The Digital Certificate Journey from RACF to PKI Services Part 2

Session J10
May 11th 2005

Wai Choi
IBM Corporation
RACF Development
Poughkeepsie, NY

Phone: (845) 435-7623
e-mail: wchoi@us.ibm.com

Trademarks

- **The following are trademarks or registered trade marks of the International Business Machines Corporation:**
  - DB2
  - CICS
  - OS/390
  - RACF
  - S/390
  - z/OS
- **UNIX is a registered trademark of The Open Group in the United States and other countries.**

Agenda

- PKI Services Introduction
- Architecture
- PKI Services Web pages
- Summary
- Using RACF as a CA VS PKI Services

What is PKI?

- Public Key Infrastructure based on the public key cryptography to create, manage, store, distribute, verify digital certificates

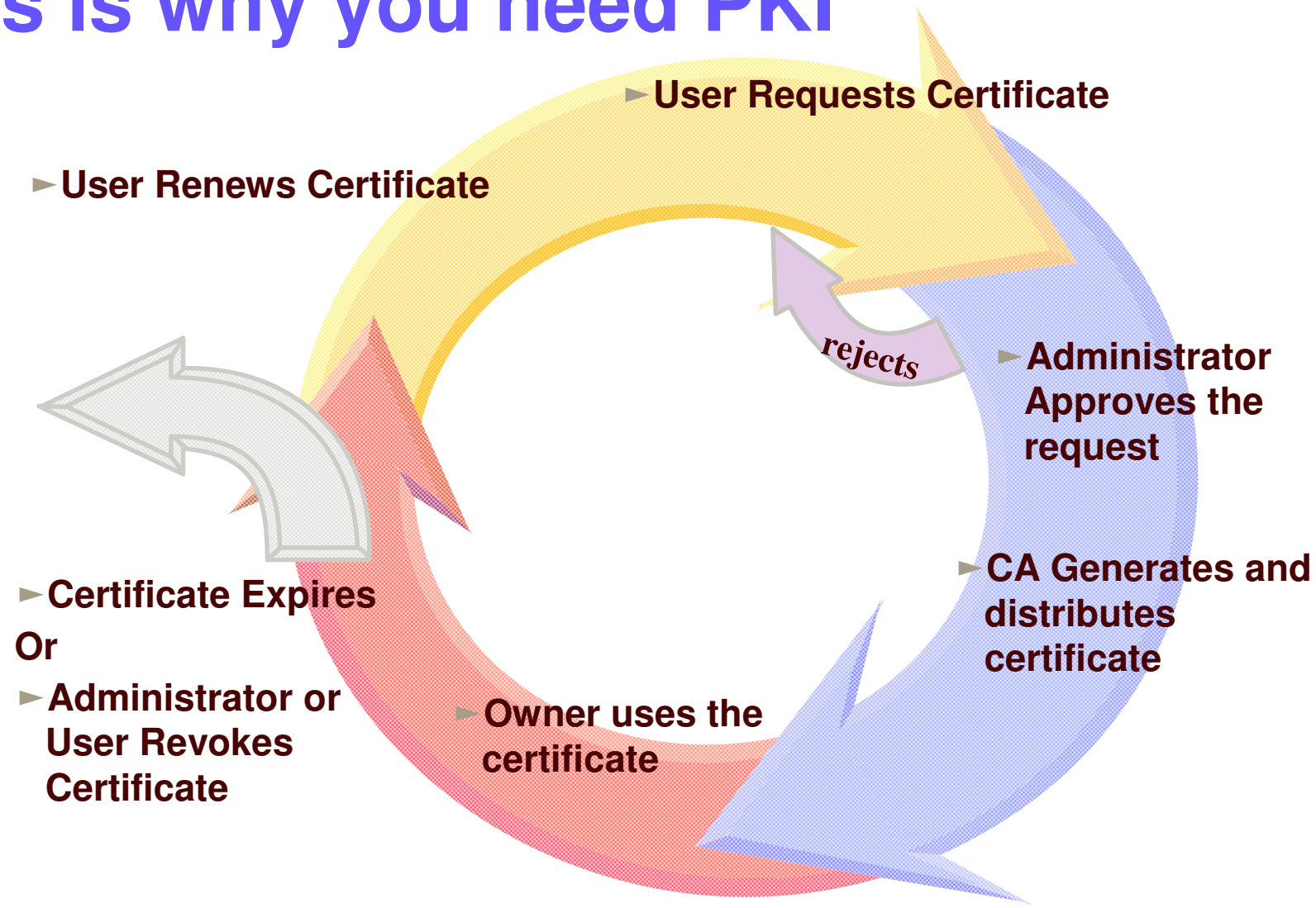
Introduction to PKI Services

- New component on z/OS since V1R3
- Closely tied to RACF, but supports more functions than RACDCERT
- Complete Certificate Authority /Registration Authority (CA/RA) package
  - Full certificate life cycle management: request, create, renew, revoke
- Generation and administration of certificates via customizable web pages
- Support automatic or administrator approval process
- Create Certificate Revocation Lists (CRLs)
- Certificates and CRLs can be posted to LDAP
- Provides email notification for completed certificate request and expiration warnings

Introduction to PKI Services…

- Provides Trust Policy Plug-in for certificate validation
- Manual - "PKI Services Guide and Reference"

Certificate Life Cycle – This is why you need PKI



Benefits of using PKI Services on z/OS

- Not a priced product. Licensed with z/OS. An alternative to purchasing third party certificates
- Relatively low mips to drive thousands of certificates
- Leverage existing z/OS skills and resources
- Ability to host Digital Certificate management for the banks, government agencies…
- Run independently of other workloads
- Run in separate z/OS partitions (integrity of zSeries LPARs)
- Scalable (Sysplex exploitation)
- Secure with zSeries cryptography

Two Basic PKI Operations

Certificate generation (In response to a user request)

- Both RACF and PKI Services can be used as a Certificate Authority

Certificate validation

involves the questions of:

- Whether you *trust* the issuer of the certificate – is it in your certificate store, key ring…
- Whether the certificate has a valid *signature* of the issuer
- Whether the certificate is *expired*
- Whether the certificate has been *revoked* (see next slide)
- Whether the certificate contains *information that is specific* to your application that uses that certificate. This includes specific extensions that your application is looking for.

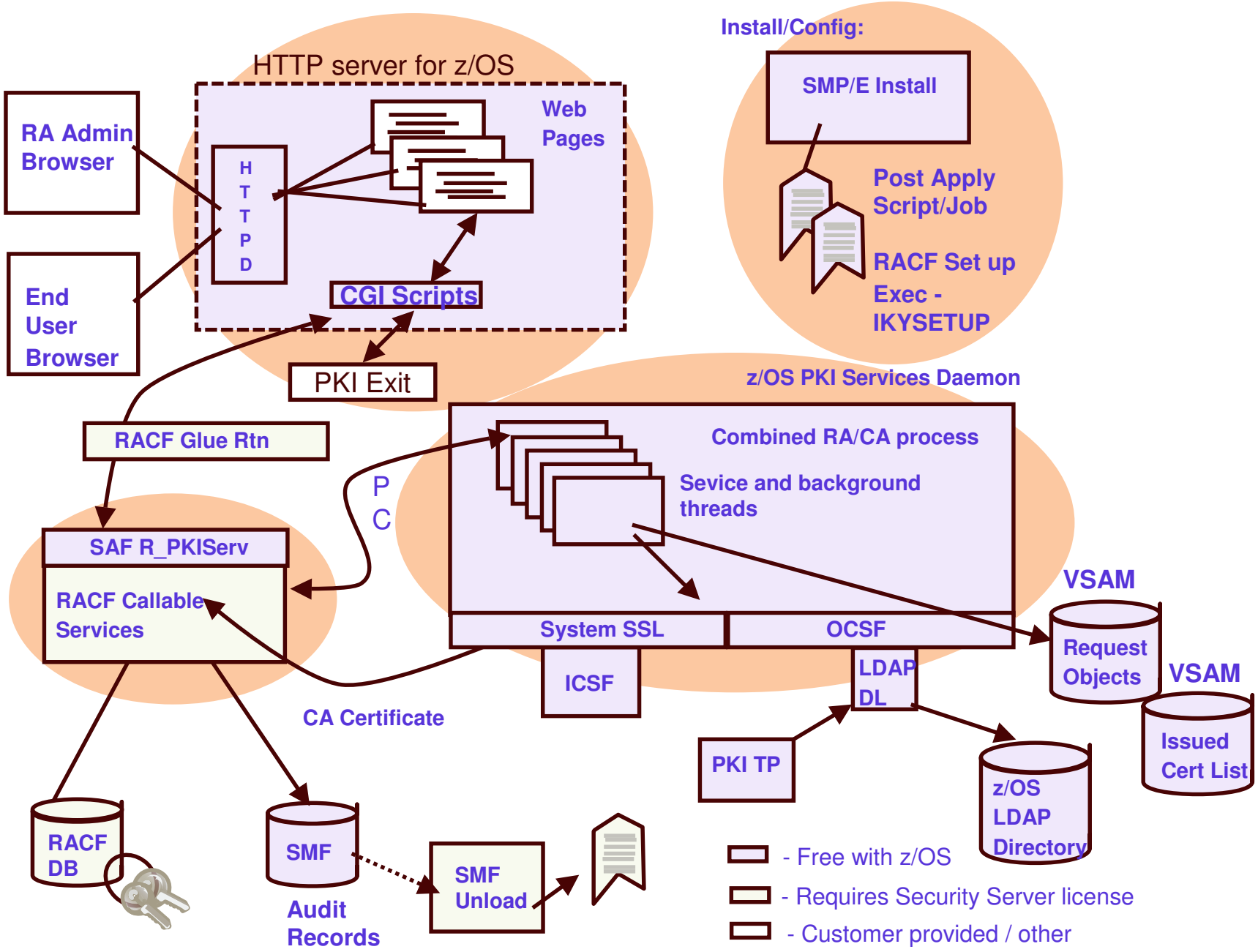
Two ways to determine if a certificate is revoked

- Using Online Certificate Status Protocol (OCSP)
  - The application contacts the CA every time when the certificate is used. The contact information is specified in the certificate's Authority Information Access (AIA) extension.

- Using Certificate Revocation List (CRL)
  - The CA publishes CRL to a public place, eg. LDAP server, periodically. The application checks if the certificate is on the Certificate Revocation List (CRL) published by the CA.

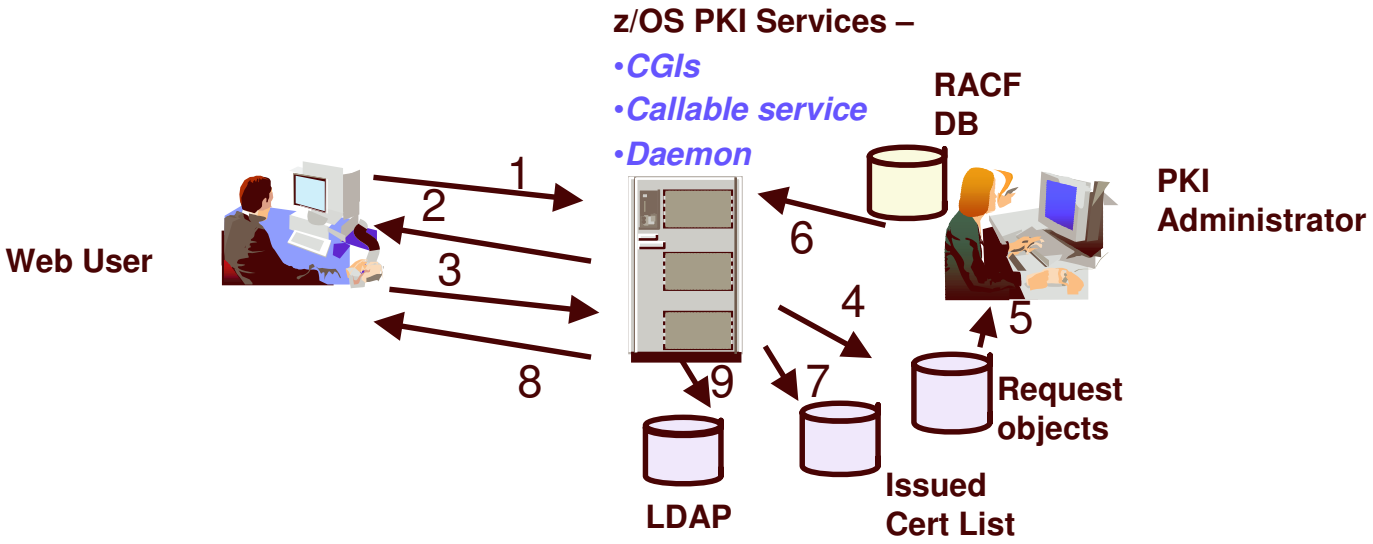
  - As time goes, the CRL may be very large, publishing and retrieving CRL may be time consuming. Creating CRL Distribution Points to publish partial CRLs is a way to solve this problem. Again CRL Distribution Point is a certificate extension.

z/OS PKI Services Architecture



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

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



Screen Shots from PKI Services Web pages

PKI Services Certificate Generation Application

Install our CA certificate into your browser

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

  Request Certificate

- **Pick up a previously requested certificate**

  Enter the assigned transaction ID

  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 Page

email: webmaster@your-company.com

Install our CA certificate into your browser

Choose one of the following:

Pick a template

- **Request a new certificate using a model**

Select the certificate template to use as a model: 1-Year PKI SSL Browser Certificate

- 1-Year PKI SSL Browser Certificate
- 1-Year PKI S/MIME Browser Certificate
- 2-Year PKI Browser Certificate For Authenticating To z/OS
- 5-Year PKI SSL Server Certificate
- 5-Year PKI IPSEC Server (Firewall) Certificate
- 5-Year PKI Intermediate CA Certificate
- 1-Year SAF Browser Certificate
- 1-Year SAF Server Certificate
- 2-Year PKI Authenticode - Code Signing Certificate

Request Certificate

- **Pick up a previously requested certifi**

Enter the assigned transaction ID

Select the certificate return type: PKI Browser Certificate

Pick up Certificate

Browser cert is chosen

- **Renew or revoke a previously issued browser certificate**

Renew or Revoke Certificate

- **Administrators click here**

Go to Administration Page

email: webmaster@your-company.com

1-Year SSL Browser Certificate

Choose one of the following:

Fill in the info

- **Request a New Certificate**

Enter values for the following field(s)

Your name for tracking this request (optional)
Wai Choi

Email address for distinguished name (optional)
user1@yahoo.com

Common Name
NY RUG USER1

Email address for notification purposes (optional)
user1@yahoo.com

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

Reenter your pass phrase to confirm
****

Select the following key information

Cryptographic Service Provider Microsoft Base Cryptographic Provider v1.0

Enable strong private key protection? No

Submit certificate request Clear

- **Pick Up a Previously Issued Certificate**

Retrieve your certificate

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

Get back a transaction ID, save it

Retrieve Your 1-Year PKI SSL 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

1jTQjs0h/cpk2SHV++++++++

If you specified a pass phrase when submitting the certificate request, type it here, exactly as you typed it on the request form

****

Retrieve and Install Certificate

To check that your certificate installed properly, follow the procedure below:

Netscape V6 - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificates button to start the Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then click View to see more information.

Netscape V4 - Click the Security button, then Certificates-> Yours. Your certificate should appear in the list. Select it then click Verify.

Internet Explorer V5 - Click Tools->Internet Options, then Content, Certificates. Your certificate should appear in the Personal list. Click Advanced to see additional information.

Home page

email: webmaster@your-company.com

Enter the same pass phrase you entered before

Request was not successful

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

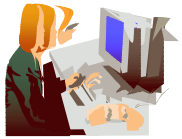
```
IKYI002I SAF Service IRRSPX00 Returned SAF RC = 8 RACF RC = 8 RACF RSN = 56
Request is still pending approval or yet to be issued
```

email: webmaster@your-company.com

Certificate not ready

PKI Services Certificate Generation Application

Install our CA certificate into your browser



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

- **Renew or revoke a previously issued browser certificate**

  Renew or Revoke Certificate

- **Administrators click here**

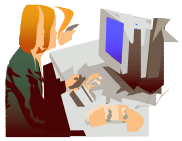
  Go to Administration Page

Administrator starts working

email: webmaster@your-company.com

PKI Services Administration

Choose one of the following:



- **Work with a single certificate request**

  Enter the Transaction ID:

  [ ] Process Request

- **Work with a single issued certificate**

  Enter the Serial Number:

  [ ] Process Certificate

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

Choose a task

Certificate Requests

- ○ Show all requests
- ◉ Show requests pending approval
- ○ Show approved requests
- ○ Show completed requests
- ○ Show rejected requests
- ○ Show rejections in which the client has been notified

Issued Certificates

- ○ Show all issued certificates
- ○ Show revoked certificates
- ○ Show suspended certificates
- ○ Show expired certificates
- ○ Show active certificates (not expired, not revoked, not suspended)
- ○ Show disabled certificates (suspended or revoked, not expired)

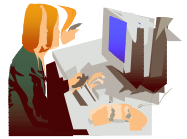
Additional search criteria (Optional)

Requestor's name [ ]

Show recent activity only [(Not Selected) ▾]

Find Certificates or Certificate Requests

Home Page



Certificate Requests

The following certificate requests matched the search criteria specified:

All ☑	Requestor	Certificate Request Information	Status	Dates
☑	Wai Choi	**Trans ID:** 1jTQjs0h/cpk2SHV++++++++ **Template:** 1-Year PKI SSL Browser Certificate **Subject:** MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=The Firm	Pending Approval	**Created:** 2004/10/05 **Modified:** 2004/10/05

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**

Request summary info

Action Comment (Optional)

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

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

Delete - Delete all requests selected above

Respecify Your Search Criteria

Home Page

email: webmaster@your-company.com

Single Request

Requestor:	Wai Choi	**Created:**	2004/10/05
Status:	Pending Approval	**Modified:**	2004/10/05
Transaction Id:	1jTQjs0h/cpk2SHV++++++++	**Passphrase:**	passw0rd
Template:	1-Year PKI SSL Browser Certificate	**NotifyEmail:**	user1@yahoo.com

Previous Action Comment:

Subject:	MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=The Firm
Issuer:	OU=HR Cert Auth,O=IBM,C=US
Validity:	2004/10/05 00:00:00 - 2005/10/04 23:59:59
Usage:	handshake(digitalSignature, keyEncipherment)
Extended Usage:	clientauth

Action to take:

Request detail info

Action Comment (Optional)

Approve Request As It is

Approve Request with Modifications

Choose the action

Reject Request

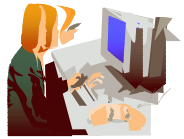
Delete Request

Administration Home Page

Home Page

email: webmaster@your-company.com

Modify and Approve Request



Requestor	Request Information	Dates
Wai Choi	**Trans ID:** 1jTQjs0h/cpk2SHV++++++++ **Template:** 1-Year PKI SSL Browser Certificate	**Created:** 2004/10/05 **Modified:** 2004/10/05

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

Common Name (optional)
NY RUG USER1

Email for distinguished name
user1@yahoo.com

Organizational Unit (optional)
Class 1 Internet Certificate CA

Organizational Unit (optional)

Organization (optional)
The Firm

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

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

Date certificate becomes valid: 2004 / 10 / 5

Date certificate expires (at end of day): 2005 / 10 / 4

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

Action Comment (Optional)

Approve with specified modifications

Reset Modified Fields

Administration Home Page

Page primed with requested info

Modify and Approve Request

Requestor	Request Information	Dates
Wai Choi	**Trans ID:** 1jTQjs0h/cpk2SHV++++++++ **Template:** 1-Year PKI SSL Browser Certificate	**Created:** 2004/10/05 **Modified:** 2004/10/05

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

Common Name (optional)
NY RUG USER1

Email for distinguished name
user1@yahoo.com

Organizational Unit (optional)
Class 1 Internet Certificate CA

Organizational Unit (optional)

Organization (optional)
New York RUG

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

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

Date certificate becomes valid: 2004 / 10 / 5

Date certificate expires (at end of day): 2005 / 10 / 4

Action Comment (Optional)

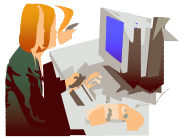
Approve with specified modifications

Reset Modified Fields

Administration Home Page

Can modify some info

Processing successful



Request with transaction ID 1jTQjs0h/cpk2SHV++++++++ is successfully approved.

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

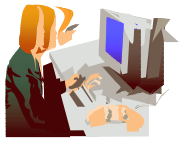
Process More Request(s)

Administration Home Page

Home Page

email: webmaster@your-company.com

PKI Services Administration



Choose one of the following:

- **Work with a single certificate request**

  Enter the Transaction ID:

  [ ] [Process Request]

- **Work with a single issued certificate**

  Enter the Serial Number:

  [ ] [Process Certificate]

Want to display all the requests

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

Certificate Requests

- (•) Show all requests
- ( ) Show requests pending approval
- ( ) Show approved requests
- ( ) Show completed requests
- ( ) Show rejected requests
- ( ) Show rejections in which the client has been notified

Issued Certificates

- ( ) Show all issued certificates
- ( ) Show revoked certificates
- ( ) Show suspended certificates
- ( ) Show expired certificates
- ( ) Show active certificates (not expired, not revoked, not suspended)
- ( ) Show disabled certificates (suspended or revoked, not expired)

Additional search criteria (Optional)

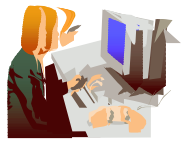
Requestor's name [ ]

Show recent activity only [(Not Selected) ▼]

[Find Certificates or Certificate Requests]

[Home Page]

email: webmaster@your-company.com



Certificate Requests

The following certificate requests matched the search criteria specified:

All ☑	Requestor	Certificate Request Information	Status	Dates
☑	Wai Choi	**Trans ID:** 1jTQjs0h/cpk2SHV++++++++ **Template:** 1-Year PKI SSL Browser Certificate **Subject:** MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=New York RUG	Approved **Serial #:** 3	**Created:** 2004/10/05 **Modified:** 2004/10/05

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**

Delete - Delete all requests selected above

Respecify Your Search Criteria

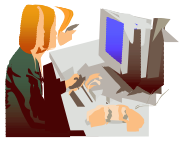
Home Page

email: webmaster@your-company.com

Request is approved and certificate is created

PKI Services Administration

Choose one of the following:



- **Work with a single certificate request**

  Enter the Transaction ID:

  [ ] Process Request

- **Work with a single issued certificate**

  Enter the Serial Number:

  [ ] Process Certificate

Want 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
- ○ Show completed requests
- ○ Show rejected requests
- ○ Show rejections in which the client has been notified

Issued Certificates

- ◉ Show all issued certificates
- ○ Show revoked certificates
- ○ Show suspended certificates
- ○ Show expired certificates
- ○ Show active certificates (not expired, not revoked, not suspended)
- ○ Show disabled certificates (suspended or revoked, not expired)

Additional search criteria (Optional)

Requestor's name [ ]

Show recent activity only [(Not Selected) ▾]

[Find Certificates or Certificate Requests]

[Home Page]

email: webmaster@your-company.com

Issued Certificates

The following issued certificates matched the search criteria specified:

All ☑	Requestor	Certificate Information	Status	Dates
☑	Wai Choi	**Serial #:** 3 **Template:** 1-Year PKI SSL Browser Certificate **Subject:** MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=New York RUG	Active	**Created:** 2004/10/05 **Modified:** 2004/10/05

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 | No Reason | - Revoke all selected active certificates

Suspend - Suspend all selected active certificates

Delete - Delete all selected certificates

Certificate summary info

Respecify Your Search Criteria

Home Page

email: webmaster@your-company.com

Single Issued Certificate

Requestor:	Wai Choi	**Created:**	2004/10/05
Status:	Active	**Modified:**	2004/10/05
Template:	1-Year PKI SSL Browser Certificate		
Serial #:	3		
Previous Action Comment:	Issued certificate		

Subject:	MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=New York RUG
Issuer:	OU=HR Cert Auth,O=IBM,C=US
Validity:	2004/10/05 00:00:00 - 2005/10/04 23:59:59
Usage:	handshake(digitalSignature, keyEncipherment)
Extended Usage:	clientauth

Certificate detail info

Action to take:

Action Comment (Optional)

Revoke Certificate | No Reason

Suspend Certificate

May choose what to do with the certificate

Delete - Delete all selected certificates

Respecify Your Search Criteria

Home Page

email: webmaster@your-company.com

PKI Services Certificate Generation Application

Install our CA certificate into your browser

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

  1jTQjs0h/cpk2SHV++++++++

  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 Page

email: webmaster@your-company.com

Enter the saved transaction ID

Retrieve Your 1-Year PKI SSL 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

1jTQjs0h/cpk2SHV++++++++

If you specified a pass phrase when submitting the certificate request, type it here, exactly as you typed it on the request form

****

Retrieve and Install Certificate

To check that your certificate installed properly, follow the procedure below:

Netscape V6 - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificates button to start the Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then click View to see more information.

Netscape V4 - Click the Security button, then Certificates-> Yours. Your certificate should appear in the list. Select it then click Verify.

Internet Explorer V5 - Click Tools->Internet Options, then Content, Certificates. Your certificate should appear in the Personal list. Click Advanced to see additional information.

Home page

email: webmaster@your-company.com

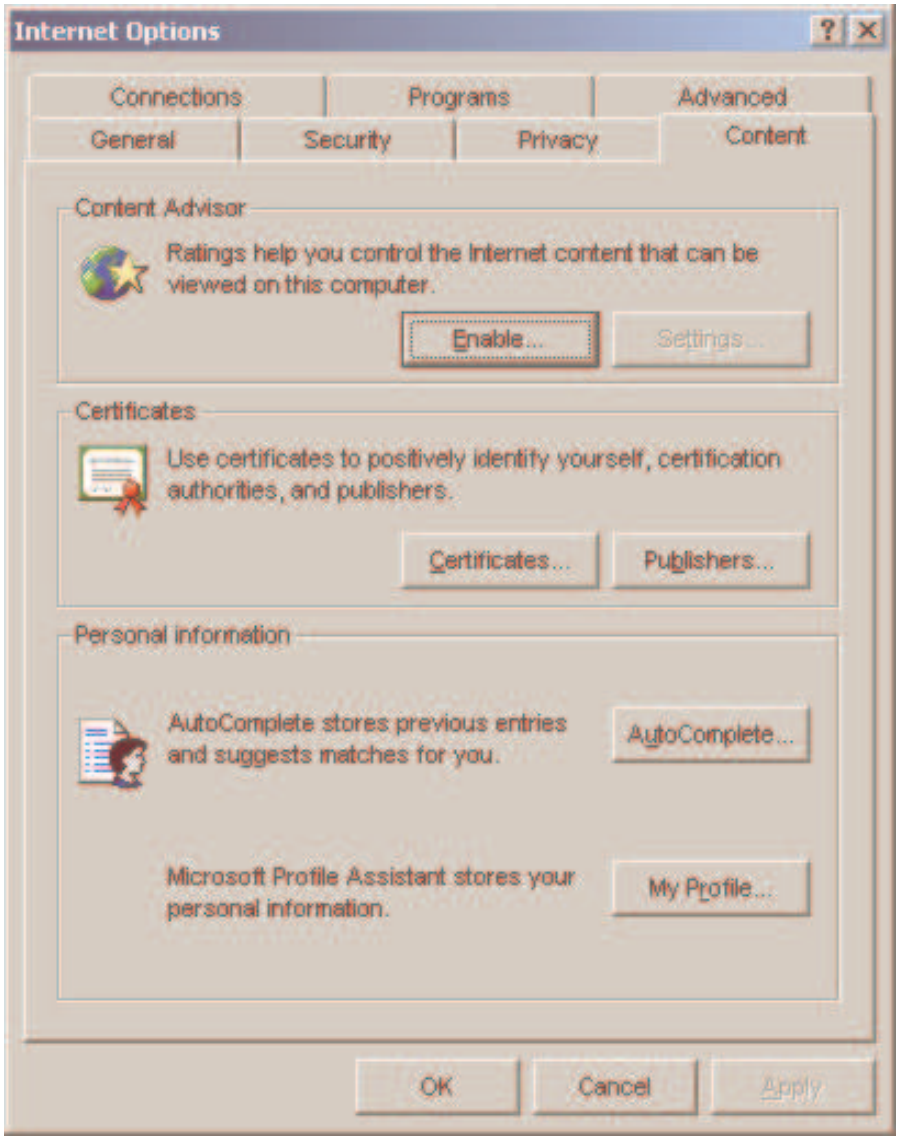
Internet Explorer certificate install

Click "Install Certificate" to store your new certificate into your browser

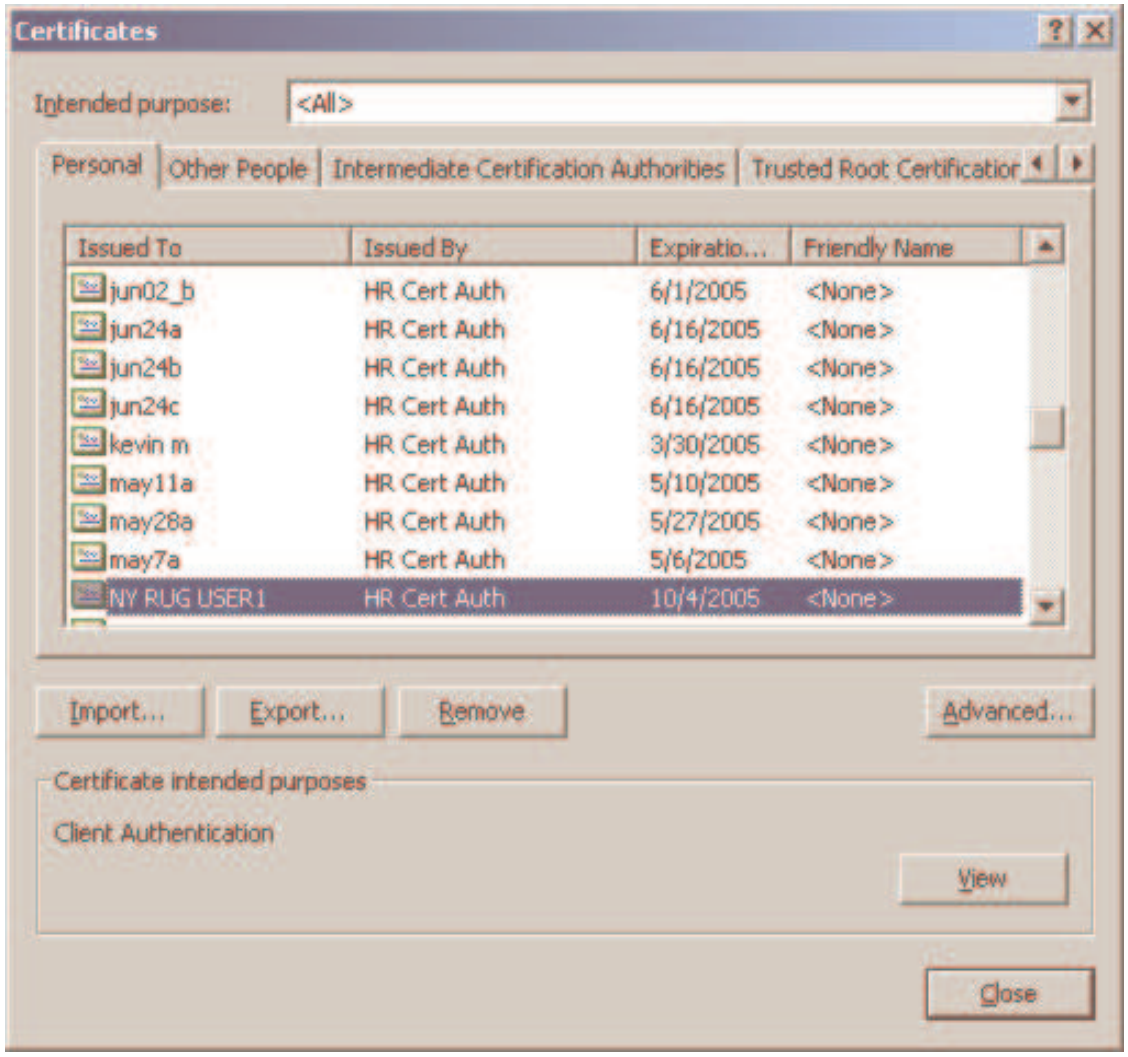
Install Certificate

Home page

From IE browser, click on Tools->Internet Options

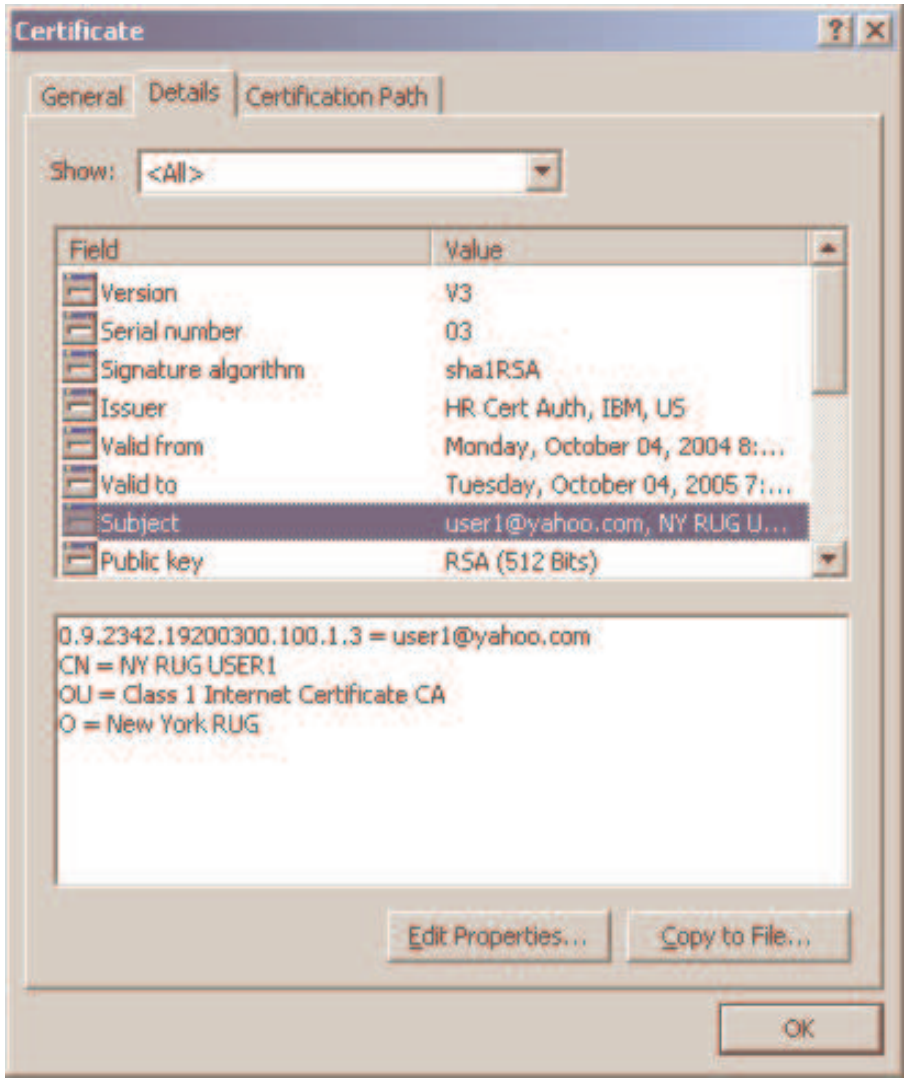


Certificate is installed in browser



You may display the certificate information…

And look at the details of each field



PKI Services Certificate Generation Application

Install our CA certificate into your browser

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

1-Year PKI SSL Browser Certificate
1-Year PKI S/MIME Browser Certificate
2-Year PKI Browser Certificate For Authenticating To z/OS
5-Year PKI SSL Server Certificate
5-Year PKI IPSEC Server (Firewall) Certificate
5-Year PKI Intermediate CA Certificate
1-Year SAF Browser Certificate
1-Year SAF Server Certificate
2-Year PKI Authenticode - Code Signing Certificate

Request Certificate

- **Pick up a previously requested certifi**

Enter the assigned transaction ID

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 Page

email: webmaster@your-company.com

This time, let's try to get a server cert

Assume the server already generated a request

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)
Wai Choi

Email address for distinguished name (Optional)

Common Name (Optional)
RUG Web Server

Organizational Unit (Optional)

Organizational Unit (Optional)

Organization (Optional)
New York RUG

Street address (Optional)

Locality (Optional)

State or Province (Optional)
New York

Zipcode or postal code (Optional)

Country (Optional)
US

Email address for alternate name (Optional)

Domain name for alternate name (Optional)

Uniform Resource Identifier for alternate name (Optional)
http://www.rugserver.com

IP address for alternate name in dotted decimal form (Optional)
9.123.45.67

Fill in info just like the browser cert case except…

Email address for notification purposes (Optional)

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

******

Reenter your pass phrase to confirm

******

Need to provide a request

Base64 encoded PKCS#10 certificate request

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDczCCAtwCAQAwQTELMAkGA1UEBhMCdXMxDDAKBgNVBAoTA2libTENMAsGA1UE
CxMEcmFjZjEVMBMGA1UEAxMMYWxsZXh0c2lnbm5jMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCUCwQOSAHZYZxWMkBPzDmfUnhfvMy7+AA+jMjdSD/06/iI9O+n
PZjWFAe31qkqQCH5j7fFuili0TjG95R1bmGLQaBmkPxaa3JxxJLz+UGzq728X6qG
Z6wNTeJBorBogYL+nr2dXywB6TiTSwGiXwtv4RGwTrHUOES/FQn860qNgQIDAQAB
oIIB8DCCAewGCSqGSIb3DQEJDjGCAd0wAdAQBgNVHREECTAHggVBQHZ2djARBgNV
HQ4ECgQIWnpMoLzMnQQwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAc4w
RQYDVR0lBD4wPAYIKwYBBQUHAwEGCCsGAQUFBwMCBggrBgEFBQcDAwYIKwYBBQUH
AwQGCCsGAQUFBwMIBggrBgEFBQcDCTBgBggrBgEFBQcBAQRUMFIwJwYIKoZIhvpl
BAGGG2h0dHBzOi8vSVYuVEMuQmFua1hZWjExLmNvbTAnBggrBgEFBQcwAYYbaHR0
cHM6Ly9JVi5UQy5CYW5rWFlaMjEuY29tMBgGBisSAAISAQQOMQwwCoED ZGVmggNh
```

Submit certificate request | Clear

- **Pick Up a Previously Issued Certificate**

Retrieve your certificate

email: webmaster@your-company.com

The request should be generated by the server which requests the certificate

Request submitted successfully

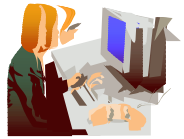
Here's your transaction ID. You will need it to retrieve your certificate. Press 'Continue' to retrieve the certificate.

1jTQXIzxQ/in2SHV++++++++

Continue

email: webmaster@your-company.com

Certificate Requests



The following certificate requests matched the search criteria specified:

All ☑	Requestor	Certificate Request Information	Status	Dates
☑	Wai Choi	**Trans ID:** 1jTQjs0b/cpk2SHV++++++++ **Template:** 1-Year PKI SSL Browser Certificate **Subject:** MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=New York RUG	Completed **Serial #:** 3	**Created:** 2004/10/05 **Modified:** 2004/10/05
☑	Wai Choi	**Trans ID:** 1jTQXIzxQ/in2SHV++++++++ **Template:** 5-Year PKI SSL Server Certificate **Subject:** CN=RUG Web Server,O=New York RUG,ST=New York,C=US	Pending Approval	**Created:** 2004/10/06 **Modified:** 2004/10/06

Choose one of the following:

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

Action Comment (Optional)

Approve it

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

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

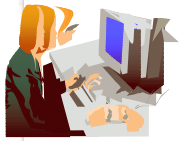
Delete - Delete all requests selected above

Respecify Your Search Criteria

Home Page

email: webmaster@your-company.com

Issued Certificates



The following issued certificates matched the search criteria specified:

All ☑	Requestor	Certificate Information	Status	Dates
☑	Wai Choi	**Serial #:** 3 **Template:** 1-Year PKI SSL Browser Certificate **Subject:** MAIL=user1@yahoo.com,CN=NY RUG USER1,OU=Class 1 Internet Certificate CA,O=New York RUG	Active	**Created:** 2004/10/05 **Modified:** 2004/10/05
☑	Wai Choi	**Serial #:** 4 **Template:** 5-Year PKI SSL Server Certificate **Subject:** CN=RUG Web Server,O=New York RUG,ST=New York,C=US	Active	**Created:** 2004/10/06 **Modified:** 2004/10/06

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 | No Reason | - Revoke all selected active certificates

Suspend - Suspend all selected active certificates

Delete - Delete all selected certificates

Respecify Your Search Criteria

Home Page

email: webmaster@your-company.com

Display Summary of all certificates

PKI Services Certificate Generation Application

Install our CA certificate into your browser

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

  1jTQXlzxQ/in2SHV++++++++

  Select the certificate return type: PKI Server Certificate

  Pick up Certificate

- **Renew or revoke a previously issued browser certificate**

  Renew or Revoke Certificate

- **Administrators click here**

  Go to Administration Page

email: webmaster@your-company.com

Enter Transaction ID to pick up certificate

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

```
-----BEGIN CERTIFICATE-----
MIIGhwYJKoZIhvcNAQcCoIIGeDCCBnQCAQExADALBgkqhkiG9w0BBwGgggZcMIID
9TCCA16gAwIBAgIBBDANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJVUzEMMAoG
A1UEChMDSUJNMRUwEwYDVQQLEwxIUiBDZXJOIEF1dGgwHhcNMDQxMDA2MDAwMDAw
WhcNMDkxMDA0MjM1OTU5WjBQMQswCQYDVQQGEwJVUzERMA8GA1UECBMITmV3IFlv
cmsxFTATBgNVBAoTDE5ldyBZb3JrIFJVRzEXMBUGA1UEAxMOUlVHIFdlYiBTZXJ2
ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJQLBDRIAdlhnFYyQE/MOZ9S
eF+8zLv4AD6MyN1IP/Tr+Ij3T6c9mNYUB7fWqSpAIfmPt8W6KWLROMb3lHVuYYtB
oGaQ/FprcnHEkvP5QbOrvbxfqoZnrA1N4kGisGiBgv6evZ1fLAHpOJNLAaJfC2/h
EbBOsdQ4RL8VCfzrSo2BAgMBAAGjggH7MIIB9zApBgNVHREEIjAghhhodHRwOi8v
d3d3LnJ1Z3NlcnZlci5jb22HBAl7LUMwDgYDVROPAQH/BAQDAgWgMBMGA1UdJQQM
MAoGCCsGAQUFBwMBMIIBYwYDVR0fBIIBWjCCAVYwSaBHoEWkQzBBMQswCQYDVQQG
DAJVUzEMMAoGA1UECgwDSUJNMRUwEwYDVQQLDAxIUiBDZXJOIEF1dGgxDTALBgNV
BAMMBENSTDEwXaBboFmGV2xkYXA6Ly85LjU2LjUOLjEzMDozODkvQ049Q1JMMSxP
VT1IUiUyMENlcnQlMjBBdXRoLE89SUJNLEM9VVM/Y2VydGlmaWNhdGVSZXZvY2FO
aW9uTGlzdDBxoG+gbYZrbGRhcDovL2I5b3RoZXJsZGFwc2VydmVyLm15Y29tcGFu
eS5jb2O6Mzg5LONOPUNSTDEsT1U9SFIlMjBDZXJOJTIwQXVOaCxPPUlCTSxDPVVT
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwN6A1oDOGMWhOdHA6Ly93d3cubXlj
b21wYW55LmNvbS9QSO1TZXJ2L2NhY2VydHMvQ1JMMS5jcmwwHQYDVROOBBYEFFp6
TKC8zJOGNu/lvjWmjqx/S2+NMB8GA1UdIwQYMBaAFLdu6pMUI9gIBAPXMeK3zu1Z
M+arMAOGCSqGSIb3DQEBBQUAA4GBADpj6blOeBL+z2GQmd9EQGXyP5zrPYoALIJ8
LP3ugJ5sI1R55mtNsUm358JzYwtT/46uP6zmDnn3hxAt6cwMiWYHNpKzIQHfx+O2
lSL/fX/5u8QCFhR8E7a18Z+AeppcoOi6/YxHfHl+5qIcMv5/oekbH28foxSNwlRb
n/tKWewmMIICXzCCAcigAwIBAgIBADANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQG
EwJVUzEMMAoGA1UEChMDSUJNMRUwEwYDVQQLEwxIUiBDZXJOIEF1dGgwHhcNMDQx
MDAOMDQwMDAwWhcNMjAwMTAyMDM1OTU5WjAyMQswCQYDVQQGEwJVUzEMMAoGA1UE
ChMDSUJNMRUwEwYDVQQLEwxIUiBDZXJOIEF1dGgwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALAbZJJN/FEu/VDi+mRmuJzpwKl6V4ATqNHztjuEMbdzl3rtIpaR
OqIh61atRRsddACuH4vkxaNxg/WHOdzFp/kknDHmrh1EwlIwRLCEfU3LAiBg8URO
QiPhwV61cQUHSTW+uxnXJq56OKQAOo4weiFr+GRm6ISa3i1/Yt4oIeIDAgMBAAGj
gYQwgYEwPwYJYIZIAYb4QgENBDITMEdlbmVyYXRlZCBieSBOaGUgU2VjdXJpdHkg
U2VydmVyIGZvciB6LO9TIChSQUNGKTAOBgNVHQ8BAf8EBAMCAQYwDwYDVROTAQH/
BAUwAwEB/zAdBgNVHQ4EFgQUt27qkxQj2AgEA9cx4rfO7Vkz5qswDQYJKoZIhvcN
AQEFBQADgYEAqWTnhDcf7GUAww7hBk5XWbODsT5N/A/P2mVFs7mSpJpT3IldbE+I
Ipf4kRFruoN6bIFDwOyFnCp71BbWH8dF/OnMwBGMsFEhLrF6Fjw12ovObWVqCiAE
-----END CERTIFICATE-----
```

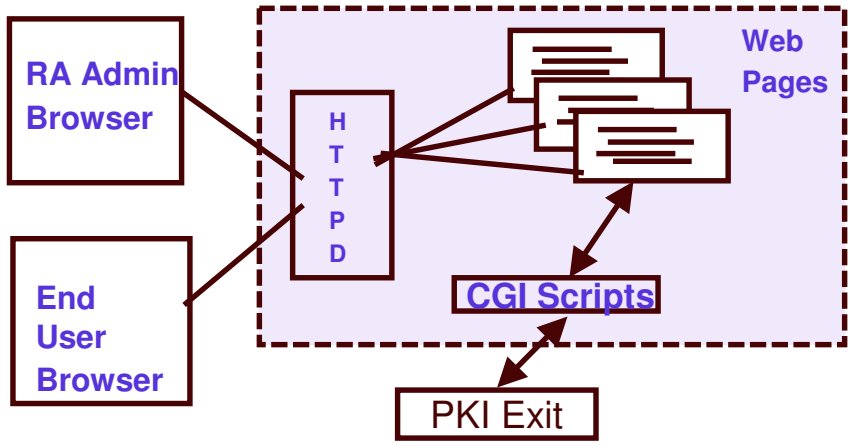
email: webmaster@your-company.com

The cert is returned in B64 format for you to cut and paste it to a file in the server side

z/OS PKI Services In Summary

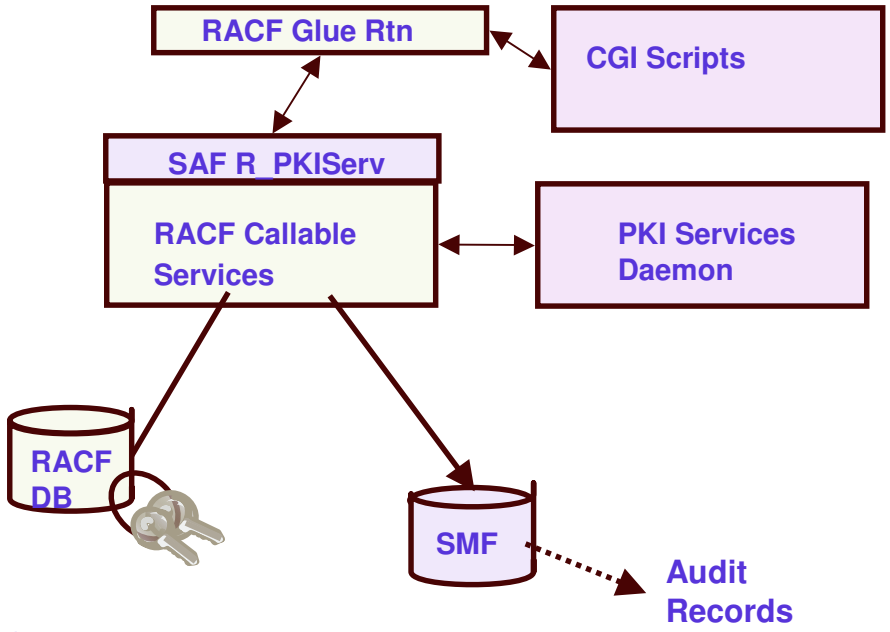
- **IKYSETUP**
  - A REXX exec shipped in SYS1.SAMPLIB to perform RACF administration tasks for setting up PKI Services.

- **Browser/CGI interface**
  - Web page contents are defined in a certificate template file, pkiserv.tmpl
  - The CGIs read the template file to form the web pages
  - Invoke the R_PKIServ callable service
  - provide hooks to exit routine for customization



z/OS PKI Services In Summary…

- **SAF callable service – R_PKIServ**
  - Interface between CGIs and the PKI Services Daemon (through the glue routine)
  - Provides functions for end user and administrator



User:

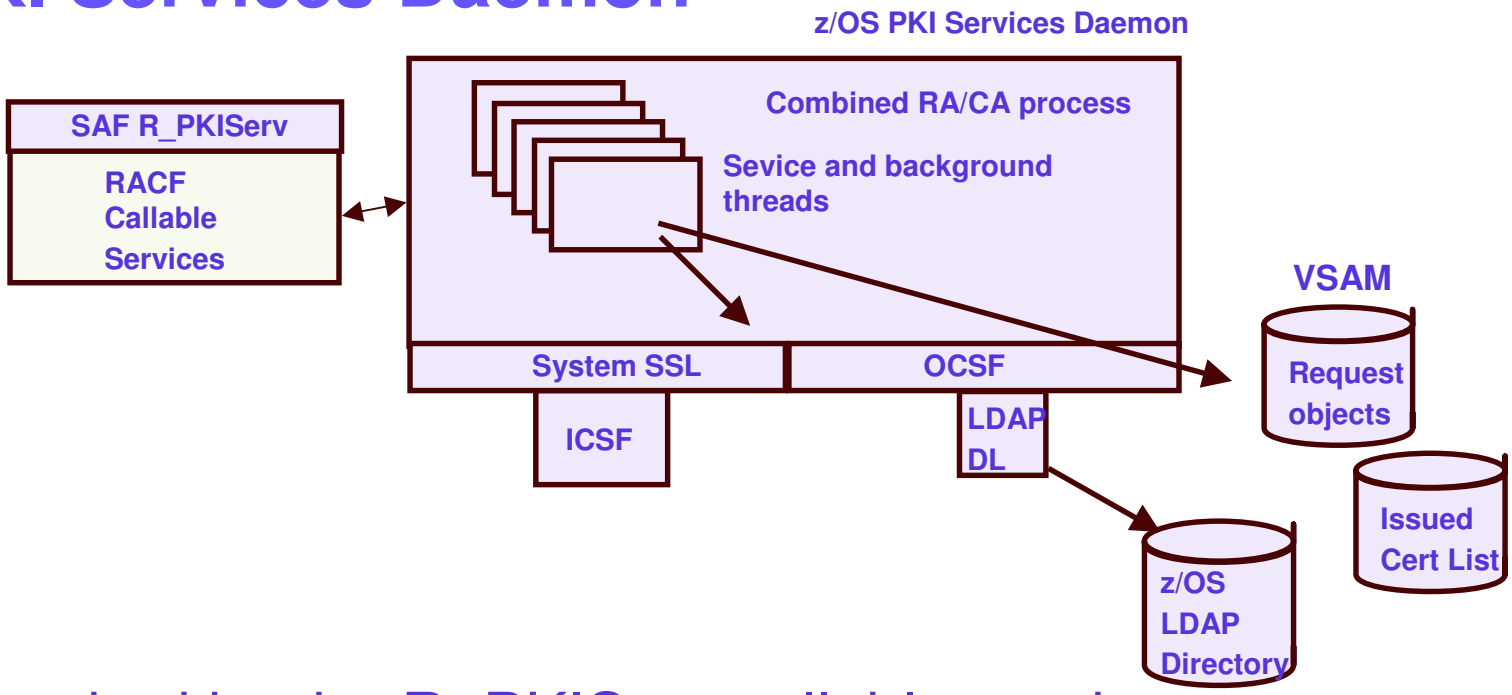
- Request (certificate)
- Export (certificate)
- Verify (certificate)
- Renew (certificate)
- Suspend (certificate)
- Revoke (certificate)

Administrator:

- Query (request, certificate)
- Approve (request)
- Modify (request)
- Reject (request)
- Suspend (certificate)
- Resume (certificate)
- Revoke (certificate)

z/OS PKI Services In Summary…

- **PKI Services Daemon**



  - Invoked by the R_PKIServ callable service
  - Perform the real work
  - Read the configuration file, pkiserv.conf, to determine the set up values

Using RACF as a CA VS PKI Services

Use RACDCERT if	Use PKI Services if
Just need to generate a handful of certificates	**Need to generate a large number of certificates**
You can manually keep track of the expiration dates of the certs	**You want to get notification on the expiration dates of the certs**
You want to manually send the certs to the other parties	**You want the other parties to retrieve the certs themselves**
You don't care if the certs are revoked	**You want to create CRLs for the revoked certs**
You just need basic extensions in the certs	**You want more supported extensions in the certs**

Major Prerequisite Products

- RACF (or equivalent)
  - For storing PKI CA certificate
- IBM z/OS HTTP Server
  - For web page interface
- LDAP Directory
  - For publishing issued certificates and CRLs
- ICSF (optional)
  - For more secure CA private key
- z/OS Communications Server (optional)
  - For email notification

References

- **PKI Services web site:**

http://www.ibm.com/servers/eserver/zseries/zos/pki

- **PKI Services Red Book:**

http://www.redbooks.ibm.com/abstracts/sg246968.html

- **RACF web site:**

http://www.ibm.com/servers/eserver/zseries/zos/racf

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

Questions???

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.**