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.



- 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://mvsl.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://mvsl.centers.ihost:8041/Sharb01/public-
  cqi/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):
 <u>http://mvs1.centers.ihost.com:8041/Sharbxx/public-cgi/camain.rexx</u>
- 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

	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
	Request Certificate
	Pick up a previously requested certificate
	Enter the assigned transaction ID
	Select the certificate return type PKI Browser Certificate
	Pick up Certificate
2	Renew or revoke a previously issued browser certificate
	Penew or Revoke Cartificate
	Neitew of Nevoke Celulicate
	Administrators click here
	Go to Administration Page
j	email: webmaster@your-company.com
J	email: webmaster@your-company.com

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

Г

the CA certificate to enable SSL sessions for PK	
Request a new certificate using a model	
Select the certificate template to use as a model	1-Year PKI SSL Browser Certificate
Request Certificate	1-Year PKI SSL Browser Certificate 1-Year PKI S/MIME Browser Certificate 2-Year PKI Windows Logon Certificate
Pick up a previously requested certificate	2-Year PKI Browser Certificate For Authenticating To z/OS 5-Year PKI SSL Server Certificate 5-Year PKI IPSEC Server (Firewall) Certificate
Enter the assigned transaction ID	2-Year PKI Intermediate CA Certificate 2-Year PKI Authenticode - Code Signing Certificate
Select the certificate return type PKI Browse	5-Year SCEP Certificate - Preregistration 1-Year PKI Generated Key Certificate
Pick up Certificate	In Year PKi Ceruicate for Extensions Demonstration
Renew or revoke a previously issued brow Renew or Revoke Certificate Recover a previously issued certificate wh Enter the email address when the original certifi	ser certificate ose key was generated by PKI Services cate was requested
Enter the same pass phrase as on the request fo	m Recover Certificate
Administrators click here	

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

1-Year PKI SSL Browser Certificate	
Choose one of the following: • Request a New Certificate	Fill in the info
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 Reenter your pass phrase to confirm	These input fields are controlled by the <content> entries on p7</content>
Email address for distinguished name MAIL = attribute (optional) Common Name Select the following key information Cryptographic Service Provider Microsoft Base Cryptographic Provider v1.0 v Enable strong private key protection? No v	The browser will use the selecte crypto provider to generate public/private key pair. Pick Microsoft Base Cryptographic Provider.
Sutmit certificate request Clear Pick Up a Previously Issued Certificate Retrieve your certificate email: webmaster@your-company.com	

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

Request submitt	d successfull	y 🚑		
Here's your transaction ID. You will r	ed it to retrieve your certifica	te. Press 'Continue' to retriev	e the certificate.	
1jTQjs0h/cpk2SHV+++++++				
Continue				
email: webmaster@your-company.co	:			

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

Please bookmark this page	
Since your certificate may not have been issued yet, we recommend teasiest way to check your status.	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
Enter the assigned transaction ID	
1kA6s3KFhriZ2Tc+++++++	
If you specified a pass phrase when submitting the certificate reques	t, type it here, exactly as you typed it on the request form
Retrieve and Install Certificate	
Home page	

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



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

instear a	e CA certificate to enable SSL sessions for PKI Services
Choo	ose one of the following:
• F	Request a new certificate using a model
S	elect the certificate template to use as a model 1-Year PKI SSL Browser Certificate
	Request Certificate
• 1	ick up a previously requested certificate
E	inter the assigned transaction ID
S	elect the certificate return type PKI Browser Certificate 💌
[Pick up Certificate
• F	Renew or revoke a previously issued browser certificate
ſ	Renew or Revoke Certificate
• 2	Administrators click here

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

ose one of the following:		
Work with a single certificate request		
Enter the Transaction ID:		
Prod	cess Request	
Work with a single issued certificate Enter the Serial Number: Pro	cess Certificate	
Specify search criteria for certificates an	d certificate requests	
Show all requests	Steel Certificates	
Show requests pending approval	Show revoked certificates	
O Show approved requests	Show suspended certificates	
O Show completed requests	Show expired certificates	
O Show rejected requests	Show active certificates (not expired, not revoked, not suspended)	
O Show rejections in which the client has be	een notified O Show disabled certificates (suspended or revoked, not expired)	
O Show preregistered requests	O Show active, automatic renewal enabled certificates	
	Show active, automatic renewal disabled certificates	
	O Show active, not renewable certificates	
Additional search criteria (Optional)		
Requestor's name		
Show recent activity only (Not Selected)	V	
Show certificates that will expire (Not Sele	cted) (Only applicable to active certificates when recent activity is not selected)	
Find Certificates or Certificat	e Requests	

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

	unca	e Requests		
		Req	uest sur	<mark>mary info</mark>
he f	ollowin	g certificate requests matched the search criteria s	pecified:	
u 🗹	Requestor	Certificate Request Information	Status	Dates
	ian)7a	Trans ID: <u>1kA8sDZcZjkZ2Tc+++++++</u> Template1 Ver PKLSSI Brower Certificate	Pending Approval	Created: 2011/01/27
	Juizza	Subject: CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	- chang Approva	Modified:2011/01/27
• (• s	Click on a Select and	transaction ID to see more information or to modify, approve, rejec take action against multiple requests at once tent (Optional)	t, or delete requ	ests individually
• • • • • •	Click on a Select and Action Comm	transaction ID to see more information or to modify, approve, reject take action against multiple requests at once tent (Optional)	t, or delete requ	ests individually
• • • • • • [[(Click on a Select and Action Comm Approve Reject	transaction ID to see more information or to modify, approve, reject take action against multiple requests at once tent (Optional) - Approve without modification all requests selected above that are "Pending App Reject all requests selected above that are "Pending Approval"	t, or delete requ roval''	ests individually
• • • • • • [[[[[[[Click on a Select and Action Comm Approve Reject	transaction ID to see more information or to modify, approve, reject take action against multiple requests at once tent (Optional) - Approve without modification all requests selected above that are "Pending App Reject all requests selected above that are "Pending Approval"	t, or delete requ	ests individually
• • • • • • [[[[[[Click on a Select and Action Comm Approve Reject	transaction ID to see more information or to modify, approve, reject take action against multiple requests at once tent (Optional) - Approve without modification all requests selected above that are "Pending App Reject all requests selected above that are "Pending Approval" Delete all requests selected above	t, or delete requ proval" Criteria	ests individually

- 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'

		2000 - F 30.	1111111111111111111		- 0 1 '			
Requestor:	jan27a	Created:	2011/01/27	Th	e Subj	ect's	nam	e va.
Status:	Pending Approval	Modified:	2011/01/27	CO	me fro	m the	use	r inp
Transaction Id:	1kA8sDZcZjkZ2Tc+++++++++	Passphrase:	a	an	d hard	coded	val	ue in
Template:	1-Year PKI SSL Browser Certificate			pk	iserv.	tmpl		
Subject:	CN=jan27a,OU=Class 1 Internet Ce	rtificate CA,O=	The Sharb01 Firm,C=U					
Issuer:	CN=Sharb01 CA,OU=Test,O=The	Sharb01 Firm,C=	=US					
Validity:	2011/01/27 00:00:00 - 2012/01/26 23	3:59:59						
Usage:	handshake(digitalSignature, keyEncip	pherment)						
Extended Usage	: clientauth							
Fingerprints:				Peo		dota	s i 1	inf
Fingerprints: SHA1:	99:56:1F:05:34:3A:3D:51:A2:F2:3A	:DC:A0:E1:0F:F	F6:CC:72:19:79	Req	[uest	deta	ail	inf
Fingerprints: SHA1: MD5:	99:56:1F:05:34:3A:3D:51:A2:F2:3A 24:9F:4E:F6:D2:A1:FB:B8:E6:BB:3	:DC:A0:E1:0F:F 7:F8:96:58:0D:9	F6:CC:72:19:79	Req	<mark>luest</mark>	deta	ail	inf
Fingerprints: SHA1: MD5: SHA256:	99:56:1F:05:34:3A:3D:51:A2:F2:3A 24:9F:4E:F6:D2:A1:FB:B8:E6:BB:3 A8:4F:8A:7B:74:74:28:84:27:9F:ED	:DC:A0:E1:0F:F 7:F8:96:58:0D:9 9:95:79:95:16:D8	F6:CC:72:19:79)7):68:10:59:09:F5:54:5A	Reg 1:96:BA:41:5E:24	[<mark>uest</mark> :8F:3C:3F:F	deta	ail	inf
Fingerprints: SHA1: MD5: SHA256: SHA512:	99:56:1F:05:34:3A:3D:51:A2:F2:3A 24:9F:4E:F6:D2:A1:FB:B8:E6:BB:3 A8:4F:8A:7B:74:74:28:84:27:9F:ED 29:04:6C:5B:50:1C:D5:AC:A9:3C:A 11:55:CD:7B:3B:9B:71:7C:4B:E0:0	:DC:A0:E1:0F:F 7:F8:96:58:0D:9 9:95:79:95:16:D8 44:ED:04:4B:9A A:60:BB:0F:36:I	F6:CC:72:19:79 7 5:68:10:59:09:F5:54:5A :B8:52:B5:16:6A:00:F1 DC:B8:6B:D6:B1:49:F	Rec 1:96:BA:41:5E:24 6:7D:05:4E:8A:D 1:07:5C:61:08:B3	[Uest :8F:3C:3F:F C:B0:19:3F :11:E5:C6:0	deta 55 :48:4C: 0:27	ail	inf
Fingerprints: SHA1: MD5: SHA256: SHA512: ction to take ction Comment ((Approve)	99:56:1F:05:34:3A:3D:51:A2:F2:3A 24:9F:4E:F6:D2:A1:FB:B8:E6:BB:3 A8:4F:8A:7B:74:74:28:84:27:9F:ED 29:04:6C:5B:50:1C:D5:AC:A9:3C:A 11:55:CD:7B:3B:9B:71:7C:4B:E0:0 : Coptional)	:DC:A0:E1:0F:F 7:F8:96:58:0D:9 9:95:79:95:16:D8 A:ED:04:4B:9A A:60:BB:0F:36:I	F6:CC:72:19:79 7 5:68:10:59:09:F5:54:5A :B8:52:B5:16:6A:00:F1 DC:B8:6B:D6:B1:49:F	Rec 1:96:BA:41:5E:24 6:7D:05:4E:8A:D 1:07:5C:61:08:B3	[Uest :8F:3C:3F:F C:B0:19:3F :11:E5:C6:0	deta 75 :48:4C: 0:27	ail	info
Fingerprints: SHA1: MD5: SHA256: SHA512: Action to take ction Comment (Approve) Reject Requ	99:56:1F:05:34:3A:3D:51:A2:F2:3A 24:9F:4E:F6:D2:A1:FB:B8:E6:BB:3 A8:4F:8A:7B:74:74:28:84:27:9F:ED 29:04:6C:5B:50:1C:D5:AC:A9:3C:A 11:55:CD:7B:3B:9B:71:7C:4B:E0:0 : : Optional) Request As It is	:DC:A0:E1:0F:F 7:F8:96:58:0D:9 9:95:79:95:16:D8 A4:ED:04:4B:9A A:60:BB:0F:36:I	F6:CC:72:19:79 17 1:68:10:59:09:F5:54:5A 1:B8:52:B5:16:6A:00:F1 DC:B8:6B:D6:B1:49:F	Reg 1:96:BA:41:5E:24 6:7D:05:4E:8A:D 1:07:5C:61:08:B3	[Uest :8F:3C:3F:F C:B0:19:3F :11:E5:C6:0	deta 55 548:4C: 0:27	ail	info
Fingerprints: SHA1: MD5: SHA256: SHA512: ction to take ction Comment ((Approve) Reject Requ Delete Req	99:56:1F:05:34:3A:3D:51:A2:F2:3A 24:9F:4E:F6:D2:A1:FB:B8:E6:BB:3 A8:4F:8A:7B:74:74:28:84:27:9F:ED 29:04:6C:5B:50:1C:D5:AC:A9:3C:A 11:55:CD:7B:3B:9B:71:7C:4B:E0:0 : Optional) Request As It is uest	:DC:A0:E1:0F:F 7:F8:96:58:0D:9 9:95:79:95:16:D8 44:ED:04:4B:9A A:60:BB:0F:36:I	F6:CC:72:19:79 17 1:68:10:59:09:F5:54:5A 1:B8:52:B5:16:6A:00:F1 DC:B8:6B:D6:B1:49:F	Rec 1:96:BA:41:5E:24 6:7D:05:4E:8A:D 1:07:5C:61:08:B3	[uest :8F:3C:3F:F C:B0:19:3F :11:E5:C6:0	deta :48:4C: :0:27	ail	info

- 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'

equestor	Request Information	Dates	
1	Trans ID:1kA8sDZcZjkZ2Tc++++++++	Created: 2011/01/27	
127a	Template:1-Year PKI SSL Browser Certificate Subject:CN=jan27a OU=Class 1 Internet Certificate CA O=The Sharb01 Firm C=US	Modified:2011/01/27	
u may n Subject	odify the following fields by providing new values. To remove a field simply blar Distinguished Name: ame (optional)	ık it out or de-select it.	
n27a			
manizatio	nal Unit (Aptional)		
lass 1 lr	nternet Certificate CA		Page primed with
rganizatio	nal Unit (optional)		requested info
			requested IIIO.
rganizatio	n (optional)		Administrator can
The Shar	b01 Firm		change them if
ountry			
JS			necessary.
Data er ndicate th Server s Client s Code si Email p	extended key usage the certificate side authentication (serverAuth) de authentication (clientAuth) gning (codeSigning) rotection (emailProtection) ppings Extension value(s) in subject-id@host-name form (optional)		
lostIdMa	ppings Extension value(s) in subject-id@host-name form (optional)		
lostIdMa	ppings Extension value(s) in subject-id@host-name form (optional)		
lostIdMa	ppings Extension value(s) in subject-id@host-name form (optional)		
Validi	ty Period:		
	ificate becomes valid Date certificate expires (at end of day)		
2011			
2011	1 27 2012 1 26 Renewal: Not set		
2011 automatic	1 27 2012 1 26 1 Renewal: Not set mment (Optional) 1		
2011 Automatic	1 27 2012 1 26 Renewal: Not set mment (Optional) Approve with specified modifications]

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

Processing succe	esstul
Request with transaction ID 1j913qJF	RQoNp2Tc++++++++ is successfully approved.
You may continue to approv	e/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'

ose one of the following:	to display all the requests
Work with a single certificate request	
Enter the Transaction ID:	
Process Req	uest
Work with a single issued certificate	
Enter the Serial Number:	
Process Cert	ficate
Specify search criteria for certificates and certifica Certificate Requests	te requests Issued Certificates
Show all requests	O Show all issued certificates
O Show requests pending approval	○ Show revoked certificates
O Show approved requests	O Show suspended certificates
Show completed requests	○ Show expired certificates
O Show rejected requests	Show active certificates (not expired, not revoked, not suspended)
\bigcirc Show rejections in which the client has been notified	Show disabled certificates (suspended or revoked, not expired)
O 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 Reques	ts

- 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
		Trans ID: <u>1kA8sDZcZjkZ2Tc++++++++</u>	Approved	Created: 2011/01/27
	jan2/a	Subject: CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Serial #: 3	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)

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

Delete - Delete all requests selected above

Respecify Your Search Criteria

Home Page

• 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 Rec	quest
Work with a single issued certificate Enter the Serial Number:	To display all the certificates
Process Cer	tificate
• Specify search criteria for certificates and certific	ate requests
Certificate Requests	Issued Certificates
O Show all requests	● Show all issued certificates
O Show requests pending approval	O Show revoked certificates
O Show approved requests	O Show suspended certificates
O Show completed requests	O Show expired certificates
O Show rejected requests	O Show active certificates (not expired, not revoked, not suspended)
\bigcirc Show rejections in which the client has been notified	1 \bigcirc Show disabled certificates (suspended or revoked, not expired)
O Show preregistered requests	O Show active, automatic renewal enabled certificates
	\bigcirc Show active, automatic renewal disabled certificates
	O Show active, not renewable certificates
Additional search criteria (Optional)	
Requestor's name	
Show recent activity only (Not Selected)	Y
AL-0.1.1.5	

- 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
v	jan27a	Serial #: <u>3</u> Template: 1-Year PKI SSL Browser Certificate		Active	No	Created: 2011/01/27
		Subject: CN=jan27a,OU=Class 1 Internet Certificate CA,O=T1	he Sharb01 Firm,C=US			Modified:2011/01/27
10056	e one of t	he following:	Certifica	ate	summ	ary info
. (lick on a s	erial number to see more information or to perform action	on a single certificat	e		
. 5	elect and ta	ike action against multiple certificates at once				
A	ction Comm	ent (Optional)				
Γ						
_						
	Revoke	No Reason 🖌 - Revoke all selected a	ctive certificates			
	Suspend	- Suspend all selected active certificates				
~						
L	Delete	Delete all selected certificates				
		_				
			Respecify Your Sea	arch Ci	riteria	
			Home Pag	je		

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

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		
	handshake(digitalSignature, kevEncipherment)		
Usage:			

Action to take:

Revoke Certificate	No Reason	~
Suspend Certificate		
Disable Automatic	Renewal	
Enable Automatic C	Donowal	

Certificate detail info

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'

	e 📺	
oose one of the following:		
Request a new certificate using a model		
Select the certificate template to use as a model 1-Year P	KI SSL Browser Certificate	
Request Certificate		
Pick up a previously requested certificate		
Enter the assigned transaction ID		
1j9l3qJRQoNp2Tc+++++++		
Select the certificate return type PKI Browser Certificate	✓	
Pick up Certificate		
Renew or revoke a previously issued browser	• certificate	
Renew or Revoke Certificate		
Administrators click here		
Go to Administration Fage		
l: webmaster@your-company.com		

• 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'

100	se 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	•
	Request Certificate	1-Year PKI SSL Browser Certificate 1-Year PKI S/MIME Browser Certificate 2-Year PKI Windows Logon Certificate]
•	Pick up a previously requested certificate	2-Year PKI Browser Certificate For Authenticating To z/OS 5-Year PKI SSL Server Certificate 5-Year PKI IPSEC Server (Firewall) Certificate	
	Enter the assigned transaction ID	5-Year PKI Intermediate CA Certificate 2-Year PKI Authenticode - Code Signing Certificate	
	Select the certificate return type PKI Browse	5-Year SCEP Certificate - Preregistration 1-Year PKI Generated Key Certificate n-Year PKI Certificate for Extensions Demonstration	
	Pick up Certificate		
•	Renew or revoke a previously issued brows Renew or Revoke Certificate	er certificate	
	Recover a previously issued certificate who	se key was generated by PKI Services	
	Enter the email address when the original certific	ate the remeted	
		are was requested	
	Enter the same pass phrase as on the request for	m Recover Certificate	
	Enter the same pass phrase as on the request for Administrators click here	m Recover 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'

	llowing:		Fill in the info
• Request a New Ce	rtificate		
Enter values for the	following field(s)		
Enter the requestor'	email address		
Pass phrase for sect	ring this request. You will need to supply this value whe	n retrieving your certificate	These input fields are controlled by the
Reenter your pass p	hrase to confirm		<content> entries on p</content>
Common Name			
Email address for di	tinguished name MAIL= attribute (optional)		
Email address for di	tinguished name MAIL= attribute (optional)		
Email address for di	ntinguished name MAIL= attribute (optional)		~
Email address for di Select the key type RSA - 512 RSA - 512	and key size	Select th	e key type and key si
Email address for di Select the key type RSA - 512 RSA - 512 RSA - 1024 RSA - 1024	and key size	Select the	e key type and key si o generate
Email address for di Select the key type RSA - 512 RSA - 512 RSA - 1024 RSA - 2048 RSA - 4096 NISTECC - 192	and key size	Select the for PKI to public/pr	e key type and key si o generate ivate key pair.
Email address for di Select the key type RSA - 512 RSA - 512 RSA - 1024 RSA - 2048 RSA - 2048 RSA - 4096 • NISTECC - 192 NISTECC - 224	and key size	Select the for PKI to public/pr	e key type and key si o generate ivate key pair.
Email address for di Select the key type RSA - 512 RSA - 512 RSA - 1024 RSA - 2048 RSA - 4096 • NISTECC - 192 NISTECC - 224 NISTECC - 234	attinguished name MAIL= attribute (optional) and key size atte request Issued Certificate certificate	Select the for PKI to public/pr	e key type and key si o generate ivate key pair.
Email address for di Select the key type RSA - 512 RSA - 1024 RSA - 2048 RSA - 4096 NISTECC - 192 NISTECC - 224 NISTECC - 234 NISTECC - 521	and key size	Select the for PKI to public/pr	e key type and key si o generate ivate key pair.
Email address for di Select the key type RSA - 512 RSA - 512 RSA - 1024 RSA - 1024 RSA - 4096 • NISTECC - 192 NISTECC - 284 NISTECC - 284 NISTECC - 284 NISTECC - 284 NISTECC - 284 NISTECC - 160 BPECC - 160 BPECC - 192 DPECC - 192	tinguished name MAIL= attribute (optional) and key size rate request Issued Certificate certificate ty.com	Select the for PKI to public/pr	e key type and key si o generate ivate key pair.

• 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

• 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.)

Requestor: Status: Transaction Id:	jan27b@gmail.com Approved IkASYYeAwtcZ2Tc++++++++	Created: Modified: Passphrase:	2011/01/27 2011/01/27 a	Request	detail	info
Template: Serial #:	1-Year PKI Generated Key Certificate	NotifyEmail:	jan27b@gmail.com			
Subject:	CN=jan27b,OU=Class 1 Internet Certii	ficate CA,O=The	Sharb01 Firm,C=US			
Issuer: Validity:	CN=Sharb01 CA,OU=Test,O=The Sha 2011/01/27 00:00:00 - 2012/01/26 23:51	rb01 Firm,C=US				
Usage:	handshake(digitalSignature, kevEnciphe	rment)				
Extended Usage	not specified					
	•					
Delete Req	Jest					
Delete Req	Jest		Administrati	on Home Page		
Delete Req	lesi		Administrati	on Home Page		
Delete Req	lest		Administrati	on Home Page		

• 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.

serial #: 3 Template: 1. Year PKI SSL Browser Certificate Subject: CN=jan27a, OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=U3 Active No Serial #: 3 Template: 1. Year PKI Generated Key Certificate Active Yes Created: 2011/01/27 jan27b@gmail.com Template: 1. Year PKI Generated Key Certificate Active Yes Wodified:2011/01/27 jan27b@gmail.com Template: 1. Year PKI Generated Key Certificate Active Yes Wodified:2011/01/27 jan27b@gmail.com Template: 1. Year PKI Generated Key Certificate Active Yes Wodified:2011/01/27 see 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 Certificate summary inf Active No Reason • Revoke all selected active certificates . Suspend • Suspend all selected active certificates Delete • Delete all selected certificates Respecify Your Search Criteria Respecify Your Search Criteria	u 🗹	Requestor	Certificate Information	Status	Key archived	Dates
Image: Subject: CN=jan27a,OU=Class I Internet Certificate CA,O=The SharbOI Firm,C=US Active [Yes Modified:2011.01.27 jan27b@gmail.com Template:1-Year PKI Generated Key Certificate Active [Yes Greated:2011.01.27 jan27b@gmail.com Template:1-Year PKI Generated Key Certificate Active [Yes Modified:2011.01.27 subject: CN=jan27b,OU=Class I Internet Certificate CA,O=The SharbOI Firm,C=US Active [Yes Modified:2011.01.27 see 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 Certificate Summary inf Action Comment (Optional)			Serial #: 3	Anting	No	Created: 2011/01/27
Serial #: 4 un27b@gmail.com Template:1-Year PKI Generated Key Certificate Subject: CN=jan27b,OU=Class 1 Internet Certificate CA,O=The SharbO1 Firm,C=US Active Yes Modified:2011/01/27 Active 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 No Reason • Revoke all selected active certificates Suspend • Suspend all selected active certificates Delete • Delete all selected certificates Respecify Your Search Criteria		Jan27a	Subject: CN=jan27a,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Active	NO	Modified:2011/01/27
Introggnation Propagation to generative Action Concerner Action Concerner Certificate CA,O=The Sharb01 Firm,C=US Item item item item item item item item i	-57	ian 77h@amail.com	Serial #: 4 Tamplate 1. Vaar DVI Generated Key Certificate	Activa	Vac	Created: 2011/01/27
Action Comment (Optional) Revoke No Reason · Revoke all selected active certificates Suspend - Suspend all selected active certificates Respecify Your Search Criteria		Janz / Oleginan.com	Subject: CN=jan27b,OU=Class 1 Internet Certificate CA,O=The Sharb01 Firm,C=US	Active	103	Modified:2011/01/27
Delete all selected certificates Respecify Your Search Criteria		Suspend - St	uspend all selected active certificates			
Respecify Your Search Criteria						
		Delete - Delete	all selected certificates			
		Delete _ Delete	all selected certificates Respecify Your Search Crit	teria		
		Delete . Delete	all selected certificates Respecify Your Search Crit	teria		
		Delete - Delete	all selected certificates Respecify Your Search Crit	teria		

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.

	e one of the following:
. 1	Request a new certificate using a model
	Select the certificate template to use as a model 1-Year PKI SSL Browser Certificate
ſ	Request Certificate
l	
. 1	Pick up a previously requested certificate
F	Enter the assigned transaction ID
[1kA8YYeAwtcZ2Tc++++++++
0	Select the certificate return type PKI Key Certificate
ſ	Pick up Certificate
• 1	Renew or revoke a previously issued browser certificate
	December Develop Op (for the participation)
	Renew or Revoke Certificate
1	Pacavar a previously issued cartificate whose law was generated by PKI Services
	Recorer a prenousi, issued certificate anose ne, aus generated by I to services
	Enter the email address when the original certificate was requested
H	
F	
1	

- 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

Enter the assigned transaction ID				
1kA8YYeAwtcZ2Tc+++++++++			15 m 2	2
f you specified a pass phrase when subm	nitting the certificat	e request, type it her	e, exactly as you typed	it on the request form
· · · · · · · · · · · · · · · · · · ·			.,	
Retrieve Certificate				
Home Page				
Thomas Tuge				

• Click Open.

Do you w	rant to open or save this file?
	Name: mycert.p12
-je	Type: Personal Information Exchange, 3.02 KB
	From: mvs1.centers.ihost.com
	Open Save Cancel
🔊 Y	While files from the Internet can be useful, some files can potentially
🥑 !	arm your computer. If you do not trust the source, do not open or ave this file. What's the risk?

• Click Next.

Tokan -	Welcome to the Certificate Import Wizard
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, click Next.
	🛀

• Click Next.

F	ile to Import
	Specify the file you want to import.
	Eile name:
	s\Temporary Internet Files\Content.IE5\8LG9C10V\mycert[1].p12 Browse
	Note: More than one certificate can be stored in a single file in the following formats:
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
	Microsoft Serialized Certificate Store (.SST)
	< Back Next > Cancel

• Enter the password and check the key as exportable.



• Click Next.

Certificate Store		L
Certificate stores are system a	areas where certificates are kept.	2
Windows can automatically sel	lect a certificate store, or you can specify a location fo	or
 Automatically select the 	certificate store based on the type of certificate	
O Place all certificates in the	he following store	
Certificate store:		
	Browse	

• Click Finish.

Completing the C Wizard	eted the Certificate Import
You have specified the follow	wing settings:
Certificate Store Selected Content File Name	Automatically determined by 1 PFX C:\Documents and Settings\A
«]	•
< <u>B</u> ack	Finish Cancel

• 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



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

A. Create a request

<u>F</u> ile	<u>E</u> dit	<u>V</u> iew <u>C</u> ommunica	tion <u>A</u> ctions	<u>W</u> indow	<u>H</u> elp			
	È È	a 💀 🖼 🔳 🗃	ba 起 💩 📾	F 🗎 🌰	•			
		SHARE I	SPF 5.9 SC	ROLLAB	LE PRIMARY	OPTION MENU		<mark>\$1</mark>
0P	TION	===> <mark>6</mark> _						
	D Al	ternate Dialo	q ===> CMD)(%????)			
	D2 A1	ternate Dialo	g ===> PAN	IEL (???	?)			
							۱	lore:
	The t	ime is 12:30	p.m. on Tu	iesday,	July 22,	2008 (2008.2)	04)	
ľ í	Your	uid is SHARBO	1 dsn pre	efix is	SHARB01	proc is <mark>SHA</mark>	RE sys	is <mark>\$1</mark>
	9	SETTINGS	- Specifu	ISPE	parameters			
	1	VIEW	- View so	ource d	ata or out	put listina		
	1 P	VIEW-OE	- View/Br	owse f	iles in th	e Open Editi	on file su	ustem
	2	EDIT	- Create	or cha	nge source	data		,
	2P	EDIT-0E	- Edit fi	les in	the Open	Edition file	system	
:	3	UTILITIES	- Perform	ı utili	ty functio	ns		
:	3P	ISHELL-0E	- Open Ec	lition	ISPF shell			
· ·	4	FOREGROUND	- Invoke	langua	ge process	ors in foreg	round	
	5	BATCH	- Submit	job fo	r language	processing		
	6	COMMAND	- Enter 1	SO com	mand, CLIS	T, or REXX e	xec	
	7	DIALOG TEST	- Perform	ı dialo	g testing			
	8	LM UTILITIES	- Perform	ı libra	ry adminis	trator utili	ty functio	ons
	9	IBM PRODUCTS	- Additio	onal IB	M program	development	products	
	10	SCLM	- Softwar	e Conf	iguration	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')
 - o RACDCERT id(Sharbxx) GENREQ(LABEL('MySSLCertxx')) DSN(myssl)



<u>M</u> enu	<u>L</u> ist	M <u>o</u> de	<u>F</u> unctions	<u>U</u> tilities	<u>H</u> elp	
Enter	TSO or	Workst	ation comma	ISPF Comman nds below:	d Shell	
===> <u>R</u>	ACDCERT	id(Sh	arbxx) GENR	EQ(LABEL('M	<u>ySSLCertxx'))</u>	<u>DSN(myssl)</u>

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

<u>F</u> ile	<u>E</u> dit <u>V</u> iew	Communication	Actions Wind	ow <u>H</u> elp			
B	à 🛍 📠	🔜 🔳 🐋 🌭	🐱 💩 💼	٠			
		• SHARE ISPF	5.9 SCROLL	ABLE PRIMARY	Y OPTION MEN	IU	- <mark>\$1</mark>
OPT	ION ===>	3.4					
D D T Y	Alterna 2 Alterna he time i our uid i	ate Dialog = ate Dialog = .s 12:45 p.m is SHARB01	==> CMD(%?? ==> PANEL(? . on Tuesda dsn prefix	??) ???) y, July 22, is SHARB01	2008 (2008. proc is SH	Mor 204) IARE sys is	re: + s \$1
0	SETT	INGS -	Specify ISP	F parameters	3		
1	VIEV	I –	View source	data or out	tput listing		
1	P VIEV	I-0E -	View/Browse	files in th	ne Open Edit	ion file sys	tem
2	EDIT	-	Create or c	hange source	e data		
2	P EDI1	-0E –	Edit files	in the Open	Edition fil	e system	
3	UTIL	ITIES -	Perform uti	lity function	ons		

• enter 'Sharbxx.myssl' on the 'Dsname Level' input line and hit enter

<u>M</u> enu <u>R</u> ef	List	R <u>e</u> fMode	<u>U</u> tilities	<u>H</u> elp					
0			Data Set	List Utili	ty				
blank Di V Di Enter one c Dsname L Volume s	splay splay or both evel . serial	data set VTOC inf of the <u>SHA</u>	list ormation parameters RBxx.myssl	P PV below: _	Print Print	data VTOC	set list informati	More: .on	+

- 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.

==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 MIIBhTCB7wIBADAWMRQwEqYDVQQDEwtNWVNTTENFUlQwMTCBnzANBqkqhkiG9w0B 000003 AQEFAAOBjQAwqYkCqYEA0C8ulvTwd0ywl/T9dyRqkbuR7765h3R406tZWqpp2YaM 000004 cXw0DjQkckHQgWqwr/FXHCbh/IJkFTa3B5cGKEILlPQBJH1hCfDH6Kb311vFaYCb 000005 svELyRofKVsItUL54Q/ZREuczpcKcv8dMJsr33CZQW/uViqou0Q4DFHdZD2LoJMC 000006 AwEAAaAwMC4GCSqGSIb3DQEJDjEhMB8wHQYDVR00BBYEF00H9DduiqJsku3i1IVF 000007 z2aHQmopMA0GCSqGSIb3DQEBBQUAA4GBAGcCY/fJUqr1qj36sRiBdGfj33y18XJn 000008 fBWiZ4q8N0En76+iVtTdxP0a4ZIH4A+ncaEq29H6ckIloXAsCHSuNENdYP+vGicH 000009 OtVe4tYcovvmVSwKoj1jmiZc55DMh2qebxYmkqqvNbvizPdjs/aj8iWA5AyxH0Pw 000010 th59aL4s0fug 000011 ----END NEW CERTIFICATE REQUEST----

• 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 Gene	ration Application					
Install the CA certificate to enable SSL sessions for PKI	Services					
Choose one of the following:	This	s ti	ime.	let's	try to	
• Request a new certificate using a model	get	as	SSL	Server	cert	
Select the certificate template to use as a model	5-Year PKI SSL Server Certificate	6	~			
Request Certificate	1-Year PKI S/MIME Browser Certificate 2-Year PKI Windows Logon Certificate 2-Year PKI Browser Certificate For Authenticating To	7/05				
Pick up a previously requested certificate	5-Year PKI SSL Server Certificate 5-Year PKI IPSEC Server (Firewall) Certificate	52/00				
Enter the assigned transaction ID	5-Year PKI Intermediate CA Certificate 2-Year PKI Authenticode - Code Signing Certificate 5-Year SCEP Certificate - Prevenistration					
Select the certificate return type PKI Browse	1-Year PKI Generated Key Certificate n-Year PKI Certificate for Extensions Demonstration	l				
Pick up Certificate						
• Renew or revoke a previously issued brows	er certificate					
Renew or Revoke Certificate						
• Recover a previously issued certificate who	ise key was generated by PKI Services					
Enter the email address when the original certific	ate was requested					
Enter the same pass phrase as on the request for	m Recover Certificate					
• Administrators click here						
Go to Administration Page						

• Fill in the information

oose one of the following:	•
Request a New Certificate	
Enter values for the following field(s)	
Your name for tracking this request (Optional)	
	<mark>Fill in info just lik</mark>
Email address for notification purposes (Optional)	the browser cert case
Pass phrase for securing this request. You will need to supply this value when retrieving your certificate	except
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)	

- 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

		Paste	the	request	here
MIIBfTCB5wIBADAOMQwwCgYDVQQDEwN3YWkwg28wDQYJKoZlhvcNAQ MIGJAoGBARMThisMmQOoN37iGqk+400QJS+J/0yqnP9wgeazcssRX9 PgbRXwEx+vqPjLH28ZdHbBbXQJ7zmXLwJEw6H8bf1BFYigPerRmjn+ 9wvVNVlQh3wojC90ENT5J6cavhHkvY8XTnmj6zMAYy2+QA/XuWYlAg BgkqhkiG9w0BCQ4xITAfMB0GA1UdDgQWBBRhu1ZQyMtwTgDhRI2g+9 BgkqhkiG9w0BAQUFAAOBgQBeTu4hH9punDv+eQ4Isxbm4YSMZkkCvo z4ArioBWf9SCA2pchr3gg0IhauX503pHiELnEx6bP/KDbcQVumzEFk lhyirdK4LaMW4mjfMVvv11f2JxQ/QZaAeVrhMxfHkT3dJq2v7KWceU GQ== END NEW CERTIFICATE REQUEST	EBBQADGYOA dJHHPM2o2Q OHaLQwOFcn MBAAGGMDAu xPDI21kjAN /sM3h2uw10 fQBLt9kTKU JKIDZfVf0x				
Submit certificate request Clear		>			
Pick Up a Previously Issued Certificate					
Retrieve your certificate					



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.)

HIIGhwYJKoZIhvcNAQcCoIIGeDCCBnQCAQExADALBgkqhkiG9w0BBwGgggZcMIID 9TCCA16gAwIBagIBBDANBgkqhkiG9w0BAQUFADAyMOswCQVDVQQCEwJUUZENMAOG AlUEChMDSUJNNRUWEWYDVQQLEwxIUiBDZXJ0IEF14GgwHcNNDQxMDA2MDAWDAW WhcNMDxXMDAOMjM1OTUSWjBQMQswCQYDVQQEBwJUUZENMAOGA1UECBMITmV3IF1v cmsxFTATBgMVBAoTDE51dyBZb3JrIFJVRZEXMBUGA1UEAMOUIVHIFG1ViBTZXJ2 ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJAOGBAJQLBDRIAd1hnFYQCF/MC928 EF+8zLv4AD6MyM1IP/Tr+1j3T6c9mNVUB7ZWGSpAITmPc8W6KWLROM331HVuYvE oGaQ/FprcnHEkvP5QbOrvbxfqoZnrA1N4kGisGiBgv6evZ1fLAHpOJNLAAJfC2/h EbBOSdQ4RLSVCfzrSo2BAgMBAAGjggH7MIIB9zApBgNVHHEEIJAghhodHkw018V d3d3LnJ1Z3M1cnZici5jb2ZHBA17LUMwDg7VNC0PAQH/BAQDAgWgMBMGA1UdJQQM MAGGCCGAQUFBwMBMIIB7wVPC0fBIIEWjCCAVYWSSBHOEWAC2BBMQswCQTVVQG DAJVUZEMMAoGA1UECgwDSUJNMRUWEwTVVQQLDAxIU1BDZXJ0IEF14GgxTALBgMV BAMBENSTDEwXaBboFmGV2xKYXA6Ly85LjU2LjU0LjEZMDozODkvQ049Q1JMMSXP VTIIU1WMEN1cnQ1MjBBdXRoLE89SUJNLEM9VVM/Y2VydG1maWNhdGV3ZXZVY2F0 aW9uTG1zdDBxoG+gbY2rbGRhcDovL215b3RoZXJ3ZGFwc2VydmVyLm15Y29tcGFu eS5jb206Msg5LON0FUNSTDEST1US5F11MjBDZXJ01TWQXVQCxPPU1CTSNSPVVT P2N1cnRpZm1jYXR1UmV2b2NhAG1bVkxpc3QwN6A1oDOGMWhOdHA6Ly93d3cubX1j b21wFWS5LmNVbS9QS01TZXJ2LNNY2V9dHMvQ1JMS5jcmwwHQ7VVRO0BBYEFFp6 TKC2zJ0GNu/1vjWmjqx/52+NMB6GHUGYQVAQ94QJ4WJMNS5jcmwwHQ7VVRO0BBYEFFp6 TKC2zJ0GNu/1vjWmjqx/52+NMB6GHUGYQLEwxIU1BDZXJ01F1dGgwHASXNXLJ3 H+arNA0GCSQS1J3QEBQUAA4GBADpj6b10EL+z2GQm95QGY95zTV0ALIJ3 LP3ugJSSIIS3QEBF7a18Z+Aeppc0016/YXHfH1+5qIcMv5/0ekbH28foxSNw1Rb n/KWwwMIICX2CAcigJWIBAGBADpj6b10EL+z2GQM95QGYP5zTV0ALIJ3 ChJ0JMNGWAEWZDVQQLEwxIU1BDZXJ01F1dGgwHACMNQX MJAGHALAWJKANJAWDA1OTUSWJAYMO2WVZNQCEwJUZEMMA6GA1UE ChMDSUJNMRUWEWZDVQQLEwxIU1BDZXJ01F1dGgwHACMNQX QTAAIGJA6GBALAbZJJN/FEU/UD1+mRmuJzpwK16V4ATQNHZtjUEBAJAGJ GYQWYEWMJJIZIAYBDYUQLEWXIU1BDZXJ01F1dGgwHAC3JztrIpAR QTA61at RseddALWHykxNNJWBUOTUSWJAYMO2KE0ZMJQZWZDVQZGVWQQEWJVVZEIBAA6J31FTPAR GTHAUSCH7AdBgNVHQ4EFFQUUZ7QKXQJZAgEA9CX+TG7VKSZGSWDQYJK0ZIHAAGJUU ChMDSUJNRWWEWZDVQQLEwXIU1BDZXJ01F1dggWBAAGJ UZYdmVyIGZvc1B6LD9TIChSQUNGKTAOBGNVHQBBAFBEAMCAQYWWYDVROTAQH/ AQFFBQADgYEAGJYKQIAPFFC71BbWH3F7MNZJZAFFSmSpJpT31LdbE+1 Ipf4RRFru0N6DFFWC7GU	The cert is return in B64 format for you to cut and pas it to a file from the server side. Y may not be able to paste the entire content into the server dataset. Do it in parts OR use function provided 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'

Г

General Security Privacy Content Connections Programs Advance Content Advisor Image: Security Ratings help you control the Internet content that can be viewed on this computer. Image: Security Ratings help you control the Internet content that can be viewed on this computer. Image: Security Image: Security Settings Image: Security Image: Security Settings Certificates Image: Security Settings Image: Security Use certificates to positively identify yourself, certification authonties, and publishers Clear SSL State Certificates Publishers Personal information Image: Security AutoComplete stores previous entries and suggests matches for you. AutoComplete Microsoft Profile Assistant stores your personal information. My Profile My Profile
Certificates Image: Certificates
Personal information AutoComplete stores previous entries and suggests matches for you. Microsoft Profile Assistant stores your personal information. My Profile
Microsoft Profile Assistant stores your My Profile

٦

- 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

Certific	ates				? >
Intende	d purpose:	All>			~
Persor	other People	Intermediate Certification	Authorities Trus	ted Root Certification	<]>
Iss	ued To	Issued By	Expiratio	Friendly Name	
100	jan27a	Sharb01 CA	1/26/2012	<none></none>	_
Certifi	cate intended pur	poses		Advance	20
Client	Authentication			View	
				Clos	•

Certificate		? 🔀		
General Details Certification I	Path			
Field	Value	^		
Serial number	V3 03	10	Fields suppl	ied k
Signature algorithm	sha 1RSA		or hardcoded	l by
Issuer	Sharb01 CA. Test. The Sharb0.		administrato	nr in
Valid from	Thursday, January 27, 2011 1.		nkigory +mn]	~ 11
Valid to	Thursday, January 26, 2012 1		priserv.cmpi	
Subject	jan27a, Class 1 Internet Certif		7/	
Public key	RSA (512 Bits)	~		
¦2N = jan27a OU = Class 1 Internet Certifica O = The Sharb01 Firm C = US	ite CA			

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

Certificate		? 🔀	
General Details Certification Path			
Show: <all></all>	~		
Field	Value		
Valid to Subject Public key Enhanced Key Usage Authority Information Access	Thursday, January 26, 2012 1 jan27a, Class 1 Internet Certif RSA (512 Bits) Client Authentication (1.3.6.1 [1]Authority Info Access: Acc [1]CRL Distribution Point: Distr	• • • =	
Subject Key Identifier	f6 ee bd 21 d9 af 82 bf 58 c5 KeyID=32 1e f7 dd 1b 9b 03 8	This is pkisery	s set up in v.conf
OU=Test O=The Sharb01 Firm C=US [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://mvs1.centers.ihost.com	m:8041/Sharb01/crls/CRL1.crl		

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

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

Certificate					
General De	tails Certification Path	1			
Show: </th <th>ll></th> <th>~</th> <th></th> <th></th> <th></th>	ll>	~			
Field		Value			
Valid t Subject Public	o t ced Key Usage	Thursday, January 26, 2012 1 jan27a, Class 1 Internet Certif RSA (512 Bits) Client Authentication (1.3.6.1			
Autho	ity Information Access	[1]Authority Info Access: Acc		This is	, hardcoded h
CRL D	stribution Points	[1]CRL Distribution Point: Distr		adminis	strator in
Autho	ity Key Identifier	KeyID=32 1e f7 dd 1b 9b 03 8	~	pkiserv	r.tmpl
[1]Authorii Access (1.3.6.1.5 Alterna URL	y Info Access Method =On-line Certific 5.7.48.1) ive Name: =http://mvs1.centers.ih	ate Status Protocol ost:8041/Sharb01/public-cgi/caocsp	4		

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'

Requestor:	jan27a	Created:	2011/01/27				
Status:	Active	Modified:	2011/01/27				
Template:	1-Year PKI SSL Browser Certificate	PassPhrase	: a	、 、			
Serial #:	3			\mathbf{N}			
revious Action	on Comment: Issued certificate				tatus cha	nges fi	rom Activ
Subject:	CN=jan27a,OU=Class 1 Internet Certificate CA,C)=The Sharb01	Firm,C=US		o Suspend	ed	
Issuer:	CN=Sharb01 CA,OU=Test,O=The Sharb01 Firm	C=US		1	- Bustona		
Validity:	2011/01/27 00:00:00 - 2012/01/26 23:59:59				\		
Usage:	handshake(digitalSignature, keyEncipherment)				\mathbf{A}		
Usage: Extended Usage ction to take	handshake(digitalSignature, keyEncipherment) ge: clientauth ge: (Optional)						
Usage: Extended Usag ction to take tion Comment (Revoke Co Suspend (Disable	handshake(digitalSignature, keyEncipherment) ge: clientauth ce: (Optional) Certificate No Reason Certificate	×		Requestor: Status: Template: Serial #:	jan27a Suspended 1-Year PKI SSL E 3	Browser Certificate	Created: 2011/01/2' Modified: 2011/01/2' PassPhrase: a
Usage: Extended Usag ction to take tion Comment (Revoke Co Suspend (Disable Enable /	handshake(digitalSignature, keyEncipherment) ge: clientauth (Optional) Certificate No Reason Certificate Automatic Renewal Automatic Renewal	×		Requestor: Status: Template: Serial #: Previous Action O	jan27a Suspended 1-Year PKI SSL E 3 Comment:	Browser Certificate	Created: 2011/01/2 Modified: 2011/01/2 PassPhrase: a



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)
 - o 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

Γ

- 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?)

	Cert with		
ate Revocation Lis	t ?	Certificate Revocation	List
Revocation List		General Revocation List	
Certificate Revo	cation List Information	Revoked certificates:	
3		Sent number	Revocation date
əld	Value	03	Tuesday, May 02, 2006
Version	V2	04	Tuesday, May 02, 2006
Issuer	Demo Customer Design Centre Ce		
Effective date	Tuesday, May 02, 2006 1:49:22 PM		
Next update	Thursday, May 04, 2006 1:49:22 PM		
Signature algorithm	sha 1RSA	Revocation entry	
CRL Number	35	Field	Value
Authority Key Iden Issuing Distribution	KeyID=5d 33 e3 de eb 85 cc 83 f6 Distribution Point Name:Full Name:	Serial number Revocation date	03 Tuesday, May 02, 2006 10:40:16 AM
		CRL Reason Code	Certificate Hold (6)
e:		Value:	
	OK		

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,
 - o enter 'cd \openssl\bin'
 - o enter 'statusof c:\temp\mycert.cer xx' (xx is the number part of your assigned id)

- o 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	n OCSP	using	openSSL	
CSP Response Data:				
OCSP Response Status: successful (0x0)			
Response Type: Basic OCSP Response				
Version: 1 (0x0)				
Responder Id: 0 = The Share03 Firm	, OU = Tea	st, CN = Sh	are03 CA	
Produced At: Dec 7 03:13:46 2006	GMT			
Responses:				
Certificate ID:				
Hash Algorithm: shal				
Issuer Name Hash: 1BA48167FFFD2E	C4D90BB2E	LF66B109E05	5C34BE	
Issuer Key Hash: ACDDB2434055FF8	7FFB8790B	3F09AED8A3E	B0816	
Serial Number: 01		1 1 / 6	0	C)
Cert Status: revoked Cert 01	is susp	ended (I	rom reason Ux	(6)
Revocation Time: Dec 6 22:36:04 2	006 GMT			
Revocation Reason: certificateHold	(0x6)			
This Update: Dec 7 03:13:46 2006	GMT			
CSP Response Data:				
OCSP Response Status: successful (0x0)			
Response Type: Basic OCSP Response				
Version: 1 (0x0)				
Responder Id: 0 = The Share03 Firm	, OU = Tes	st, CN = Sh	are03 CA	
Produced At: Dec 7 03:27:54 2006	GMT			
Responses:				
Certificate ID:				
Hash Algorithm: shal				
Issuer Name Hash: 1BA48167FFFD2E	C4D90BB2E	lF66B109E05	5C34BE	
Issuer Key Hash: ACDDB2434055FF8	7FFB8790B	3F09AED8A3E	B0816	
Serial Number: 01	is not	revoked	or suspended	
Cert Status: good	13 100	LCVORED	or suspended	
This Update: Dec 7 03:27:54 2006	GMT			



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

<u>File Edit View Communication Actions Window Help</u>
<u>M</u> enu <u>L</u> ist M <u>o</u> de <u>F</u> unctions <u>U</u> tilities <u>H</u> elp
ISPF Command Shell Enter TSO or Workstation commands below: ===> omvs

• 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)
 - o Go to MVS system, ISPF S.LOG

<u>File Edit View Communication Actions Window H</u> elp
SHARE ISPF 5.9 SCROLLABLE PRIMARY OPTION MENU S1
OFFICE S. (09_
D Alternate Dialog ===> CMD(%????)
D2 Hiternate Dialog ===> PHNEL(????) 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 INPOT> /p pRISEDXXSCRULL> CSP
• Then restart PKI Services, enter '/', hit enter
<u>File Edit View Communication Actions Window H</u> elp
<u>D</u> isplay <u>F</u> ilter <u>V</u> iew <u>P</u> rint <u>O</u> ptions <u>H</u> elp
SDSF SYSLOG 14434.103 S1 S1 07/22/2008 0W 13633 COLUMNS 1 80
COMMAND INPUT ===> /
LK 035 0000090 LUCHE IF 5 IND00
 Enter 's pkiservd,jobname=pkiseaxx,dir='/sharelab/sharbxx/pkilab'
Display Filter View Print Options Search Help
Suctom Command Extension
System command Extension
Type or complete typing a system command, then press Enter.
<pre>s pkiservd,jobname=pkisebxx,dir='/sharelab/sharbxx/pkilab'</pre>

• 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

Luc For	<u>.</u>	<u>e</u> ommanication	<u>/1</u> 00000	<u></u>	Terb					
	1 🛃 🗣		.	F 🗎 🌰	<i></i>					
Enter	Your	Userid:								
Passwo	ond:				New	passw	ord:			
Applic	ation	: tso								
Applie	ation	Required. N	o Insta	allatio	n Defa	ult				
	F . ()	Le sur d'al contra de								
b	. Enter l	Jserid: sharbxx								
()	Wherev	er the lab shows	s sharbx)	< substitu	ite your	userid,	, e.g. sha	arb02)		
<u>F</u> ile <u>E</u> di	t <u>V</u> iew	Communication	<u>A</u> ctions	<u>W</u> indow	<u>H</u> elp					
				4 4						

🖻 🗈 🗗 🚛 🛼 🔜 🔳 📓	a 🛃 💼 🗎 🔮 🔗
IKJ56700A ENTER USERID	
sharbxx_	

c. Password: given by the instructor

<u>File Edit View Communication Actions Window Help</u>	
T\$0/E LOGON	
Enter LOGON parameters below:	RACF LOGON parameters:
Userid ===> SHARB01	
Password ===>	New Password ===>
Procedure ===> SHARE	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 ocsp
-issuer \temp\mycacert.cer
-cert \temp\mycert.cer
-url http://mvsl.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: <u>http://www.ibm.com/servers/eserver/zseries/zos/pki</u>
- PKI Services Red Book: <u>http://www.redbooks.ibm.com/abstracts/sg246968.html</u>
- RACF web site: <u>http://www.ibm.com/servers/eserver/zseries/zos/racf</u>
- 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 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.