IBM ITSO Poughkeepsie
OS/390 in an e-business environment

DGW 5.0
Domino Go CA

OS/390 Web Server Certification Authority

Roland Trauner
trauner@us.ibm.com

Domino Go CA

- **DGW 5.0 Certification Authority**
  - DGW 5.0 provides a feature allowing to act as a certification authority for client and server certificates.
  - It has a limited function in respect of managing certificate requests since it can just store about 250 certificate requests in the database. This might be not an issue since it is possible to issue a certificate and delete the cert request the process.
    - The database `cert.db` is located at `/usr/lpp/ServletExpress/web/resources/en_US /CAServlet/certs/`
  - Domino Go CA provides a user interface consisting of html forms and servlets for administration.
  - It requires DGW 5.0 ServletExpress
    - In fact it is delivered within the SE structure.
    - It is not delivered within the WebAS structure

Roland Trauner trauner@us.ibm.com

Domino Go CA

- **Access Domino Go CA**
  - To access Domino Go CA use the following URL:

```
http://www.the-apple.com/ServletExpress/resources/CAServlet/Welcome.html
```

  - Add the following definitions to httpd.conf to be able to handle certificates and protect the CAServlet administration
    - MIME Section:

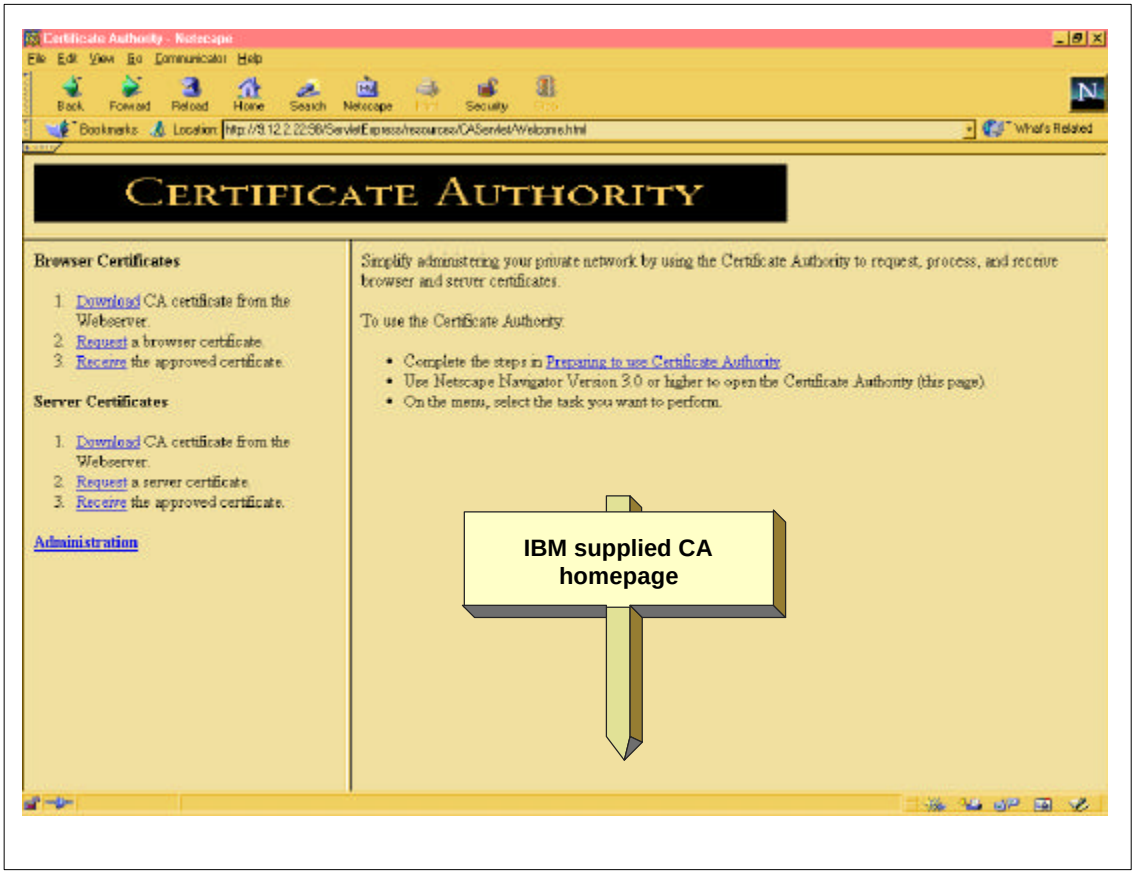
```
AddType .cer application/x-x509-user-cert ebcdic 0.5 #User certificate
AddType .der application/x-x509-ca-cert   binary 1.0 #Browser CA certificate
```

    - Protection Section:

```
Protect /ServletExpress/resources/CAServlet/Ca_admin.html  IMW_Admin WEBADM
```

  - If you access the CA now, you will get the following screen

Roland Trauner trauner@us.ibm.com



- This page is not the greatest artwork. You might create your own CA pages!

Domino Go CA

- **CA Key Database**
  - The CA key database and the stash file need to exist in the CAServlet directory.
    - The names are also fixed --- they need to be cakey.kdb and cakey.sth
    - Copy the CA key database from `/web/apple/sec` to that directory and name it accordingly:

`/usr/lpp/ServletExpress/web/resources/en_US/CAServlet/cakey.kdb`

    - If you like the CA to automatically process and approve certificate requests, then also copy the "stash" file to the directory:

`/usr/lpp/ServletExpress/web/resources/en_US/CAServlet/cakey.sth`

    - If you like to approve certificate requests manually then don't copy the "stash" file to the directory.

Roland Trauner trauner@us.ibm.com

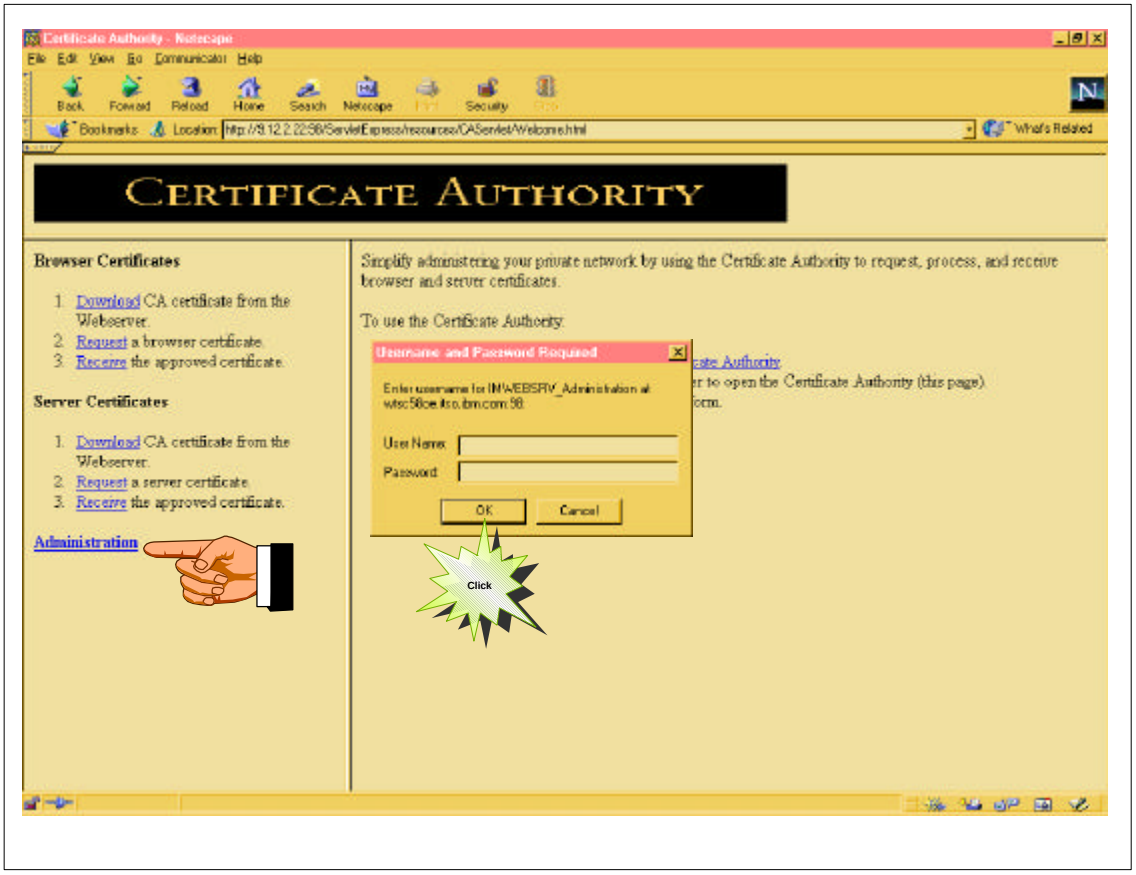
- Automatic process is ok for test or internal environments.
- Usually it's more likely that somebody controls the process.

Domino Go CA

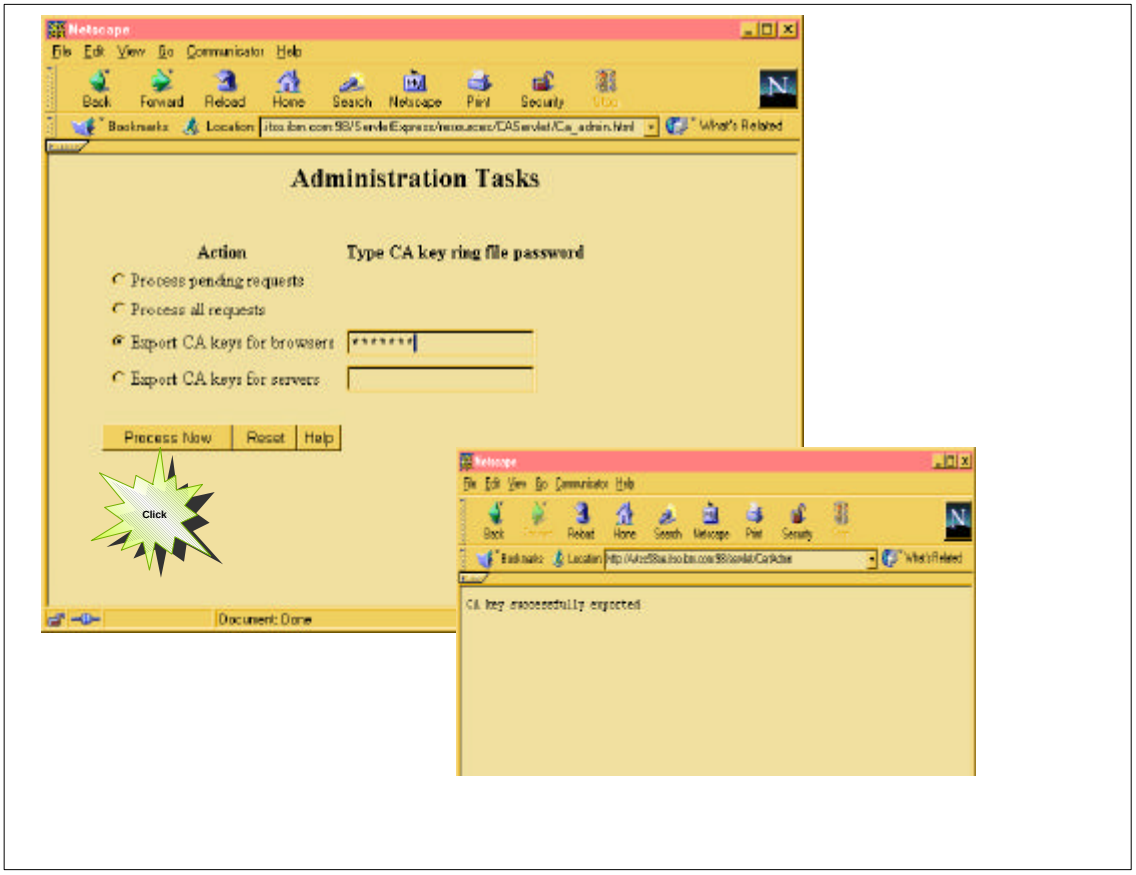
- **CA Preparation**
  - Export the server CA certificate
    - Two forms of the CA certificate, one for browsers and on for servers need to be published by the CA.
    - One of the first steps for browsers and servers is to receive the CA certificate into their own key database when using certificates of this CA.
    - This step is not necessary when using certificates from an established "commercial" CA, since their certificates are provided with the browsers and servers.
  - Certificate for Browsers in BINARY format
    - CAKEY.DER
  - Certificate for Servers in PKCS10 format
    - CAKEY.TXT

Roland Trauner trauner@us.ibm.com

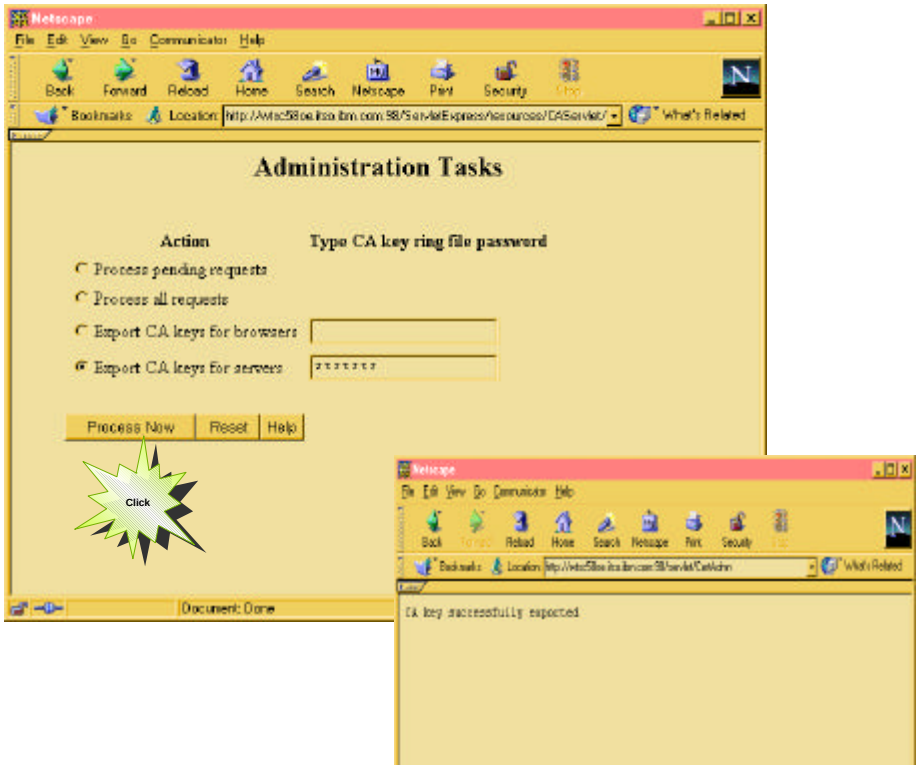
- If you need further information about certificates and especially their handling for OS/390, you may refer to a whitepaper written by Ulrich Boche of IBM Germany



- Prompt for user ID and password results from the PROTECT statement



- Export CA keys for browsers and servers need to be done in the first place to allow browsers and servers to receive the CA certificate.
- Usually this task needs to be done when you just created or renewed the CA keys.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security
Administration Tasks
Action
Type CA key ring file password
Process pending requests
Process all requests
Export CA keys for browsers
Export CA keys for servers
Process Now
Reset
Help
Click
Document: Done
CA key successfully exported

ncf.log

```
IBM ServletExpress WARNING: Cannot load service IBM: No service class specified.
java.lang.IllegalArgumentException: No service class specified
.at com.sun.server.ServiceManager.createService(Compiled Code)
.at com.sun.server.ServiceManager.loadService(Compiled Code)
.at com.sun.server.ServiceManager.loadServices(Compiled Code)
.at com.sun.server.ServiceManager.startServices(Compiled Code)
.at com.sun.server.ServerProcess.main(Compiled Code)
.at com.ibm.ServletExpress.service.ServerProcessThread.run(Compiled Code)
.at java.lang.Thread.run(Compiled Code)
CERTADMN:  Beginning service
SECURENI:  Successfully loaded the US security library (skit.dll)
CERTADMN:  Attempting to export CA key for use by browsers (BINARY)
CERTADMN:  GetCACert returned
CERTADMN:  CA key successfully exported to
/usr/lpp/ServletExpress/web/resources/en_US/CAServlet/cakey.der
CERTADMN:  Beginning service
CERTADMN:  Attempting to export CA key for use by servers (PKCS10)
CERTADMN:  GetCACert returned
CERTADMN:  CA key successfully exported to
/usr/lpp/ServletExpress/web/resources/en_US/CAServlet/cakey.txt
```


Roland Trauner trauner@us.ibm.com

- The NCF log shows the success - or failure - of the tasks

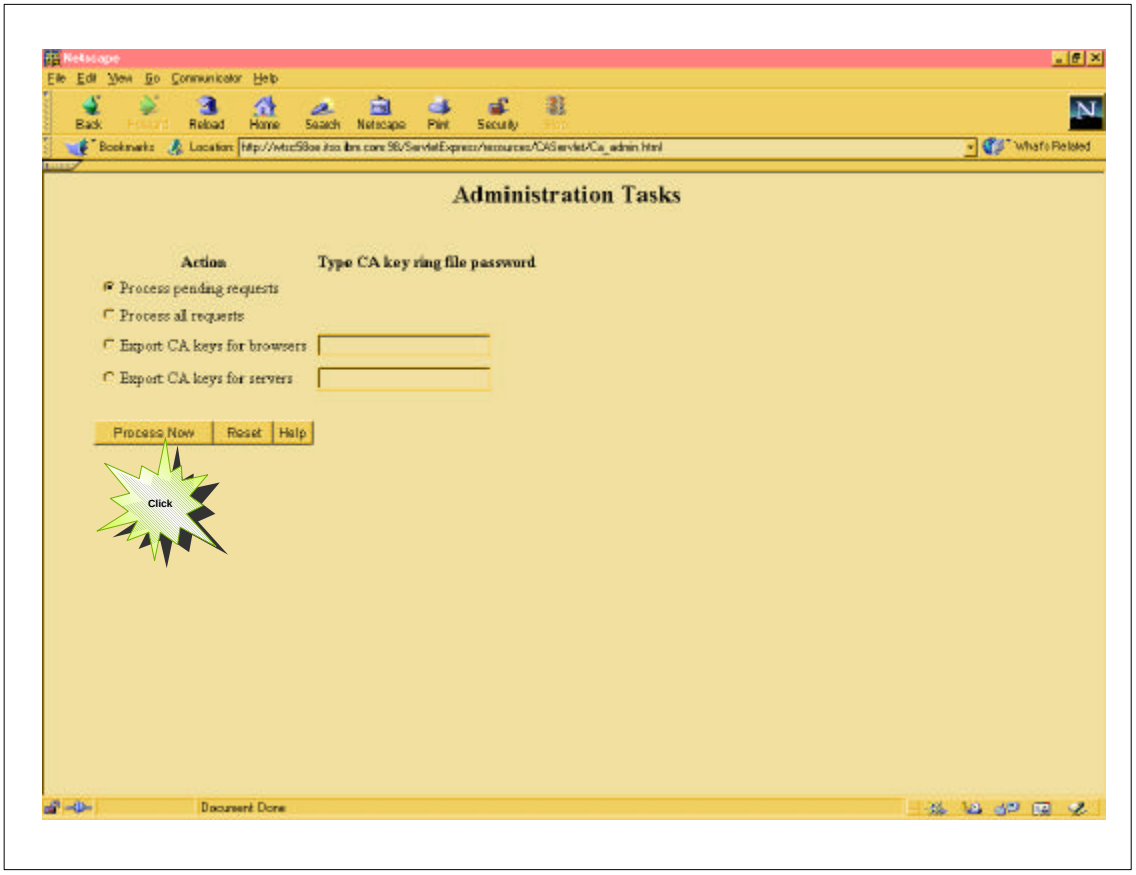
Domino Go CA

- **Administer Certificate Requests**
  - This step needs to be done if you chose not to process CA requests automatically.
    - Click on Administration
    - Authentify as WEBADM (or whatever Admin User is set in the protection setup)
    - Click on Process pending requests or Process all requests to display the list of certificate requests to be processed.
    - If there are no requests pending, the following message appears:

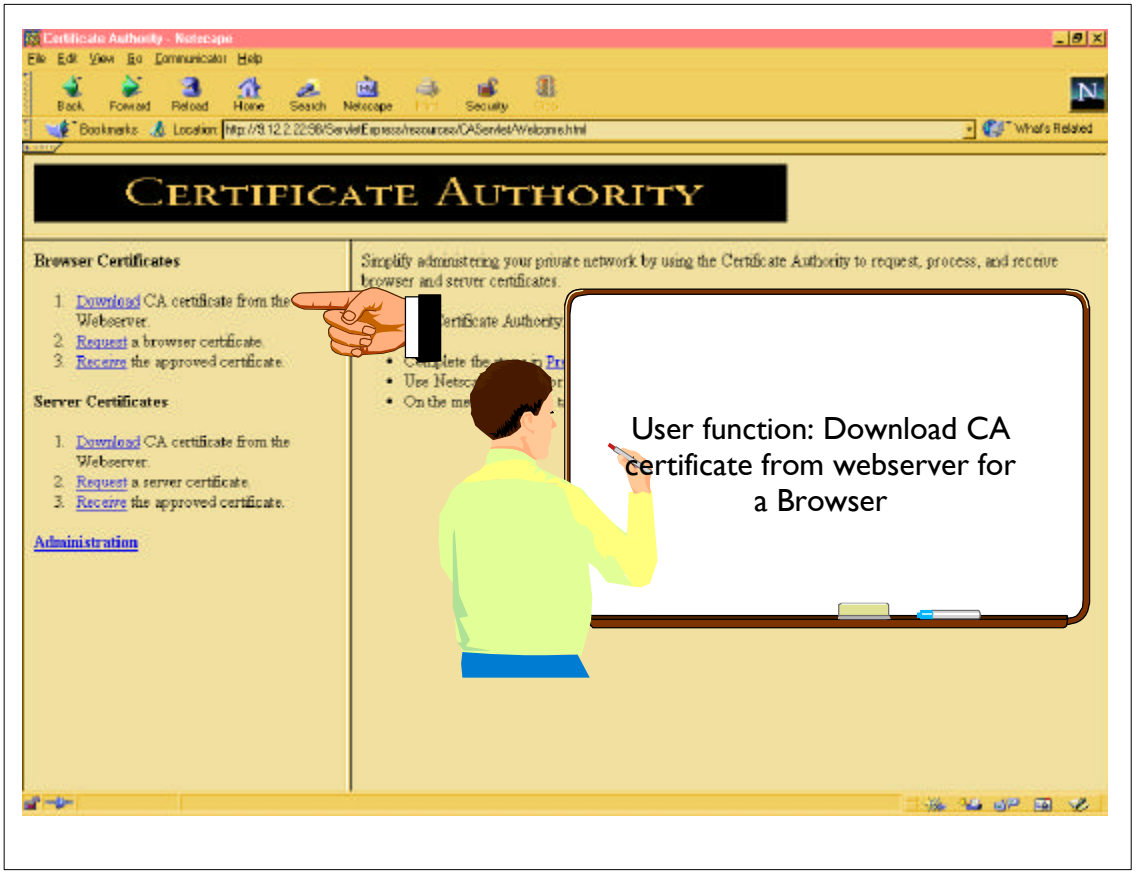
```
Unable to read and/or write database
```

    - If you selected Process pending requests and there are pending requests, then you may click Defer, Approve or Deny those requests.
    - If you selected Process all requests, you may click on Keep, or Delete those requests.

Roland Trauner trauner@us.ibm.com



- Process pending requests allows you no to Approve, Defer or Deny the certificate requests.
- Process all requests only allows to Keep or Delete those requests.
- Click on HELP for additional instructions



- The following pages show how to request and download a user (browser) certificate. It is done with the "automatic" function.
- Browser was a Netscape 4.5 US security.

Download CA Certificate

Roland Trauner trauner@us.ibm.com

- Browser function
- Varies on the Browser Model ... the following screenshots are done using a Netscape Navigator 4.5

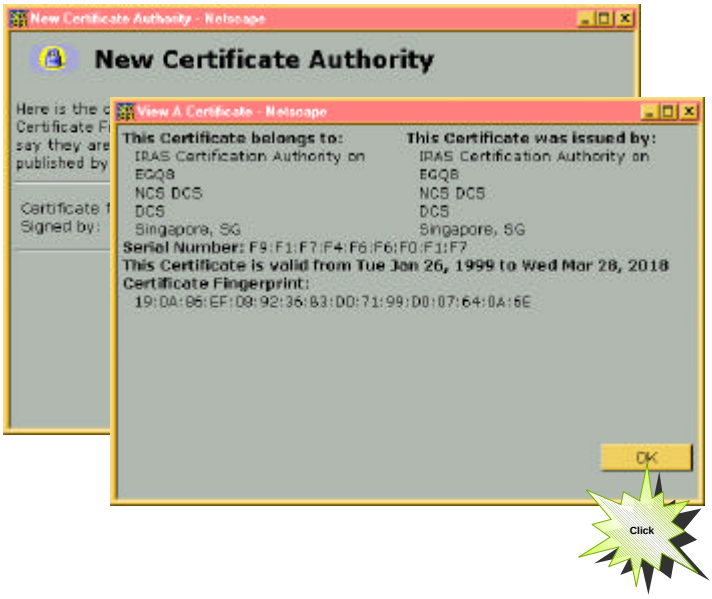
Download CA Certificate

Roland Trauner trauner@us.ibm.com

Download CA Certificate

Roland Trauner trauner@us.ibm.com

Download CA Certificate



Roland Trauner trauner@us.ibm.com

- This shows the CA certificate

Download CA Certificate

Roland Trauner trauner@us.ibm.com

Download CA Certificate

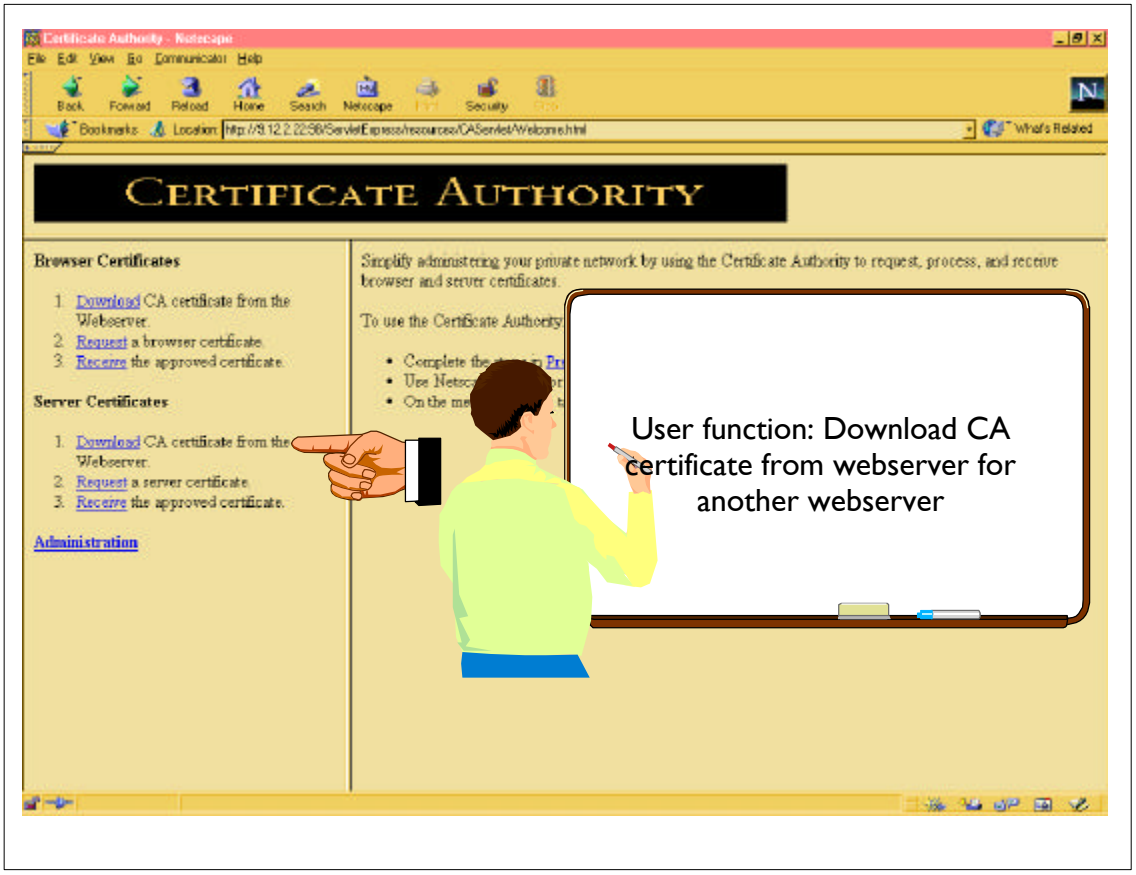
Roland Trauner trauner@us.ibm.com

Download CA Certificate

Roland Trauner trauner@us.ibm.com

Download CA Certificate

Roland Trauner trauner@us.ibm.com



- The following screenshots sho how to request and download a server certificate

- This is the cakey.txt file that have been created during "Exporting CA keys for servers".
- Use the workstation COPY funtion to copy the content of the certificate into the clipboard.
- OEDIT a new file in OS/390 UNIX
  - /web/apple/sec/cakey.txt
- Paste the clipboard content into that file.
- Save the file

Store CA Certificate

- **Store the CA Certificate into the Web Server Key Database**
  - Using Copy/Paste we created a file called cakey.txt
  - Now we can use IKEYMAN to "Store a CA Certificate" (Option 6)

Roland Trauner trauner@us.ibm.com

Store CA Certificate

```
            IBM Key Management Utility

Choose one of the following options to proceed.

   1  - Create new key database
   2  - Open key database
   3  - Change database password

   0  - Exit program

Enter your option number: 2
Enter key database name or press ENTER for "key.kdb": apple2.kdb
Enter password for the key database.......> secret
```

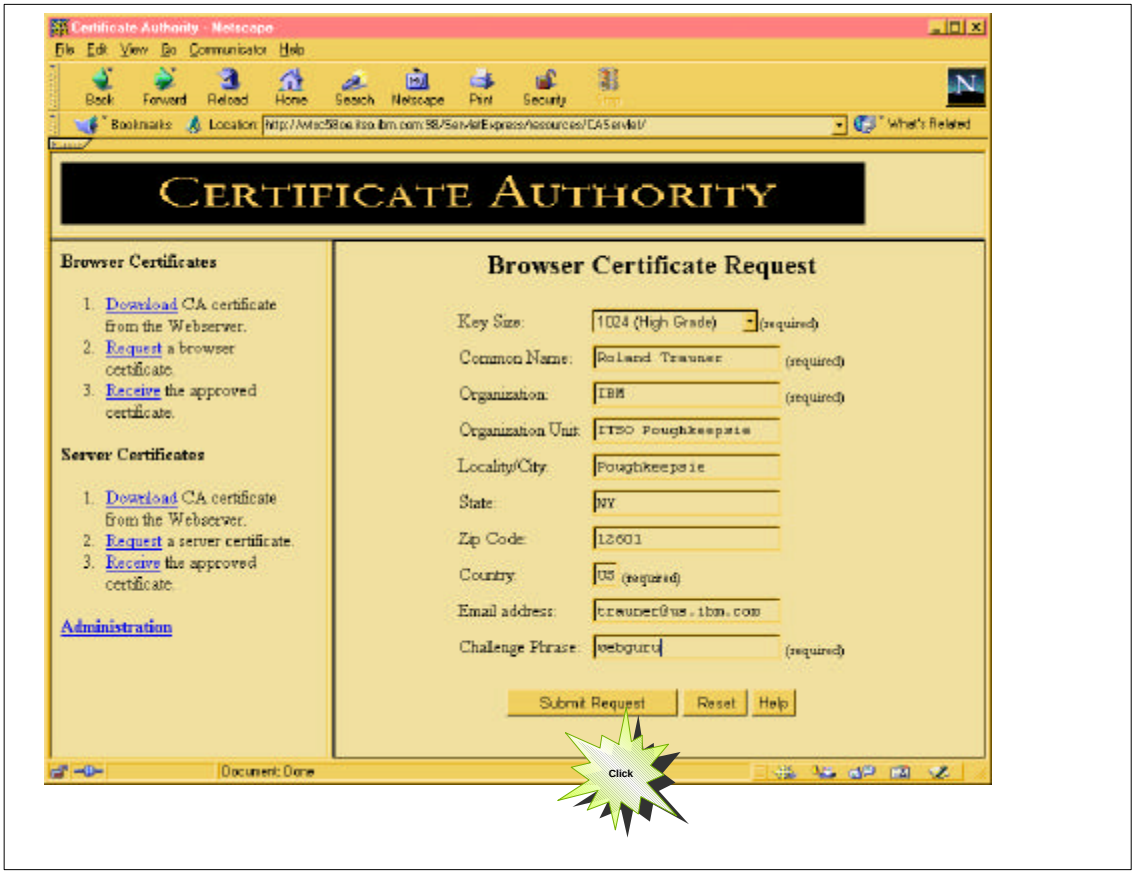

Roland Trauner trauner@us.ibm.com

Store CA Certificate

```
            Key database menu

Current key database is /web/apple/sec/apple2.kdb

     1  - List/Manage keys and certificates
     2  - List/Manage request keys
     3  - Create new key pair and certificate request
     4  - Receive a certificate issued for your request
     5  - Create a self-signed certificate
     6  - Store a CA certificate
     7  - Show the default key
     8  - Import keys
     9  - Export keys
    10  - List all trusted CAs
    11  - Store encrypted database password

     0  - Exit program

Enter option number (or press ENTER to return to the parent menu): 6
Enter certificate file name or press ENTER for "cert.arm": cakey.txt
Enter a label for this key.............> Go CA on WTSC58

Please wait while certificate is stored...

Your request has completed successfully, exit ikeyman? (1=yes, 0=no) [0]:1
```


Roland Trauner trauner@us.ibm.com


Certificate Authority - Netscape
CERTIFICATE AUTHORITY
Browser Certificates
1. Download CA certificate from the Webserver.
2. Request a browser certificate.
3. Receive the approved certificate.
Server Certificates
1. Download CA certificate from the Webserver.
2. Request a server certificate.
3. Receive the approved certificate.
Administration
Simplify administering your private network by using the Certificate Authority to request, process, and receive browser and server certificates.
To use the Certificate Authority
CA setup to process certificate requests automatically:
User function: Request a browser certificate

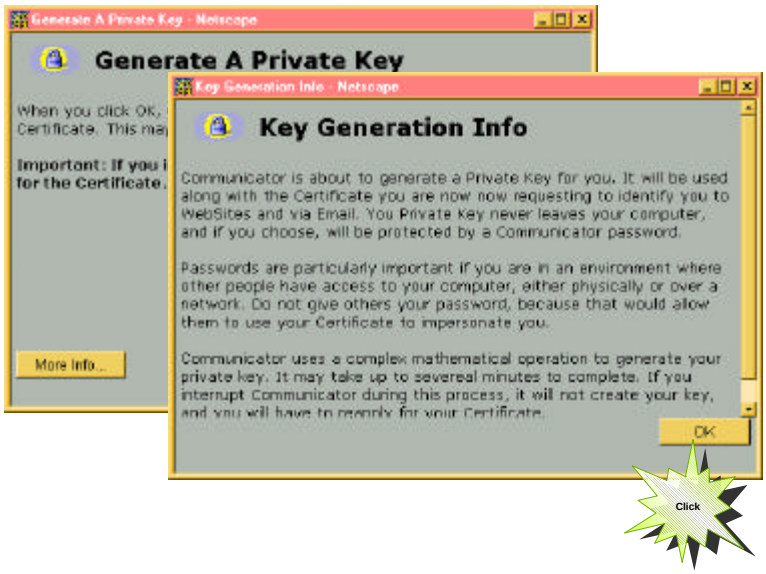


- The "Challenge Phrase" is your password at the CA

Generate a private key

Roland Trauner trauner@us.ibm.com

Generate a private key



Roland Trauner trauner@us.ibm.com

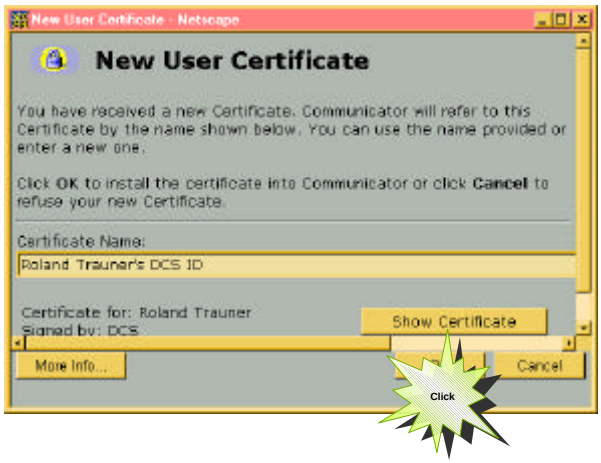
Generate a private key

Roland Trauner trauner@us.ibm.com

Generate a private key

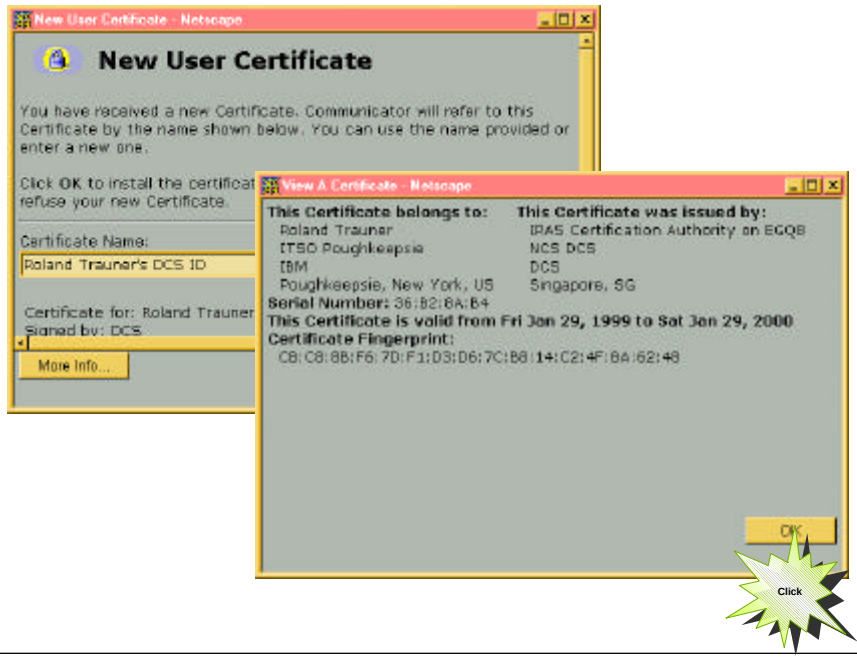
Roland Trauner trauner@us.ibm.com

New User Certificate



Roland Trauner trauner@us.ibm.com

New User Certificate



Roland Trauner trauner@us.ibm.com

New User Certificate

Roland Trauner trauner@us.ibm.com

Download User Certificate

Roland Trauner trauner@us.ibm.com

Download User Certificate

Roland Trauner trauner@us.ibm.com

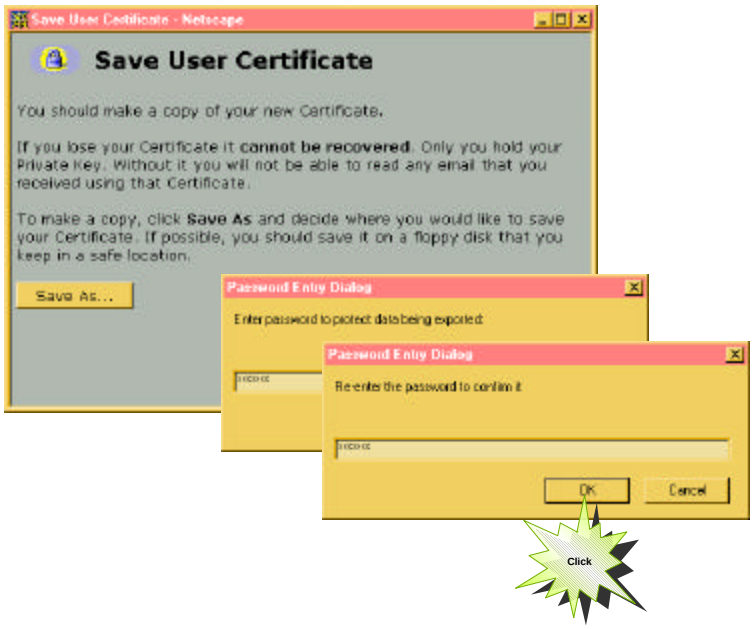
Download User Certificate

Roland Trauner trauner@us.ibm.com

Download User Certificate

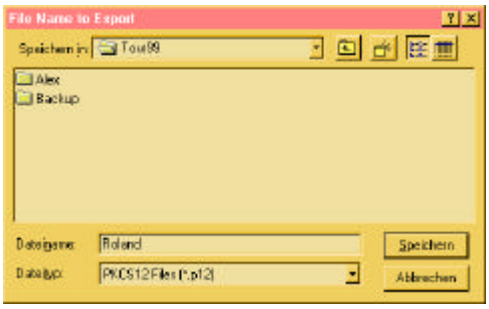
Roland Trauner trauner@us.ibm.com

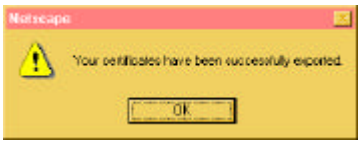
Download User Certificate



Roland Trauner trauner@us.ibm.com

Download User Certificate

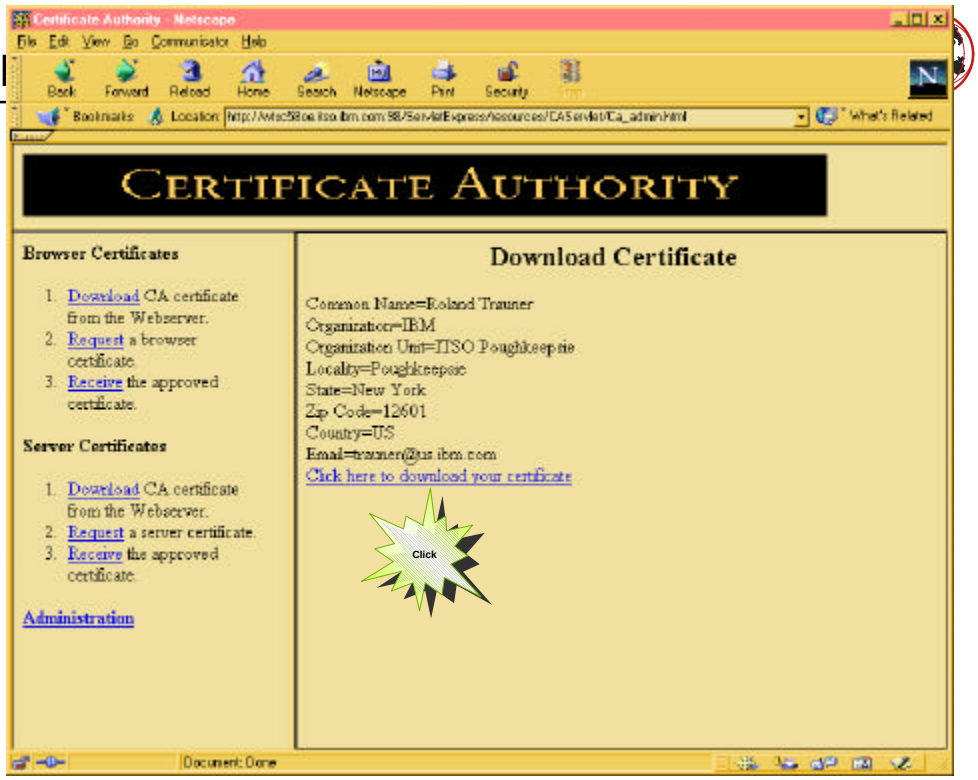




Roland Trauner trauner@us.ibm.com


Certificate Authority - Netscape
CERTIFICATE AUTHORITY
Browser Certificates
1. Download CA certificate from the Webserver.
2. Request a browser certificate.
3. Receive the approved certificate.
Server Certificates
1. Download CA certificate from the Webserver.
2. Request a server certificate.
3. Receive the approved certificate.
Administration
Simplify administering your private network by using the Certificate Authority to request, process, and receive browser and server certificates.
To use the Certificate Authority
CA setup to process certificate requests automatically:
User function: Receive the approved certificate

Roland Trauner trauner@us.ibm.com



Roland Trauner trauner@us.ibm.com

/CAServet/cert Directory

Roland Trauner trauner@us.ibm.com