a confirmation message on a web page. At the top right, there is a small icon of a person at a computer. The main heading is "Processing successful". Below this, a message states: "Request with transaction ID: 149130JROpNo2Tc+++++++ is successfully approved." A grey bar highlights the text below: "You may continue to approve/reject/delete more request(s) by clicking the button below:". Three buttons are visible: "Process More Request(s)", "Administration Home Page", and "Home Page".

Processing successful

Request with transaction ID: 149130JROpNo2Tc+++++++ is successfully approved.

You may continue to approve/reject/delete more request(s) by clicking the button below:

[Process More Request\(s\)](#)

[Administration Home Page](#)

[Home Page](#)

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

To display all the requests



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

Show all requests

Issued Certificates

Show all issued 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) ▼

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



All <input checked="" type="checkbox"/>	Requestor	Certificate Request Information	Status	Dates
---	-----------	---------------------------------	--------	-------

Choose one of the following:

Click on a transaction ID to see more information or to modify, approve, reject, or delete requests individually.

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'

• Work with a single certificate request

Enter the Transaction ID:

Process Request



• Work with a single issued certificate

Enter the Serial Number:

Process Certificate

To display all the certificates

• Specify search criteria for certificates and certificate requests

Certificate Requests

- Show all requests
- Show requests pending approval
- Show approved requests

Issued Certificates

- Show all issued certificates
- Show revoked certificates
- Show suspended certificates

Show pre-registered 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

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 <input checked="" type="checkbox"/>	Requestor	Certificate Information	Status	Key archived	Dates
		Serial #: 3			Created: 2011/01/27

Choose one of the following:

Certificate summary info

- Select and take action against multiple certificates at once

Action Comment (Optional)

- Revoke all selected active certificates

- Suspend all selected active certificates

- Delete all selected certificates

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

Requester: [redacted] Serial #: [redacted] Created: 2011/01/27

Serial #: 3

Previous Action Comment: Issued certificate

[redacted]

Usage: handshake(digitalSignature, keyEncipherment)

Extended Usage: clientauth

Action to take:

Action Comment (Optional)

Revoke Certificate

Suspend Certificate

Disable Automatic Renewal

Enable Automatic Renewal

Delete Certificate

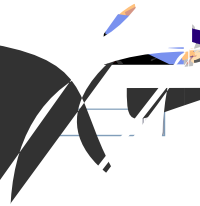
C. Pick up the certificate

- 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'

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)


Choose one of the following:



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

Retrieve Your PKI Browser Certificate

Please bookmark this page



your transaction ID. This is the easiest way to check your status.

Enter the assigned transaction ID


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'

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)



Choose one of the following:

- Request a new certificate using a model

Select the certificate template to use as a model

	1-Year PKI Generated Key Certificate
	1-Year PKI SSL Browser Certificate
	1-Year PKI S/MIME Browser Certificate
	5-Year PKI SSL Server Certificate
	5-Year PKI IPSEC Server (Firewall) Certificate
	5-Year PKI Intermediate CA Certificate
	2-Year PKI Authentication Code Signing Certificate
	1-Year PKI Certificate for Extensions Demonstration

Enter the assigned transaction ID

- Renew or revoke a previously issued browser certificate

Enter the email address when the original certificate was requested

Enter the same pass phrase as on the request form

- Administrators click here

- 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'

1-Year PKI Key Generated Certificate

Choose one of the following:

- Request a New Certificate



Enter values for the following field(s)

Enter the requestor's email address

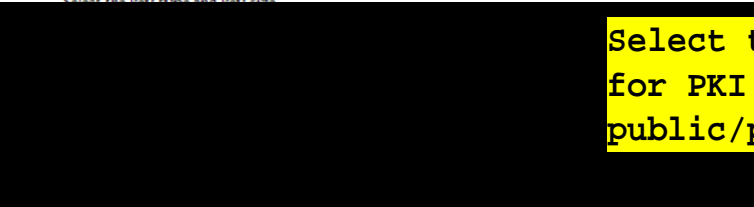
Pass phrase for securing this request. You will need to supply this value when retrieving your certificate

Reenter your pass phrase to confirm

Common Name

Email address for distinguished name (DN) attributes (optional)

Select the key type and key size




Fill in the info

These input fields are controlled by the <CONTENT> entries on p7

Select the key type and key size for PKI to generate public/private key pair.

email: v	NIST ECC - 384	y.com
	NIST ECC - 521	
	BPECC - 160	
	BPECC - 192	
	BPECC - 224	
	BPECC - 256	
-----	---	

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

Request submitted successfully 

A link to pick up the certificate was sent to the specified requestor's email address at jan27b@gmail.com.

[Home Page](#)

[email: webmaster@your-company.com](mailto:webmaster@your-company.com)

- 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.)

Single Request

Requestor: jan27b@gmail.com Created: 2011/01/27

Request detail info

Subject: CN=jan27b@15-GLOBAL-Internet-Certificates, C=A, O=The Bank of Tokyo-Mitsubishi Bank, OU=...

[Delete Request](#)

[Administration Home Page](#)

[Home Page](#)

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

Issued Certificates

The following issued certificates match the search criteria specified:

All <input checked="" type="checkbox"/>	Requestor	Certificate Information	Status	Key archived
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	jan27b@gmail.com	Serial #: 4 Template: 1-Year PKI Generated Key Certificate Subject: CN=jan27b,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Active	Yes

Choose one of the following:

- 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 - Revoke all selected certificates

Suspend - Suspend all selected active certificates

Delete - Delete all selected certificates

Respecify Your Search Criteria

certificate summary info

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.

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)

Choose one of the following:

- Request a new certificate using a model



Request Certificate

- Pick up a previously requested certificate



Enter the assigned transaction ID

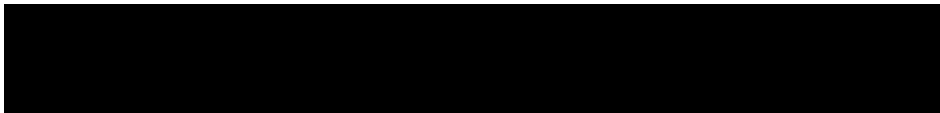
1kA8YYeAwtcZ2Tc++++++

Select the certificate return type PKI Key Certificate

Pick up Certificate

- Renew or revoke a previously issued browser certificate

Renew or Revoke Certificate



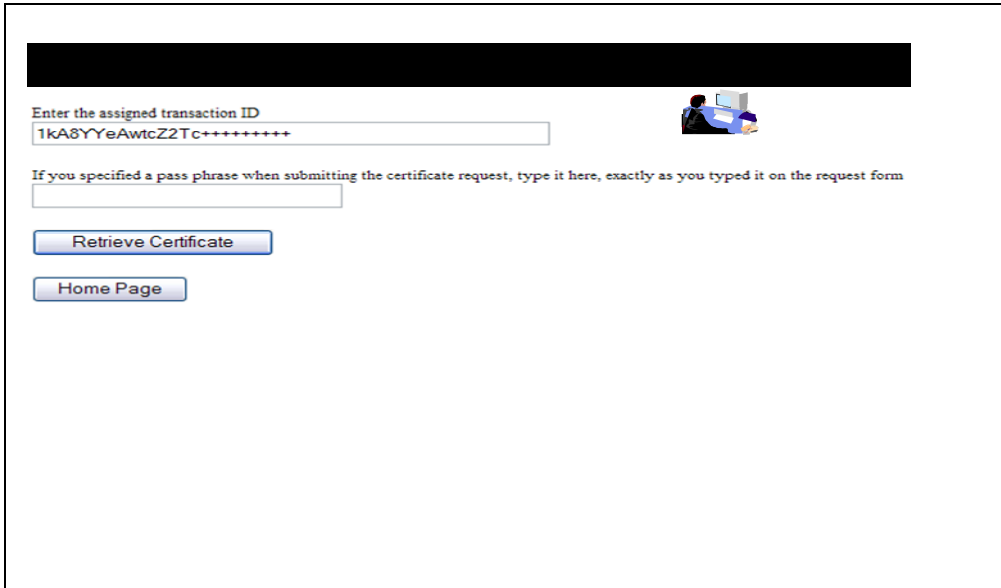
Enter the same pass phrase as on the request form

Recover Certificate

- Administrators click here

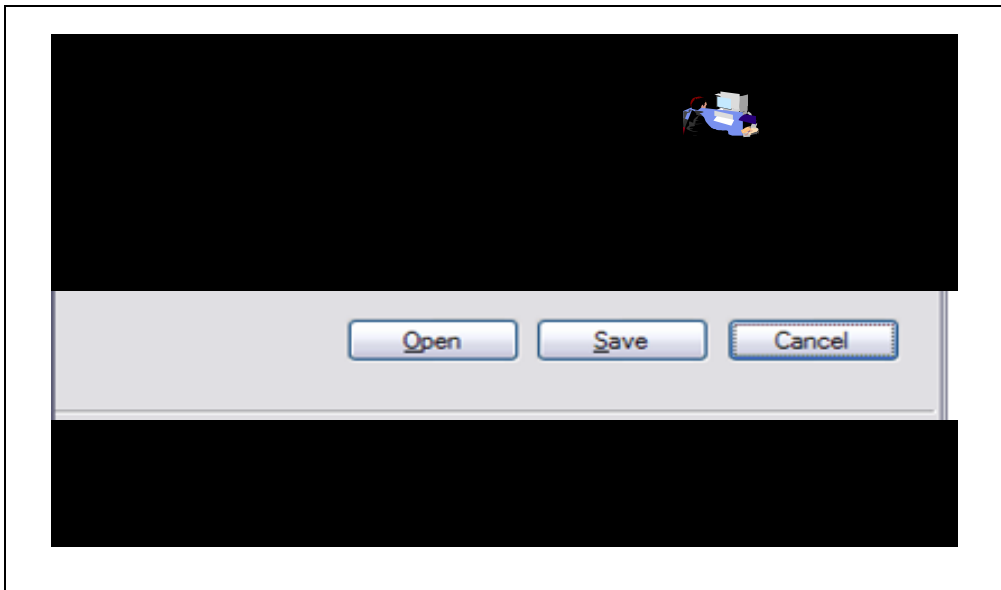
Go to Administration Page

- 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

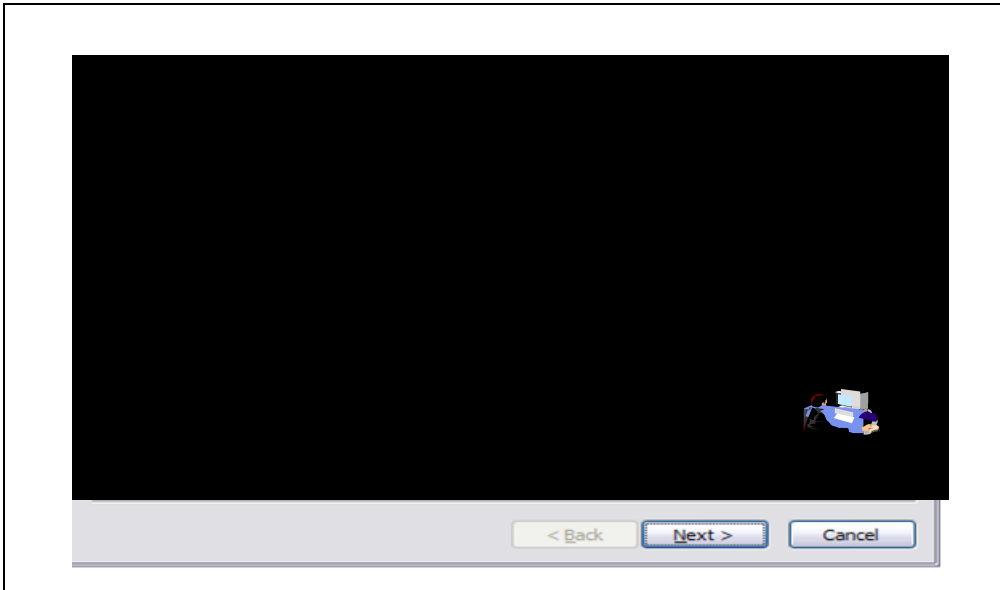


The screenshot shows a web application interface. At the top, there is a blacked-out header. Below it, the text "Enter the assigned transaction ID" is displayed. A text input field contains the value "1kA8YYeAwtcZ2Tc++++++". To the right of this field is a small icon of a person at a computer. Below the input field, the text "If you specified a pass phrase when submitting the certificate request, type it here, exactly as you typed it on the request form" is shown, followed by an empty text input field. At the bottom of the form area, there are two buttons: "Retrieve Certificate" and "Home Page".

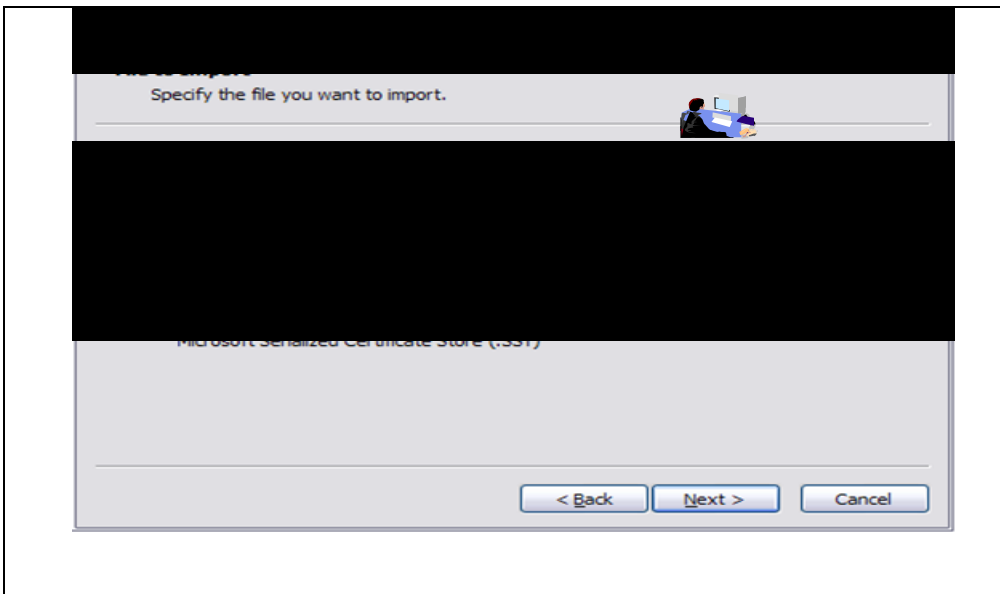
- Click Open.



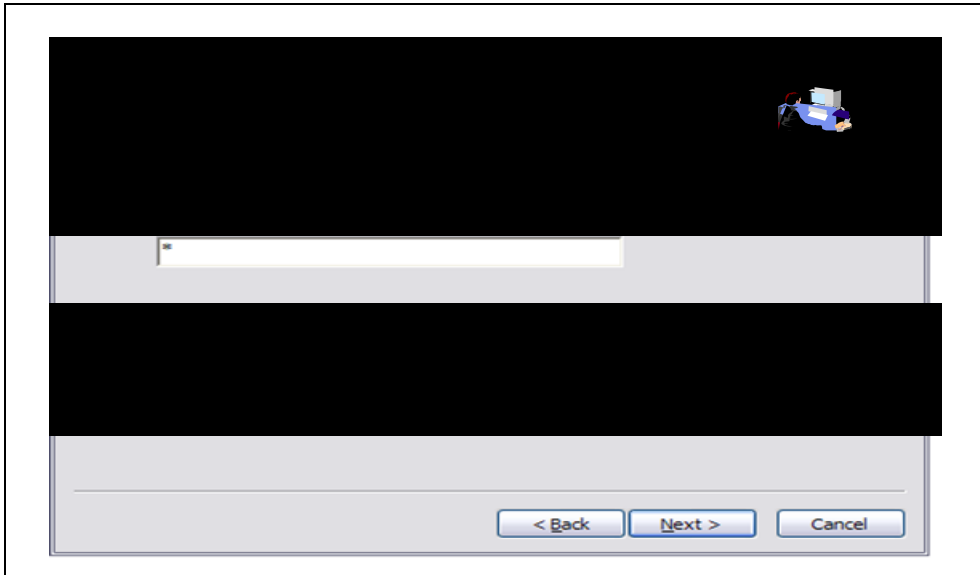
- Click Next.



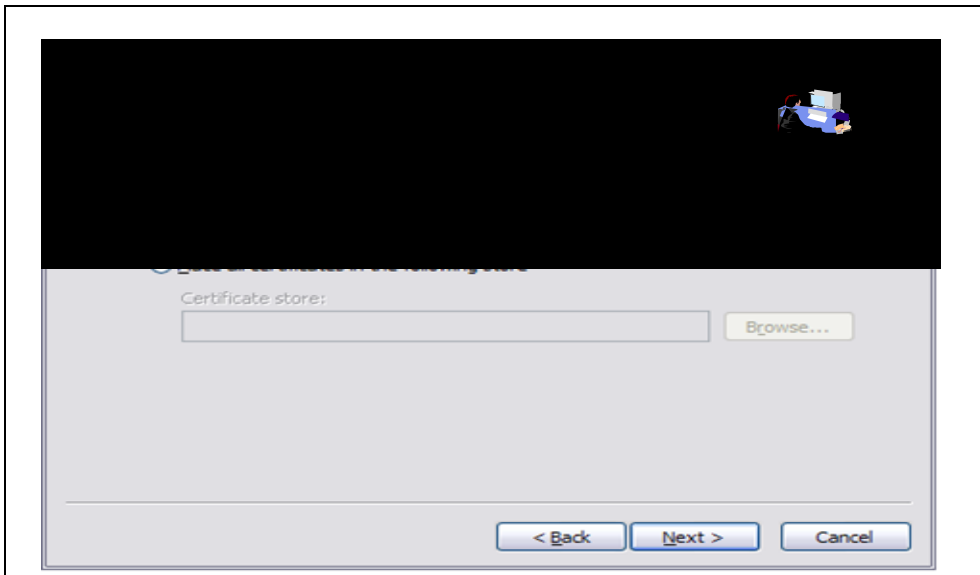
- Click Next.



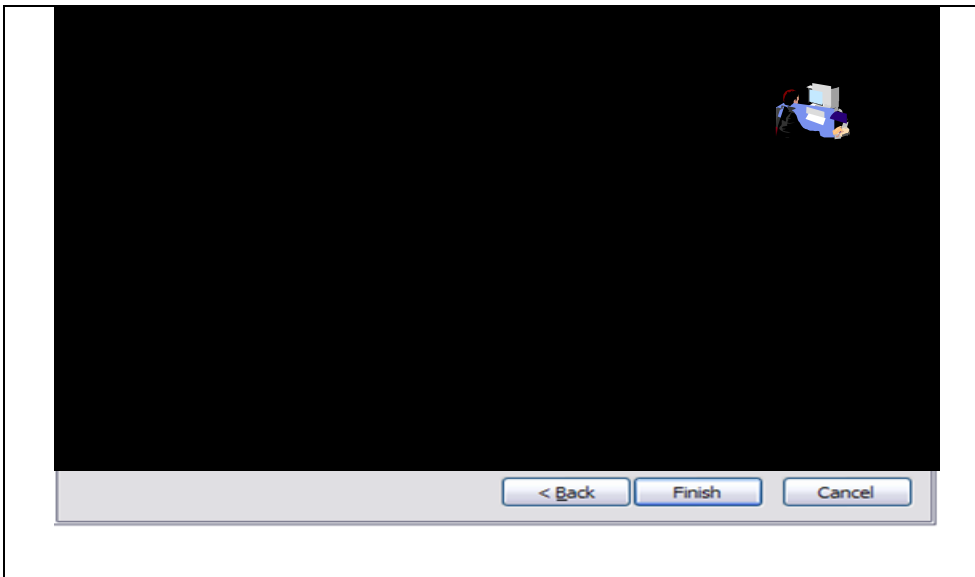
- Enter the password and check the key as exportable.



- 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(????)

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 'Dcname Level' input line and hit enter

```

Menu RefList RefMode Utilities Help
-----
Data Set List Utility

Option ==> _____

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:
Dcname 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.

```
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 -----BEGIN NEW CERTIFICATE REQUEST-----
000002 MIIBhTCB7wIBADAWMRQwEgYDVQQDEwtNWVNTTENFULQwMTCBnzANBgkqhkiG9w0B
000003 AQEFAA0BjQAwgYkCgYEA0C8ulvTwd0ywl/T9dyRgkbuR7765h3R406tZWgpp2YaM
000004 cXw0DjQkckHQgWqwr/FXHCbh/IJkFTa3B5cGKEIL1PQBJH1hCfDH6Kb311vFaYCb
000005 svELyRofKVsItUL54Q/ZREuczpcKcv8dMJsR33CZQW/uViqou0Q4DFHdZD2LoJMC
000006 AwEAAaAwMC4GCSqGSIB3DQEJDjEhMB8wHQYDVR00BBYEF00H9DduigJsku3i1IVF
000007 z2aHQmopMA0GCSqGSIB3DQEBBQUAA4GBAGcCY/fJUqr1gj36sRiBdGfj33y18XJn
000008 fBWiZ4g8N0En76+iVtTdxP0a4ZIH4A+ncaEq29H6ckILOXAsCHSuNENDYP+vGicH
000009 0tVe4tYcovvmVSwKoj1jmiZc55DMh2gebxYmkqqvNbvizPdjs/aj8iWA5AyxHOPw
000010 th59aL4s0fyg
000011 -----END NEW CERTIFICATE REQUEST-----
***** ***** Bottom of Data *****
```

- 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'.

PKI Services Certificate Generation Application

[Install the CA certificate to enable SSL sessions for PKI Services](#)



Choose one of the following:

- Request a new certificate using a model

This time, let's try to get a SSL Server cert

5 Year PKI SSL Server Certificate

- Renew or revoke a previously issued browser certificate

Renew or Revoke Certificate

- Recover a previously issued certificate whose key was generated by PKI Services

Enter the same pass phrase as on the request form

- Administrators click here

- 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 messages (Optional)

Password for tracking this request (Required)

Reenter your pass phrase to confirm

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 'Submit certificate request' page to the 'Request' field in the 'Request' dataset
- Click the 'Submit certificate request' button to submit the transaction ID (see p.13)
- Go to the Administrator pages to view the certificate request in the same way you did in the browser certificate case

Resource Identifier for alternate name ()

IP addresses for alternate name in dotted decimal form ()

3. Encoded PKCS#10 certificate request

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

Paste the request here

```

MIIBADAwDQYJKoZIhvcNAQEBBQADGYYoA
AKMThisMmQ0cn371Gqk++0OQJS+J/0
+vpPjLHZ8ZdHbBbXQU7zmXLwJew6H8
3wojC9OENTSJ6cavhHkvY8XTnmj6z
w0BCQ4xITAFMB0GA1UdDgQWBRRhu1.
w0BAQUFAAOBgQBeTu4hH9punDv+eQ+
9SCA2pchr3gg0IhauX503pHiELnEx6
hMW4mjfMVvvi1f2JxQ/QzaAeVrhMxf
-----BEGIN CERTIFICATE REQUEST-----
  
```

Submit certificate request Clear

Previously Issued Certificate

Submit certificate

email@company.com

req
previous exercises



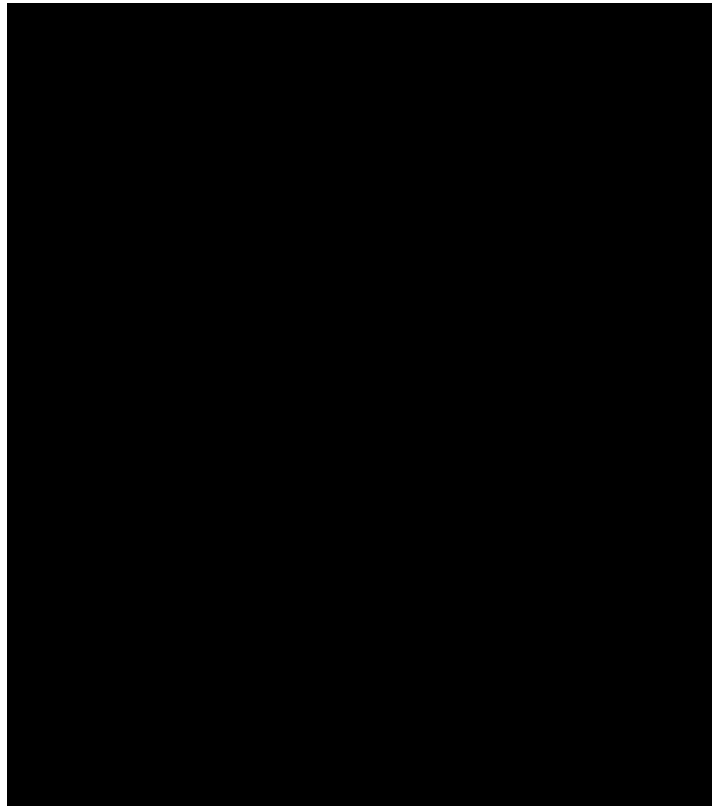
E. Install the certificate in the server

- 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.)

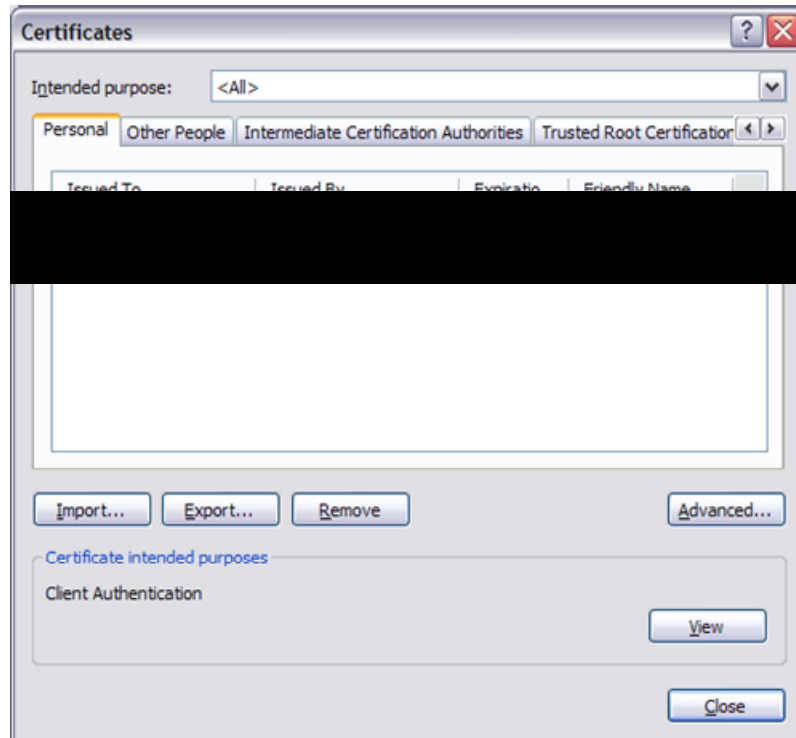
Exercise 4 - View the installed certificate from the IE browser

- From IE, click on Tools -> Internet Options...
- Go to the Content tab
- Click on 'Certificates'




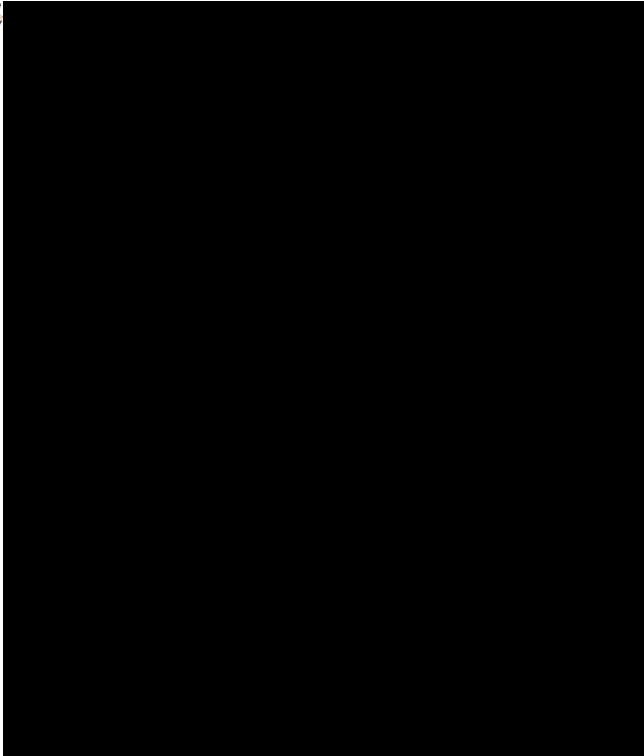
- Go to the 'Personal' tab and find the certificate you have just installed. Find it by the name you entered when you made the request
- Click on 'View' and go to the 'Details' tab' to look at some certificate details

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

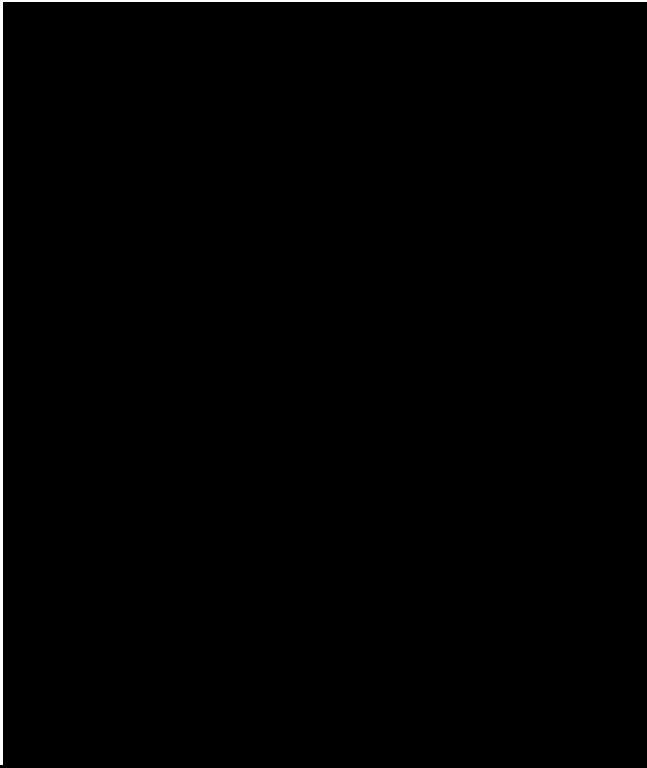
And look at the details of each field - Subject



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)

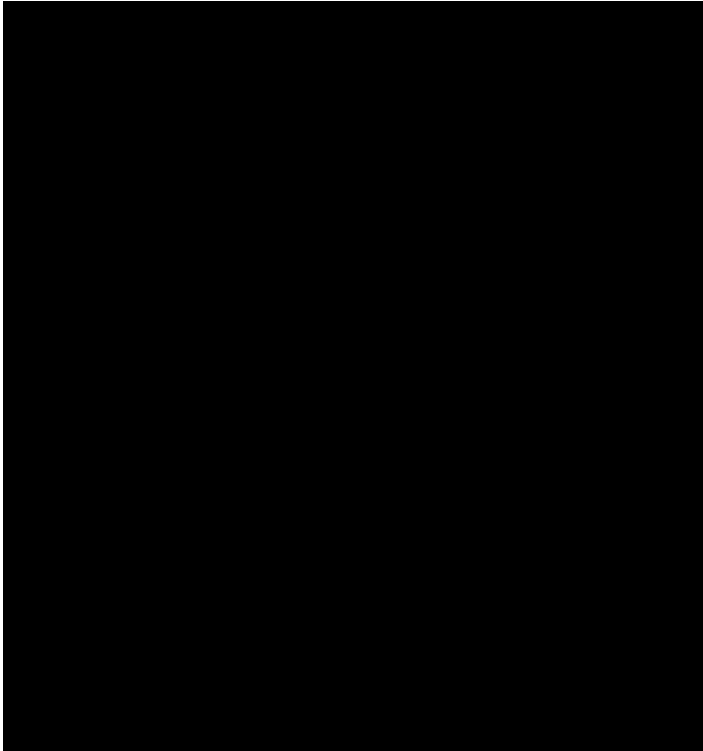
And look at the details of each field - CRL DP location



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



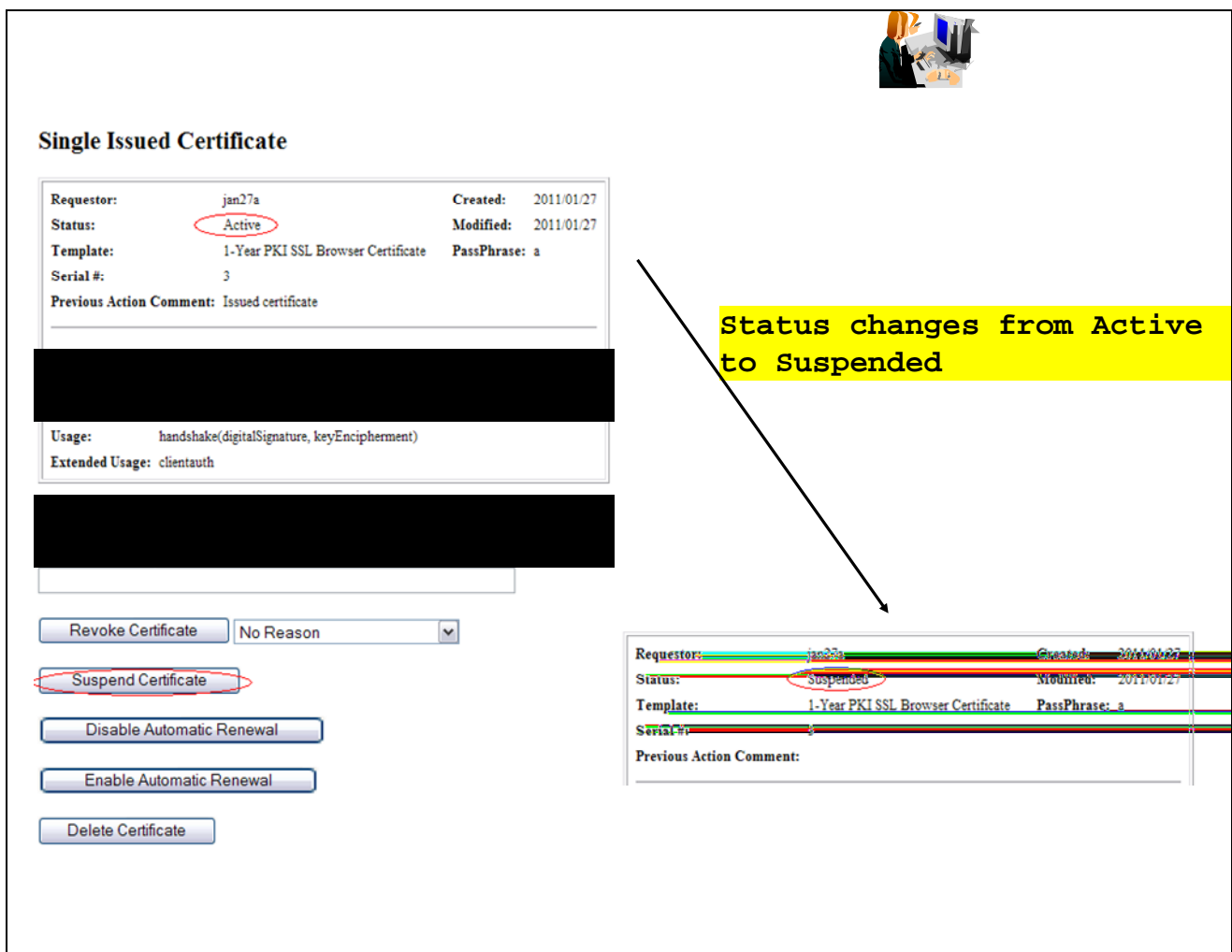
This is hardcoded by administrator in pkiserv.tmpl

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'



The screenshot displays a web interface for managing certificates. At the top right, there is a small icon of a person at a computer. The main heading is "Single Issued Certificate". Below this, a table-like structure shows certificate details: Requestor: jan27a, Created: 2011/01/27, Status: Active (circled in red), Modified: 2011/01/27, Template: 1-Year PKI SSL Browser Certificate, PassPhrase: a, Serial #: 3, and Previous Action Comment: Issued certificate. Below the details are two large black redaction boxes. Further down, the Usage is listed as "handshake(digitalSignature, keyEncipherment)" and Extended Usage as "clientauth". At the bottom, there are several buttons: "Revoke Certificate" with a dropdown menu set to "No Reason", "Suspend Certificate" (circled in red), "Disable Automatic Renewal", "Enable Automatic Renewal", and "Delete Certificate". To the right of the main interface, a yellow box contains the text "Status changes from Active to Suspended" with an arrow pointing to a smaller, semi-transparent version of the certificate details table below. In this smaller table, the Status is now "Suspended" (circled in red).

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		

Usage: handshake(digitalSignature, keyEncipherment)
Extended Usage: clientauth

Revoke Certificate No Reason

Suspend Certificate

Disable Automatic Renewal

Enable Automatic Renewal

Delete Certificate

Status changes from Active to Suspended

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



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*

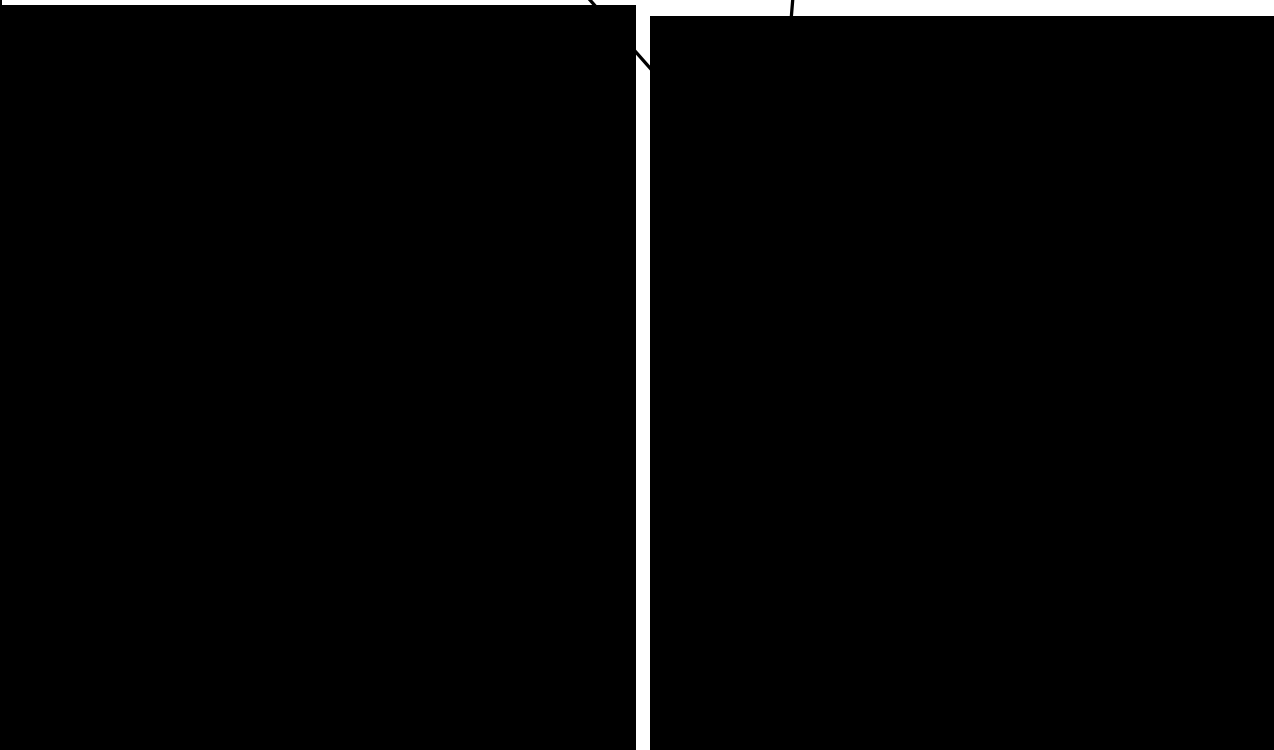
Note: *In this lab, in addition to the roles of the certificate owner and the PKI Services administrator, you also play the role of any third party who wants to verify your certificate's status. In this lab setup, you can export the certificate you've just created, and its issuers' chain in the way described 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: 0 = 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: ACDDDB2434055FF87FFB8790B3F09AED8A3EB0816

Serial Number: 01

Cert Status: revoked Cert 01 is suspended (from reason 0x6)

Revocation Time: Dec 6 22:36:04 2006 GMT

Revocation Reason: certificateHold (0x6)

This Update: Dec 7 03:13:46 2006 GMT

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: 0 = 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: ACDDDB2434055FF87FFB8790B3F09AED8A3EB0816

Serial Number: 01 Cert 01 is not revoked or suspended

Cert Status: good

This Update: Dec 7 03:27:54 2006 GMT



Exercise 7 – Customization

A. Customize a template in pkiserv.templ

- 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

```
File Edit View Communication Actions Window Help
[Icons]
Menu List Mode Functions Utilities Help
ISPF Command Shell
Enter TSO or Workstation commands below:
===> omvs_
```

- Edit the pkiserv.templ file under /sharelab/sharbx/pkilab in a similar way shown below.
(Note: Save a copy before you make any changes – cp pkiserv.templ pkiserv.templ.backup)

```
MVS1:SHARA01:/sharelab/shara01: >
===> cd pkilab
RUNNING
MVS1:SHARA01:/sharelab/shara01: > cd pkilab
MVS1:SHARA01:/sharelab/shara01/pkilab: >
===> cp pkiserv.templ pkiserv.templ.backup
INPUT
MVS1:SHARA01:/sharelab/shara01: > cd pkilab
MVS1:SHARA01:/sharelab/shara01/pkilab: >
===> oedit pkiserv.templ
INPUT
```

You want to

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

Here are the steps:

- o 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:

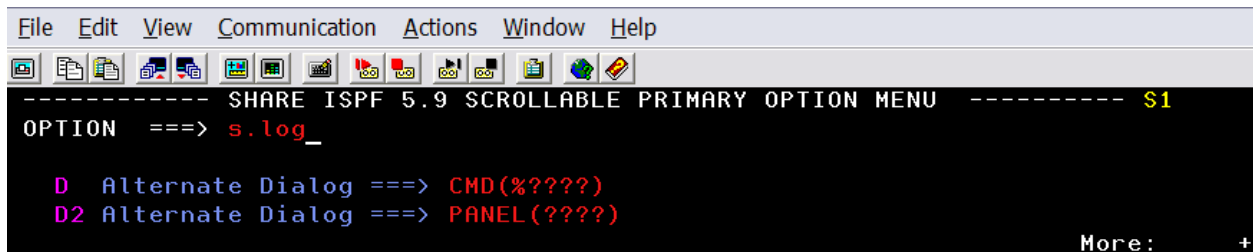
under **<CONTENT>**

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/sharbx/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



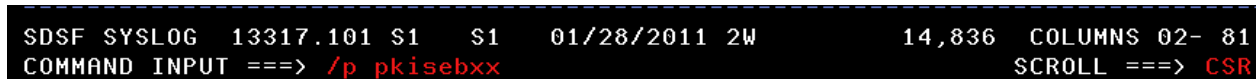
File Edit View Communication Actions Window Help

```
----- SHARE ISPF 5.9 SCROLLABLE PRIMARY OPTION MENU ----- $1
OPTION ==> s.log_

D Alternate Dialog ==> CMD(%????)
D2 Alternate Dialog ==> PANEL(????)

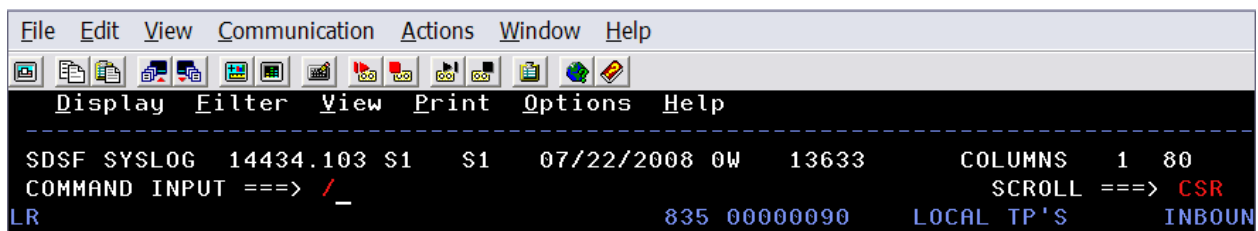
More: +
```

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



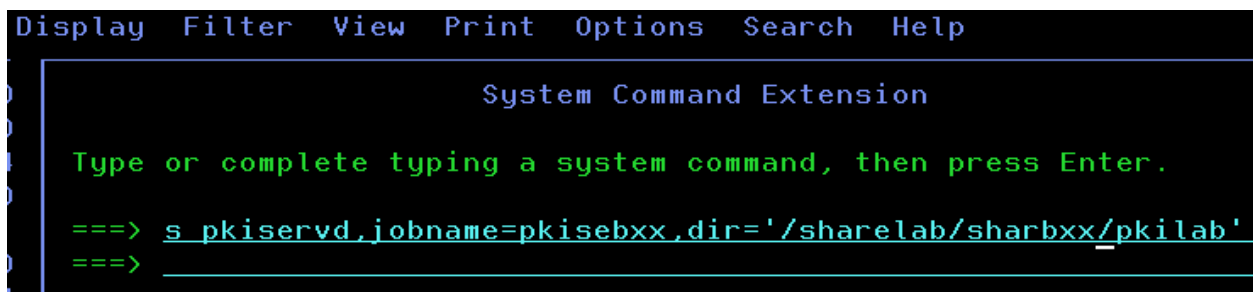
```
SDSF SYSLOG 13317.101 S1 S1 01/28/2011 2W 14,836 COLUMNS 02- 81
COMMAND INPUT ==> /p pkisebxx SCROLL ==> CSR
```

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



```
File Edit View Communication Actions Window Help
Display Filter View Print Options Help
-----
SDSF SYSLOG 14434.103 S1 S1 07/22/2008 0W 13633 COLUMNS 1 80
COMMAND INPUT ==> / SCROLL ==> CSR
LR 835 00000090 LOCAL TP'S INBOUN
```

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



```
Display Filter View Print Options Search Help

System Command Extension

Type or complete typing a system command, then press Enter.

==> s pkiservd,jobname=pkisebxx,dir='/sharelab/sharbx/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

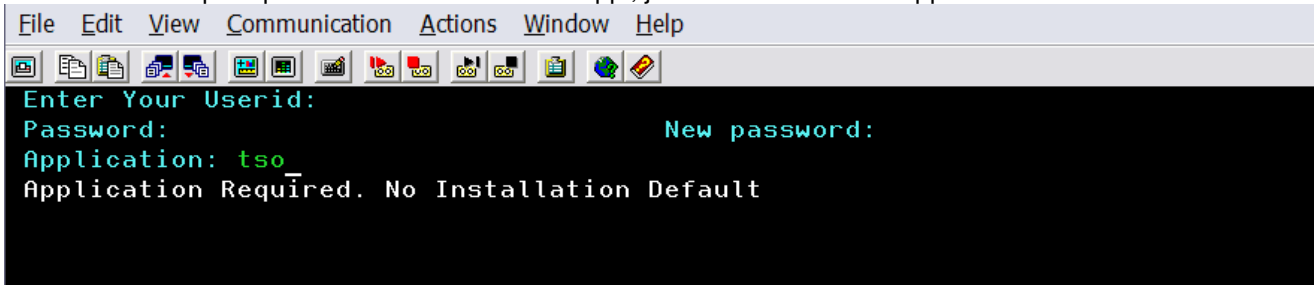
Some commands for the TSO session (3270 interface)

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

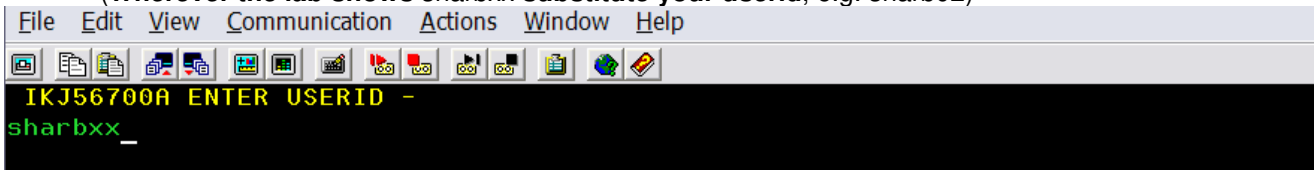
Logon to MVS system

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



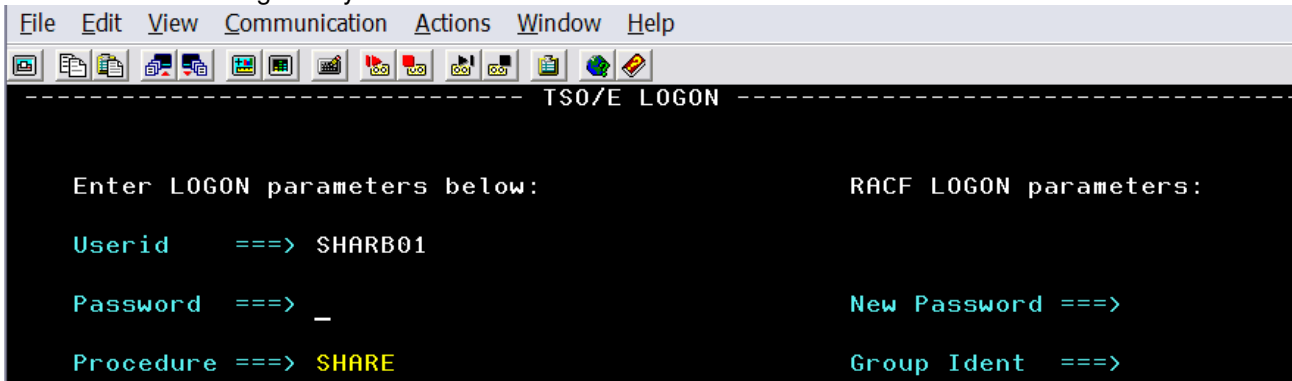
```
File Edit View Communication Actions Window Help
Enter Your Userid:
Password:
Application: tso
Application Required. No Installation Default
New password:
```

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



```
File Edit View Communication Actions Window Help
IKJ56700A ENTER USERID -
sharbxx_
```

- c. Password: given by the instructor



```
File Edit View Communication Actions Window Help
----- TSO/E LOGON -----
Enter LOGON parameters below:
Userid ==> SHARB01
Password ==> _
Procedure ==> SHARE
RACF LOGON parameters:
New Password ==>
Group Ident ==>
```

- 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 ocsf
-iissuer \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/sq246968.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**
 - f* **PKI Services Guide and Reference (SA22-7693)**
 - f* **OCSF Service Provider Developer's Guide and Reference (SC24-5900)**
 - f* **ICSF Administrator's Guide (SA22-7521)**
 - f* **System SSL Programming (SC24-5901)**
- **Security Server Manuals:**
 - f* **RACF Command Language Reference (SC28-1919)**
 - f* **RACF Security Administrator's Guide (SC28-1915)**
 - f* **RACF Callable Services Guide (SC28-1921)**
 - f* **LDAP Administration and Use (SC24-5923)**
- **IBM HTTP Server Manuals:**
 - f* **Planning, Installing, and Using (SC31-8690)**
- **Other Sources:**
 - f* **PKIX - <http://www.ietf.org/html.charters/pkix-charter.html>**

Disclaimer

- The information contained in this document is distributed on an "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.