IBM Systems Group

The Continuing Saga of PKI on the z/OS Platform
Session E4

Christine Marusek
email: marusek@us.ibm.com

June 14, 2004

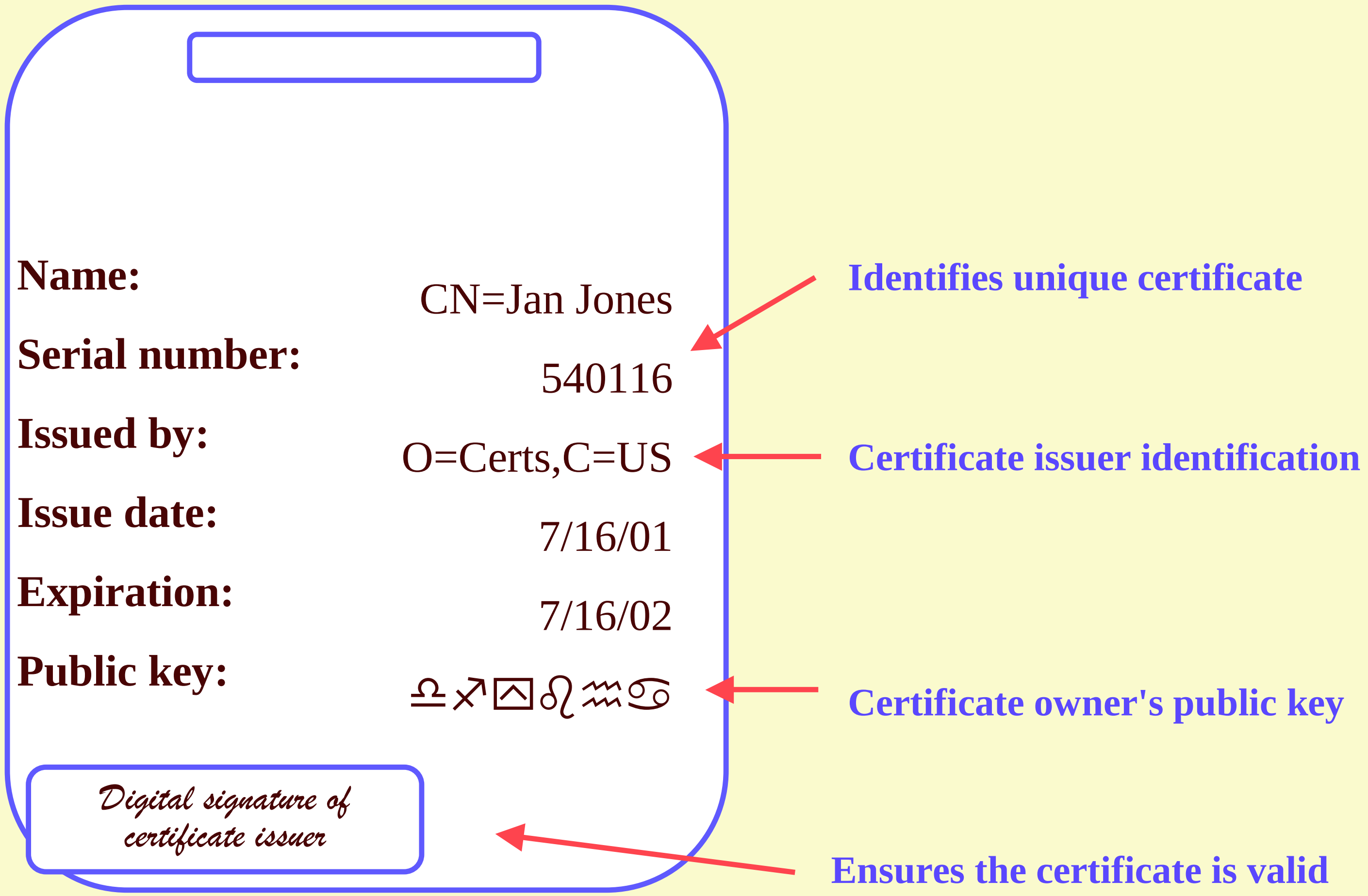
TRADEMARKS

- The following are trademarks or registered trademarks of the International Business Machines Corporation:
  - OS/390
  - RACF
  - z/OS
- UNIX is a registered trademark in the United States and other countries licensed exclusively through the Open Group.

AGENDA

- Introduction
  - Certificate Life Cycle
  - Architecture
- PKI Services on OS/390 Release 10 (Background)
- PKI Services on z/OS Release 3
  - Using PKI Services Web Interface
  - Post Installation Steps/Customization
  - Running PKI Services
- Updates to PKI Services on z/OS Release 4
- Updates to PKI Services on z/OS Release 5
- Utilities

Basic Digital Certificate



Name:	CN=Jan Jones
Serial number:	540116
Issued by:	O=Certs,C=US
Issue date:	7/16/01
Expiration:	7/16/02
Public key:	♎♐⍓♌♒♋

Digital signature of certificate issuer

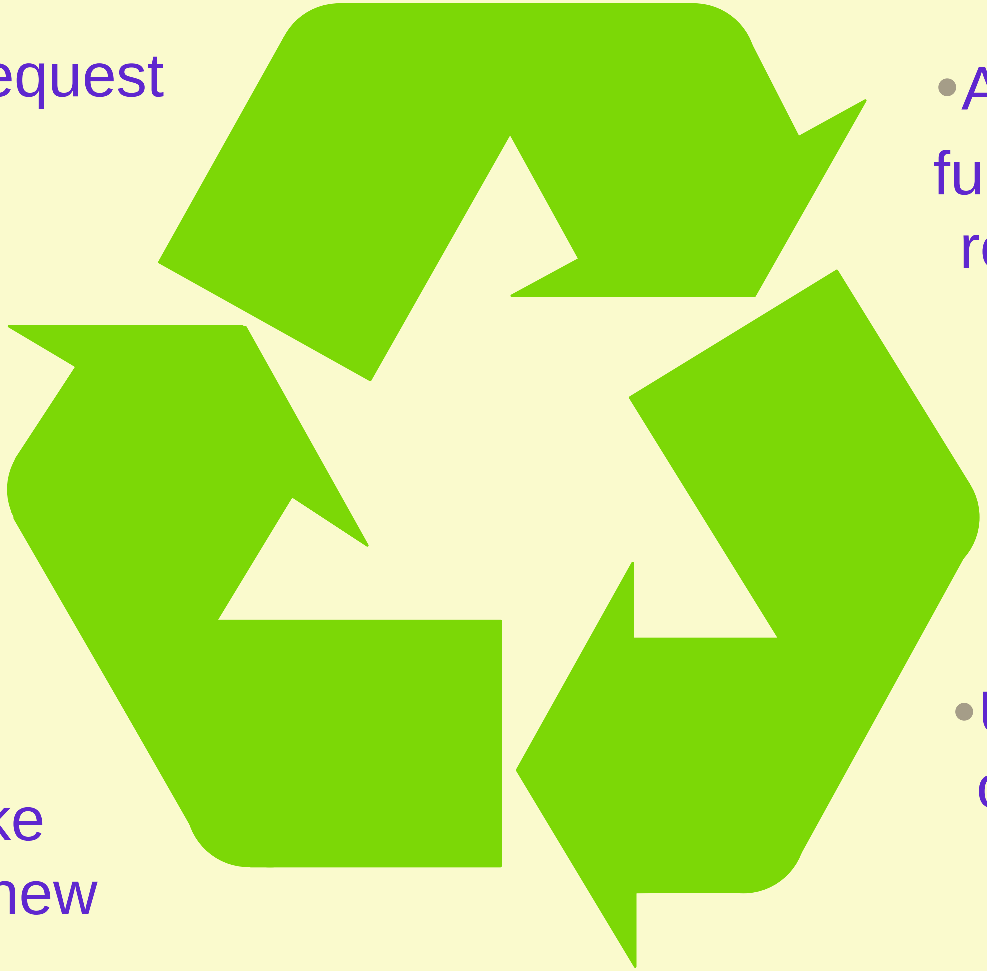
Identifies unique certificate

Certificate issuer identification

Certificate owner's public key

Ensures the certificate is valid

Certificate Life Cycle



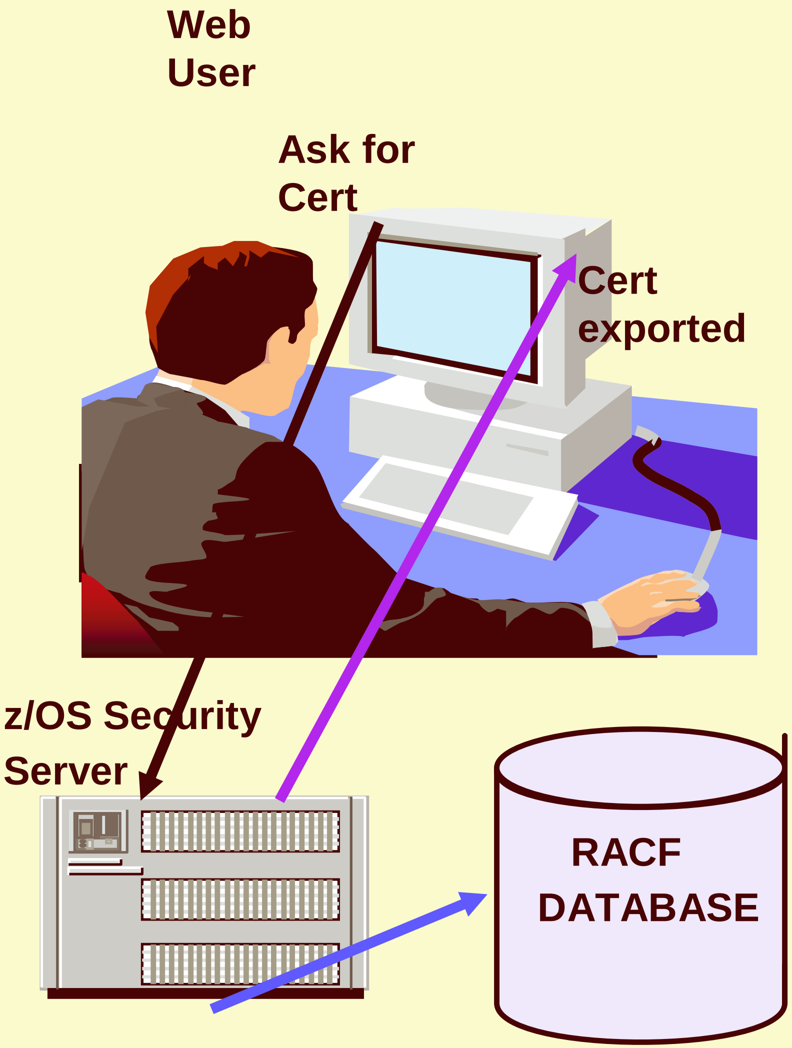
- Request
- Authorize - fulfillment of request
- Fulfillment
- Used by owner
- Revoke or Renew

Introduction PKI Services for S/390

- CA SERVLET
  - RACF SUPPORT OF FUNCTION WHICH IS ROUGHLY EQUIVALENT TO THE IBM HTTP SERVER CA SERVLET'S CERTIFICATE GENERATION AND RETRIEVAL
  - APARs
    - OW45211 - PTF UW74164
    - OW45212 - PTF UW74113
  - Creates certificates using RACF and R_PKIServ Callable Service
  - Customizable Web Page Interface
  - SMF Auditing

Introduction PKI for S/390

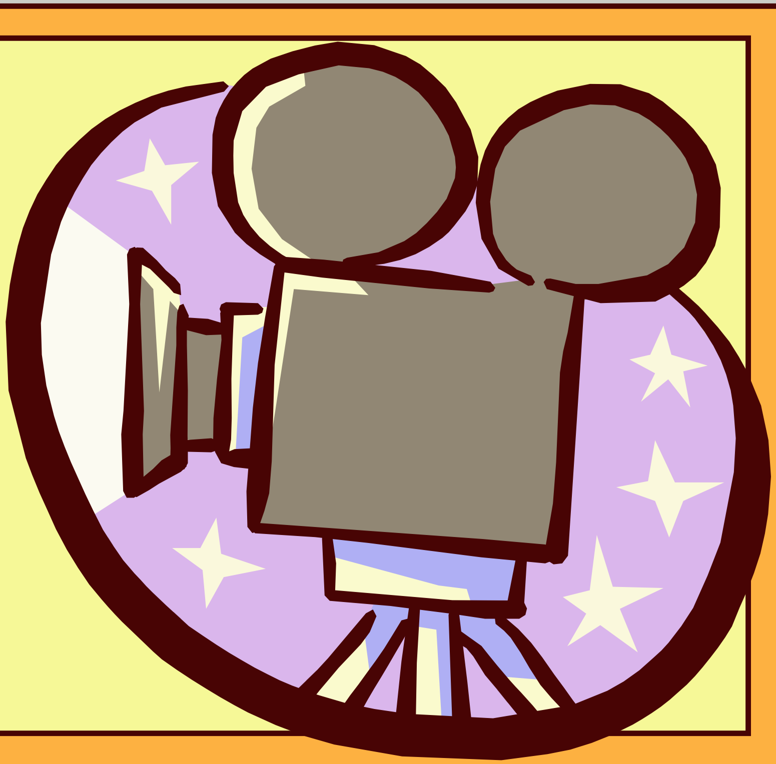
- Request for a certificate comes in through CGI scripts
- RACF accepts and massages data
- R_PKIServ Callable Service uses current RACF certificate creation
- Certificates created reside in the RACF Database
- Automatic approval process
- Certificate returned
- Export certificates into browser



Presenting ....

z/OS

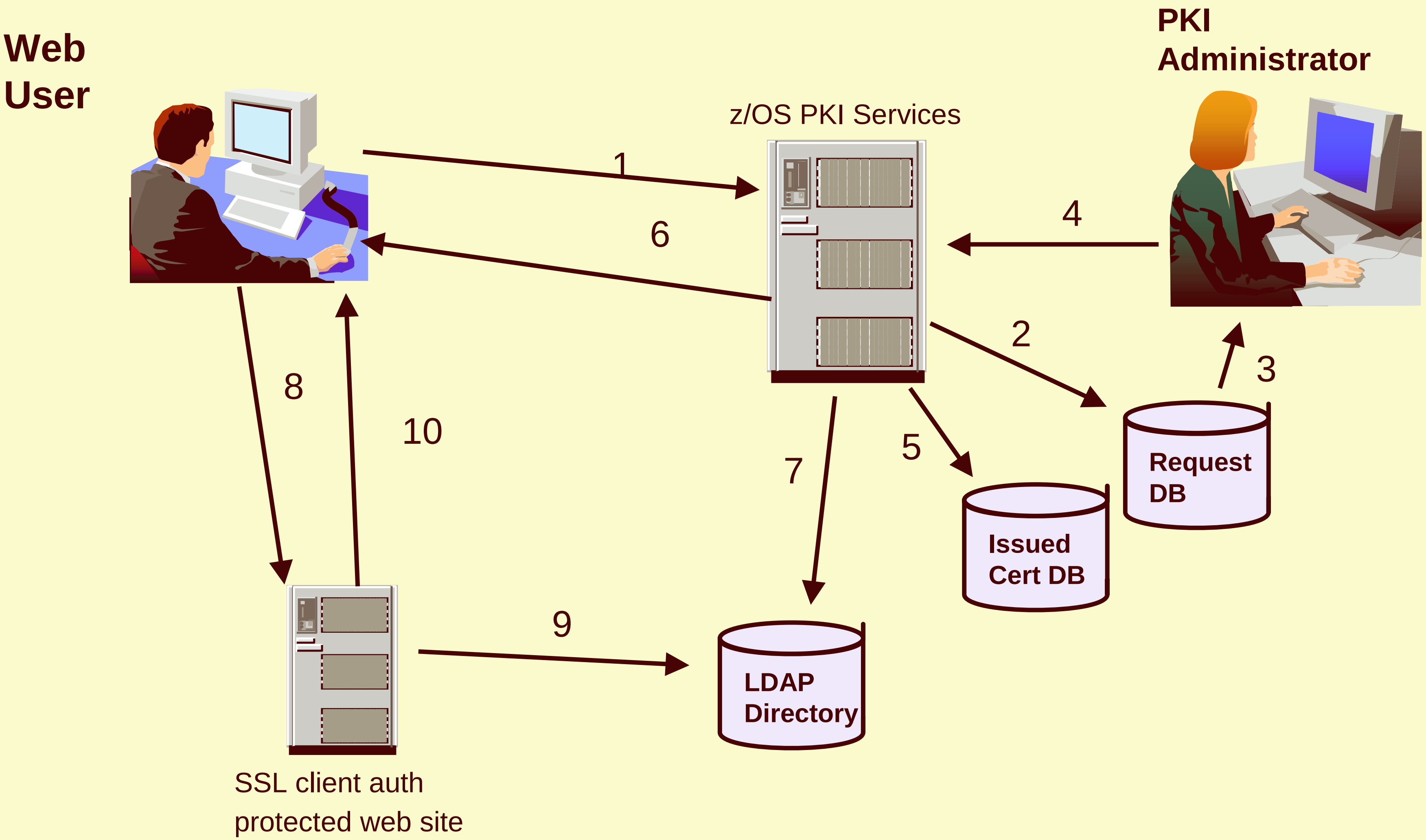
RELEASE 3



Introduction PKI Services on z/OS Release 3

- What is PKI Services?
  - New component of the z/OS Security Server
    - Always enabled but closely tied to RACF
  - Complete Certificate Authority (CA) package
    - Full certificate life cycle management
      - User request driven via customizable web pages
        - Browser or server certificates
      - Automatic or administrator approval process
        - Administered using same web interface
      - End user / administrator revocation process
  - Manual - "z/OS Security Server PKI Services Guide and Reference"

Browser Certificates



Web User

PKI Administrator

z/OS PKI Services

1

2

3

4

5

6

7

8

9

10

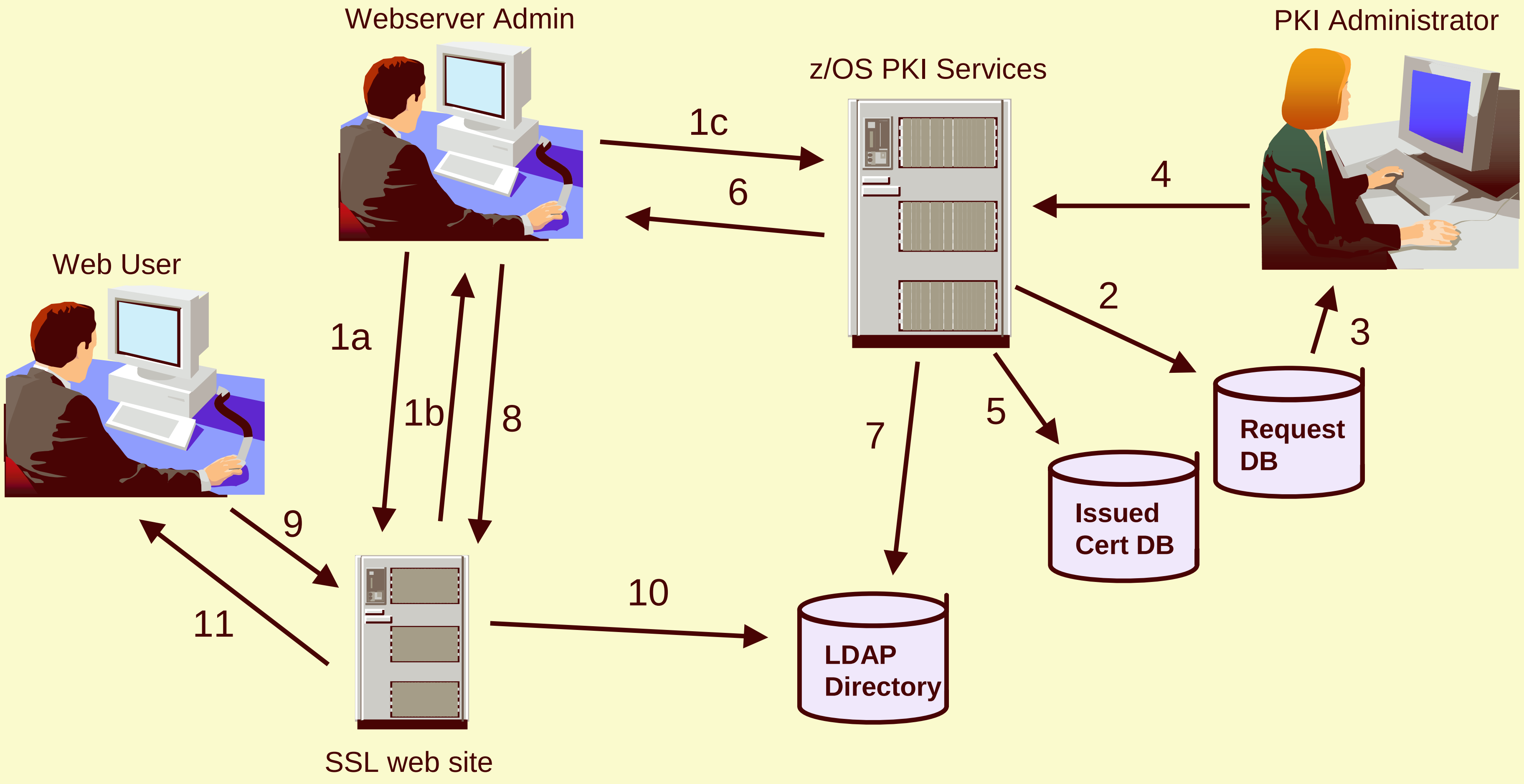
Request DB

Issued Cert DB

LDAP Directory

SSL client auth protected web site

Server Certificates



z/OS PKI Services Architecture

- HTTP Server
  - Provides browser/CGI interface for end-users and administrators
    - Web page logic defined in certificate templates file
    - CGIs - Read template file, control flow

z/OS PKI Services Architecture

- R_PKIServ - SAF callable service backed by RACF
  - End-user functions - Request, retrieve, verify, revoke, or renew a certificate
  - Administrator functions - Query, approve, modify, or reject certificate requests, query and revoke issued certificates
  - Interface to call PKI Services
  - SMF auditing

z/OS PKI Services Architecture

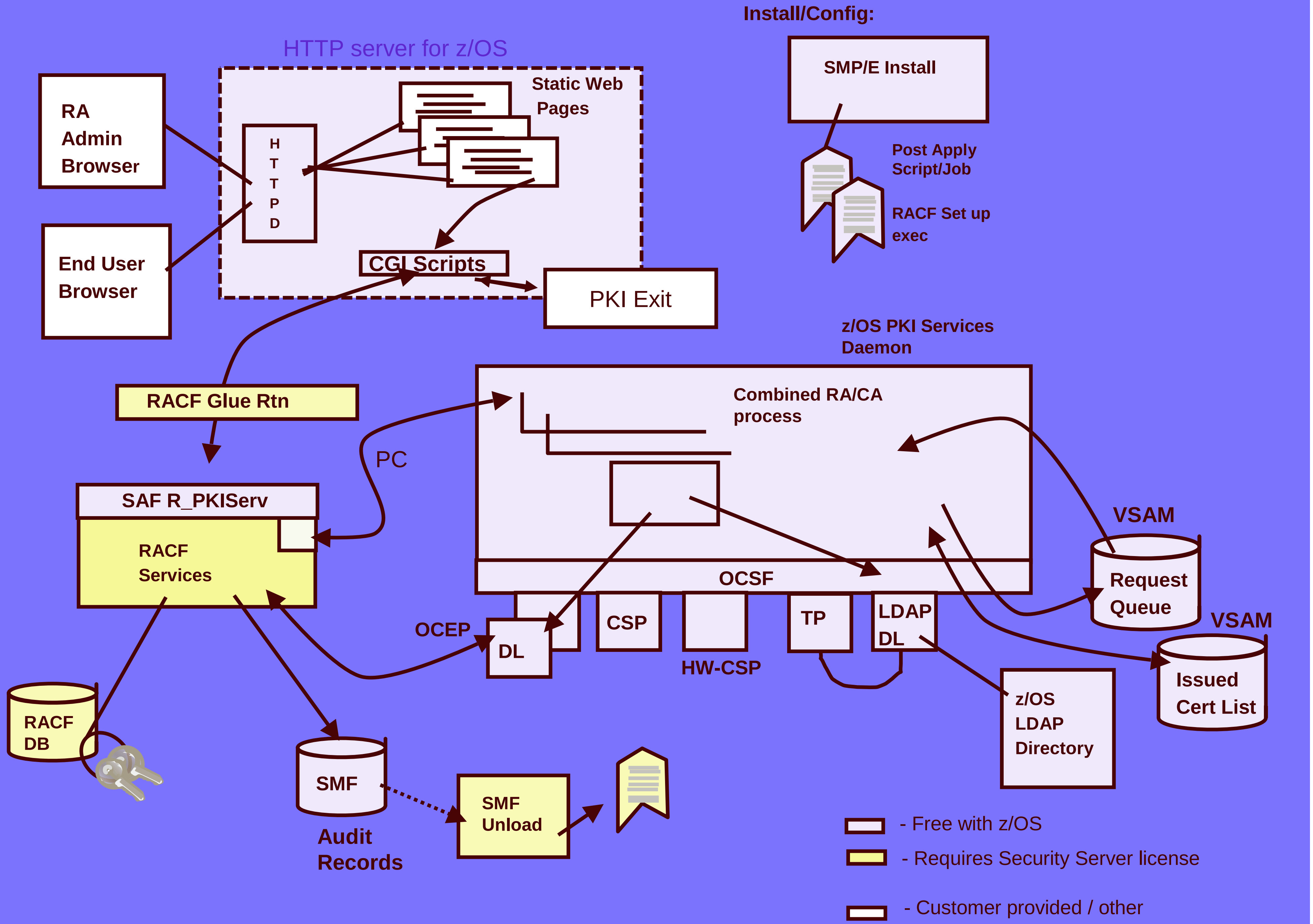
- PKI Services Daemon
  - Services threads for incoming requests
  - Background threads for certificate approval/certificate revocation list (CRL) issuance
  - VSAM DBs for requests (ObjectStore) and issued certificate list (ICL)

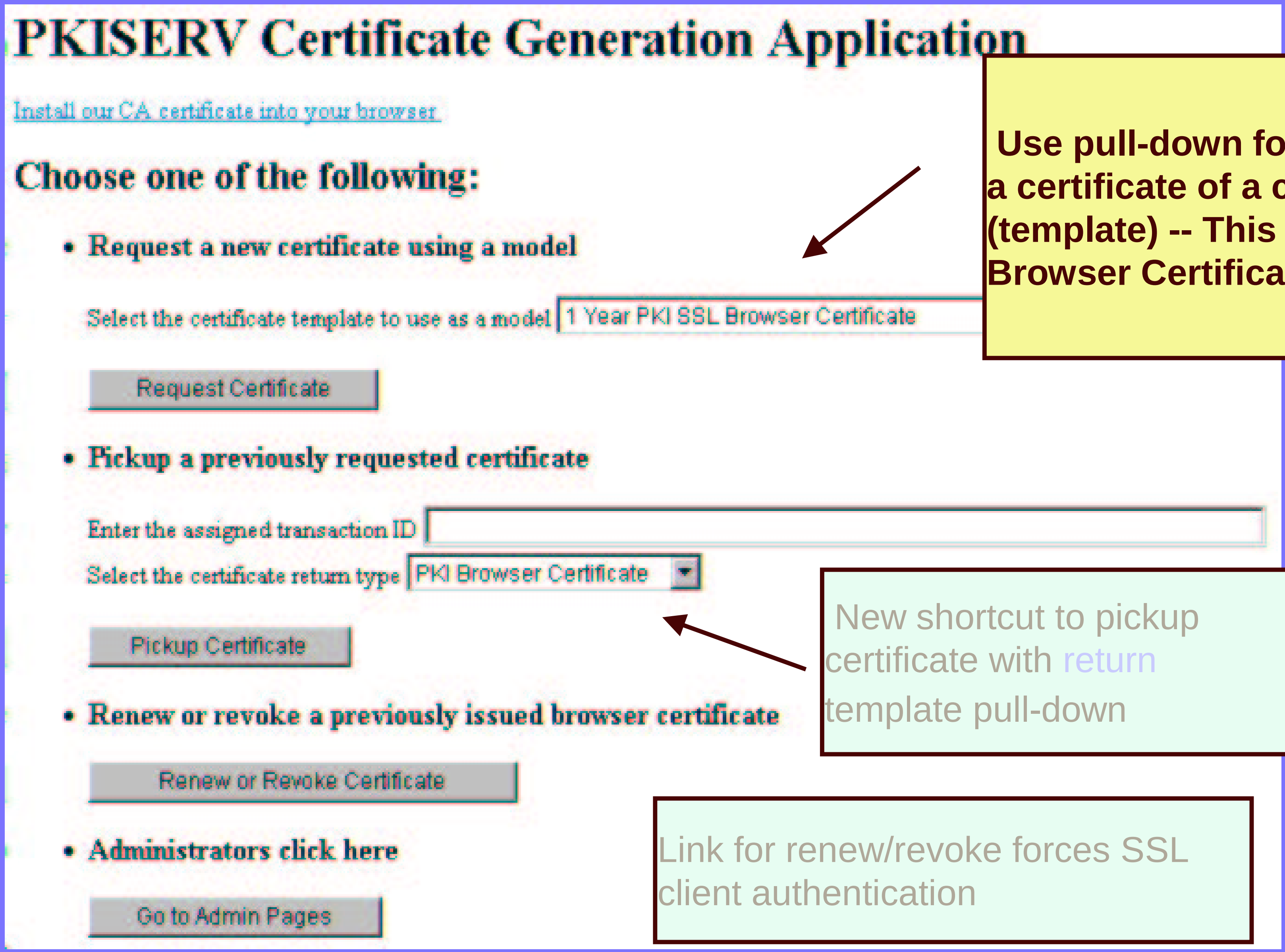
z/OS PKI Services Architecture...

- Open Cryptographic Services Facility (OCSF) and Open Cryptographic Enhanced Plug-ins (OCEP)
  - Provided the crypto facilities for PKI Services
    - OCEP - Access to CA certificate and private key in RACF
    - OCSF - BSAFE or ICSF (Hardware) crypto engines

- LDAP Directory
  - Publication of issued certificates and CRLs

z/OS PKI Services Architecture...





PKISERV 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

- **Pickup a previously requested certificate**

  Enter the assigned transaction ID

  Select the certificate return type: PKI Browser Certificate

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

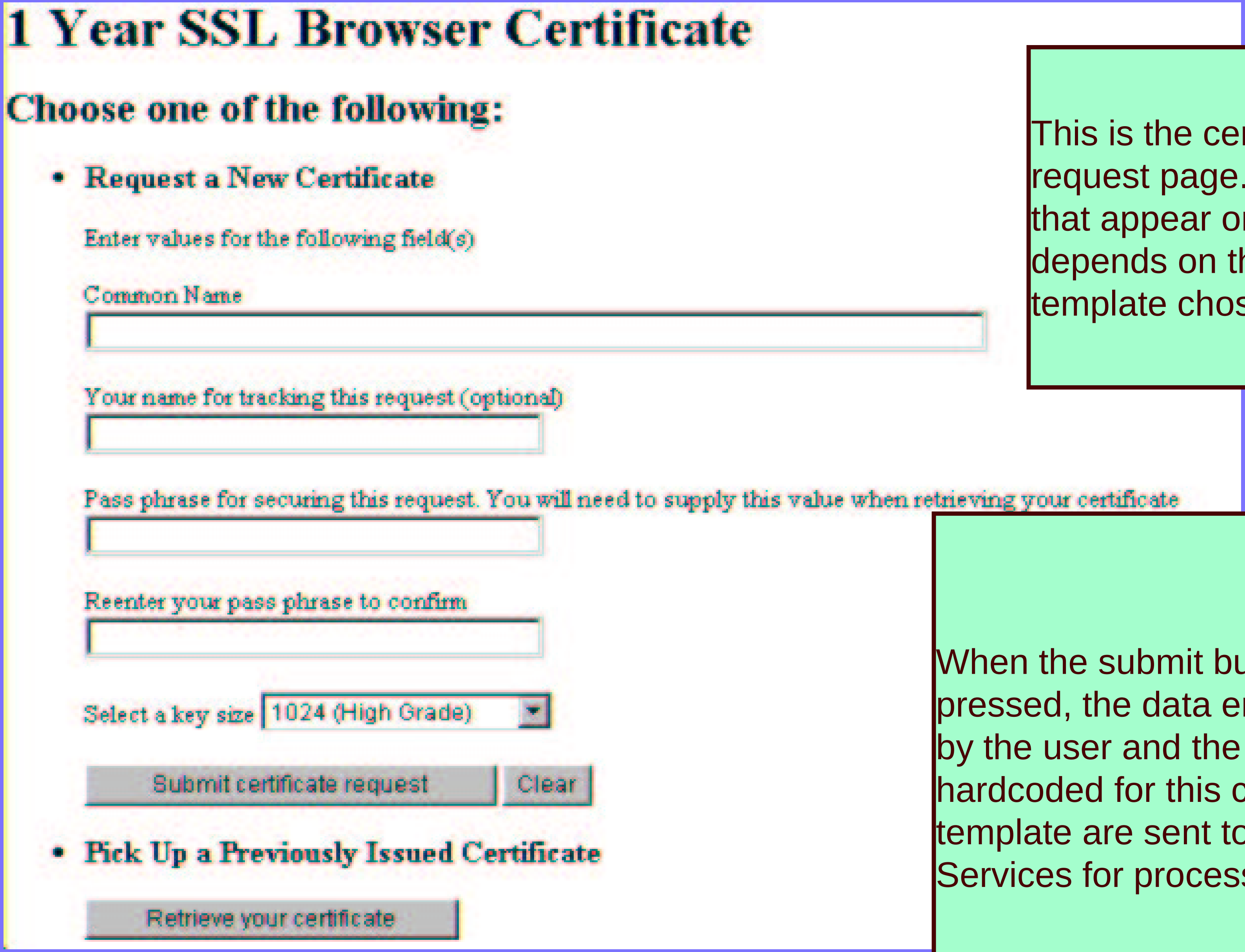
- **Administrators click here**

Use pull-down for requesting a certificate of a certain type (template) -- This case is a Browser Certificate

New shortcut to pickup certificate with return template pull-down

Link for renew/revoke forces SSL client authentication

Admin link is either userid/pw protected or forces SSL client authentication



1 Year SSL Browser Certificate

Choose one of the following:

- **Request a New Certificate**

  Enter values for the following field(s)

  Common Name

  Your name for tracking this request (optional)

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

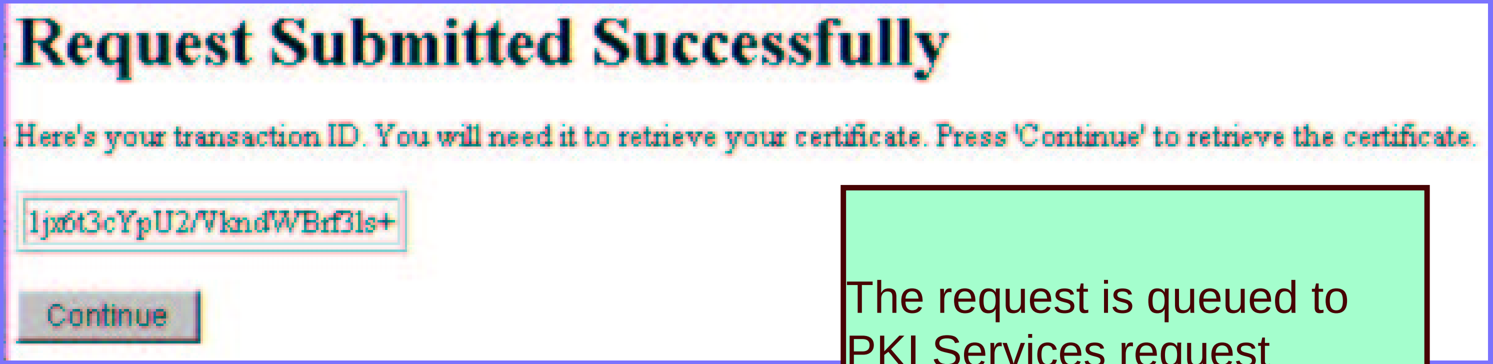
  Reenter your pass phrase to confirm

  Select a key size 1024 (High Grade)

- **Pick Up a Previously Issued Certificate**

This is the certificate request page. The dialogs that appear on this page depends on the certificate template chosen.

When the submit button is pressed, the data entered by the user and the data hardcoded for this certificate template are sent to PKI Services for processing

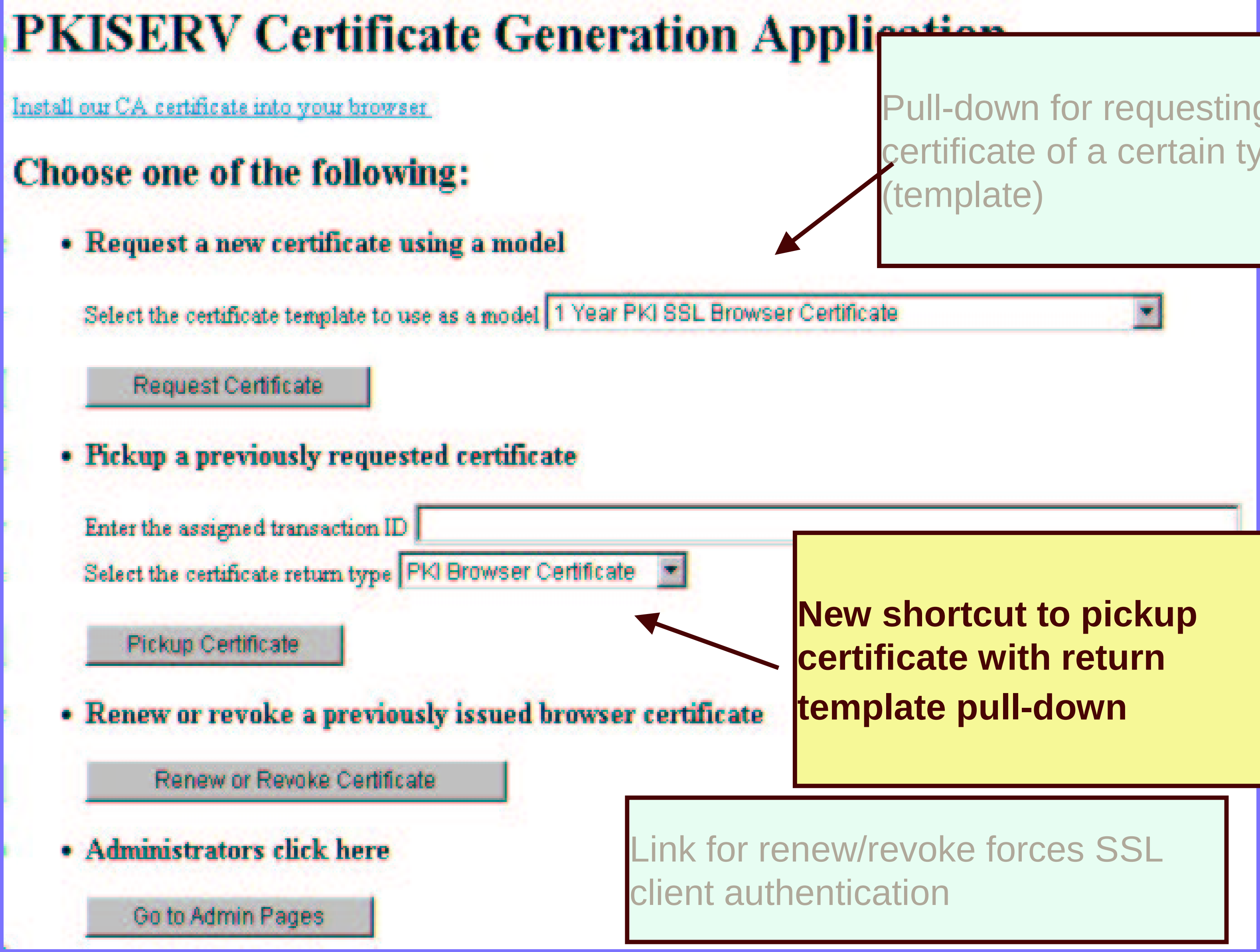


Request Submitted Successfully

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

1jx6t3cYpU2/VkndWBrf3ls+

The request is queued to PKI Services request database for approval. The result is the return of a transaction ID



PKISERV 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

- **Pickup a previously requested certificate**

Enter the assigned transaction ID

Select the certificate return type PKI Browser Certificate

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

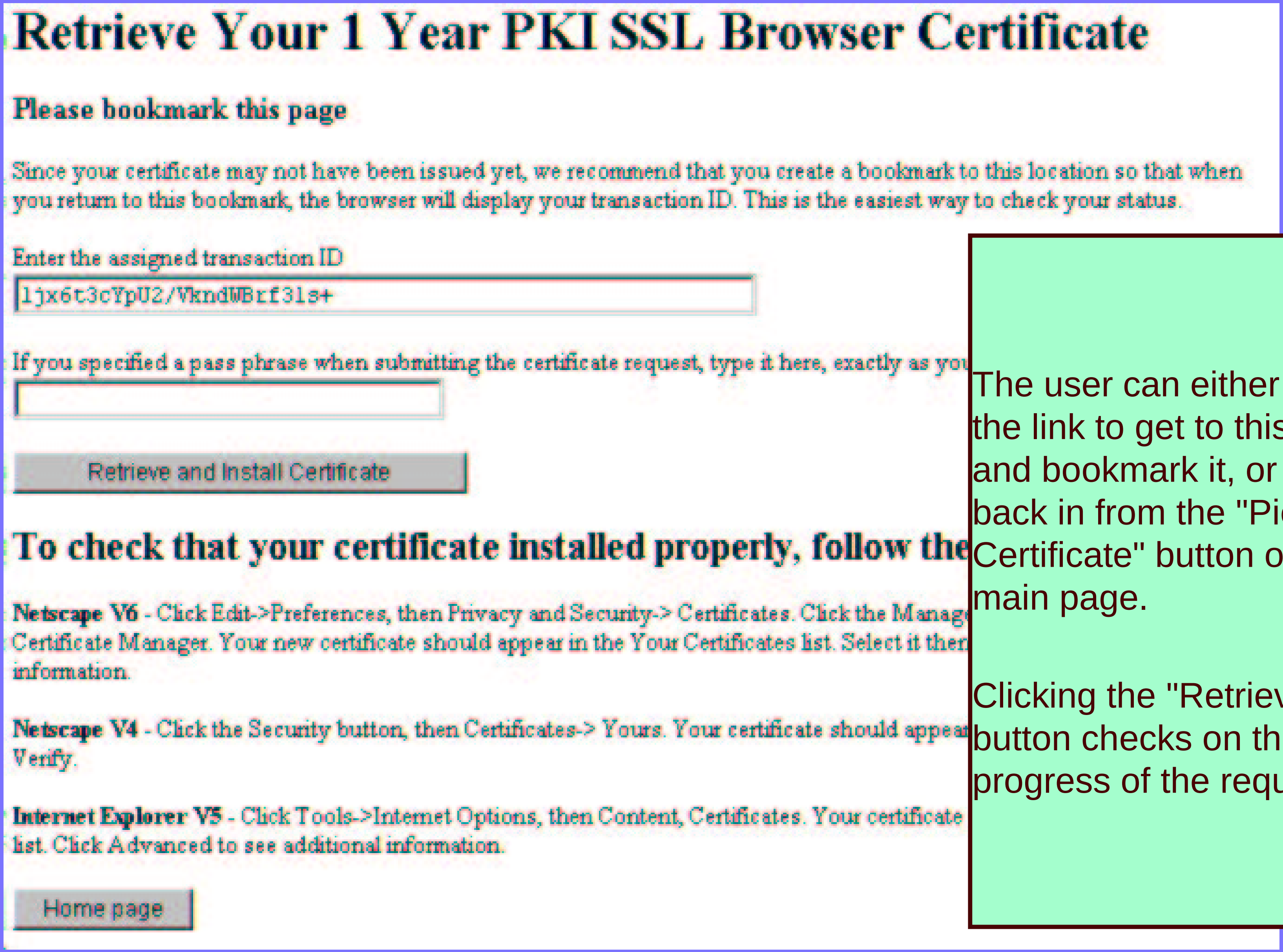
- **Administrators click here**

Pull-down for requesting a certificate of a certain type (template)

New shortcut to pickup certificate with return template pull-down

Link for renew/revoke forces SSL client authentication

Admin link is either userid/pw protected or forces SSL client authentication



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

1jx6t3cYpU2/VkndWBrf3ls+

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

To check that your certificate installed properly, follow the

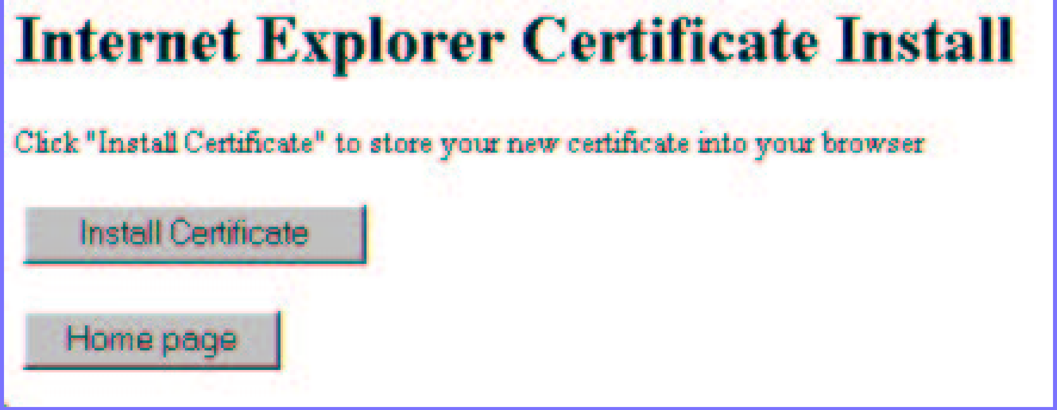
Netscape V6 - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then information.

Netscape V4 - Click the Security button, then Certificates-> Yours. Your certificate should appear Verify.

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

The user can either follow the link to get to this page and bookmark it, or come back in from the "Pick up Certificate" button on the main page.

Clicking the "Retrieve" button checks on the progress of the request.

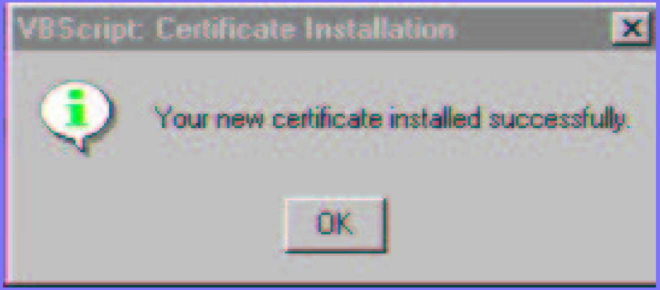


Internet Explorer Certificate Install

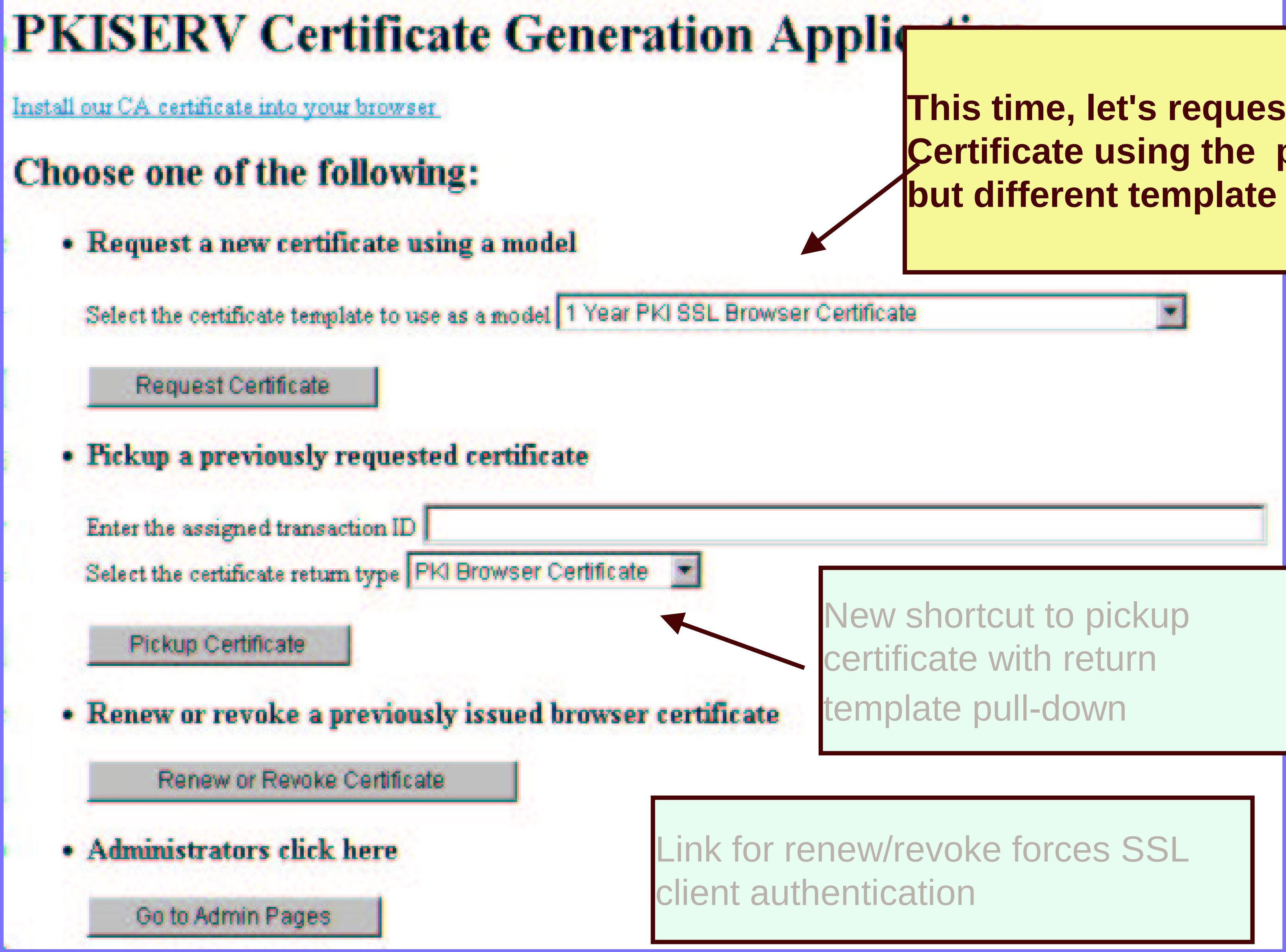
Click "Install Certificate" to store your new certificate into your browser

If the certificate has been issued, it may be installed.

This page shows how it would look for Microsoft's IE browser



Your new certificate installed successfully.



PKISERV Certificate Generation Appli

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

- **Pickup a previously requested certificate**

Enter the assigned transaction ID

Select the certificate return type: PKI Browser Certificate

Pickup Certificate

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

Renew or Revoke Certificate

- **Administrators click here**

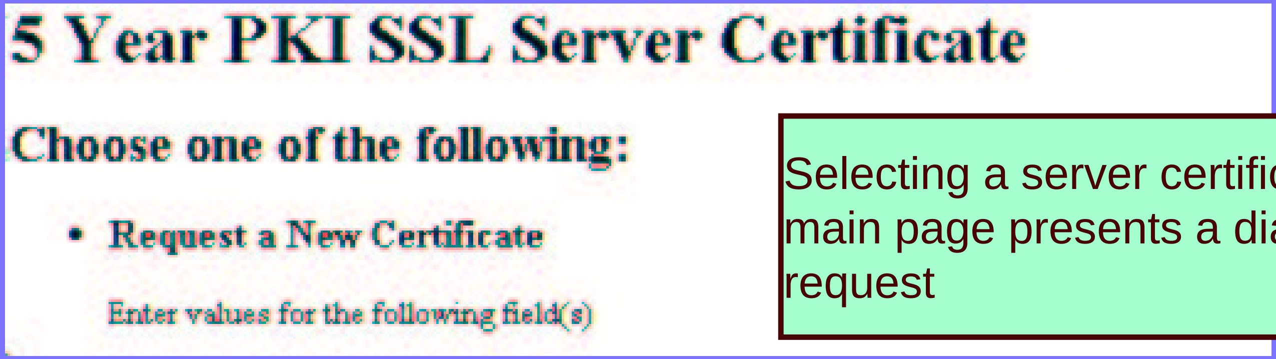
Go to Admin Pages

This time, let's request a Server Certificate using the pull-down but different template

New shortcut to pickup certificate with return template pull-down

Link for renew/revoke forces SSL client authentication

Admin link is either userid/pw protected or forces SSL client authentication



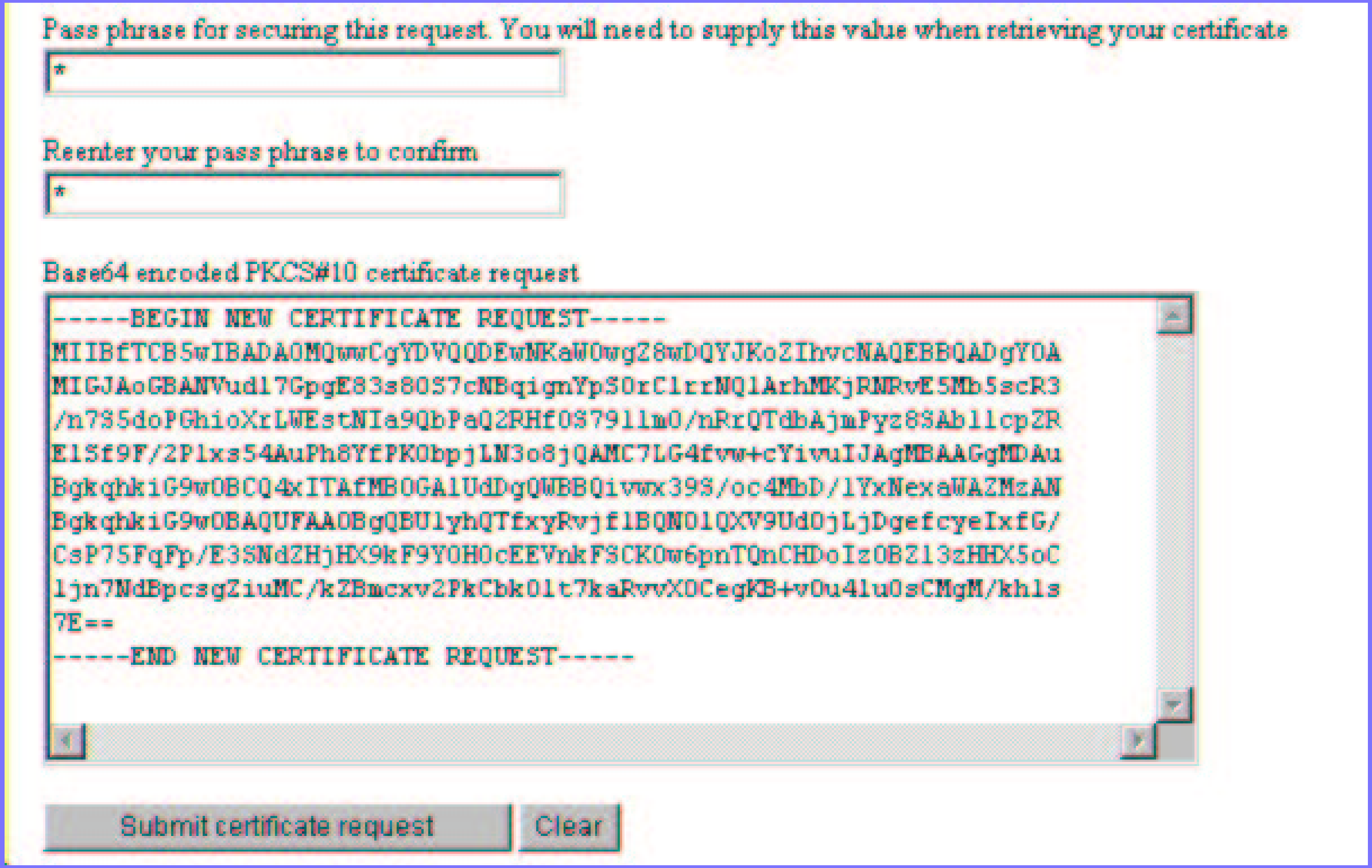
5 Year PKI SSL Server Certificate

Choose one of the following:

- **Request a New Certificate**

Enter values for the following field(s)

Selecting a server certificate template from the main page presents a dialog to enter a PKCS#10 request



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

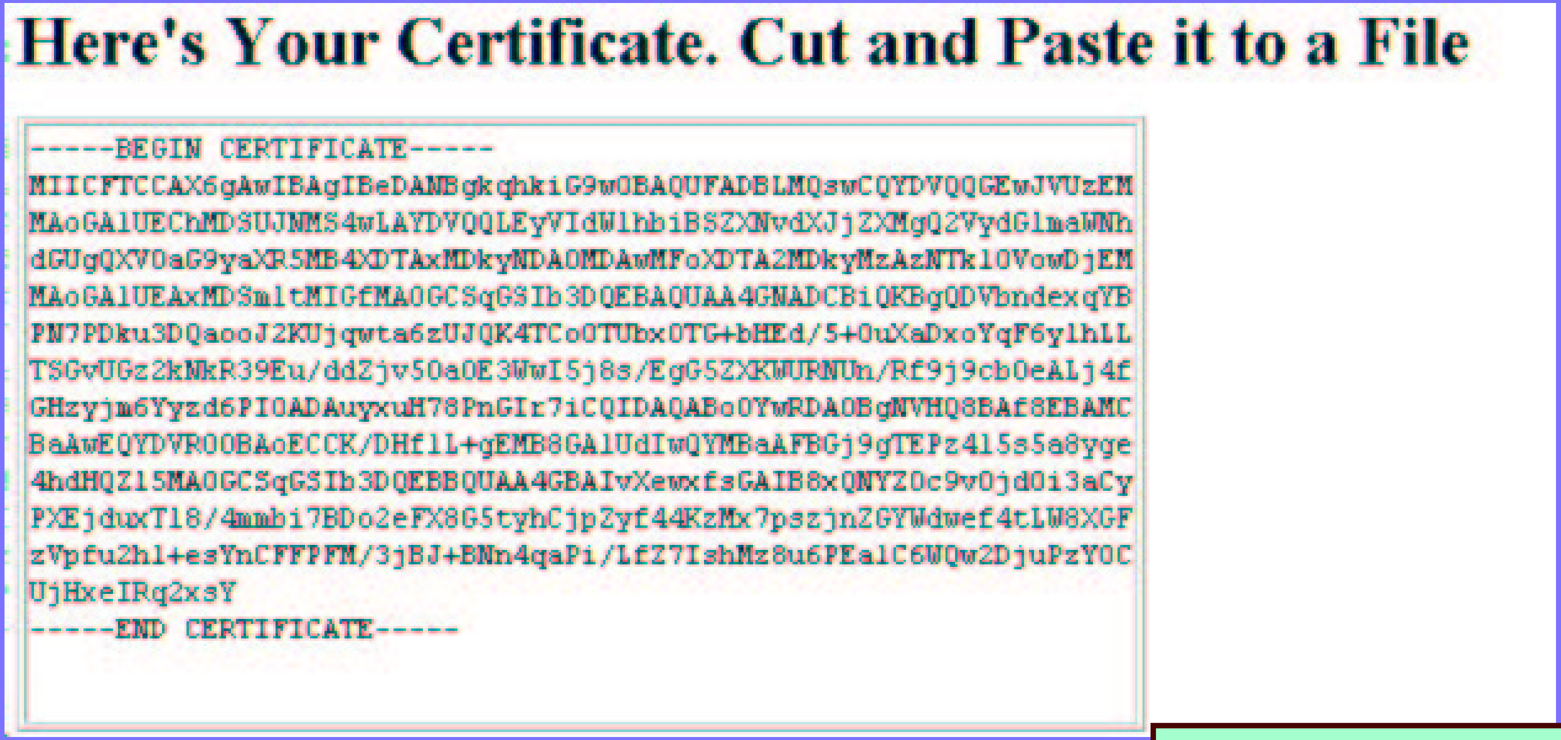
*

Reenter your pass phrase to confirm

*

Base64 encoded PKCS#10 certificate request

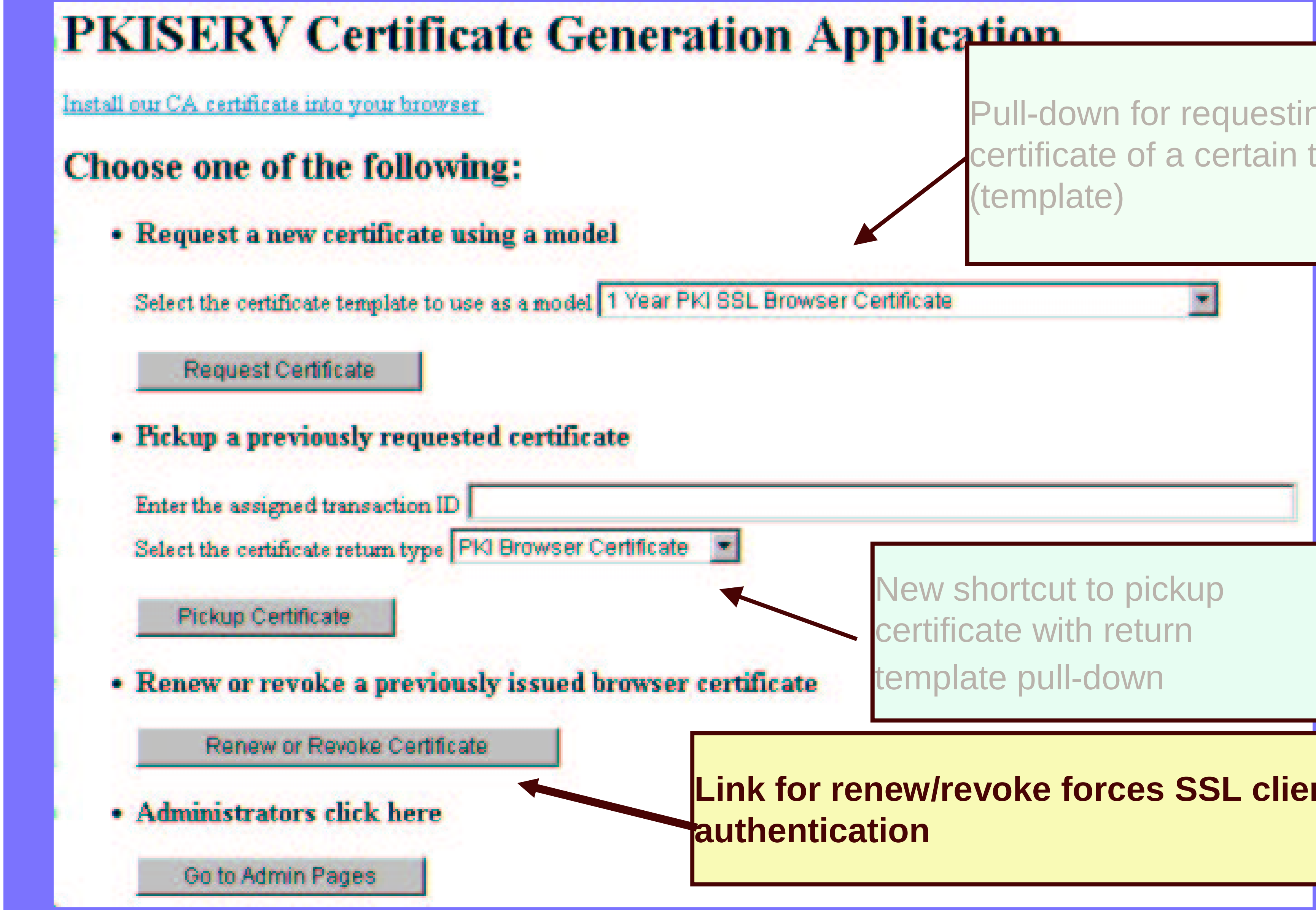
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBfTCB5wIBADA0MQwwCgYDVQQDEwNKaW0wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBANVudl7GpgE83s80S7cNBqignYpS0rClrrNQlArhMKjRNRvE5Mb5scR3
/n7S5doPGhioXrLWEstNIa9QbPaQ2RHf0S791lm0/nRrQTdbAjmPyz8SAbllcpZR
ElSf9F/2Plxs54AuPh8YfPK0bpjLN3o8jQAMC7LG4fvw+cYivuIJAgMBAAGgMDAu
BgkqhkiG9w0BCQ4xITAfMB0GA1UdDgQWBBQivwx39S/oc4MbD/lYxNexaWAZMzAN
BgkqhkiG9w0BAQUFAA0BgQBUlyhQTfxyRvjflBQN0lQXV9Ud0jLjDgefcyeIxfG/
CsP75FqFp/E3SNdZHjHX9kF9Y0H0cEEVnkFSCK0w6pnTQnCHDoIz0BZl3zHHX5oC
ljn7NdBpcsgZiuMC/kZBmcxv2PkCbk0lt7kaRvvX0CegKB+v0u4lu0sCMgM/khls
7E==
-----END NEW CERTIFICATE REQUEST-----
```



Here's Your Certificate. Cut and Paste it to a File

```
-----BEGIN CERTIFICATE-----
MIICFTCCAX6gAwIBAgIBeDANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzEM
MAoGA1UEChMDSUJNMS4wLAYDVQQLEyVIdW1hbiBSZXNvdXJjZXMgQ2VydGlmaWNh
dGUgQXV0aG9yaXR5MB4XDTAxMDkyNDA0MDAwMFoXDTA2MDkyMzAzNTk1OVowDjEM
MAoGA1UEAxMDSm1tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDVbndexqYB
PN7PDku3DQaooJ2KUjqwta6zUJQK4TCoOTUbx0TG+bHEd/5+0uXaDxoYqF6ylhLL
TSGvUGz2kNkR39Eu/ddZjv50a0E3WwI5j8s/EgG5ZXKWURNUn/Rf9j9cb0eALj4f
GHzyjm6Yyzd6PIOADAuyxuH78PnGIr7iCQIDAQABo0YwRDA0BgNVHQ8BAf8EBAMC
BaAwEQYDVR00BAoECCK/DHf1L+gEMB8GA1UdIwQYMBaAFBGj9gTEPz415s5a8yge
4hdHQZ15MA0GCSqGSIb3DQEBBQUAA4GBAIvXewxfsGAIB8xQNYZ0c9v0jd0i3aCy
PXEjduxT18/4mmbi7BDo2eFX8G5tyhCjpZyf44KzMx7pszjnZGYWdwef4tLW8XGF
zVpfu2hl+esYnCFFPFM/3jBJ+BNn4qaPi/LfZ7IshMz8u6PEalC6WQw2DjuPzY0C
UjHxeIRq2xsY
-----END CERTIFICATE-----
```

Server certificates are returned in base64 encoded form.



PKISERV 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 ▾

- **Pickup a previously requested certificate**

Enter the assigned transaction ID:

Select the certificate return type: PKI Browser Certificate ▾

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

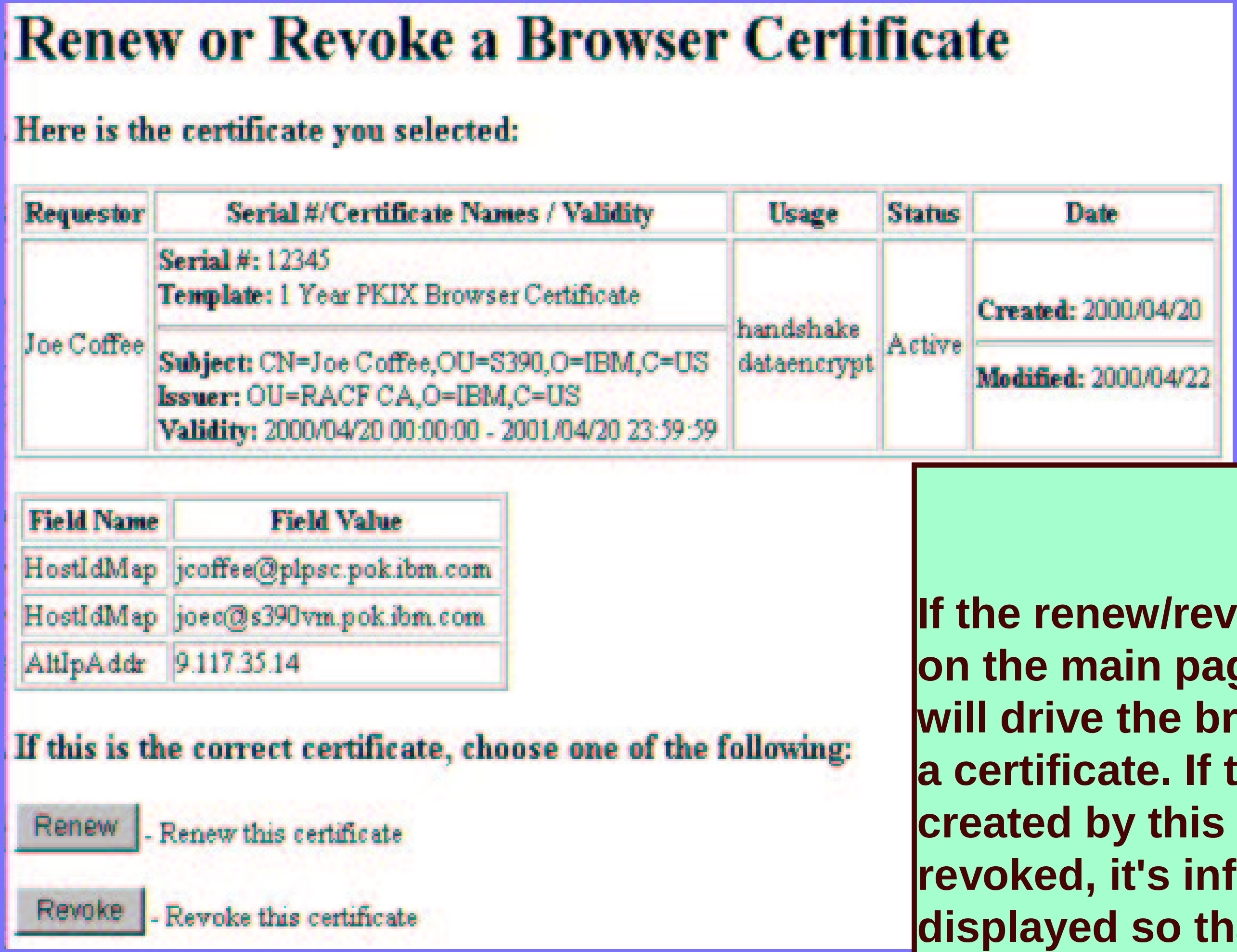
- **Administrators click here**

Pull-down for requesting a certificate of a certain type (template)

New shortcut to pickup certificate with return template pull-down

Link for renew/revoke forces SSL client authentication

Admin link is either userid/pw protected or forces SSL client authentication



Renew or Revoke a Browser Certificate

Here is the certificate you selected:

Requestor	Serial #/Certificate Names / Validity	Usage	Status	Date
Joe Coffee	**Serial #:** 12345 **Template:** 1 Year PKIX Browser Certificate **Subject:** CN=Joe Coffee,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/20 00:00:00 - 2001/04/20 23:59:59	handshake dataencrypt	Active	**Created:** 2000/04/20 **Modified:** 2000/04/22

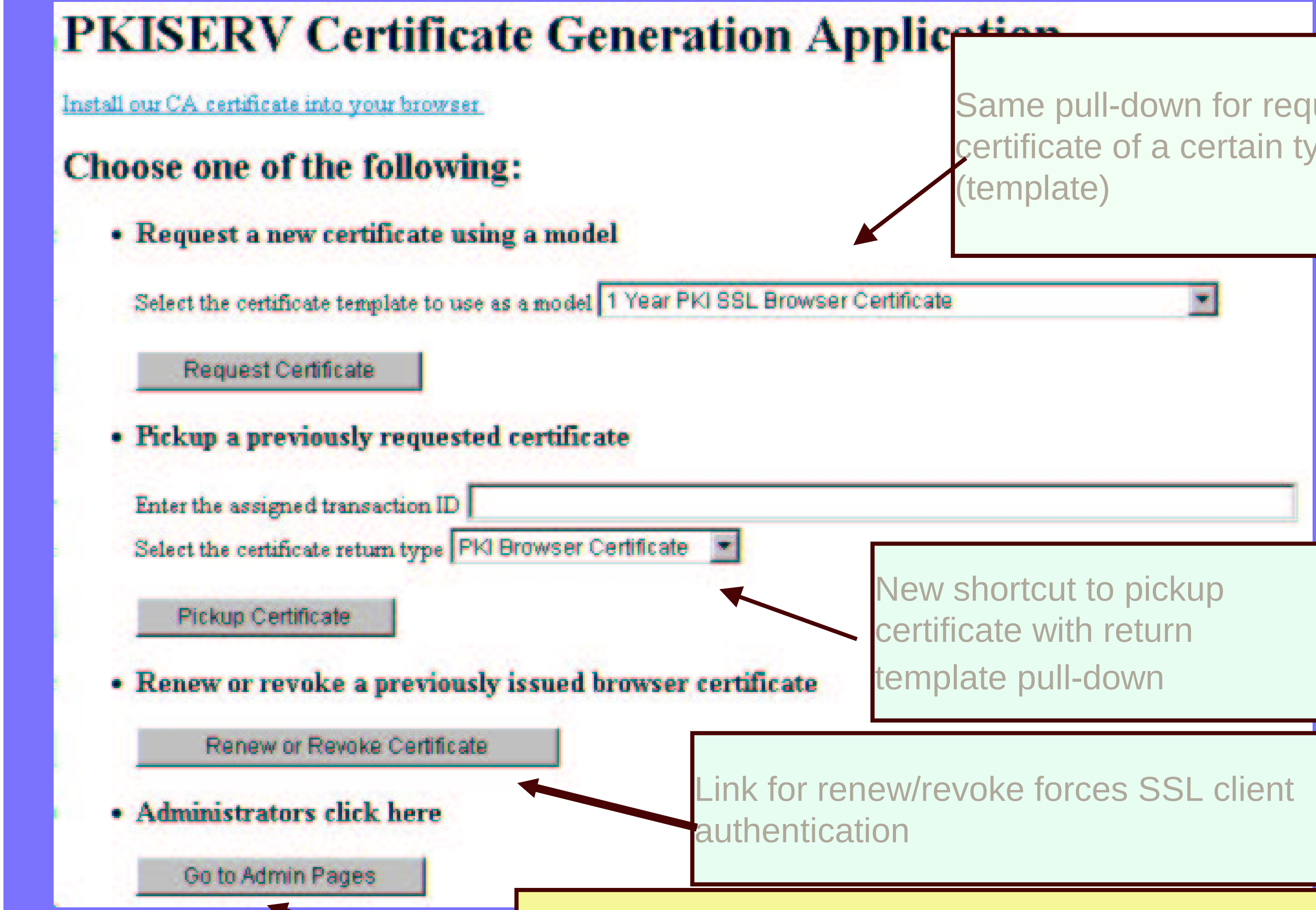
Field Name	Field Value
HostIdMap	jcoffee@plpsc.pok.ibm.com
HostIdMap	joec@s390vm.pok.ibm.com
AltIpAddr	9.117.35.14

If this is the correct certificate, choose one of the following:

Renew - Renew this certificate

Revoke - Revoke this certificate

If the renew/revoke button is pressed on the main page, client authentication will drive the browser dialogs to select a certificate. If the one selected was created by this PKI CA and is not revoked, it's information will be displayed so that the user may confirm and proceed.



PKISERV 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

- **Pickup a previously requested certificate**

Enter the assigned transaction ID

Select the certificate return type: PKI Browser Certificate

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

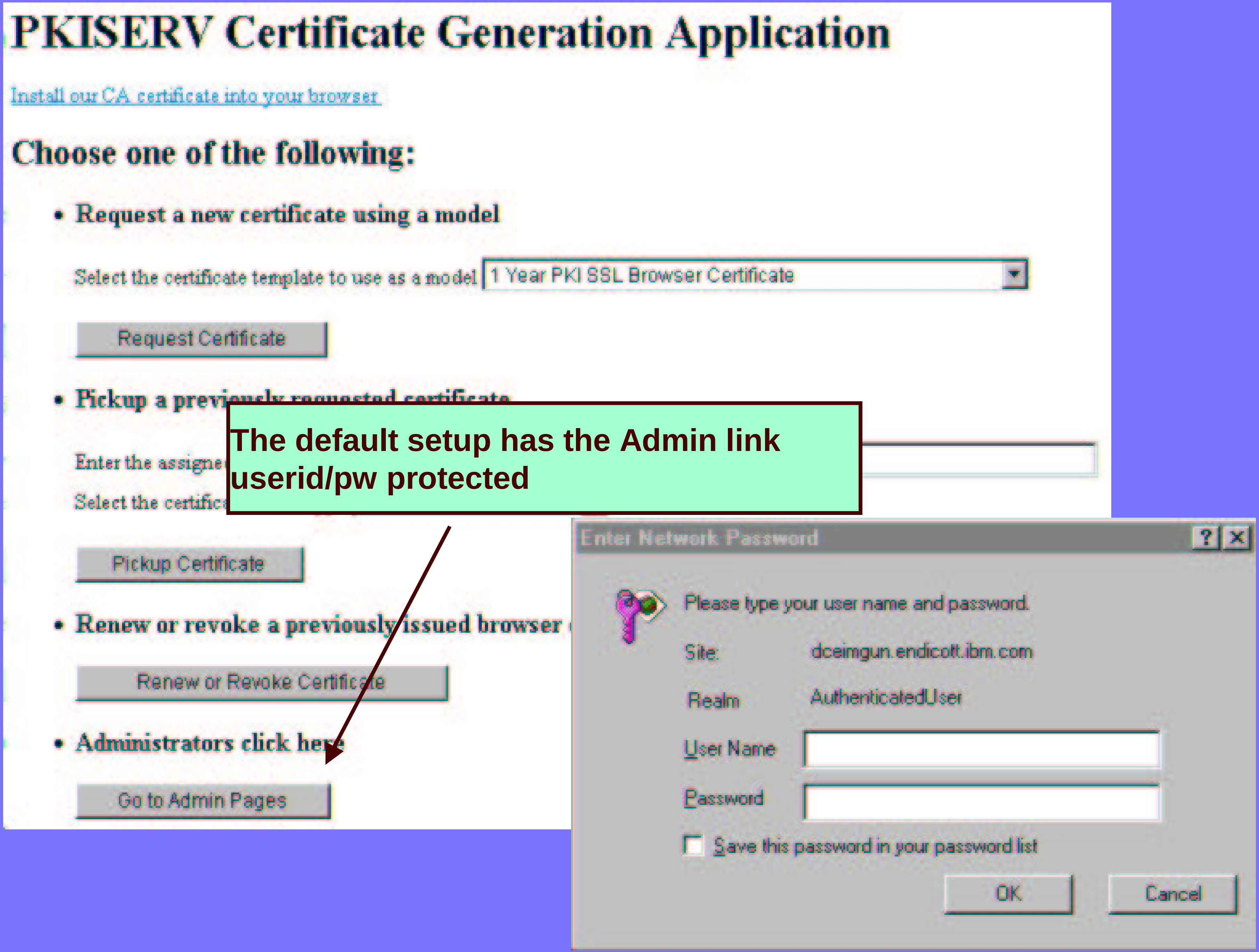
- **Administrators click here**

Same pull-down for requesting a certificate of a certain type (template)

New shortcut to pickup certificate with return template pull-down

Link for renew/revoke forces SSL client authentication

Now for RA functions. Admin link is either userid/pw protected or forces SSL client authentication



PKISERV 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

- **Pickup a previously requested certificate**

Enter the assigne

Select the certific

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

- **Administrators click here**

The default setup has the Admin link userid/pw protected

Enter Network Password

Please type your user name and password.

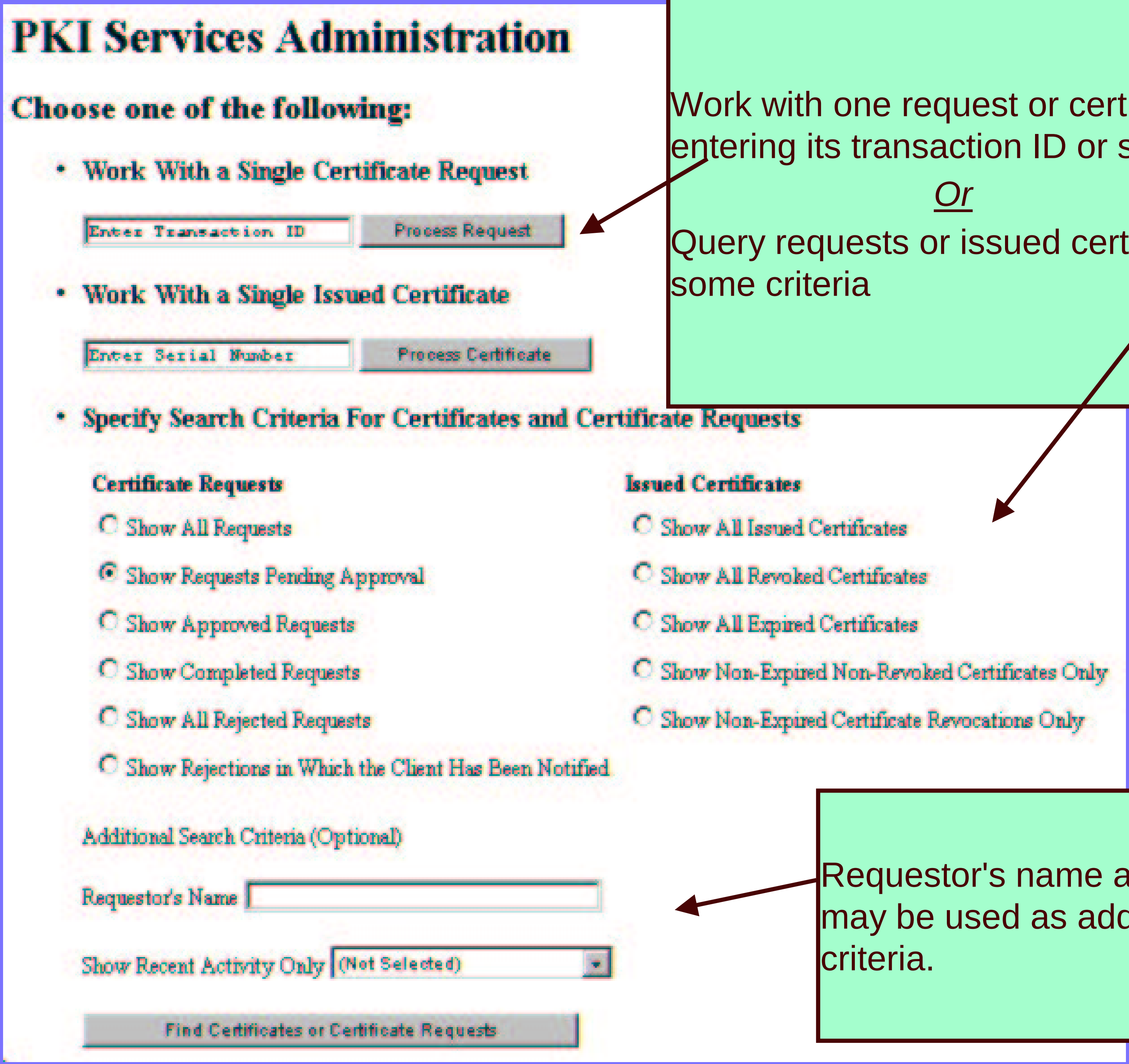
Site: dceimgun.endicott.ibm.com

Realm AuthenticatedUser

User Name

Password

□ Save this password in your password list



PKI Services Administration

Choose one of the following:

- Work With a Single Certificate Request

Enter Transaction ID [Process Request]

- Work With a Single Issued Certificate

Enter Serial Number [Process Certificate]

- Specify Search Criteria For Certificates and Certificate Requests

Certificate Requests

○ Show All Requests
● Show Requests Pending Approval
○ Show Approved Requests
○ Show Completed Requests
○ Show All Rejected Requests
○ Show Rejections in Which the Client Has Been Notified

Issued Certificates

○ Show All Issued Certificates
○ Show All Revoked Certificates
○ Show All Expired Certificates
○ Show Non-Expired Non-Revoked Certificates Only
○ Show Non-Expired Certificate Revocations Only

Additional Search Criteria (Optional)

Requestor's Name

Show Recent Activity Only (Not Selected)

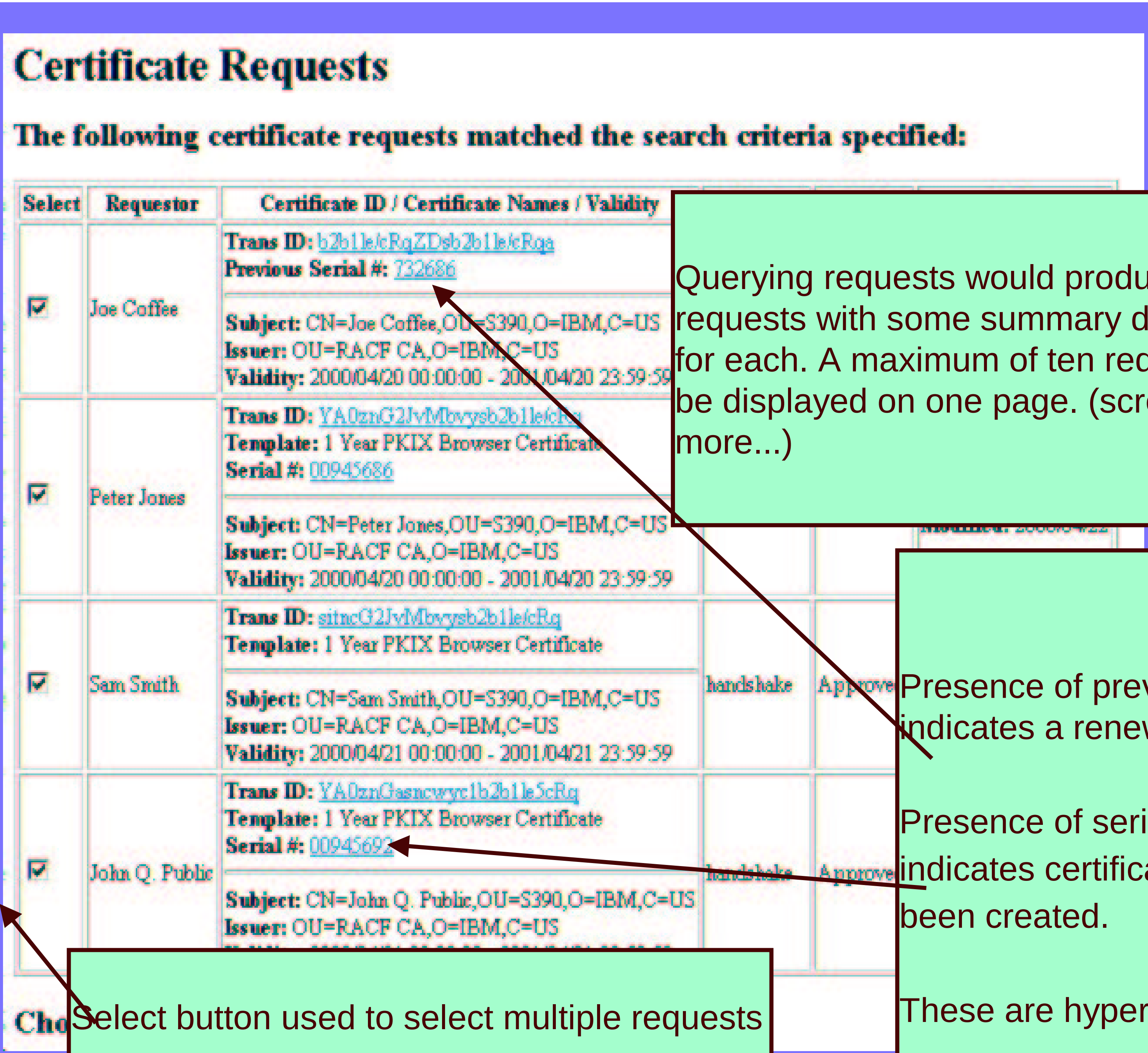
[Find Certificates or Certificate Requests]

Work with one request or certificate directly by entering its transaction ID or serial number.

Or

Query requests or issued certificates based on some criteria

Requestor's name and/or time period may be used as additional search criteria.



Certificate Requests

The following certificate requests matched the search criteria specified:

Select	Requestor	Certificate ID / Certificate Names / Validity			
☑	Joe Coffee	**Trans ID:** b2b1le/cRqZDsb2b1le/cRqa **Previous Serial #:** 732686 **Subject:** CN=Joe Coffee,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/20 00:00:00 - 2001/04/20 23:59:59			
☑	Peter Jones	**Trans ID:** YA0znG2JvMbvysb2b1le/cRq **Template:** 1 Year PKIX Browser Certificate **Serial #:** 00945686 **Subject:** CN=Peter Jones,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/20 00:00:00 - 2001/04/20 23:59:59			**Modified:** 2000/04/22
☑	Sam Smith	**Trans ID:** sitncG2JvMbvysb2b1le/cRq **Template:** 1 Year PKIX Browser Certificate **Subject:** CN=Sam Smith,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/21 00:00:00 - 2001/04/21 23:59:59	handshake	Approve	
☑	John Q. Public	**Trans ID:** YA0znGasncwyc1b2b1le5cRq **Template:** 1 Year PKIX Browser Certificate **Serial #:** 00945692 **Subject:** CN=John Q. Public,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US	handshake	Approve	

Cho

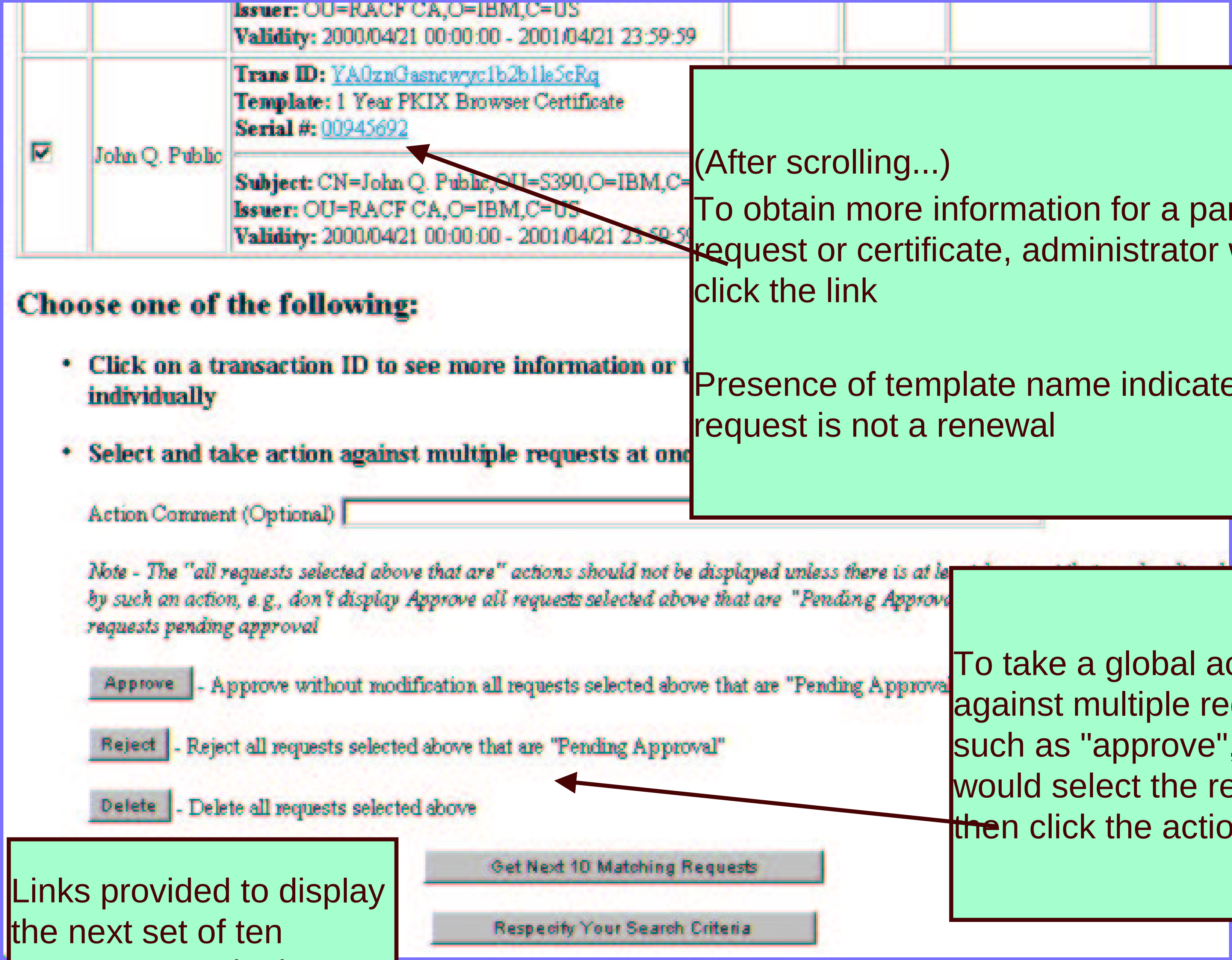
Querying requests would produce a list of requests with some summary data displayed for each. A maximum of ten requests would be displayed on one page. (scroll to see more...)

Presence of previous serial # indicates a renewal

Presence of serial # indicates certificate has been created.

These are hypertext links

Select button used to select multiple requests



		Issuer: OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/21 00:00:00 - 2001/04/21 23:59:59			
☑	John Q. Public	**Trans ID:** YA0znGasncwyc1b2b1le5cRq **Template:** 1 Year PKIX Browser Certificate **Serial #:** 00945692 **Subject:** CN=John Q. Public,OU=S390,O=IBM,C= **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/21 00:00:00 - 2001/04/21 23:59:59			

Choose one of the following:

- **Click on a transaction ID to see more information or t individually**
- **Select and take action against multiple requests at onc**

Action Comment (Optional)

Note - The "all requests selected above that are" actions should not be displayed unless there is at le by such an action, e.g., don't display Approve all requests selected above that are "Pending Approv requests pending approval

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

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

Delete - Delete all requests selected above

Get Next 10 Matching Requests

Respecify Your Search Criteria

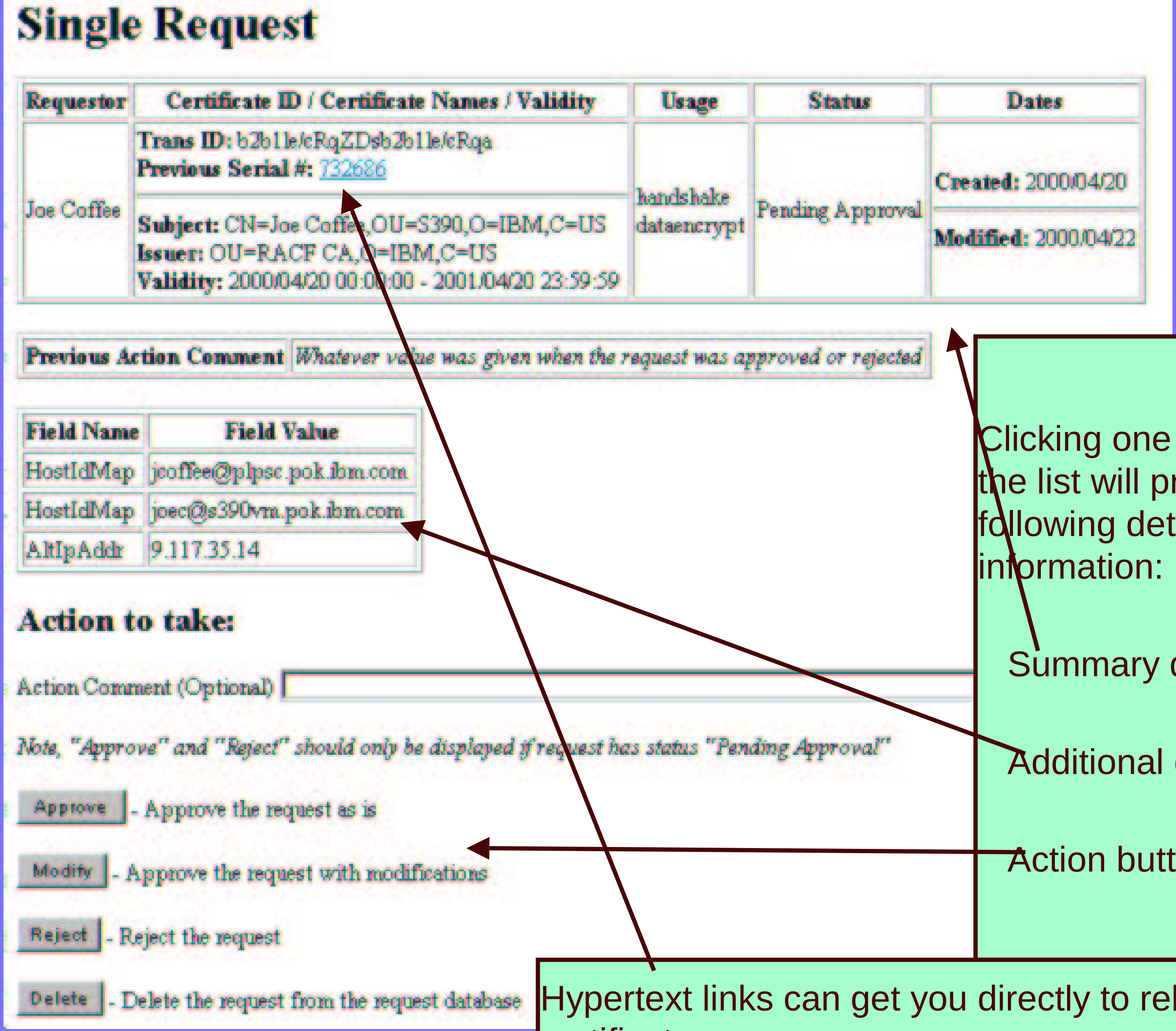
(After scrolling...)

To obtain more information for a particular request or certificate, administrator would click the link

Presence of template name indicates request is not a renewal

To take a global action against multiple requests such as "approve", user would select the requests then click the action

Links provided to display the next set of ten requests or redo the search



Single Request

Requestor	Certificate ID / Certificate Names / Validity	Usage	Status	Dates
Joe Coffee	**Trans ID:** b2b1le/cRqZDsb2b1le/cRqa **Previous Serial #:** 732686 **Subject:** CN=Joe Coffee,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/20 00:00:00 - 2001/04/20 23:59:59	handshake dataencrypt	Pending Approval	**Created:** 2000/04/20 **Modified:** 2000/04/22

Previous Action Comment	*Whatever value was given when the request was approved or rejected*

Field Name	Field Value
HostIdMap	jcoffee@plpsc.pok.ibm.com
HostIdMap	joec@s390vm.pok.ibm.com
AltIpAddr	9.117.35.14

Action to take:

Action Comment (Optional)

Note, "Approve" and "Reject" should only be displayed if request has status "Pending Approval"

Approve - Approve the request as is

Modify - Approve the request with modifications

Reject - Reject the request

Delete - Delete the request from the request database

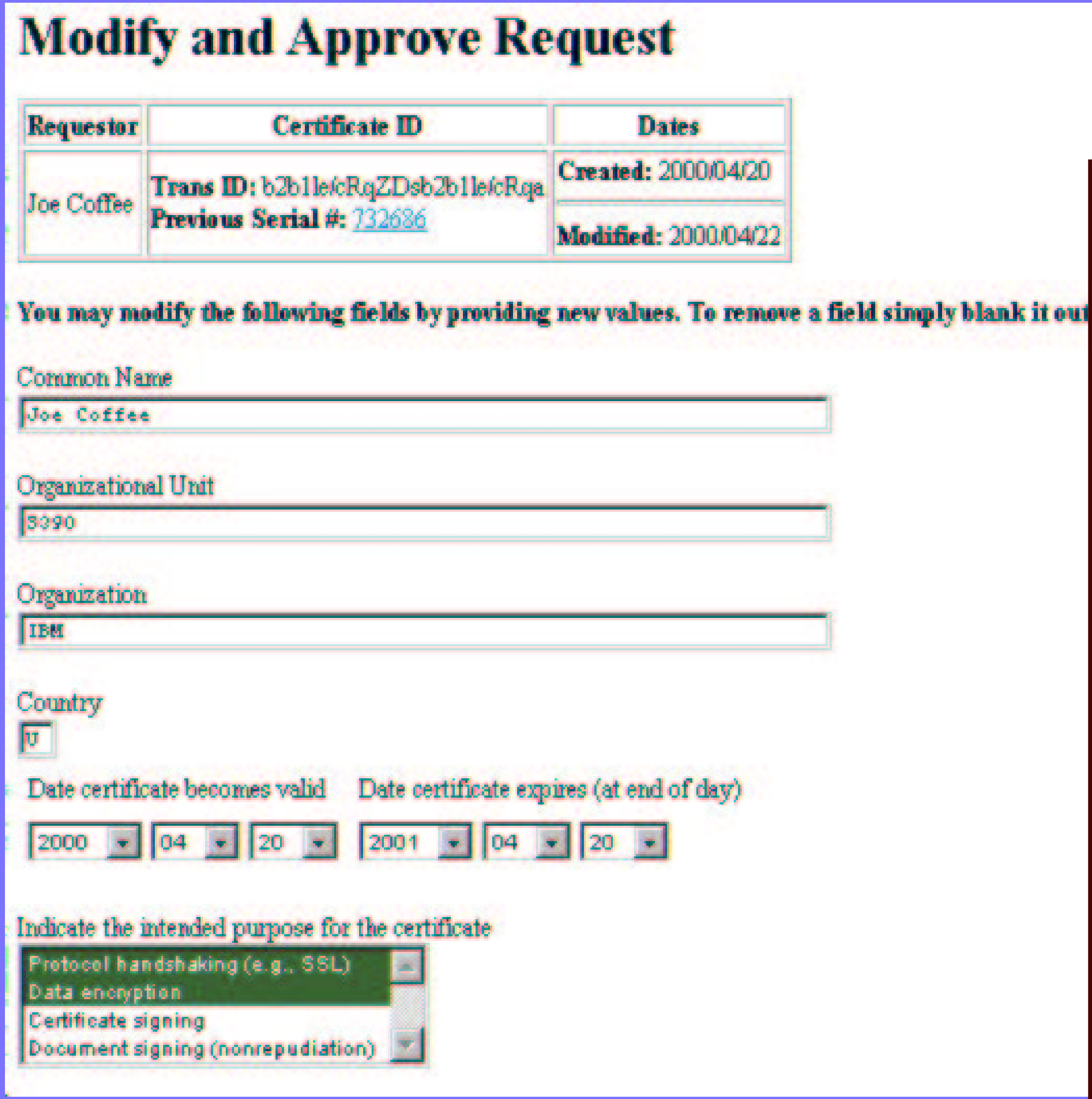
Clicking one request from the list will produce the following detailed information:

Summary data

Additional data

Action buttons

Hypertext links can get you directly to related certificates



Modify and Approve Request

Requestor	Certificate ID	Dates
Joe Coffee	**Trans ID:** b2b1le/cRqZDsb2b1le/cRqa **Previous Serial #:** 732686	**Created:** 2000/04/20 **Modified:** 2000/04/22

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

Common Name	Joe Coffee
Organizational Unit	3390
Organization	IBM
Country	U
Date certificate becomes valid	2000 ▾ 04 ▾ 20 ▾
Date certificate expires (at end of day)	2001 ▾ 04 ▾ 20 ▾

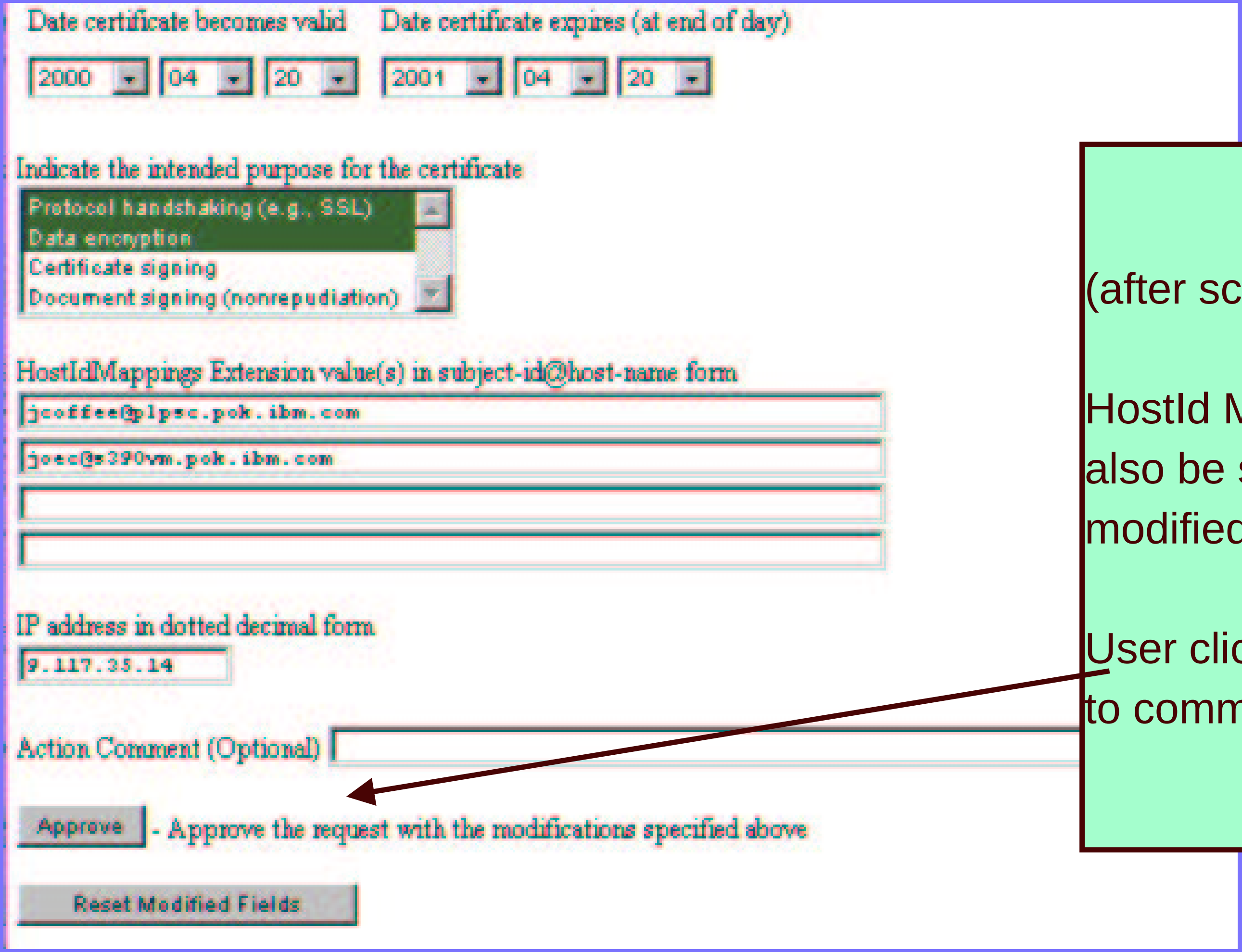
Indicate the intended purpose for the certificate

- Protocol handshaking (e.g., SSL)
- Data encryption
- Certificate signing
- Document signing (nonrepudiation)

The modify action allows "Pending Approval" requests to be approved with modifications. HTML controls for each admin modifiable field will be presented with current values if any.

List of modifiable fields
is customizable in certificate templates
file

(scroll to see more...)



Date certificate becomes valid: 2000 04 20

Date certificate expires (at end of day): 2001 04 20

Indicate the intended purpose for the certificate

- Protocol handshaking (e.g., SSL)
- Data encryption
- Certificate signing
- Document signing (nonrepudiation)

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

jcoffee@plpsc.pok.ibm.com

joec@s390vm.pok.ibm.com

IP address in dotted decimal form

9.117.35.14

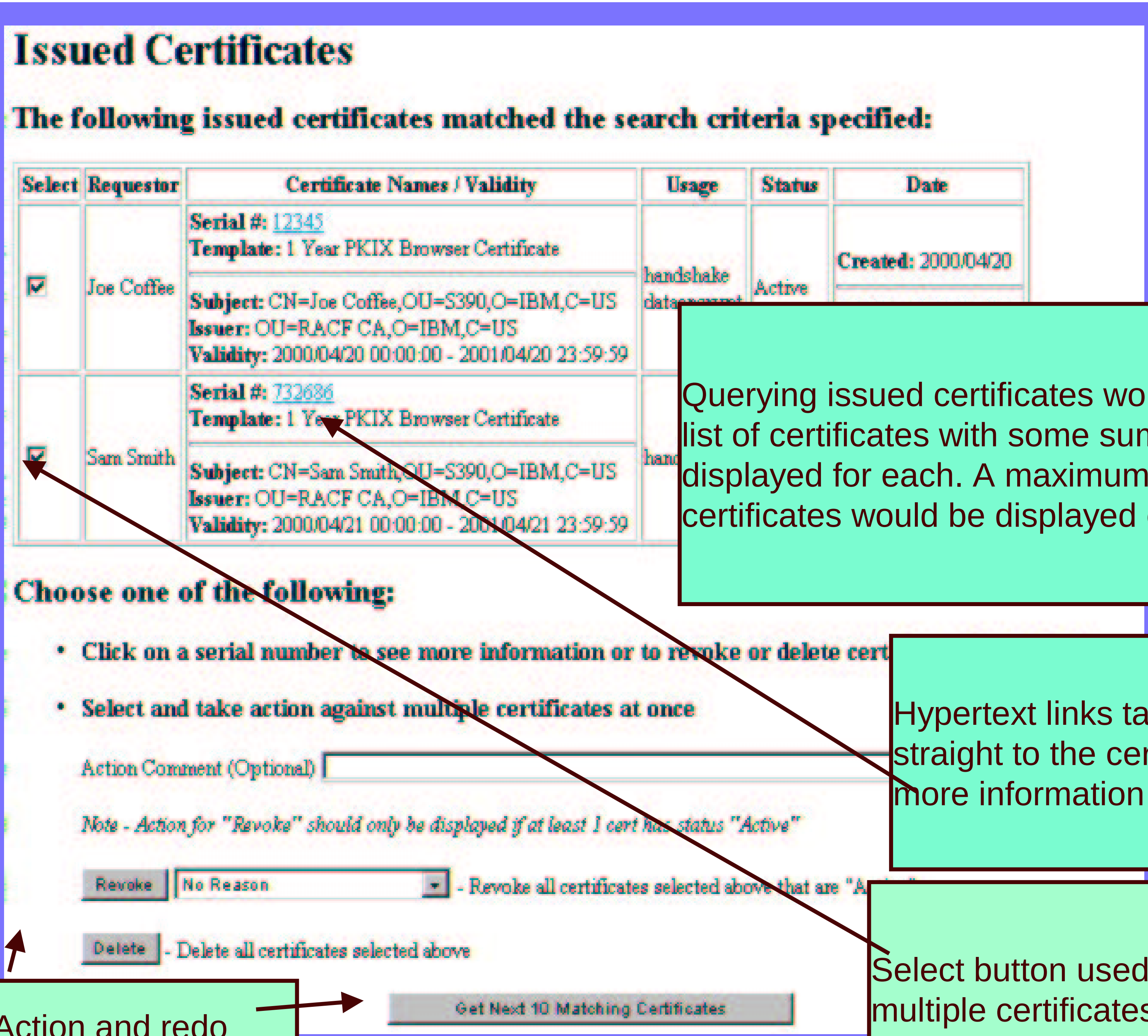
Action Comment (Optional)

Approve - Approve the request with the modifications specified above

(after scrolling...)

HostId Mappings can also be specified or modified

User clicks on "Approve" to commit changes



Issued Certificates

The following issued certificates matched the search criteria specified:

Select	Requestor	Certificate Names / Validity	Usage	Status	Date
☑	Joe Coffee	**Serial #:** 12345 **Template:** 1 Year PKIX Browser Certificate **Subject:** CN=Joe Coffee,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/20 00:00:00 - 2001/04/20 23:59:59	handshake dataencrypt	Active	**Created:** 2000/04/20
☑	Sam Smith	**Serial #:** 732686 **Template:** 1 Year PKIX Browser Certificate **Subject:** CN=Sam Smith,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/21 00:00:00 - 2001/04/21 23:59:59	hand		

Choose one of the following:

- **Click on a serial number to see more information or to revoke or delete cert**
- **Select and take action against multiple certificates at once**

Action Comment (Optional)

Note - Action for "Revoke" should only be displayed if at least 1 cert has status "Active"

- Revoke all certificates selected above that are "A

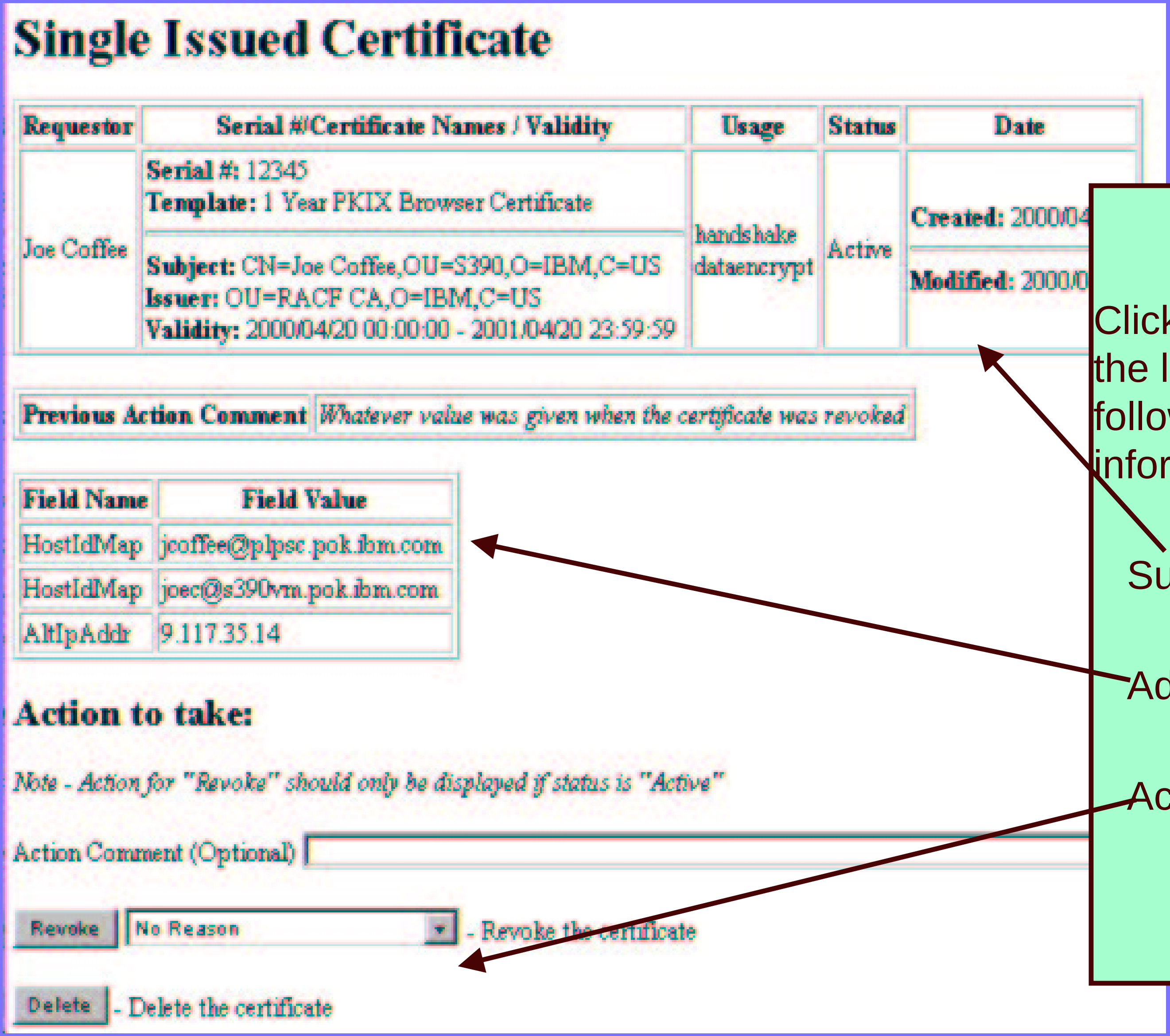
- Delete all certificates selected above

Querying issued certificates would produce a list of certificates with some summary data displayed for each. A maximum of ten certificates would be displayed on one page.

Hypertext links take you straight to the certificate where more information is displayed

Select button used to select multiple certificates

Action and redo buttons



Single Issued Certificate

Requestor	Serial #/Certificate Names / Validity	Usage	Status	Date
Joe Coffee	**Serial #:** 12345 **Template:** 1 Year PKIX Browser Certificate **Subject:** CN=Joe Coffee,OU=S390,O=IBM,C=US **Issuer:** OU=RACF CA,O=IBM,C=US **Validity:** 2000/04/20 00:00:00 - 2001/04/20 23:59:59	handshake dataencrypt	Active	**Created:** 2000/04 **Modified:** 2000/0

Previous Action Comment	*Whatever value was given when the certificate was revoked*

Field Name	Field Value
HostIdMap	jcoffee@plpsc.pok.ibm.com
HostIdMap	joec@s390vm.pok.ibm.com
AltIpAddr	9.117.35.14

Action to take:

Note - Action for "Revoke" should only be displayed if status is "Active"

Action Comment (Optional)

- Revoke the certificate

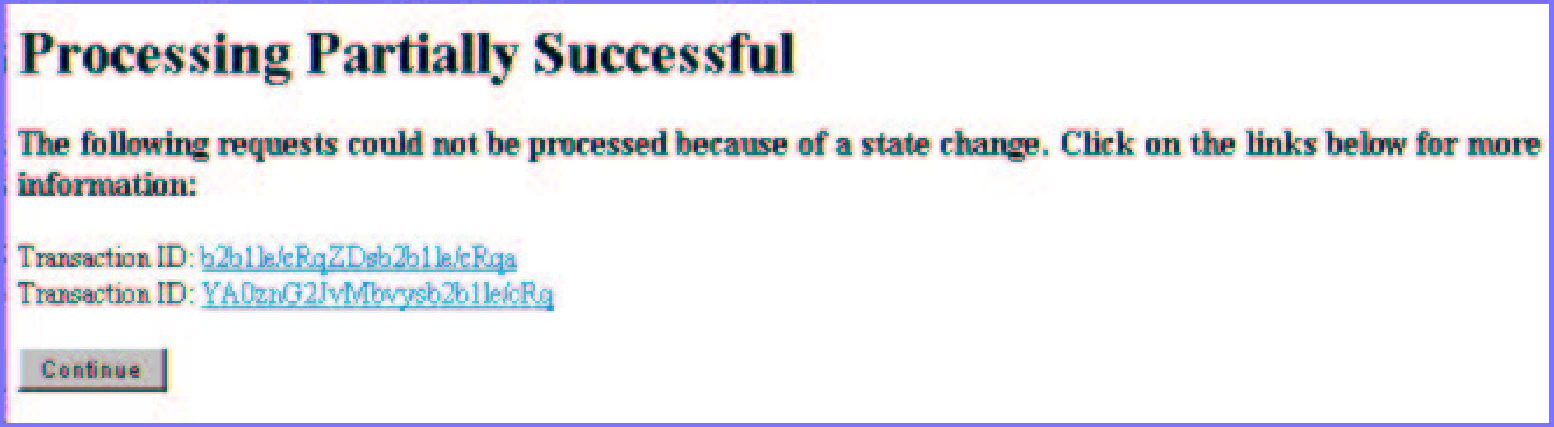
- Delete the certificate

Clicking one certificate from the list will produce the following detailed information:

Summary data

Additional data

Action buttons



Processing Partially Successful

The following requests could not be processed because of a state change. Click on the links below for more information:

Transaction ID: b2b1le/cRqZDsb2b1le/cRqa
Transaction ID: YA0znG2JvMbvysb2b1le/cRq

Here's a sample of what an error page may look like. In this case the user attempted to approve multiple requests but two were approved by someone else prior to the user pressing the "Approve" button

The hypertext links allow the user to investigate what happened

Prerequisite Products

- The following products must be installed prior to configuring PKI Services
  - IBM z/OS HTTP Server
    - get working in at least non-SSL mode
  - LDAP Directory
    - z/OS recommended - TDBM back-end required
    - Requires PKIX schema
  - Open Cryptographic Services OCSF and OCEP
    - run install and verify scripts
  - ICSF (optional)
  - RACF (or equivalent)

PKI Services Post-Install

- Post-install script to create directories
  - Must be copied from samples directory
- **RACF Setup REXX Exec - SYS1.SAMPLIB(IKYSETUP)**
  - Customizable exec to create the RACF environment needed for PKI Services
- IBM HTTP Server Setup
- LDAP Setup
- Create VSAM data sets - For ObjectStore and ICL
- PKI Services configuration file
- Web Page Customization
- Customer Modifications

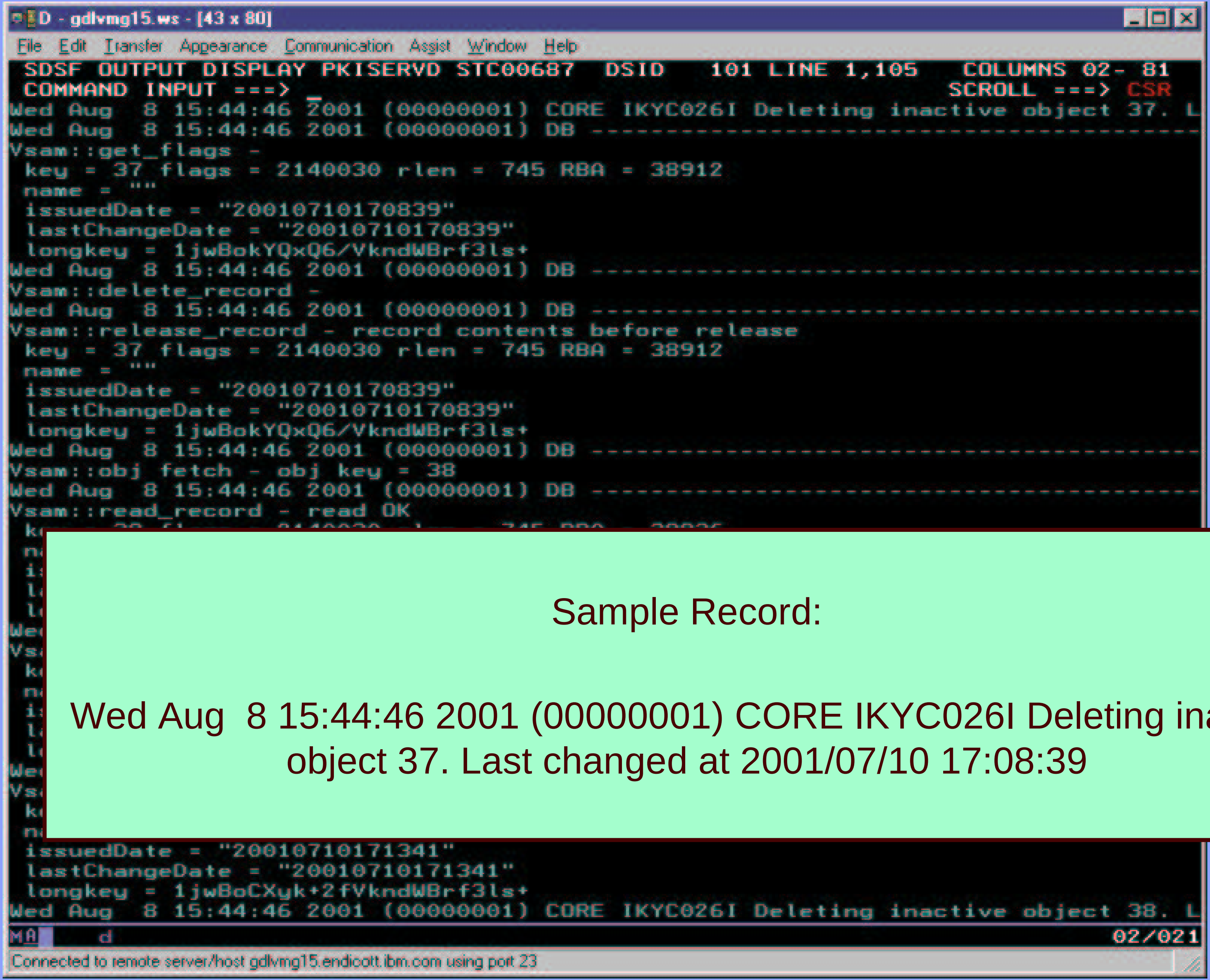
Additional Customization PKI Exit

- Customer code - sample /usr/lpp/pkiserv/samples/pkiexit.c
  - UNIX executable - Receives parms through argc, argv[]
- Surrounds the CGI calls to R_PKIServ
  - User functions only
  - Called before (pre) and after (post) the R_PKIServ call
- Used for advanced customization
  - When HTML alone isn't enough, e.g.,
    - Additional authorization checks
    - Runtime modification of request parameters
    - Capture requests/certificates to alternate DBs
    - Additional business processes

Running PKI Services

- PROC to Start The PKI Services Daemon
  - Must be started through a started procedure
  - SYS1.PROCLIB member IKYSPROC (alias PKISERVD)
  - Modify as needed - e.g., customized envars file
- Start from MVS console "S PKISERVD"
  - The LDAP server and the two webservers need to be started as well.
- Stop from the MVS console "P PKISERVD"
- Change logging options from the MVS console
  - F PKISERVD,LOG sub-comp.level[,sub-comp.level...]

Viewing the logs...



```
 SDSF OUTPUT DISPLAY PKISERVD STC00687  DSID   101 LINE 1,105    COLUMNS 02- 81
 COMMAND INPUT ===> _                                           SCROLL ===> CSR
Wed Aug  8 15:44:46 2001 (00000001) CORE IKYC026I Deleting inactive object 37. L
Wed Aug  8 15:44:46 2001 (00000001) DB ------------------------------------------
Vsam::get_flags -
 key = 37 flags = 2140030 rlen = 745 RBA = 38912
 name = ""
 issuedDate = "20010710170839"
 lastChangeDate = "20010710170839"
 longkey = 1jwBokYQxQ6/VkndWBrf3ls+
Wed Aug  8 15:44:46 2001 (00000001) DB ------------------------------------------
Vsam::delete_record -
Wed Aug  8 15:44:46 2001 (00000001) DB ------------------------------------------
Vsam::release_record - record contents before release
 key = 37 flags = 2140030 rlen = 745 RBA = 38912
 name = ""
 issuedDate = "20010710170839"
 lastChangeDate = "20010710170839"
 longkey = 1jwBokYQxQ6/VkndWBrf3ls+
Wed Aug  8 15:44:46 2001 (00000001) DB ------------------------------------------
Vsam::obj fetch - obj key = 38
Wed Aug  8 15:44:46 2001 (00000001) DB ------------------------------------------
Vsam::read_record - read OK
 k
 n
 i
 l
 l
We
Vs
 k
 n
 i
 l
 l
We
Vs
 k
 n
 issuedDate = "20010710171341"
 lastChangeDate = "20010710171341"
 longkey = 1jwBoCXyk+2fVkndWBrf3ls+
Wed Aug  8 15:44:46 2001 (00000001) CORE IKYC026I Deleting inactive object 38. L
MA     d                                                                  02/021
```

Connected to remote server/host gdlvmg15.endicott.ibm.com using port 23

Sample Record:

Wed Aug 8 15:44:46 2001 (00000001) CORE IKYC026I Deleting inactive object 37. Last changed at 2001/07/10 17:08:39

Presenting ....

<u>z/OS RELEASE 4</u>

Remove Clear text LDAP password

- Previously passwords stored in clear text in the PKI Services configuration file
- Now encrypting and storing passwords in the PROXY segment of a general resource profile
- LDAP.BINDPW.KEY profile in KEYSMSTR class.
    - When active, RACF will store the key encrypted.
- Choice:
    - IRR.PROXY.DEFAULTS profile in the FACILITY class
    - yourown.LDAP.Server1 profile in LDAPBIND class
    - yourown.LDAP.Servern profile in LDAPBIND class

Remove Clear text LDAP password

- Changes in the PKI Services configuration file to get new function
  - absence of Server*n*,AuthName*n*,AuthPwd*n*
- To use LDAPBIND class for each directory
  - BindProfile*n*
- To use IRR.PROXY.DEFAULTS profile
  - BindProfile*n* keyword missing

EMAIL NOTIFICATION

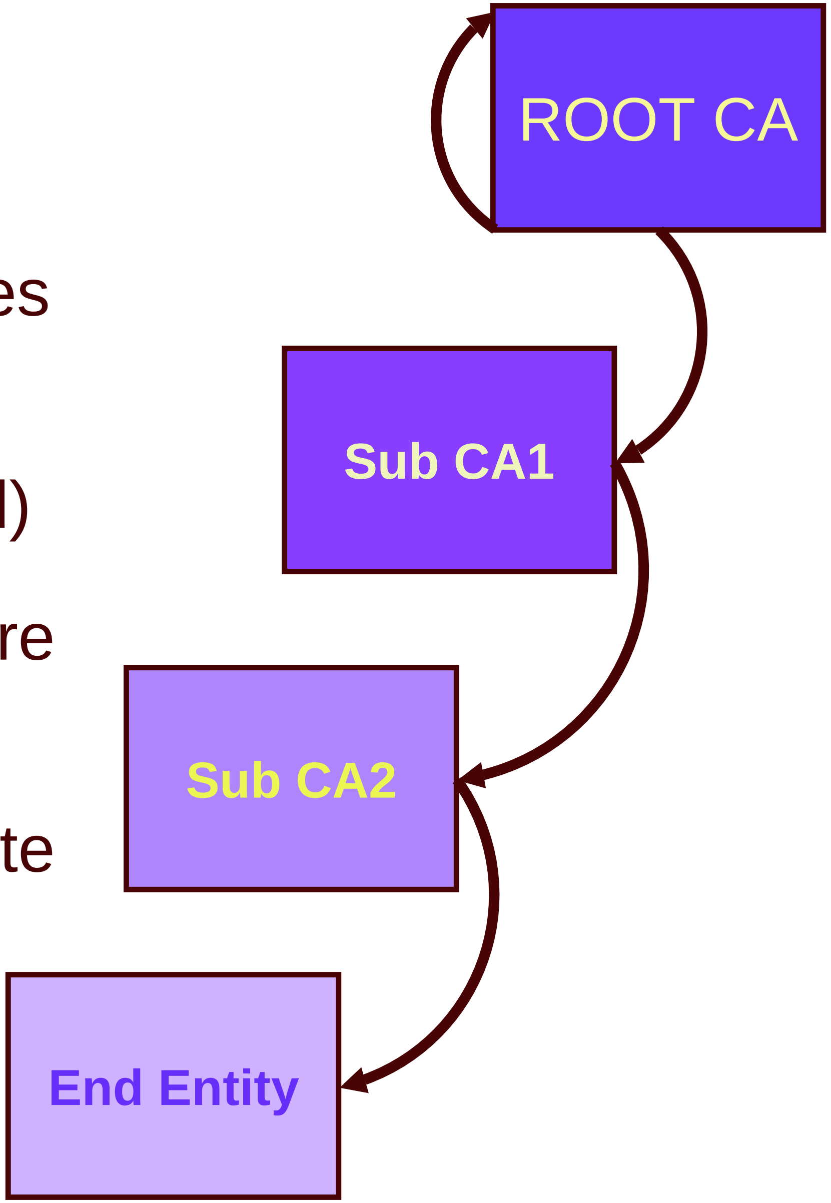
- email notification for completed certificate request and expiration warnings
  - ►NotifyEmail - non repeatable, used to specify the internet email address.
  - ►Standard form i.e. janedoe@us.ibm.com

EMAIL NOTIFICATION

- ExpireWarningTime will be added to the CertPolicy section of the config file
  - scans ICL daily
  - sends one notification message
- General section config file updates include:
  - ReadyMessageForm - 'certificate is ready'
  - RejectMessageForm - 'request rejected'
  - ExpiringMessageForm - 'certificate about to expire'

Support PKCS#7 Certificate Chains

- Support PKCS#7 Certificate Chains (Package)
- Parent authorities sign the certificates of subordinates
- Top Authority is the root (self-signed)
- RACDCERT ADD will now read entire chain
- RACDCERT EXPORT will now create entire chain
- R_PKIServ support on exporting certificate



Additional Enhancements ....

Crypto 4758 PCI Card

- ►Key created by Crypto and stored in PKDS
- ►Use with RACDCERT command
  - –New keyword - PCICC

SYSPLEX Enablement

- ►VSAM RLS
  - –New keyword in Object Store section of the config file (T/F)

Additional Enhancements ....

- Support new distinquished name qualifiers
  - MAIL
  - STREET
  - POSTALCODE
- Updated default CERTAUTH certificates in RACF

Presenting ....

z/OS RELEASE 5

Z/OS Release 5 Support

- Multiple Application Domains
  - Ability to separate ADMIN functions from end-user functions
  - Ability to subset end-user functions
  - Changes in:
    - Template File
    - End-user related CGIs
    - HTTP Server configuration file

Z/OS R5 Support Continued…

- Certificate Suspension
  - Certificates may be suspended for a period of time.
  - Suspended certificates appear on the next CRL with a reason code of certificateHold
  - New certificate status of ‘SUSPENDED’
  - MaxSuspendDuration
    - New CertPolicy keyword to indicate length of the suspended grace period in days or weeks

Z/OS R5 Support Continued…..

- CRLDistributionPoints
  - CertPolicy section of the configuration file
    - CRLDistSize – numeric value indicating the maximum number of certificates to be managed by a single DP
    - CRLDistName – the constant portion of the DP name. Each individual DP will be formed by appending the DP number. Default value is ‘CRL’
    - Example: CRLDistSize=100, certificate 99: CRL1; certificate 101: CRL2; certificate 230: CRL3…..
    - CN=CRL3.CN=BANKXYZ.OU=BANK FINANCE.O=NYBANK.C=US

Z/OS R5 Support Continued….

- Granularity for KEYUSAGE
  - digitalsignature
  - nonrepudiation
  - keyencipherment
  - dataencipherment
  - keyagreement
  - keycertsign
  - crlsign

Z/OS R5 Support Continued….

- ExtKeyUsage extension
  - serverauth
  - clientauth
  - codesigning
  - emailprotection
  - timestamping
  - ocspsigning
- CertificatePolicies extension
- AuthorityInfoAccess extension

Z/OS R5 Support Continued…

- Marking extensions Critical
  - Always critical
    - BasicConstriants
    - KeyUsage
  - Can now be marked
    - ExtKeyUsage
    - SubjectAltName
    - HostIDMappings
    - CertificatePolicies

Z/OS R5 Continued…..
Performance Enhancements

- VSAM Alternate Indexes
  - Status Index – non unique index containing the status, variable data length and requestor fields of the VSAM record.
  - Requestor Index – non unique index that will be used to improve the performance of queries when the Requester is supplied as additional search criteria
- Other Performance Enhancements
  - Buffer space for the VSAM data sets as part of the IKYSPROC started procedure
  - System SSL services

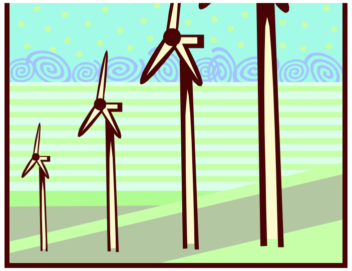
Z/OS R5 Support Continued….

- ICL Cleanup
  - RemoveExpiredCerts=days or weeks
- Miscellaneous Sample Updates (SYS1.SAMPLIB)
  - IKYSETUP is updated to support PCICC for generation of the PKI Services CA private key.
  - IKYCVSAM and IKYRVSAM are being updated for the new alternate indexes.
  - IKYMVSAM is new and contains the sample JCL to create the new VSAM alternate indexes and PATH data sets.

Z/OS R5 Support Continued…..

- Hints and Tips for Large number of certificates
  - Use CRL Distribution Points
  - Use PKI exit
    - to automate approval process
    - To avoid name collisions, enforce meaningful SDN
    - To avoid timeouts on queries, provide meaningful requestor data
  - Keep the request and ICL database small by removing records

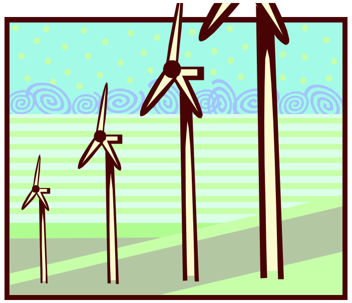
Utilities



- vosview - displays the records contained in the Request DB (ObjectStore)
  - ►Sample record:

```
--------------------------------------------------------------------------
Object key = 105
name = "John Q. Public"
longkey = 1F45AEF2D3729FA35156BC47
appldata = "PKIB1YR "
comment = ""
data len = 570
flags = 1020111 - Type = Cert        State = RA CertReqActive  [State Flag]
```

Utilities...



- iclview - displays the records contained in the Issued Certificate List (ICL)
  - Sample record:

```
--------------------------------------------------------------------------------
Cert 10: John Q. Public
    ISSUED (Issued certificate)
    Issued at 2000-10-25 14:07:05
    Last changed 2000-10-25 14:07:05
    Subject: CN=John Q. Public,OU=Tools Dept,O=IBM,C=US
    Issuer: CN=pkica,OU=zOS Security Server,O=IBM,C=US
    Requestor: John Q. Public
    Appldata: "PKIB1YR "
    Serial Number: 0A
```

SUMMARY

- Introduction
  - Certificate Life Cycle
  - Architecture
- PKI Services on OS/390 Release 10
- PKI Services on z/OS Release 3
  - Using PKI Services Web Interface
  - Post Installation Steps/Customization
  - Running PKI Services
- Updates to PKI Services on z/OS Release 4
- Updates to PKI Services on z/OS Release 5
- Utilities

References

- RACF web site: http://www.s390.ibm.com/racf/
  - PKI Services web site TBD. Will have link from RACF page
- Security Server Manuals:
  - **PKI Services Guide and Reference (SA22-7693)**
  - 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)
  - OCEP Application Programming (SC24-5925)
- Cryptographic Services
  - OCSF Service Provider Developer's Guide and Reference (SC24-5900)
  - ICSF Administrator's Guide (SA22-7521)
- IBM HTTP Server Manuals:
  - Planning, Installing, and Using (SC31-8690)
- Other Sources:
  - PKIX - http://www.ietf.org/html.charters/pkix-charter.html

DISCLAIMER

The information contained in this document is distributed on an "as is" basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that customers using the information or techniques will obtain the same or similar results in their own operational environments.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed programs may be used. Functionally equivalent programs 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 environments.

It is possible that this material may contain reference 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.