# PKI on z/OS: A View of PKI in Action

## SHARE Baltimore, MD
## Session 1796 – Part 1
## August 17th 2006

Wai Choi
IBM Corporation
Poughkeepsie, NY

Phone: (845) 435-7623
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.

# Agenda

## Showing PKI Services in action

- Customization of PKI Services from
  - Configuration file – pkiserv.conf
  - Template file – pkiserv.tmpl
- Submit and approve a certificate request
- Revoke/Suspend certificate
- Check the certificate status using
  - Certificate Revocation List (CRL)
  - Online Certificate Status Protocol (OCSP)
- How the other applications utilize the certificates from PKI Services - Part 2

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

- **Configuration is done through 2 files – pkiserv.conf, pkiserv.tmpl**

# pkiserv.conf

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

# pkiserv.tmpl

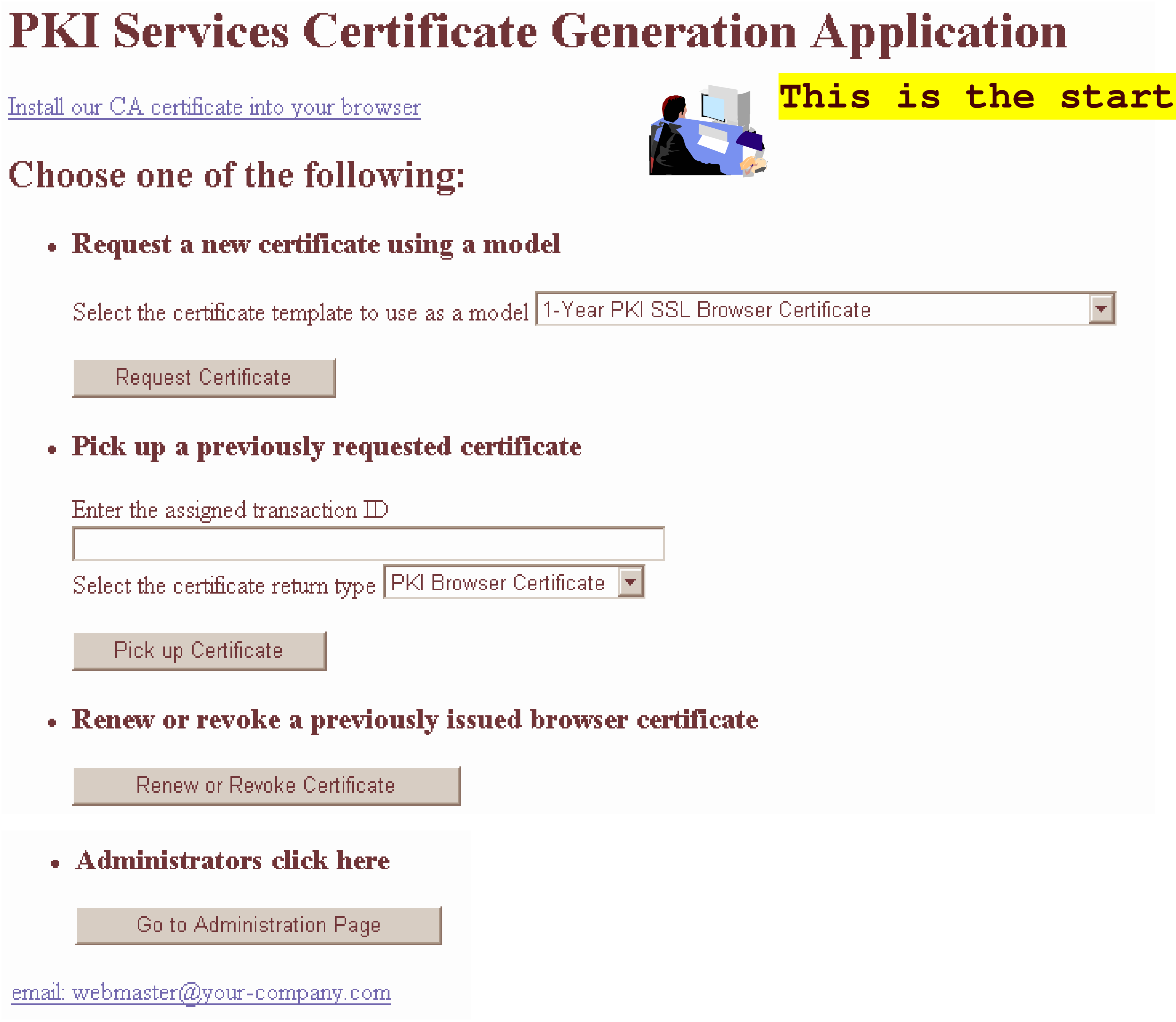
```
<TEMPLATE NAME=1-Year PKI SSL Browser Certificate>
<CONTENT>
%%Requestor (optional)%%
%%Email (optional)%%
%%CommonName%%
%%NotifyEmail (optional)%%
%%PassPhrase%%
…
</CONTENT>
```

# pkiserv.tmpl

```
<CONSTANT>
 %%NotBefore=0%%
 %%NotAfter=365%%
 %%KeyUsage=handshake%%
 %%ExtKeyUsage=clientauth%%
 %%OrgUnit=Fake Internet Certificate Unit%%
 %%Org=The Fake Organization%%
 %%AuthInfoAcc=OCSP,URL=http://mvs1.centers.ihost:8041/PKIServ/publiccgi/caocsp%%
 …
</CONSTANT>
```

# Requesting a browser certificate from PKI Services

This is the start page



# 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

- **Pick up a previously requested certificate**

  Enter the assigned transaction ID

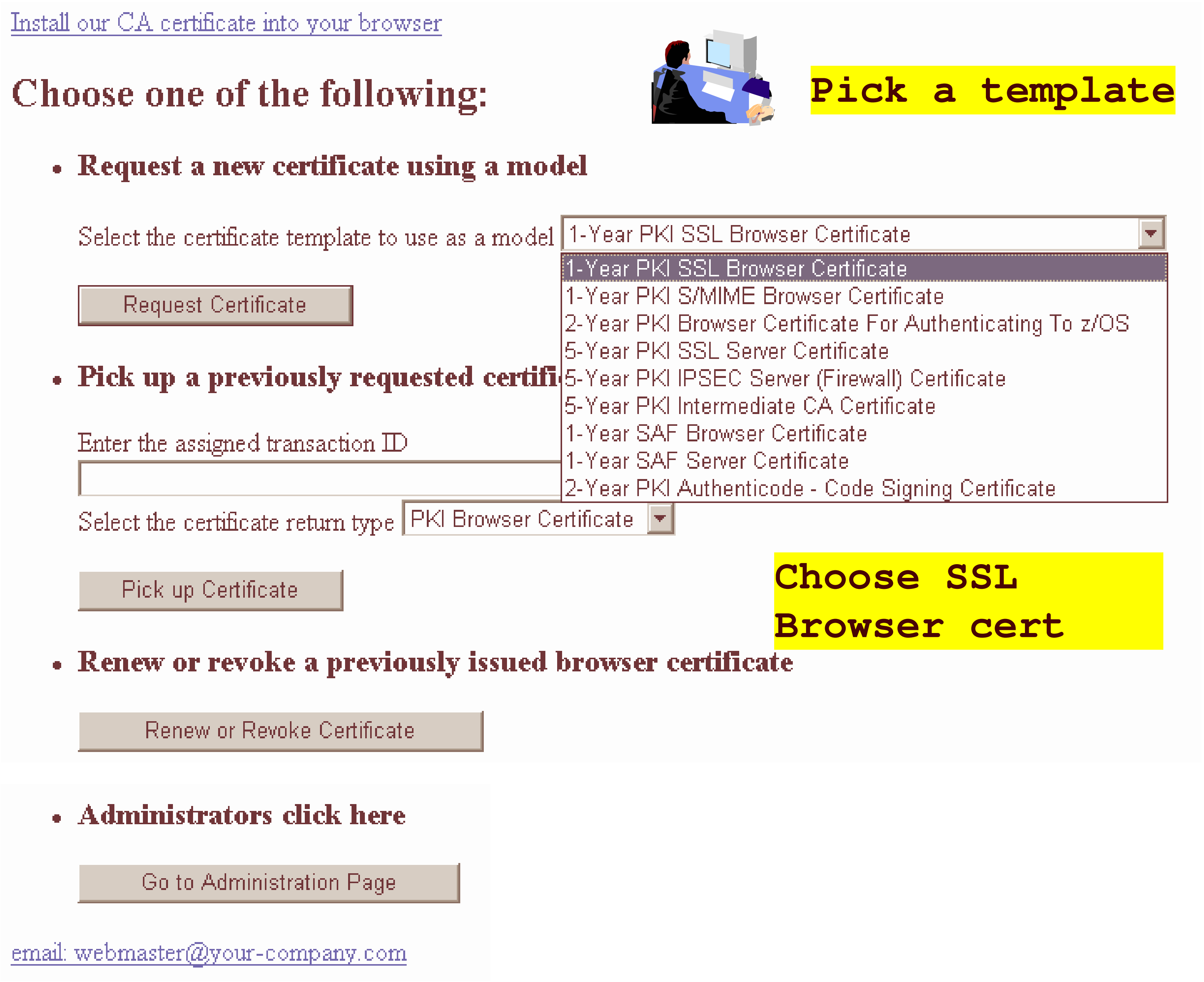
  Select the certificate return type: PKI Browser Certificate

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

- **Administrators click here**

email: webmaster@your-company.com

Click 'Open' then 'Install Certificate...'



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

- Pick up a previously requested certifi

Enter the assigned transaction ID

Select the certificate return type: PKI Browser Certificate

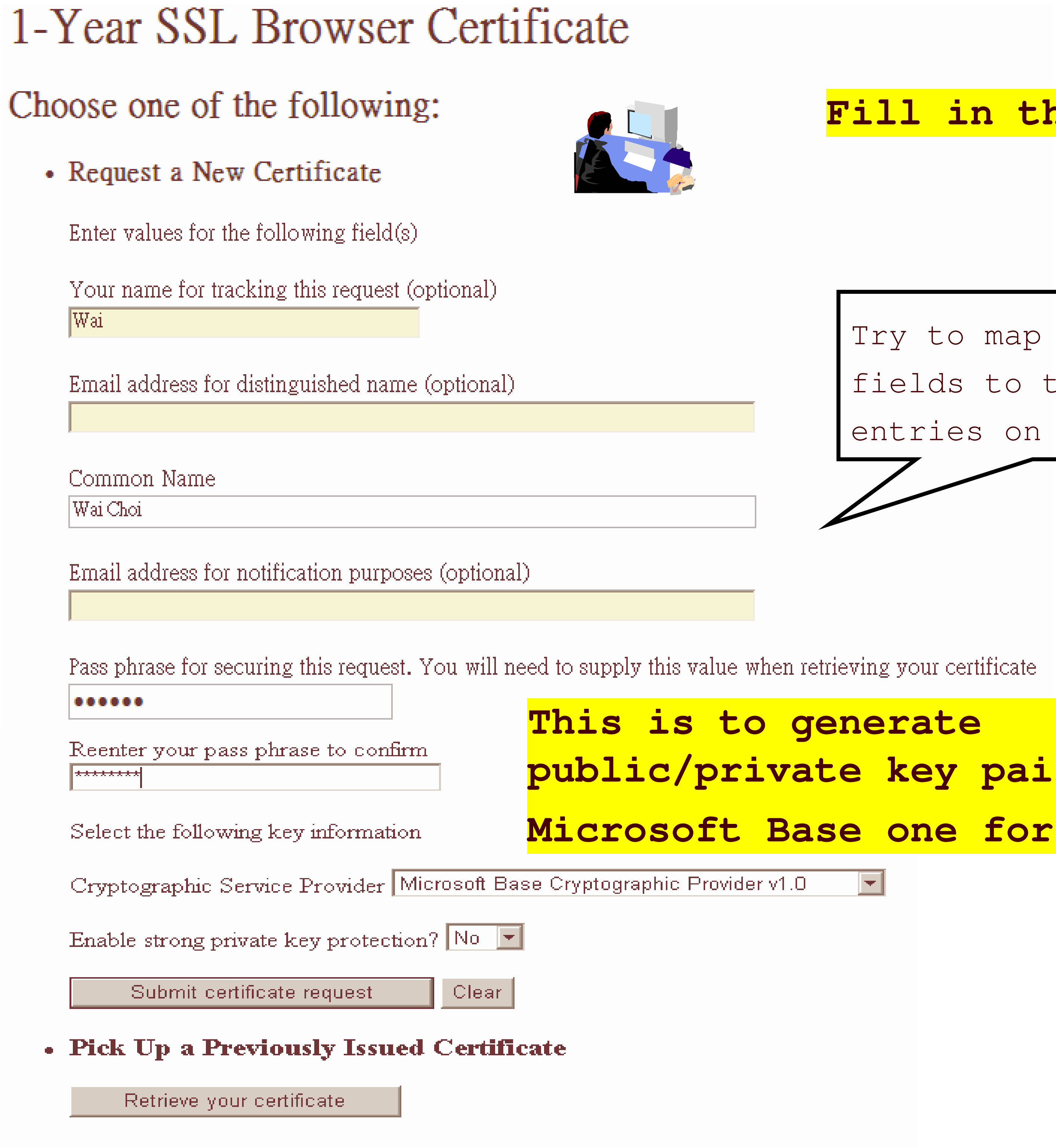
- Renew or revoke a previously issued browser certificate

- Administrators click here

email: webmaster@your-company.com

Pick a template

Choose SSL Browser cert



# 1-Year SSL Browser 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

Email address for distinguished name (optional)

Common Name
Wai Choi

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
*********

Select the following key information

Cryptographic Service Provider: Microsoft Base Cryptographic Provider v1.0

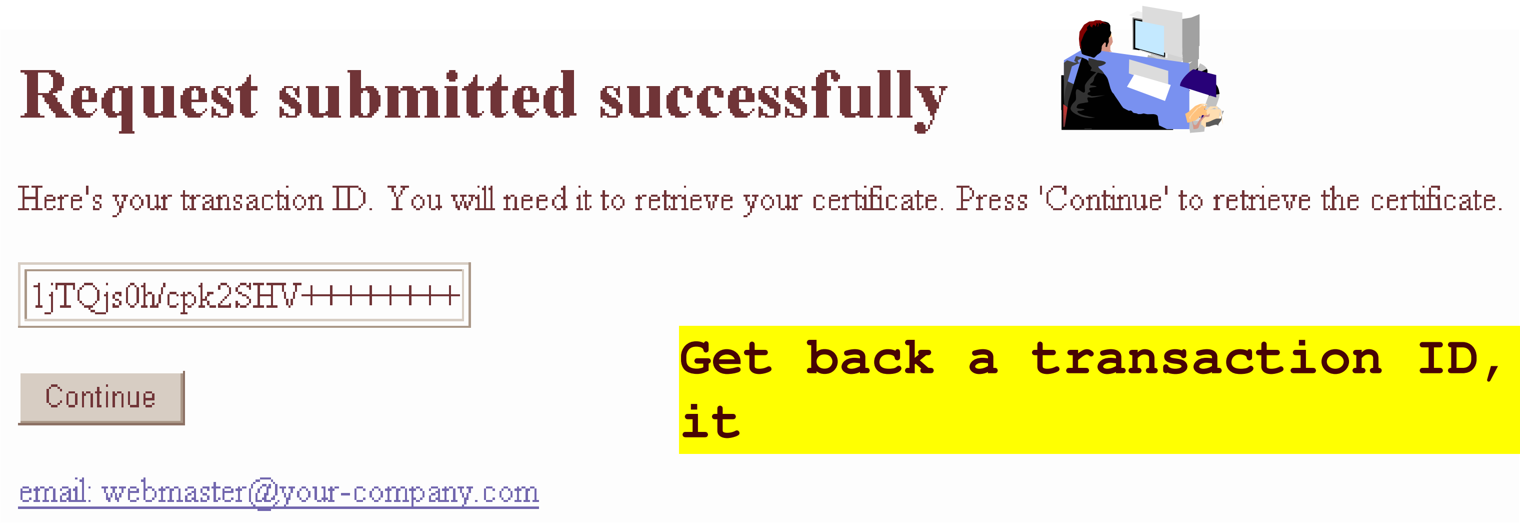
Enable strong private key protection? No

- **Pick Up a Previously Issued Certificate**

**Fill in the info**

Try to map these input fields to the <CONTENT> entries on slide 6

**This is to generate public/private key pair. Pick the Microsoft Base one for this demo.**



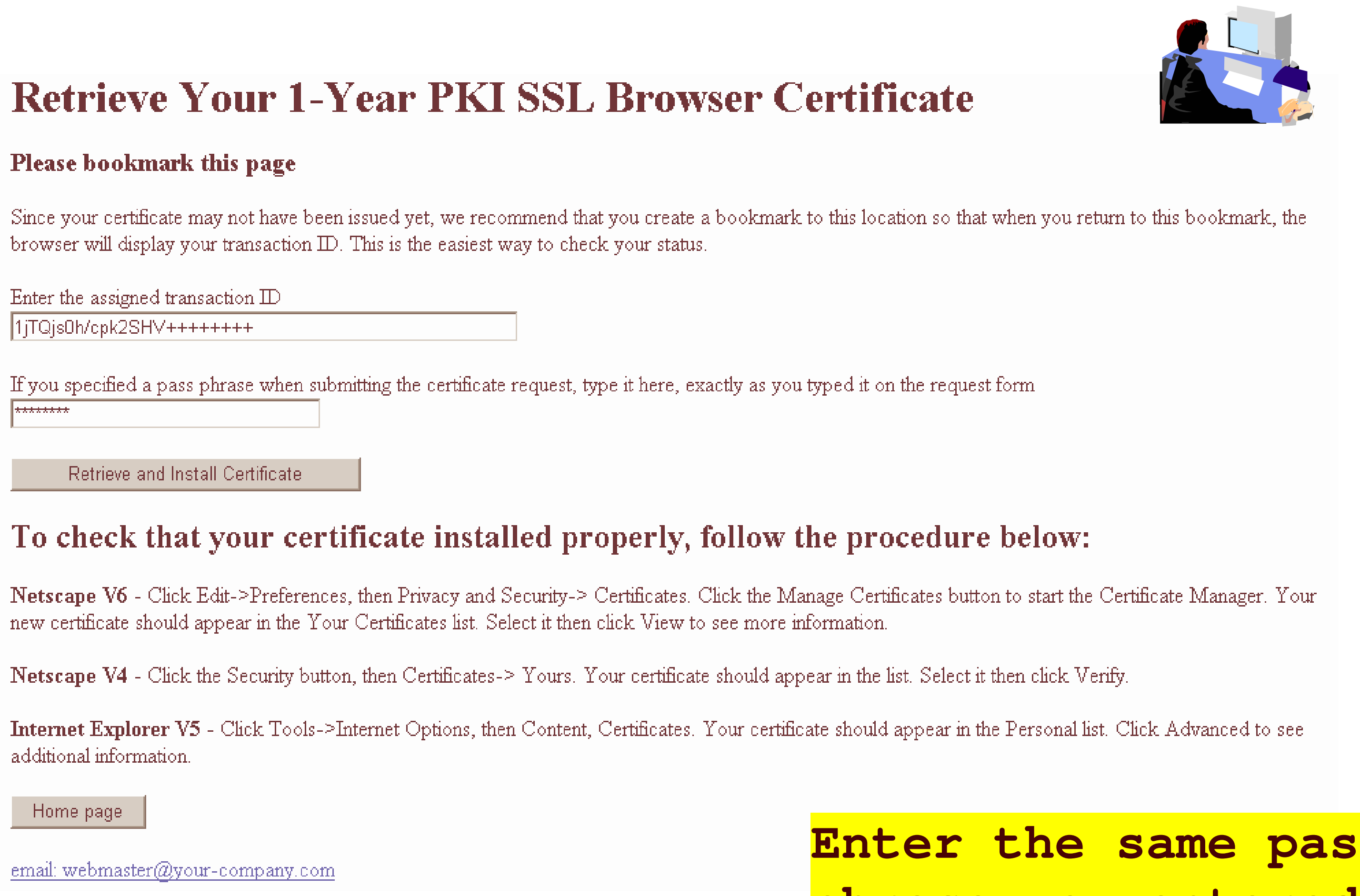
# Request submitted successfully

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

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

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

********

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

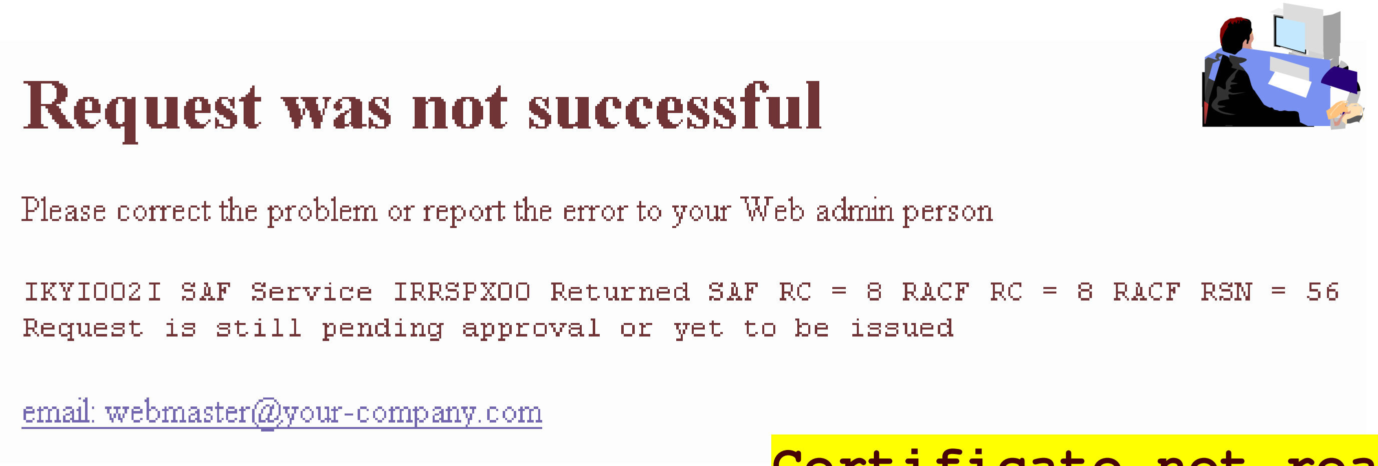
**Netscape V6** - Click Edit->Preferences, then Privacy and Security-> Certificates. Click the Manage Certificates button to start the Certificate Manager. Your new certificate should appear in the Your Certificates list. Select it then click View to see more information.

**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.

email: webmaster@your-company.com

**Enter the same pass phrase you entered before**



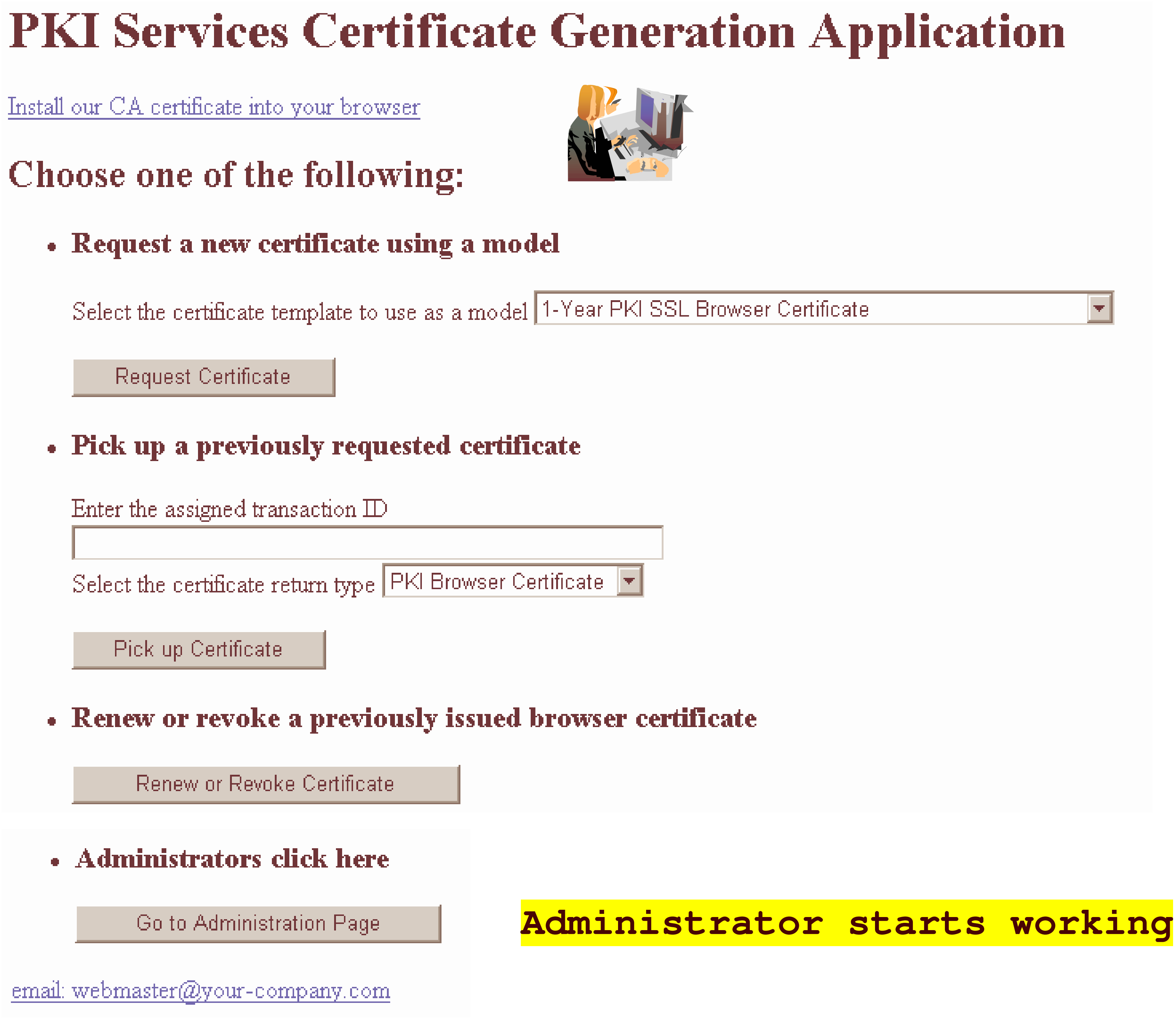
# Request was not successful

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**

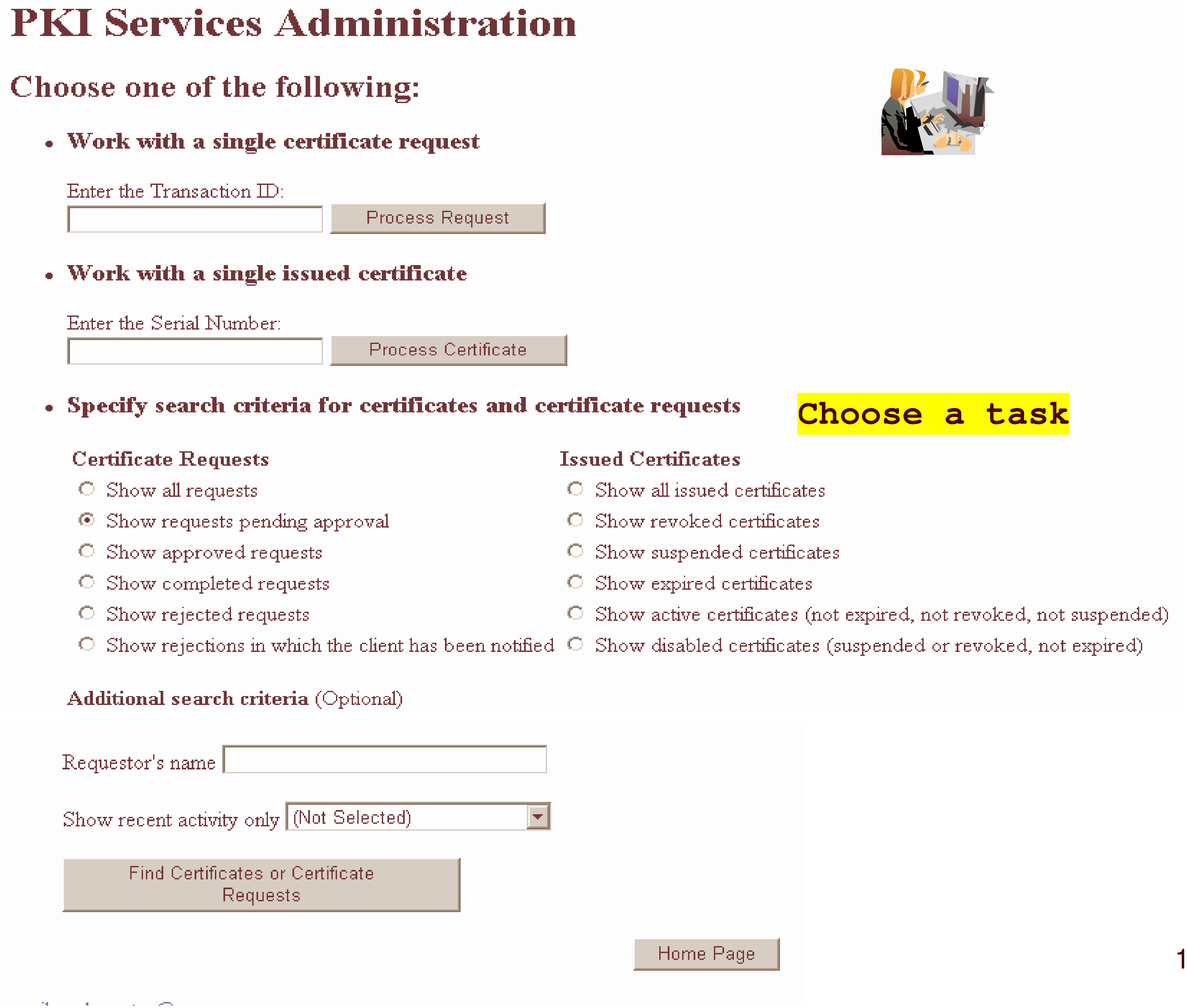
  Renew or Revoke Certificate

- **Administrators click here**

  Go to Administration Page

email: webmaster@your-company.com

**Administrator starts working**



# 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** | **Issued Certificates** |
|---|---|
| ○ Show all requests | ○ Show all issued certificates |
| ● Show requests pending approval | ○ Show revoked certificates |
| ○ Show approved requests | ○ Show suspended certificates |
| ○ Show completed requests | ○ Show expired certificates |
| ○ Show rejected requests | ○ Show active certificates (not expired, not revoked, not suspended) |
| ○ Show rejections in which the client has been notified | ○ Show disabled certificates (suspended or revoked, not expired) |

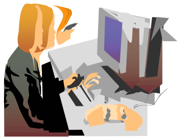
**Additional search criteria** (Optional)

Requestor's name

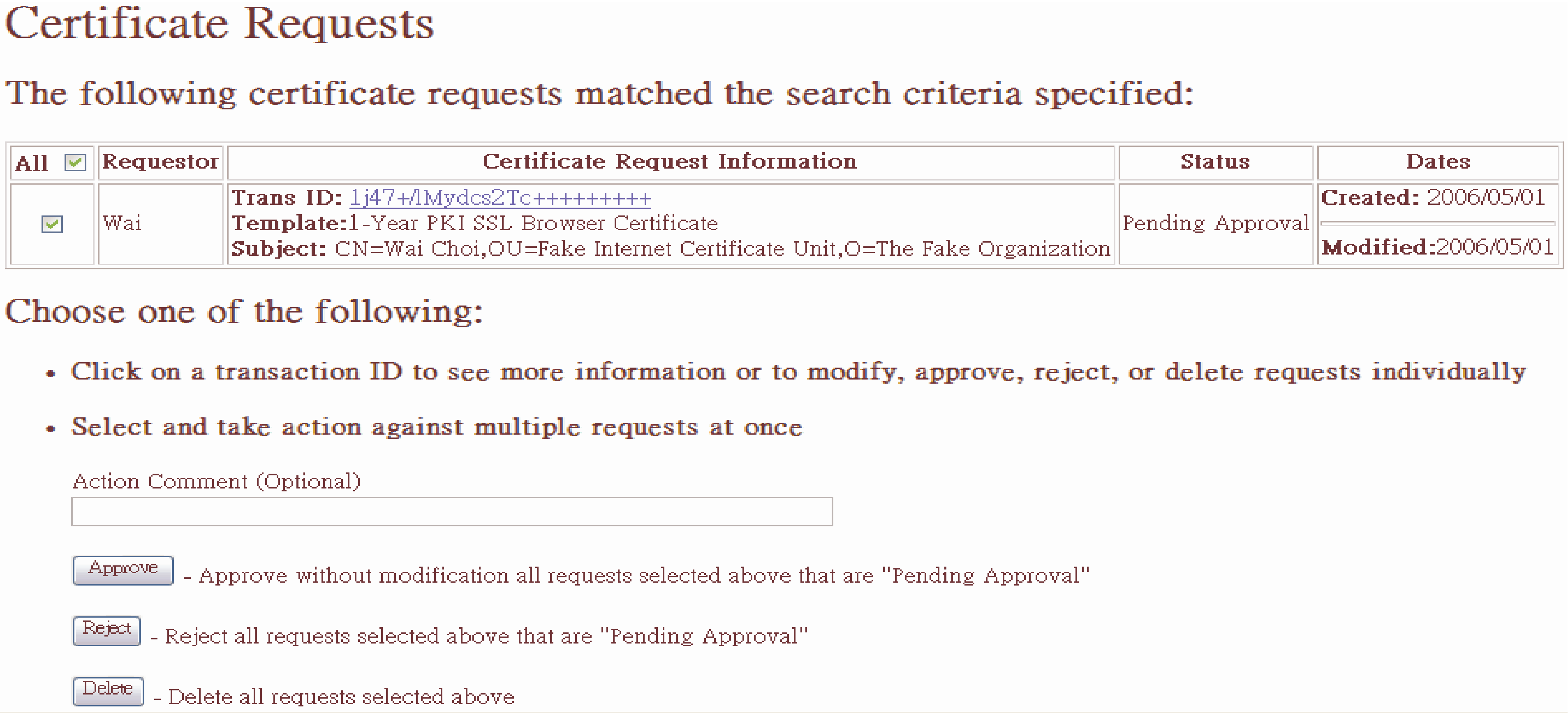
Show recent activity only (Not Selected)

Find Certificates or Certificate Requests

Home Page



## Request summary info



# Certificate Requests

The following certificate requests matched the search criteria specified:

| All ☑ | Requestor | Certificate Request Information | Status | Dates |
|---|---|---|---|---|
| ☑ | Wai | **Trans ID:** 1j47+/1Mydcs2Tc++++++++++<br>**Template:**1-Year PKI SSL Browser Certificate<br>**Subject:** CN=Wai Choi,OU=Fake Internet Certificate Unit,O=The Fake Organization | Pending Approval | **Created:** 2006/05/01<br>**Modified:**2006/05/01 |

## Choose one of the following:

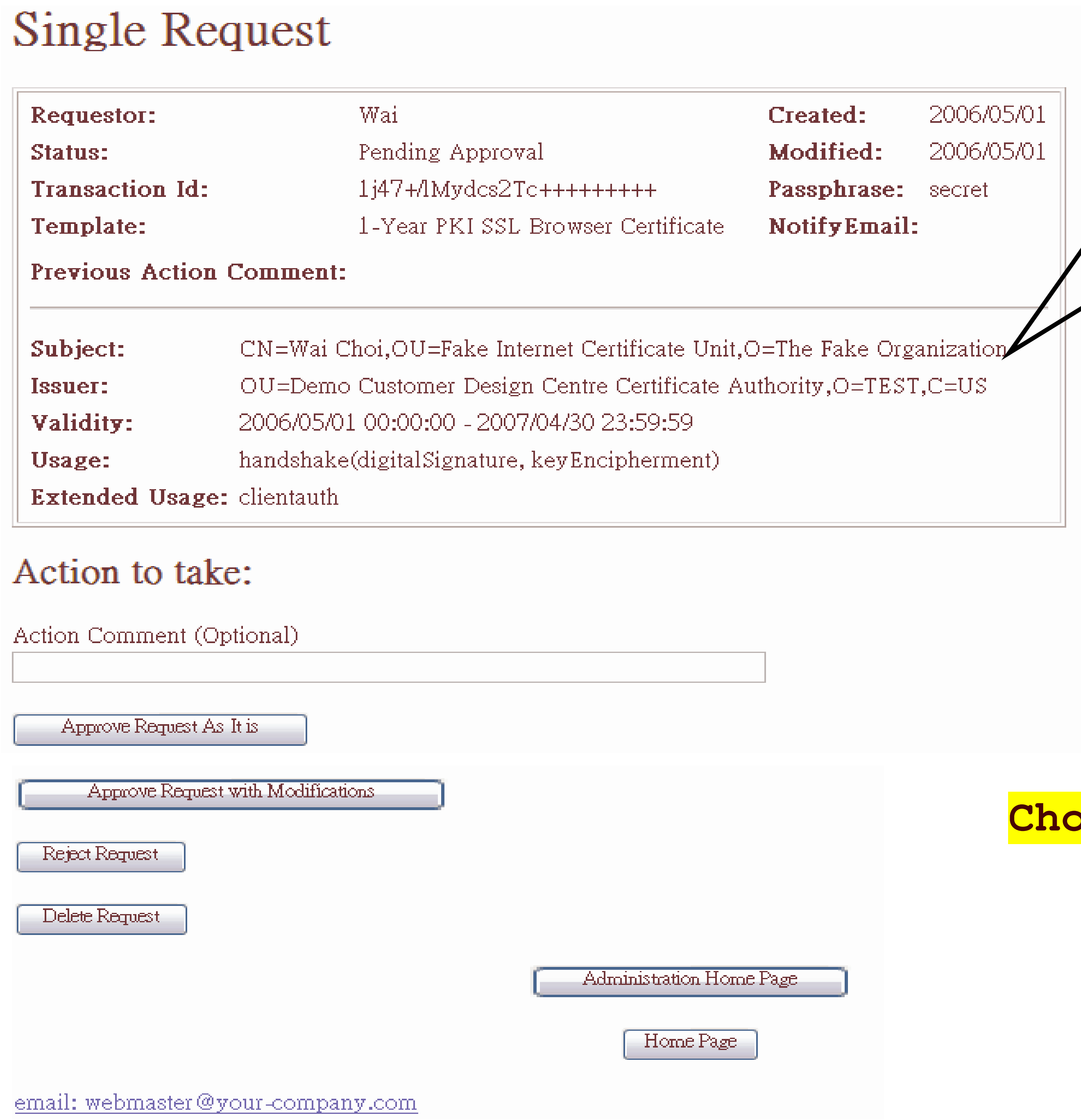
- Click on a transaction ID to see more information or to modify, approve, reject, or delete requests individually
- Select and take action against multiple requests at once

Action Comment (Optional)

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

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

- Delete all requests selected above



| | | | |
|---|---|---|---|
| **Requestor:** | Wai | **Created:** | 2006/05/01 |
| **Status:** | Pending Approval | **Modified:** | 2006/05/01 |
| **Transaction Id:** | 1j47+/lMydcs2Tc+++++++++ | **Passphrase:** | secret |
| **Template:** | 1-Year PKI SSL Browser Certificate | **NotifyEmail:** | |

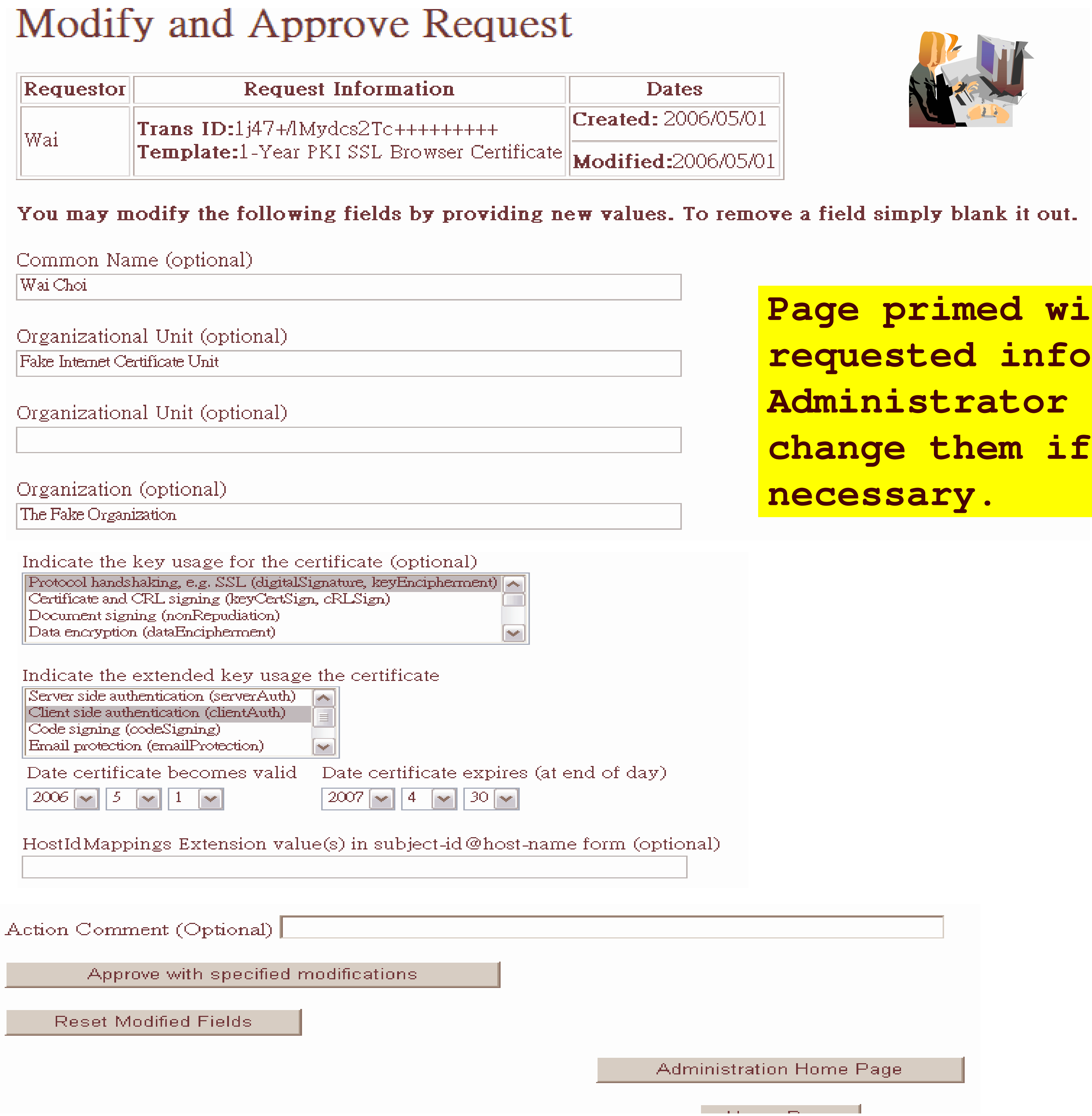
**Previous Action Comment:**

| | |
|---|---|
| **Subject:** | CN=Wai Choi,OU=Fake Internet Certificate Unit,O=The Fake Organization |
| **Issuer:** | OU=Demo Customer Design Centre Certificate Authority,O=TEST,C=US |
| **Validity:** | 2006/05/01 00:00:00 - 2007/04/30 23:59:59 |
| **Usage:** | handshake(digitalSignature, keyEncipherment) |
| **Extended Usage:** | clientauth |

The Subject's name value come from the user input and hardcoded value in pkiserv.tmpl

**Request detail info**

**Choose the action**



# Modify and Approve Request

| Requestor | Request Information | Dates |
|---|---|---|
| Wai | **Trans ID:**1j47+/lMydcs2Tc+++++++++<br>**Template:**1-Year PKI SSL Browser Certificate | **Created:** 2006/05/01<br>**Modified:**2006/05/01 |

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

Common Name (optional)
Wai Choi

Organizational Unit (optional)
Fake Internet Certificate Unit

Organizational Unit (optional)

Organization (optional)
The Fake Organization

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)

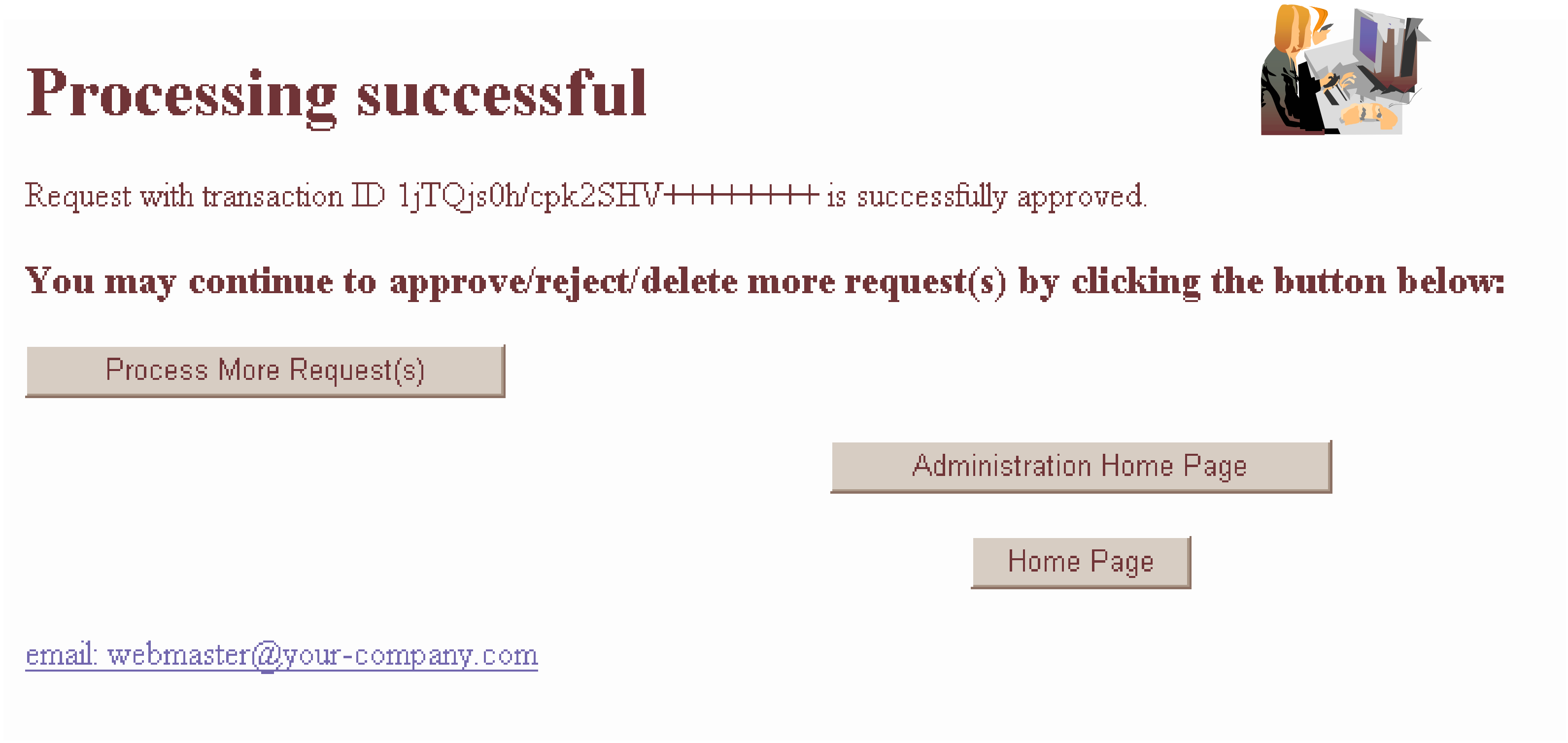
Indicate the extended key usage the certificate
Server side authentication (serverAuth)
Client side authentication (clientAuth)
Code signing (codeSigning)
Email protection (emailProtection)

Date certificate becomes valid: 2006 5 1
Date certificate expires (at end of day): 2007 4 30

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

Action Comment (Optional)

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

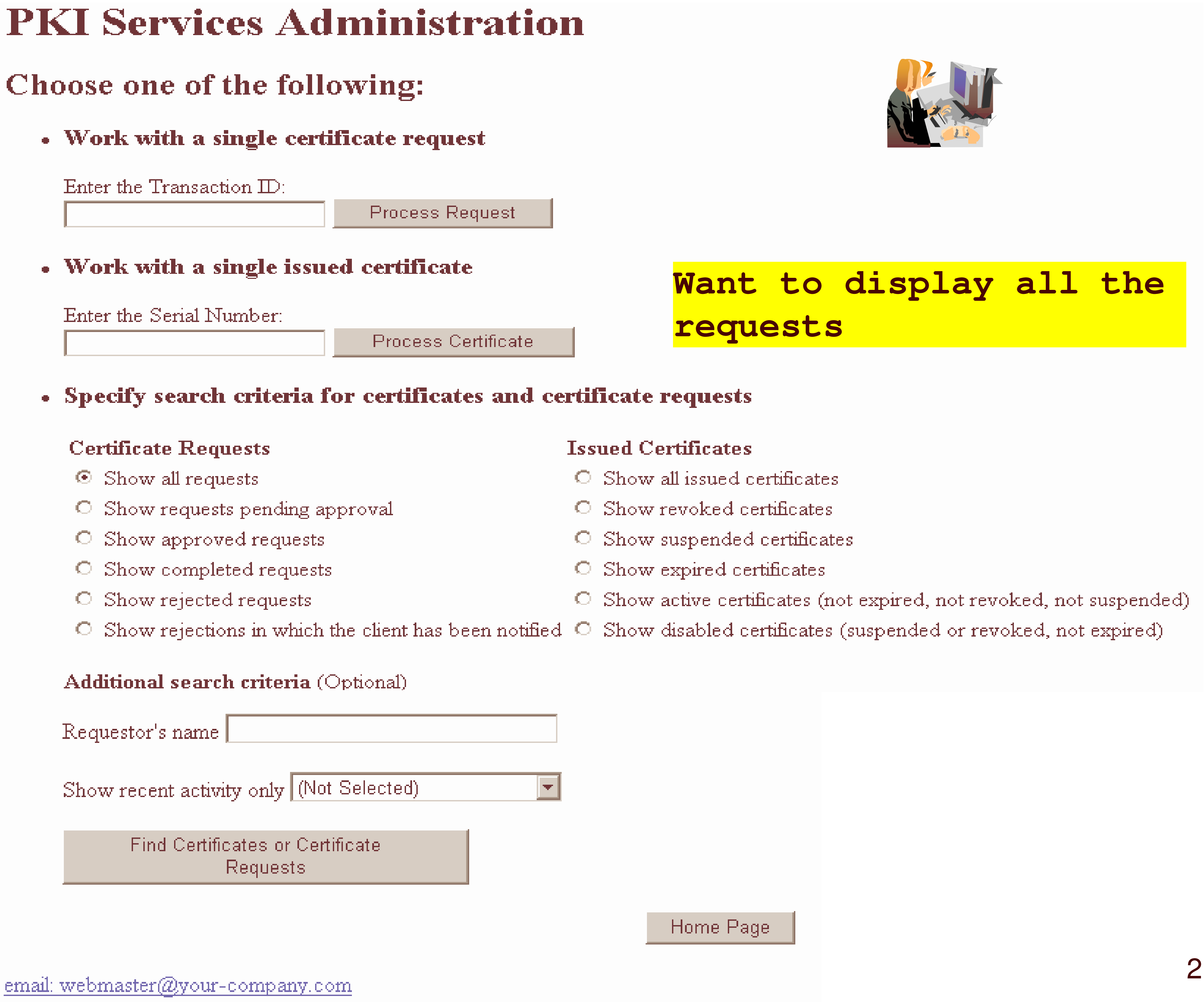


# Processing successful

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

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

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**

**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 [ ]

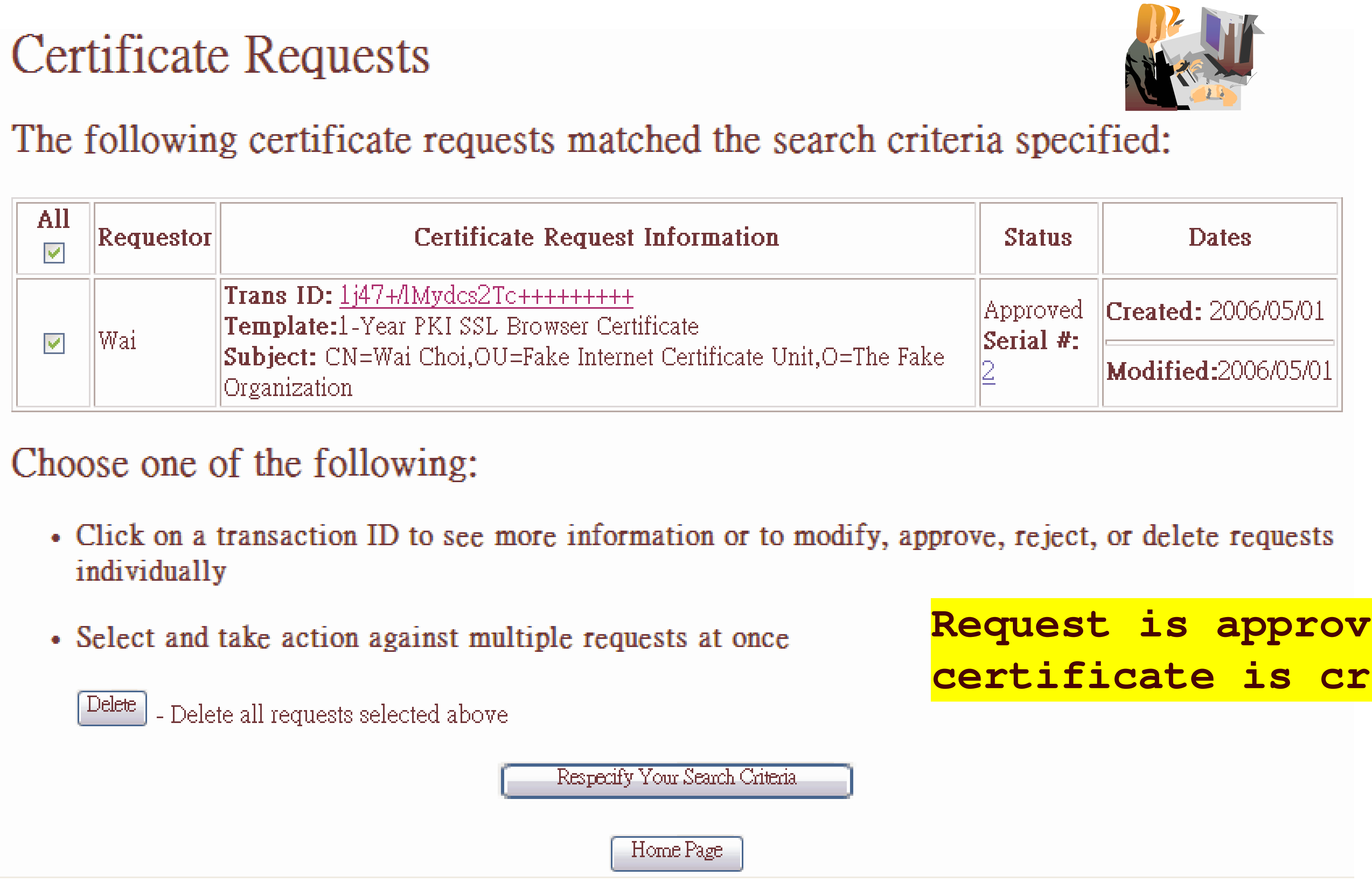
Show recent activity only (Not Selected)

Find Certificates or Certificate Requests

Home Page

email: webmaster@your-company.com

Want to display all the requests



# Certificate Requests

The following certificate requests matched the search criteria specified:

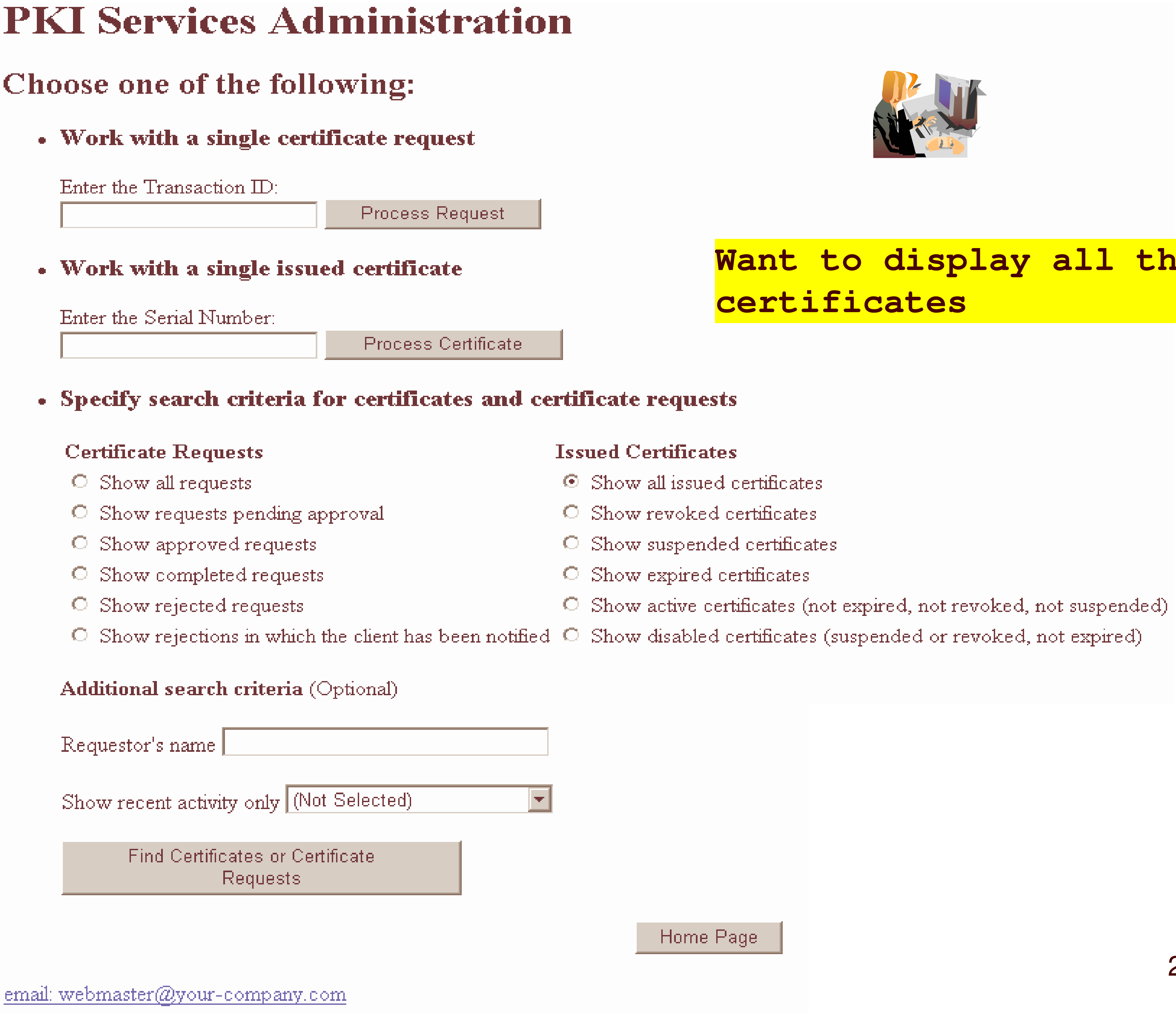
| All<br>☑ | Requestor | Certificate Request Information | Status | Dates |
|---|---|---|---|---|
| ☑ | Wai | **Trans ID:** 1j47+/lMydcs2Tc+++++++++<br>**Template:**1-Year PKI SSL Browser Certificate<br>**Subject:** CN=Wai Choi,OU=Fake Internet Certificate Unit,O=The Fake Organization | Approved<br>**Serial #:**<br>2 | **Created:** 2006/05/01<br>**Modified:**2006/05/01 |

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

**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]

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

| **Certificate Requests** | **Issued Certificates** |
|---|---|
| ○ Show all requests | ● Show all issued certificates |
| ○ Show requests pending approval | ○ Show revoked certificates |
| ○ Show approved requests | ○ Show suspended certificates |
| ○ Show completed requests | ○ Show expired certificates |
| ○ Show rejected requests | ○ Show active certificates (not expired, not revoked, not suspended) |
| ○ Show rejections in which the client has been notified | ○ Show disabled certificates (suspended or revoked, not expired) |

**Additional search criteria** (Optional)

Requestor's name [ ]

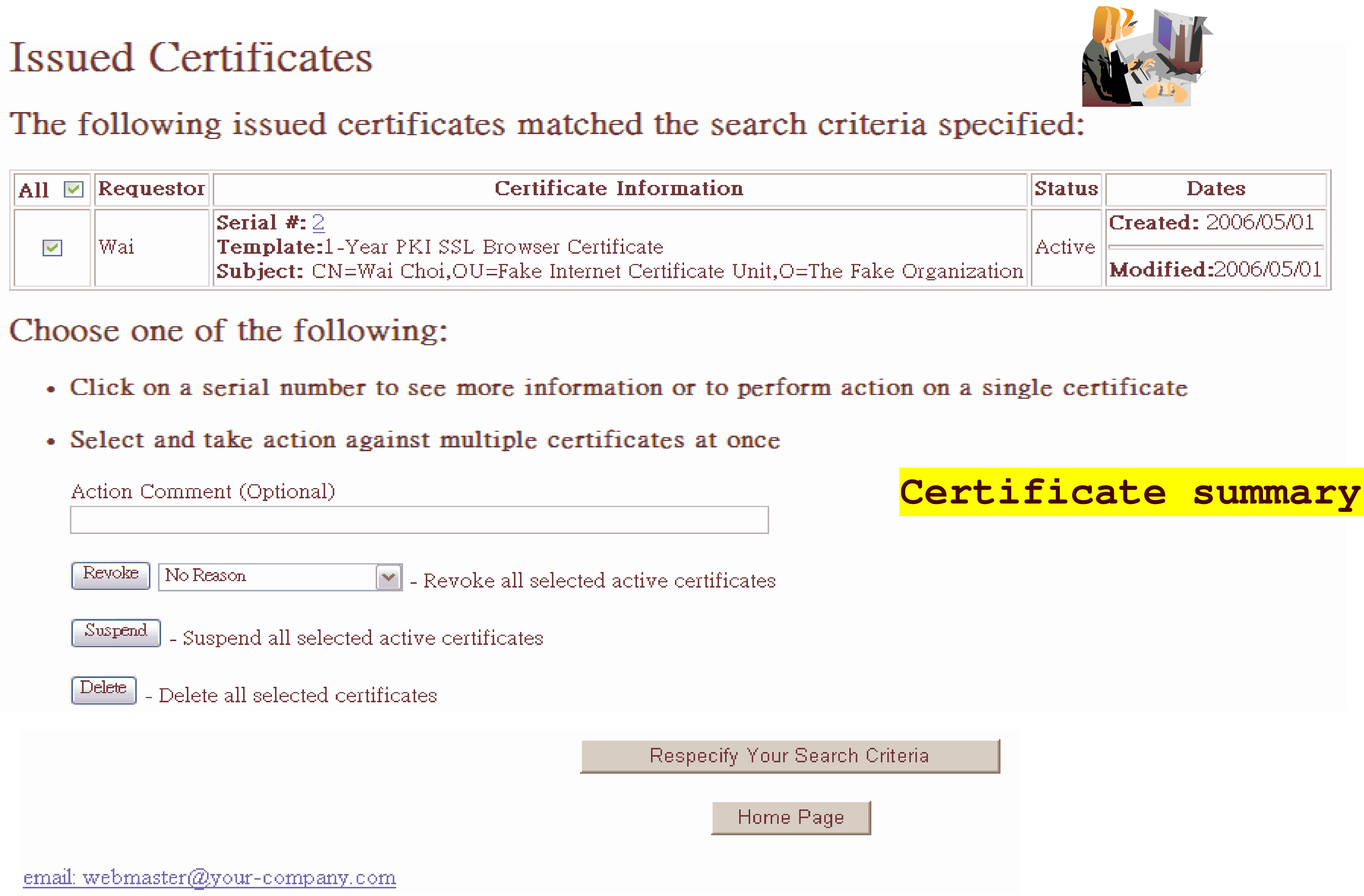
Show recent activity only (Not Selected) ▾

[Find Certificates or Certificate Requests]

[Home Page]

email: webmaster@your-company.com

**Want to display all the certificates**



# Issued Certificates

The following issued certificates matched the search criteria specified:

| All ☑ | Requestor | Certificate Information | Status | Dates |
|---|---|---|---|---|
| ☑ | Wai | **Serial #:** 2<br>**Template:**1-Year PKI SSL Browser Certificate<br>**Subject:** CN=Wai Choi,OU=Fake Internet Certificate Unit,O=The Fake Organization | Active | **Created:** 2006/05/01<br>**Modified:**2006/05/01 |

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 all selected active certificates

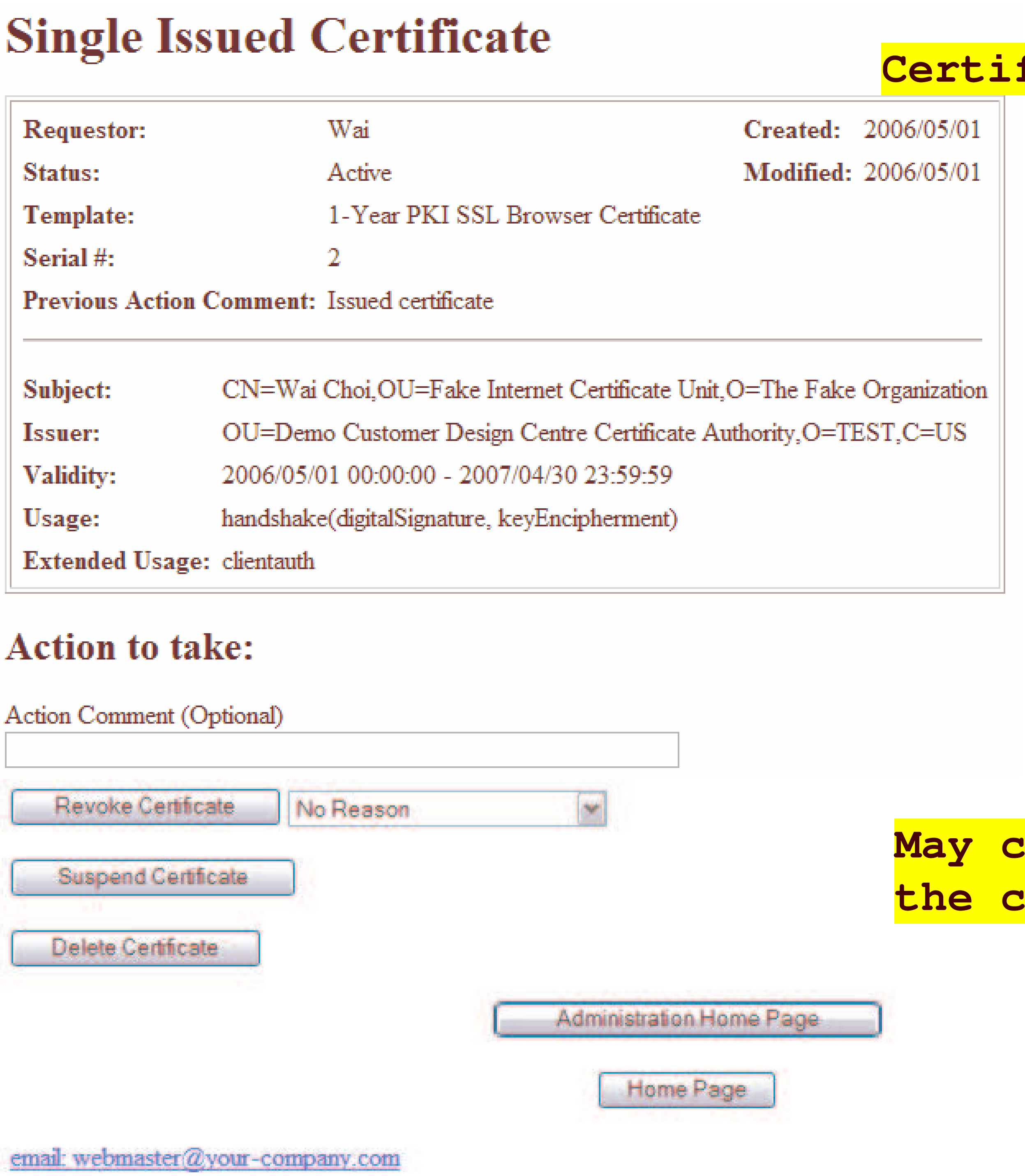
- Suspend all selected active certificates

- Delete all selected certificates

email: webmaster@your-company.com

**Certificate summary info**

Certificate detail info



## Single Issued Certificate

| | | | |
|---|---|---|---|
| **Requestor:** | Wai | **Created:** | 2006/05/01 |
| **Status:** | Active | **Modified:** | 2006/05/01 |
| **Template:** | 1-Year PKI SSL Browser Certificate | | |
| **Serial #:** | 2 | | |
| **Previous Action Comment:** | Issued certificate | | |

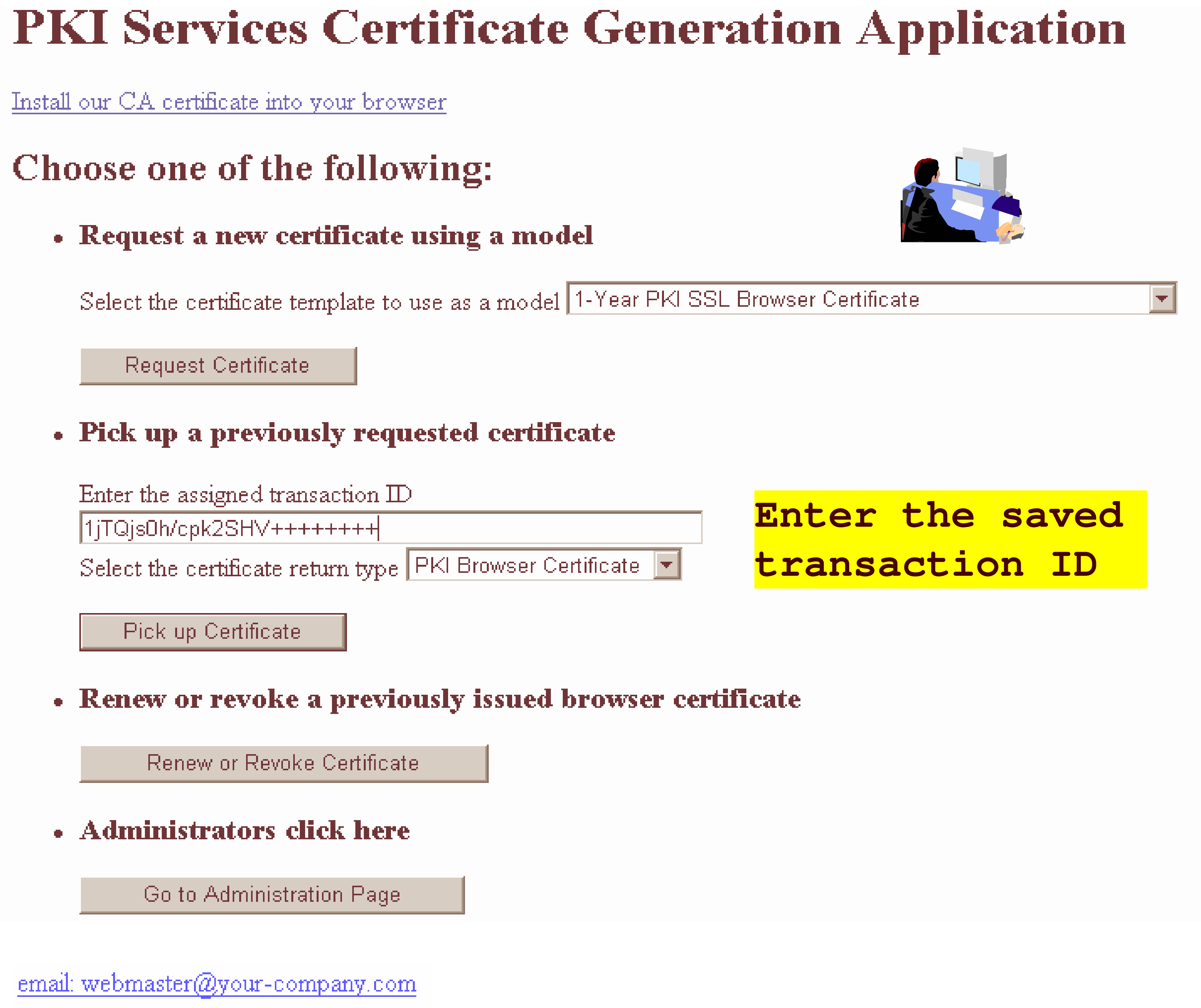
| | |
|---|---|
| **Subject:** | CN=Wai Choi,OU=Fake Internet Certificate Unit,O=The Fake Organization |
| **Issuer:** | OU=Demo Customer Design Centre Certificate Authority,O=TEST,C=US |
| **Validity:** | 2006/05/01 00:00:00 - 2007/04/30 23:59:59 |
| **Usage:** | handshake(digitalSignature, keyEncipherment) |
| **Extended Usage:** | clientauth |

## Action to take:

Action Comment (Optional)

email: webmaster@your-company.com

May choose what to do with the certificate



# 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**

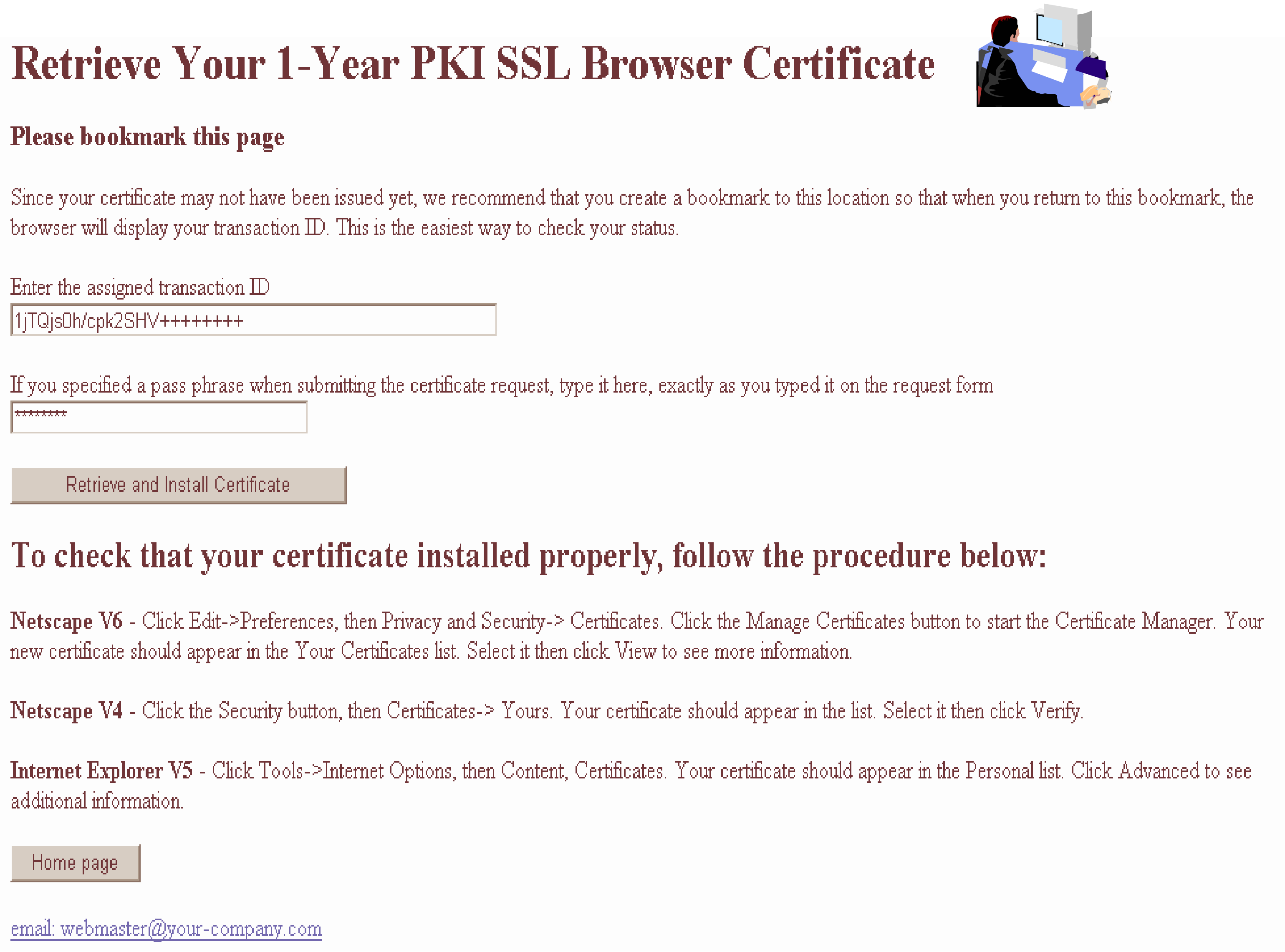
  Renew or Revoke Certificate

- **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

********

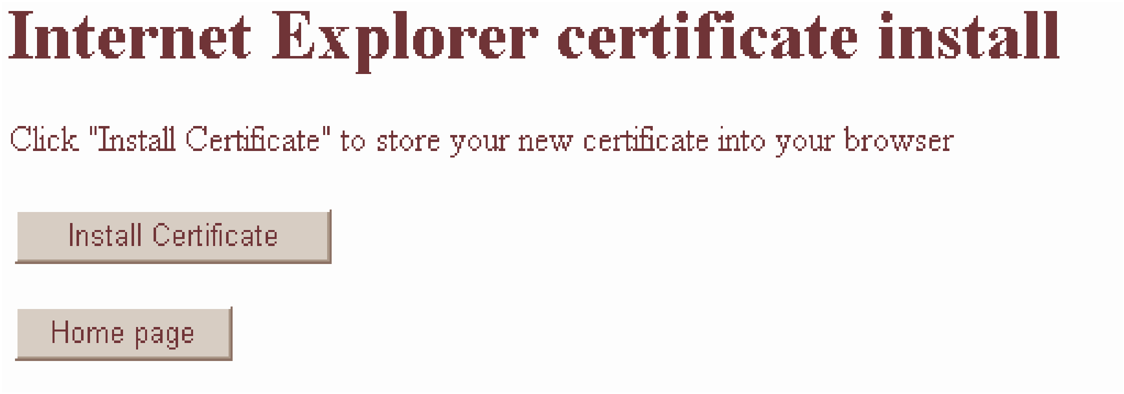
## To check that your certificate installed properly, follow the procedure below:

**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.

email: webmaster@your-company.com

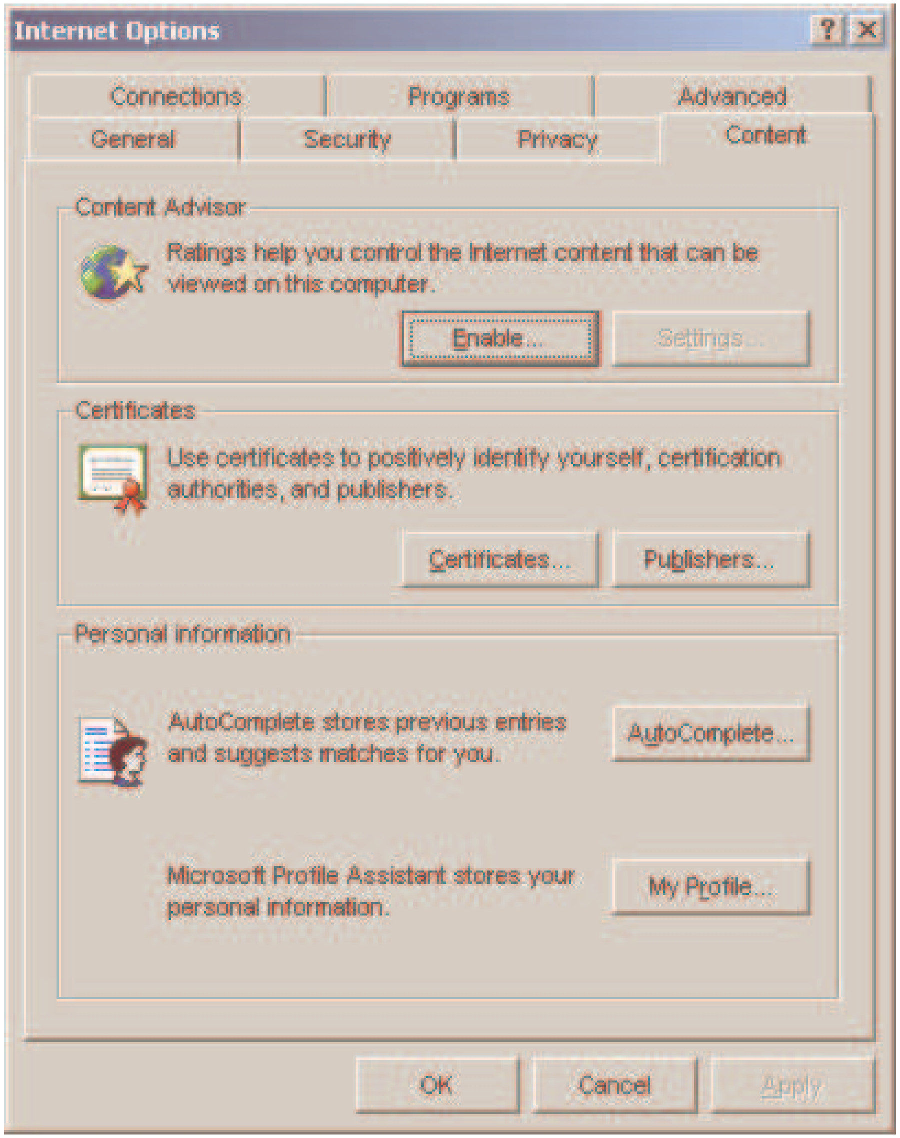


# Internet Explorer certificate install

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

Let’s take a look at the installed certificate

# From IE browser, click on Tools->Internet Options



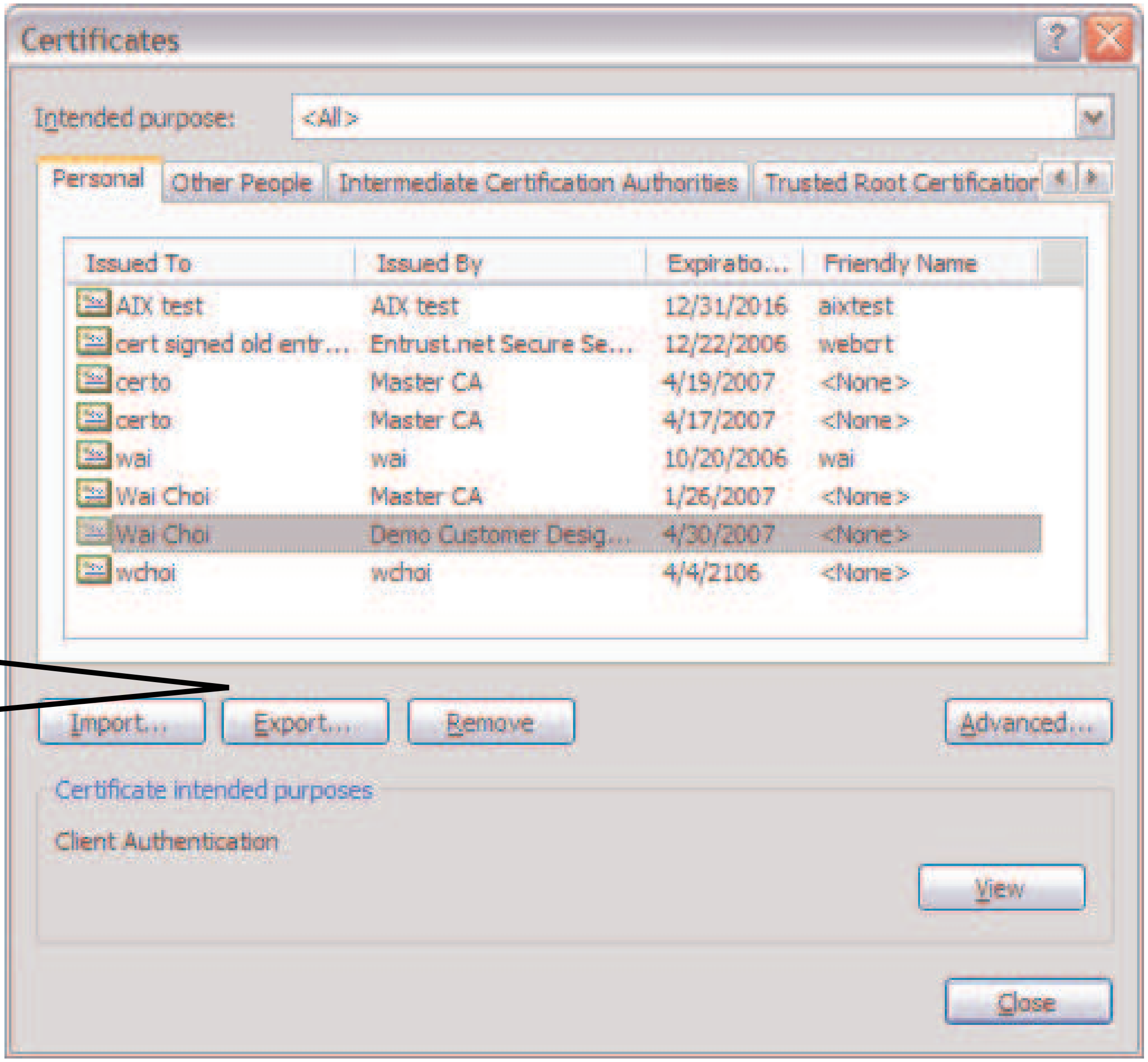
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

# Certificate is installed in browser



Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| AIX test | AIX test | 12/31/2016 | aixtest |
| cert signed old entr... | Entrust.net Secure Se... | 12/22/2006 | webcrt |
| certo | Master CA | 4/19/2007 | <None> |
| certo | Master CA | 4/17/2007 | <None> |
| wai | wai | 10/20/2006 | wai |
| Wai Choi | Master CA | 1/26/2007 | <None> |
| Wai Choi | Demo Customer Desig... | 4/30/2007 | <None> |
| wchoi | wchoi | 4/4/2106 | <None> |

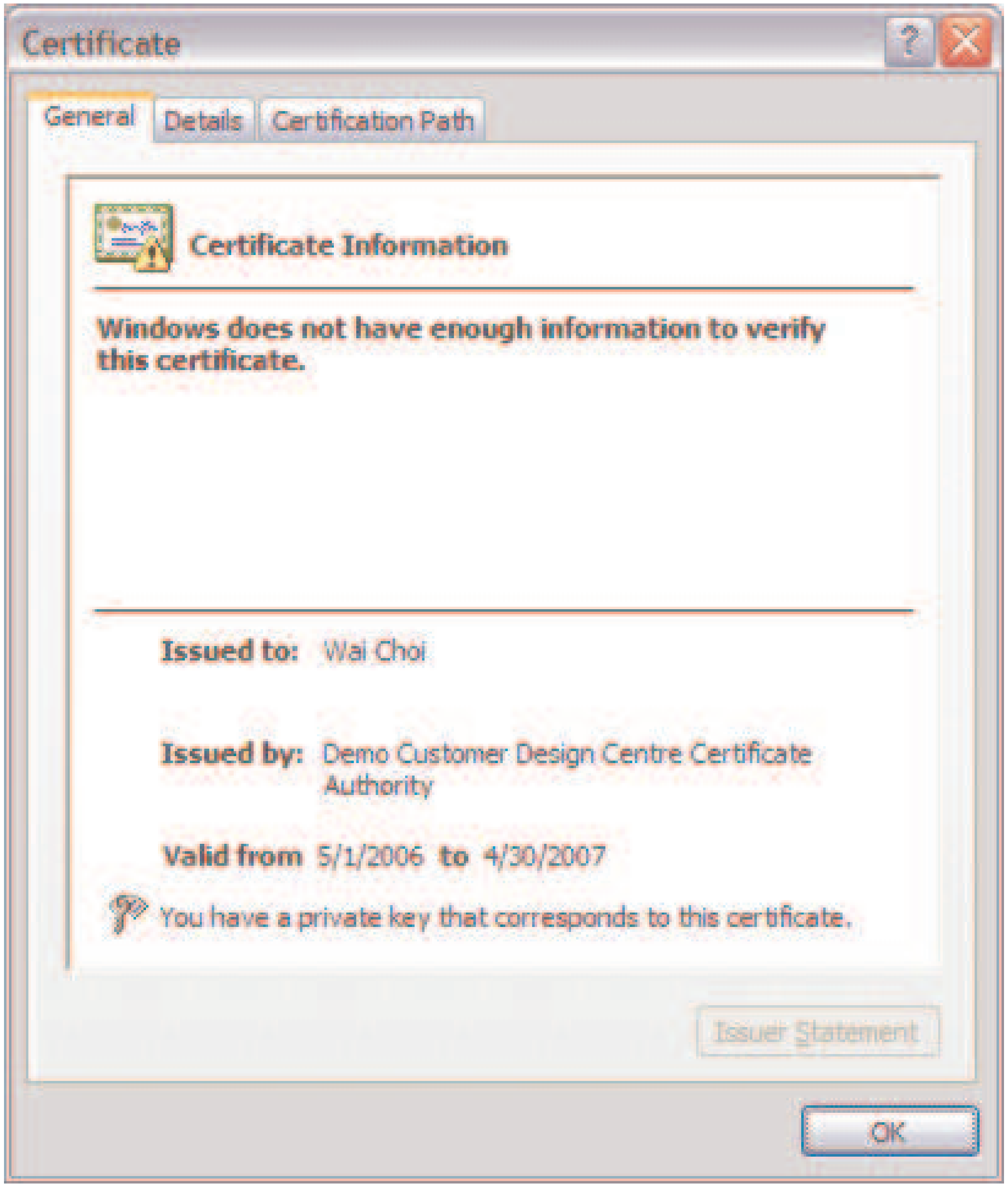
Certificate intended purposes

Client Authentication

Export it under a directory

eg /temp/mycert.cer

# You may display the certificate information…



Certificate Information

Windows does not have enough information to verify this certificate.

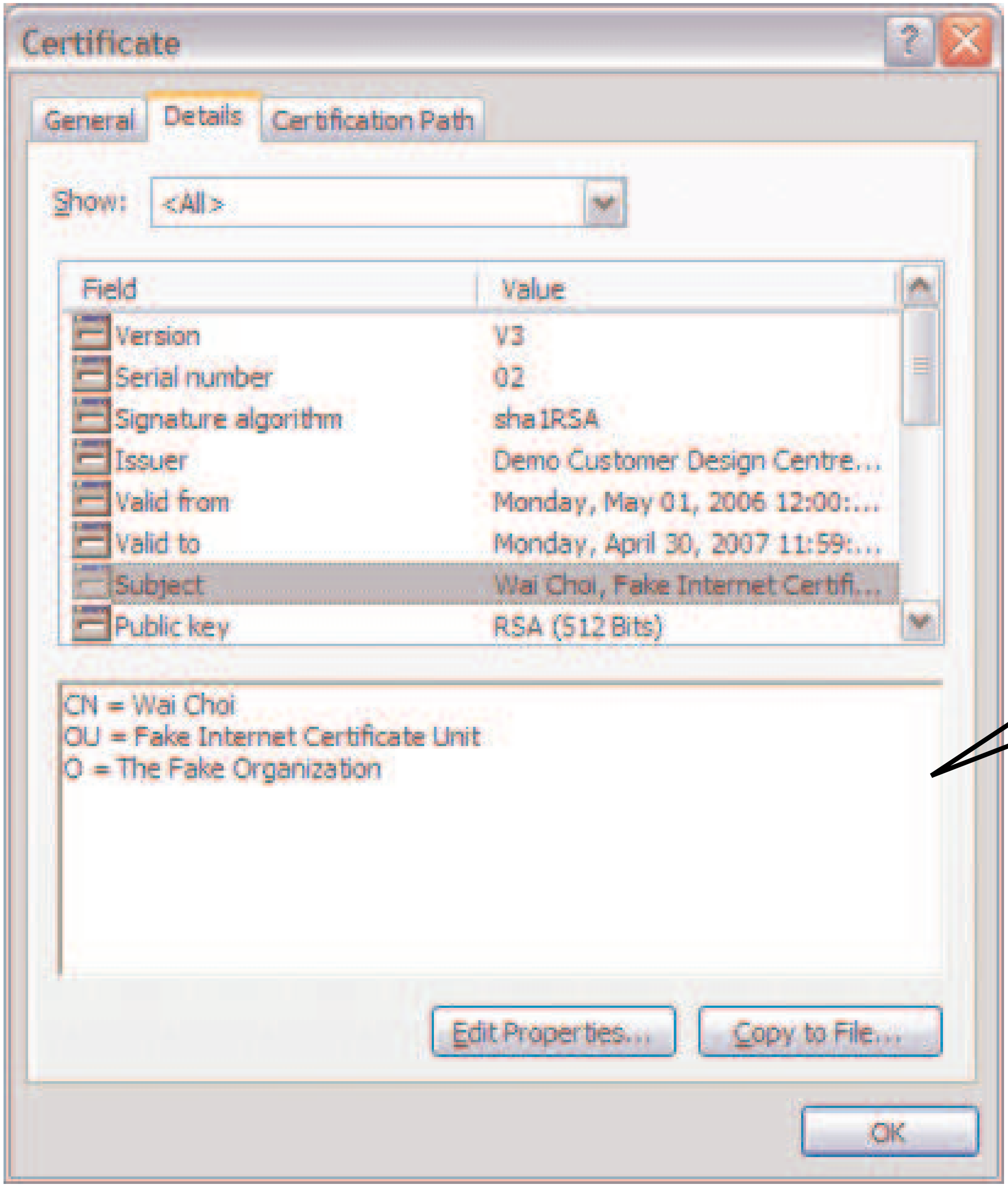
Issued to: Wai Choi

Issued by: Demo Customer Design Centre Certificate Authority

Valid from 5/1/2006 to 4/30/2007

You have a private key that corresponds to this certificate.

# And look at the details of each field – Subject

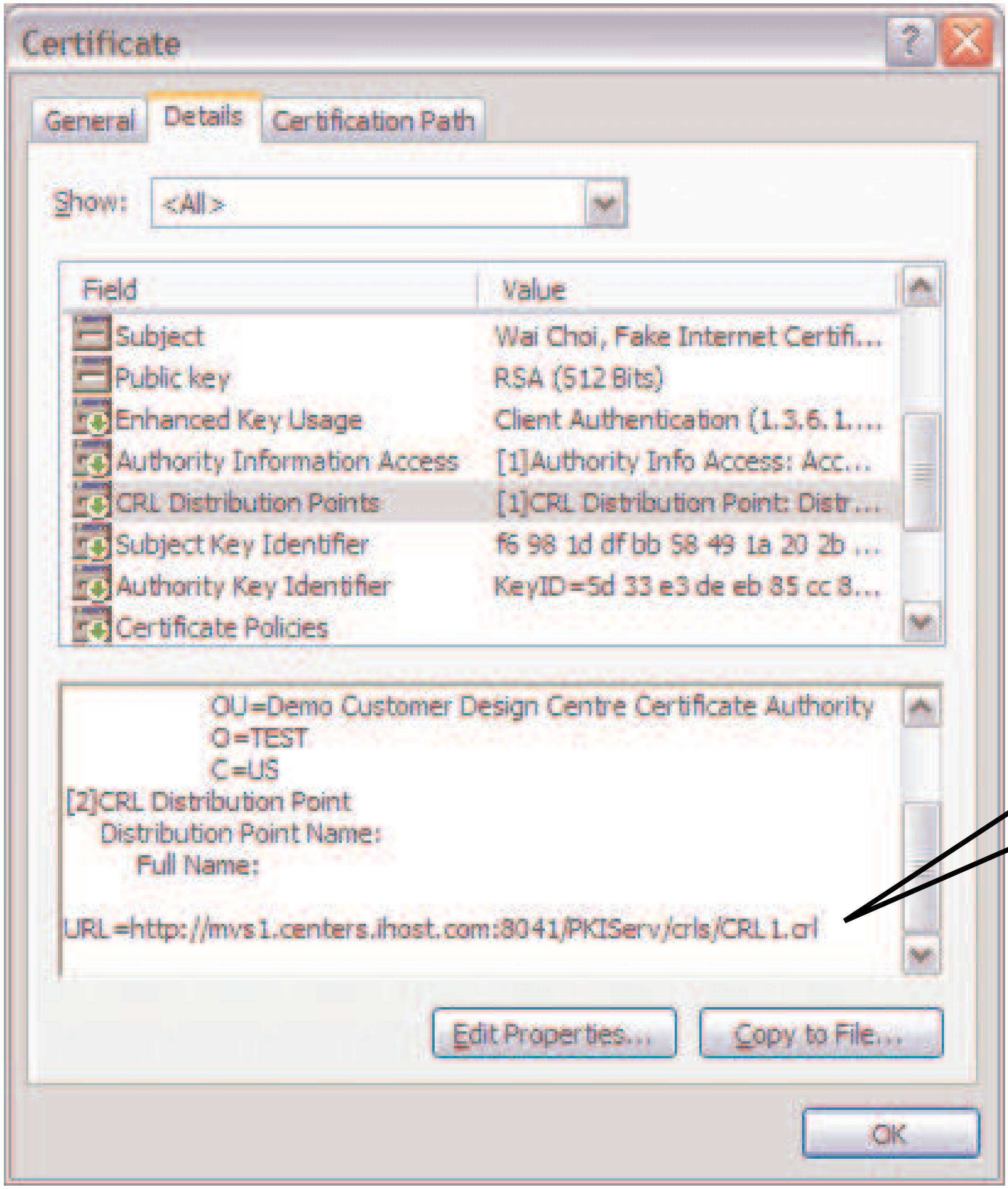


| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 02 |
| Signature algorithm | sha1RSA |
| Issuer | Demo Customer Design Centre... |
| Valid from | Monday, May 01, 2006 12:00:... |
| Valid to | Monday, April 30, 2007 11:59:... |
| Subject | Wai Choi, Fake Internet Certifi... |
| Public key | RSA (512 Bits) |

CN = Wai Choi
OU = Fake Internet Certificate Unit
O = The Fake Organization

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

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



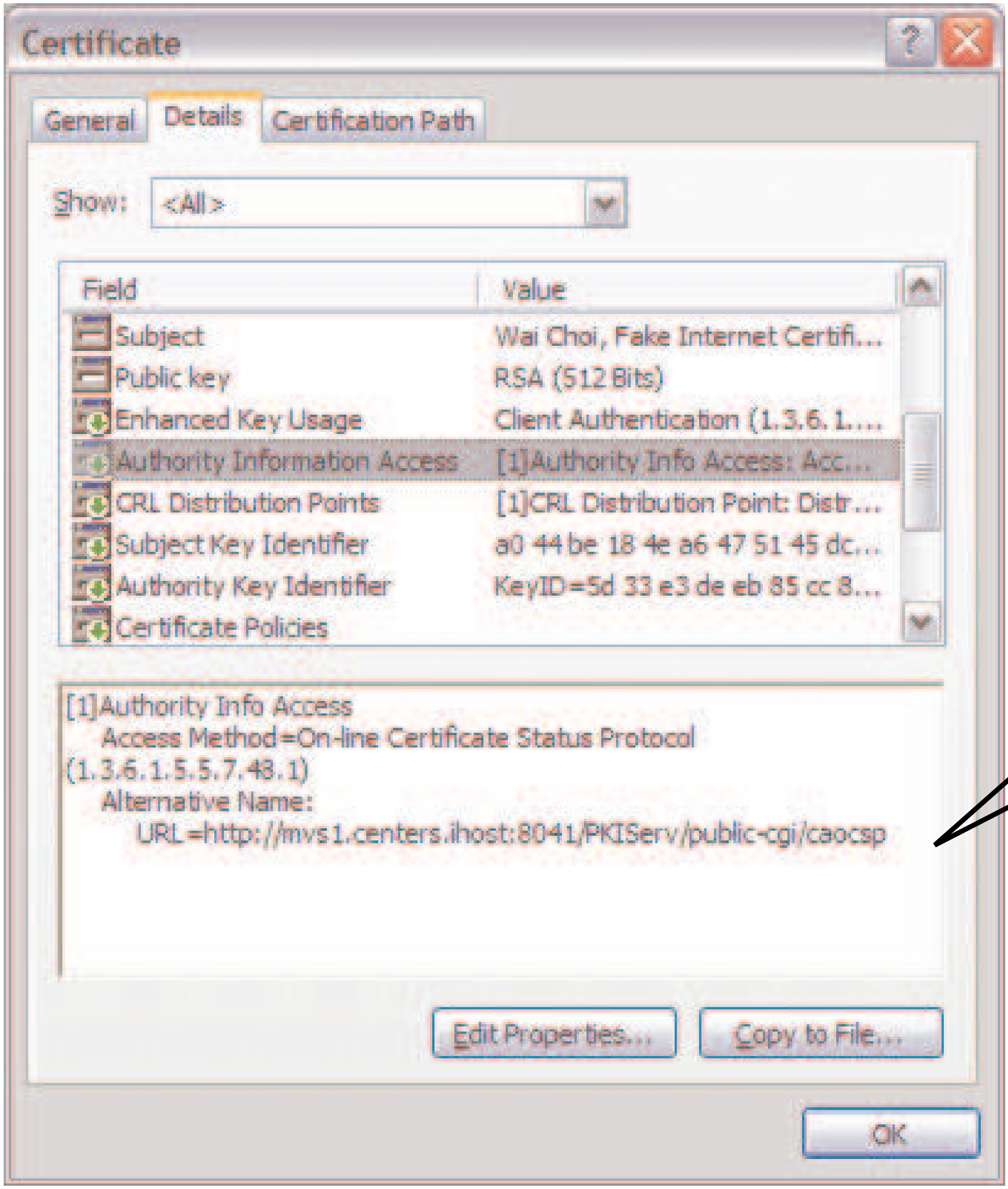
| Field | Value |
|---|---|
| Subject | Wai Choi, Fake Internet Certifi... |
| Public key | RSA (512 Bits) |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Authority Information Access | [1]Authority Info Access: Acc... |
| CRL Distribution Points | [1]CRL Distribution Point: Distr... |
| Subject Key Identifier | f6 98 1d df bb 58 49 1a 20 2b ... |
| Authority Key Identifier | KeyID=5d 33 e3 de eb 85 cc 8... |
| Certificate Policies | |

```
          OU=Demo Customer Design Centre Certificate Authority
          O=TEST
          C=US
[2]CRL Distribution Point
     Distribution Point Name:
          Full Name:

URL=http://mvs1.centers.ihost.com:8041/PKIServ/crls/CRL1.crl
```

This is set up in pkiserv.conf

# And look at the details of each field – OCSP location



| Field | Value |
|---|---|
| Subject | Wai Choi, Fake Internet Certifi... |
| Public key | RSA (512 Bits) |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Authority Information Access | [1]Authority Info Access: Acc... |
| CRL Distribution Points | [1]CRL Distribution Point: Distr... |
| Subject Key Identifier | a0 44 be 18 4e a6 47 51 45 dc... |
| Authority Key Identifier | KeyID=5d 33 e3 de eb 85 cc 8... |
| Certificate Policies | |

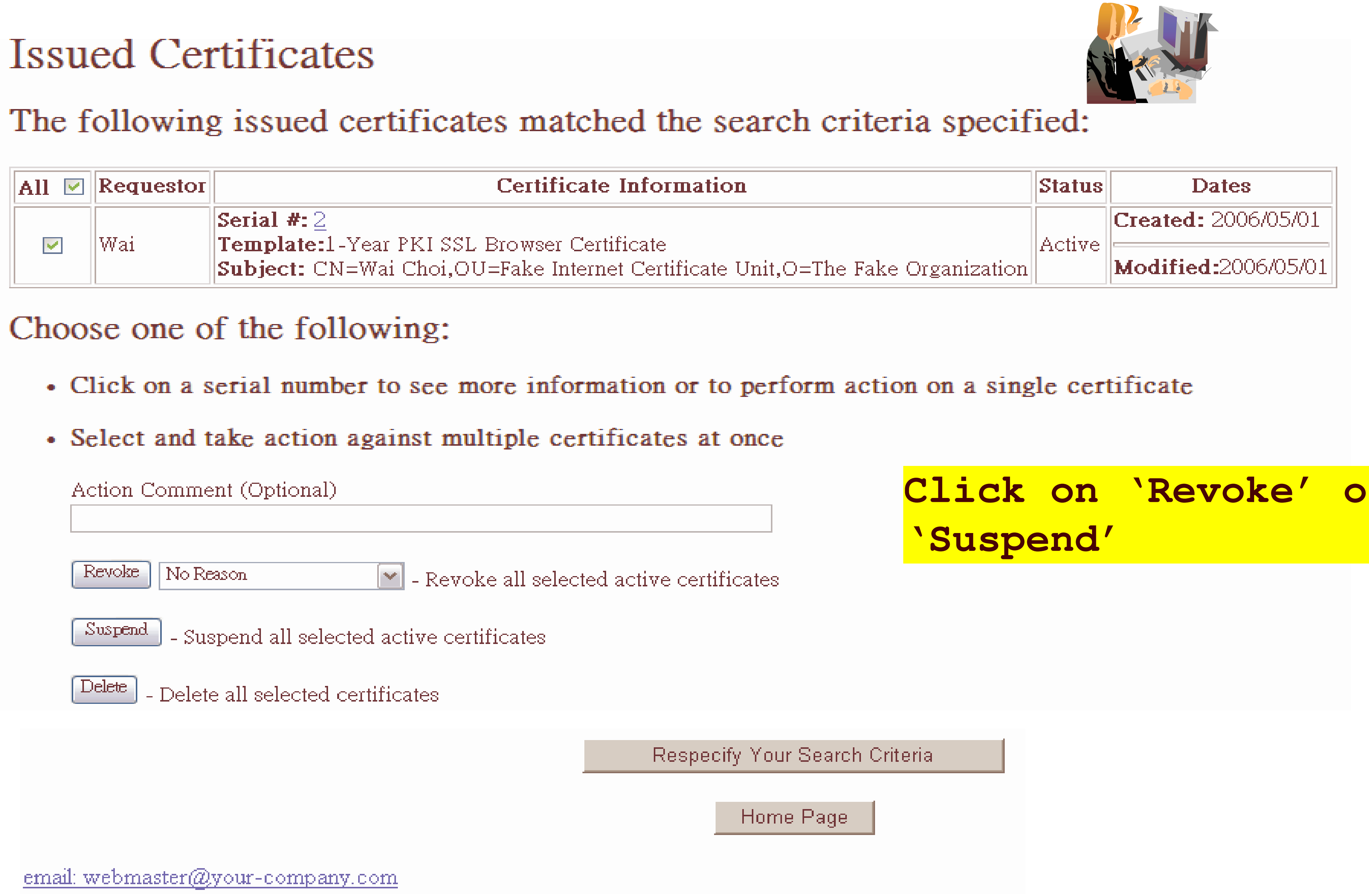
```
[1]Authority Info Access
     Access Method=On-line Certificate Status Protocol
(1.3.6.1.5.5.7.48.1)
     Alternative Name:
          URL=http://mvs1.centers.ihost:8041/PKIServ/public-cgi/caocsp
```

This is hardcoded by administrator in pkiserv.tmpl

Let’s revoke/suspend some certificates.

Note: Both user and administrator can revoke/suspend a certificate.
The user can only revoke/suspend his own, but the administrator can revoke/suspend any.

The following slide show the Administrator path.



# Issued Certificates

The following issued certificates matched the search criteria specified:

| All ☑ | Requestor | Certificate Information | Status | Dates |
|---|---|---|---|---|
| ☑ | Wai | **Serial #:** 2<br>**Template:**1-Year PKI SSL Browser Certificate<br>**Subject:** CN=Wai Choi,OU=Fake Internet Certificate Unit,O=The Fake Organization | Active | **Created:** 2006/05/01<br>**Modified:**2006/05/01 |

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

**Click on 'Revoke' of 'Suspend'**

# Check the status using Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP)

- From OCSP, you will find the live certificate status
- But you may not find the revoked certificate on the CRL list, depending on the time the CRL is refreshed

# Check the status using OCSP

# Get the status from OCSP using openSSL…

## Send a request to the responder:

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

# Get the status from OCSP using openSSL…

```
    OCSP Response Data:
        OCSP Response Status: successful (0x0)
        Response Type: Basic OCSP Response
        Version: 1 (0x0)
        Responder Id: C = US, O = TEST, OU = Demo Customer Design Centre Certificate Authority
        Produced At: May  2 19:39:46 2006 GMT
        Responses:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 776685A214FFAE51B30DBBDEB3E7FE26259192E6
          Issuer Key Hash: 5D33E3DEEB85CC83F61F9762A1B0AFB52C0311AC
          Serial Number: 02
        Cert Status: good
        This Update: May  2 19:39:45 2006 GMT
```

Cert 02 is not revoked or suspended

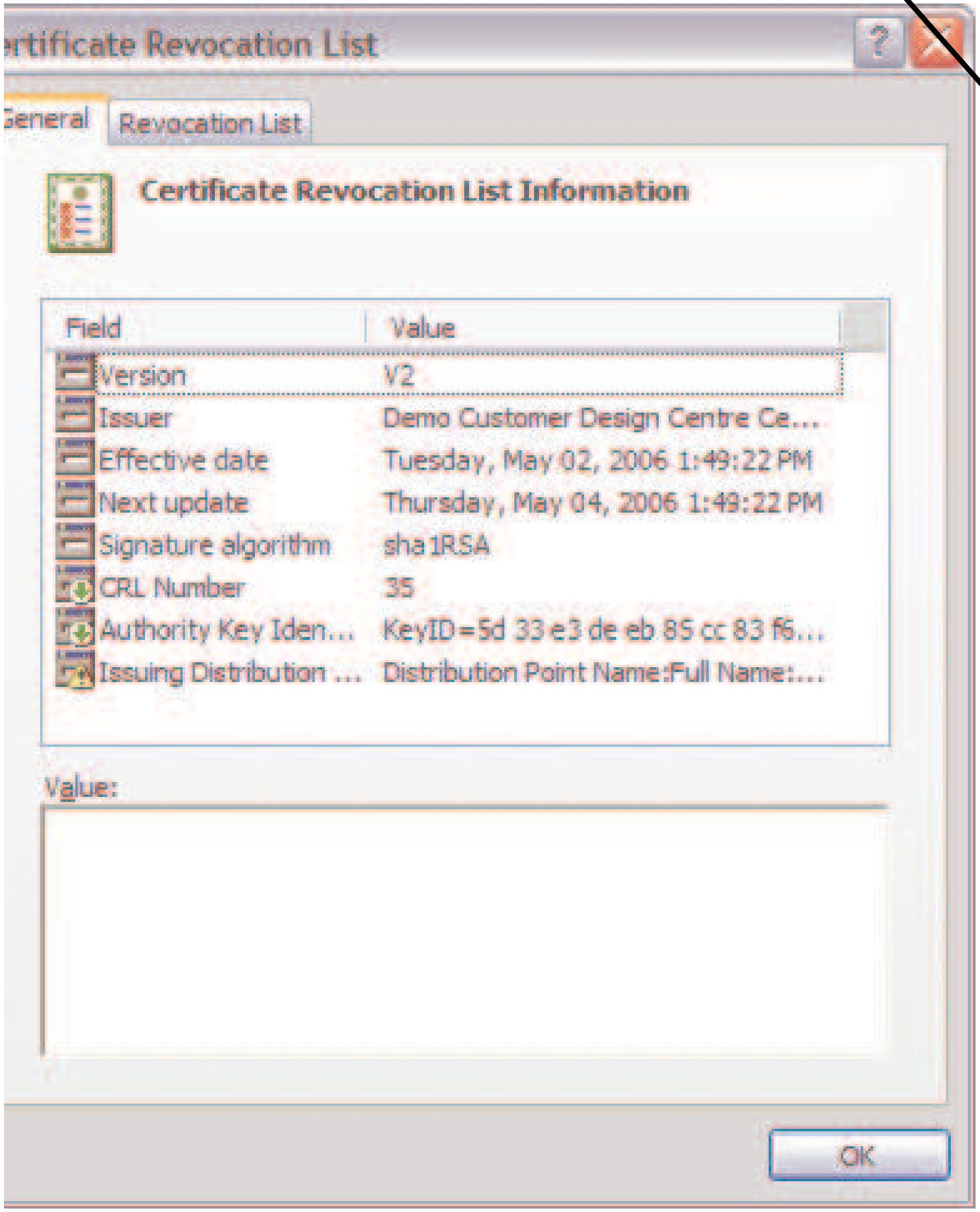
```
    OCSP Response Data:
        OCSP Response Status: successful (0x0)
        Response Type: Basic OCSP Response
        Version: 1 (0x0)
        Responder Id: C = US, O = TEST, OU = Demo Customer Design Centre Certificate Authority
        Produced At: May  2 21:56:17 2006 GMT
        Responses:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 776685A214FFAE51B30DBBDEB3E7FE26259192E6
          Issuer Key Hash: F4464613908ED37CCF4247A2B2A86368D1E87564
          Serial Number: 04
        Cert Status: revoked
        Revocation Time: May  2 21:56:11 2006 GMT
        Revocation Reason: certificateHold (0x6)
        This Update: May  2 21:56:17 2006 GMT
```

Cert 04 is suspended (from reason 0x6)

# Check the status using CRL

**Go to http://mvs1.centers.ihost:8041/PKIServ/crls/CRL1.crl**

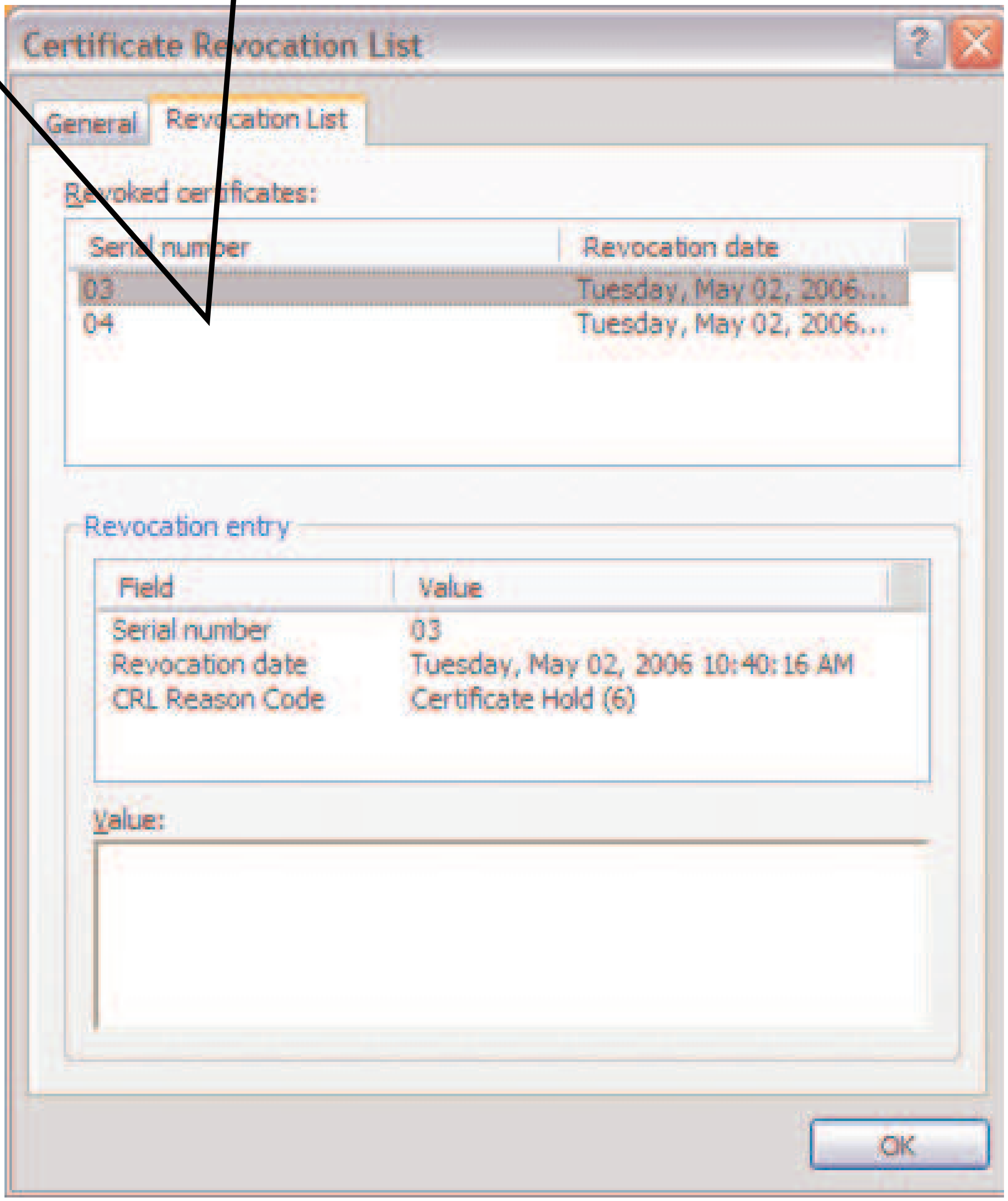
Cert with serial no. 3 and 4 are revoked or suspended



Certificate Revocation List Information

| Field | Value |
|---|---|
| Version | V2 |
| 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 | sha1RSA |
| CRL Number | 35 |
| Authority Key Iden... | KeyID=5d 33 e3 de eb 85 cc 83 f6... |
| Issuing Distribution ... | Distribution Point Name:Full Name:... |

Value:



Revoked certificates:

| Serial number | Revocation date |
|---|---|
| 03 | Tuesday, May 02, 2006... |
| 04 | Tuesday, May 02, 2006... |

Revocation entry

| Field | Value |
|---|---|
| Serial number | 03 |
| Revocation date | Tuesday, May 02, 2006 10:40:16 AM |
| CRL Reason Code | Certificate Hold (6) |

Value:

Questions???

Let’s see how the other products use certificates from PKI Services

# 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

# 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.**