



Session: 406152

## Configuring the iSeries Access Servers to Use SSL

David Boutcher, Jeff Van Heuklon,  
Carol Woodbury

© Copyright IBM Corporation, 2003. All Rights Reserved.  
This publication may refer to products that are not currently  
available in your country. IBM makes no commitment to  
make available any products referred to herein.



## Objectives

- Using a local Certificate Authority (CA)
  - ▶ Create a local CA on your iSeries
  - ▶ Create a system certificate
  - ▶ Install server certificates
  - ▶ Assign certificates to applications (iSeries Access Servers)
  - ▶ Install the Local CA certificates
    - On your PC
    - In iSeries Access
- Setting up PC5250 Client Authentication
  - ▶ Create a client certificate on your iSeries
  - ▶ Export client certificate to client
  - ▶ Enable telnet server for client authentication
  - ▶ Configure prompting modes in iSeries Access

## Objectives (continued)

- Using a well-known Certificate Authority (CA)
  - ▶ Obtain digital certificate
  - ▶ Assign certificate to applications (iSeries Access Servers)
  - ▶ Configure the iSeries Access functions to use SSL

## Server Authentication Secure Sockets Layer (SSL) Flow

### 1. The server is authenticated when

1. **iSeries Access Client** sends a secure connection request to **iSeries Access Server**

2. **Server** sends **Client** its digital certificate

3. **Client** verifies the server's certificate and determines if it trusts the issuer of the certificate



### 2. After server authentication is complete

1. Session keys are negotiated and the rest of the flows are encrypted.

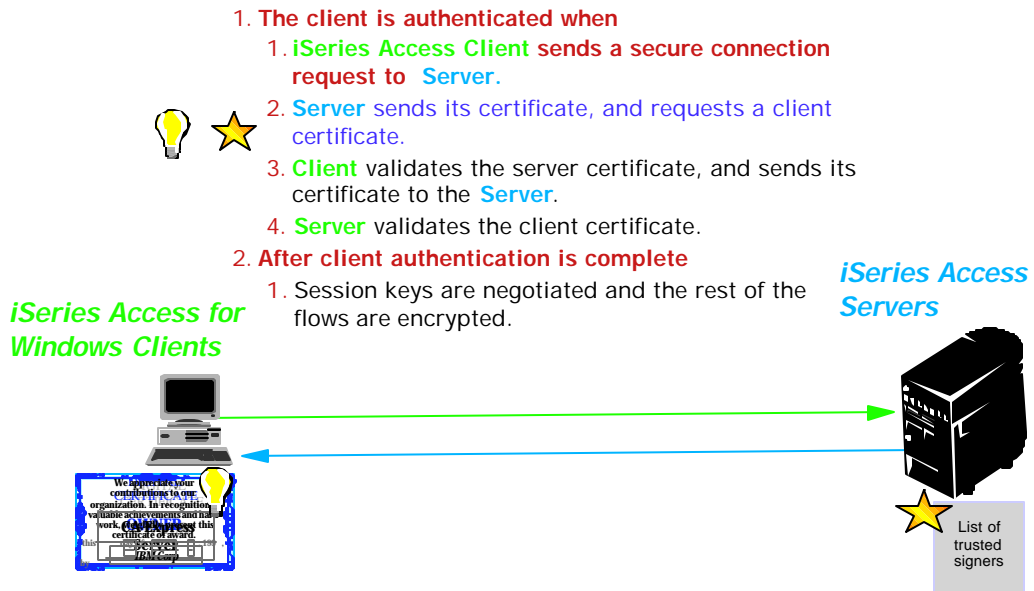
**iSeries Access for Windows Clients**



**iSeries Access Servers**

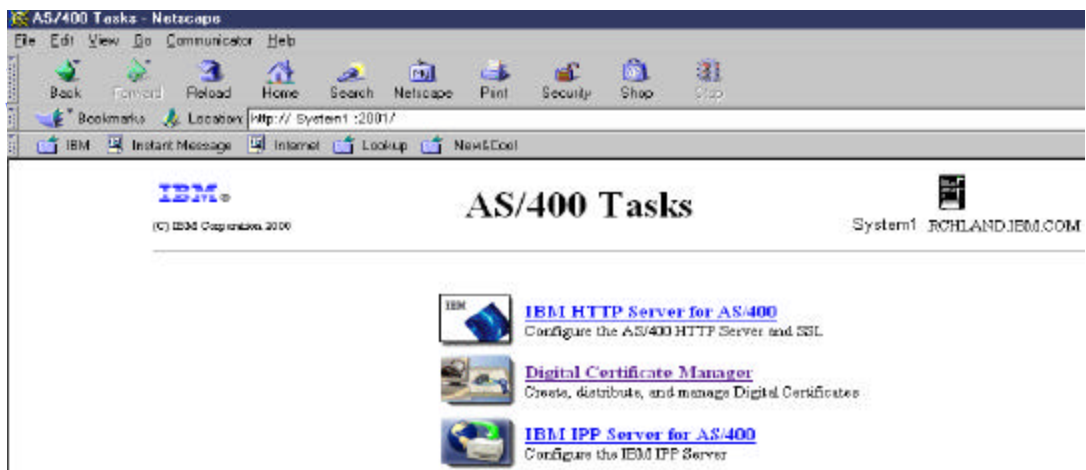
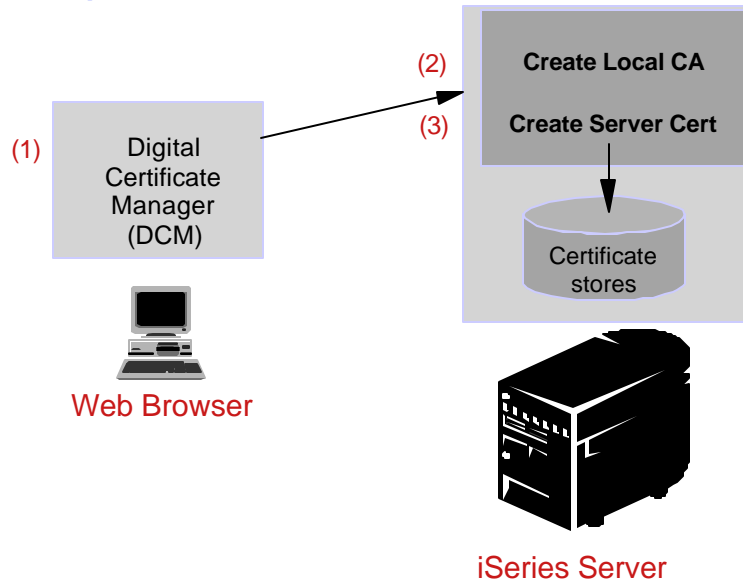


## Client Authentication Secure Sockets Layer (SSL) Flow



## Creating a Local CA on your iSeries and creating a system (server) certificate...

## Obtaining a server certificate from a local CA (the iSeries)



- Logon to the AS/400 Tasks page. Enter the URL `http://your_AS400_name:2001`
- Signon with your AS/400 userid and password (you must have \*ALLOBJ and \*SECADM)
- On the tasks page, click Digital Certificate Manager

- Click on the "Select a Certificate Store" button on the left
- Click on "Create a Certificate Authority" on the left
- Then, select "Local Certificate Authority" on the right

- Complete the form page and click OK.
- Note: Each store has its own password

■ Hint: Don't forget this password. You'll need it to work with this certificate store in the future.

**Install Local CA Certificate**

Certificate type: Certificate Authority (CA)

Certificate store: Local Certificate Authority (CA)

A certificate for your Certificate Authority (CA) was created and stored in the local Certificate Authority (CA) certificate store.

You must install the Certificate Authority (CA) certificate in your browser so the browser can verify certificates that your CA issues. Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.

[Install certificate](#)

After installing the certificate, select Continue so you can provide the policy data that will be used for signing and issuing certificates with this Certificate Authority (CA).

- The *Install Certificate* link allows you to install the CA certificate on your browser. If you want your browser to recognize certificates issued by this intranet CA, you can download the intranet CA certificate now (or do it later.)

- You can go ahead and do this, especially if you are going to have web applications that use https. However, putting the CA certificate in your browser won't help you with SSL and the Client Access Express servers. You need to get this certificate in your Client Access Express key database, which defaults to cwsslslf.kdb

- To verify that it was installed on your browser, click on the *Security* icon, then click on *Signers*.

**Note:** Installing certificate with IE will start an IE wizard for importing a certificate.

**Certificate Authority (CA) Policy Data**

Your Certificate Authority (CA) was created with the default policy data shown below. Change the data if you want and then select Continue.

Allow creation of user certificates:  Yes  No

Validity period of certificates that are issued by this Certificate Authority (CA) (1-2000):  (days)

Days until Certificate Authority (CA) expires: 1095

- Select Yes if you want to allow the creation of user certificates from this CA. This is needed for Client Authentication
- Click OK
- You have now created a local CA on your iSeries!!!

## Digital Certificate Manager



### Policy Data Accepted


Message: The policy data for the Certificate Authority (CA) was accepted.

Select Continue to create the default server certificate store (\*SYSTEM) and a server certificate signing Authority (CA). This will allow server authentication by users that use this system as a server.

- ▶ [Manage User Certificates](#)
- [Create New Certificate Store](#)
- [Create a Certificate Authority \(CA\)](#)
- ▶ [Manage CRL Locations](#)
- [Manage PKIX Request Location](#)
- [Return to AS/400 Tasks](#)

- Policy data for CA was changed message will be shown along with a list of registered applications.
- Click on Continue button

© 2003 IBM Corporation



Certificate type: Server or client  
Certificate store: \*SYSTEM

The system will create a certificate with a private key and store the certificate in the default server certificate store (\*SYSTEM)

Key size:  (bits)

Certificate label:  (required)

Certificate store password:  (required)

Confirm password:  (required)

**Certificate Information**

Common name:  (required)

Organization unit:

Organization name:  (required)

Locality or city:

State or province:  (required: minimum of 3 characters)

Country:  (required)

- ▶ [Manage User Certificates](#)
- [Create New Certificate Store](#)
- [Create a Certificate Authority \(CA\)](#)
- ▶ [Manage CRL Locations](#)
- [Manage PKIX Request Location](#)
- [Return to AS/400 Tasks](#)

- Fill out the *Create a System Certificate* form. **Note: This password is different than the CA Store.**
- Info on bottom cut off about IPV6 is for VPN. Read help on VPN for info. Ignore for now.
- Click OK

© 2003 IBM Corporation

## Configuring an Application to Use a Server Certificate ...

### Select Applications

Message Your certificate was created and placed in the \*SYSTEM certificate store.

Certificate type: Server or client

Certificate store: \*SYSTEM

Select which applications will use this certificate:

Select All

Clear All

	Application	Type	Assigned certificate
<input checked="" type="checkbox"/>	OS/400 TCP Central Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Database Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Data Queue Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Network Print Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Remote Command Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP Signon Server	Server	(None assigned)
<input checked="" type="checkbox"/>	OS/400 TCP/IP Telnet Server	Server	(None assigned)

- System Certificate created message will be shown along with a list of registered applications.
- Choose the application that will use the certificate you just created. This associates the digital certificate the server is going to use on the server authentication portion of the SSL-handshake.
- New for V5R1 - Text names are shown instead of exit point names
- Click OK



## Object Signing

### Application Status

Message The applications you selected will use this certificate.

Select Continue to create the default object signing certificate store (\*OBJECTSIGNING) and an object signing certificate signed by your Certificate Authority (CA). You can then use your system to sign objects.



- Click on Continue enable your system to sign objects
- Note: This is not needed for iSeries Access, so could be done later.

### Certificate store: \*OBJECTSIGNING

The system will create a certificate with a private key and store the certificate in the default object signing certificate store (\*OBJECTSIGNING).

Key size:  (bits)

Certificate label:  (required)

Certificate store password:  (required)

Confirm password:  (required)

#### Certificate Information

Common name:  (required)

Organization unit:

Organization name:  (required)

Locality or city:

State or province:  (required: minimum of 3 characters)

Country:  (required)

- \* Fill in form
- \* Click on OK

### Select Applications

Message Your certificate was created and placed in the \*OBJECTSIGNING certificate store.

This completes the process of setting up your system as a Certificate Authority (CA).

Users must install the Certificate Authority (CA) certificate in their browsers so their browsers can verify certificates that your CA issues.

OK

- You have now:
  - ▶ enabled the iSeries to be a CA
  - ▶ created your first server (or system) certificate signed by your CA
  - ▶ assigned that certificate to the iSeries Access servers
- After you have created your first certificate, the system creates a "\*SYSTEM certificate store." As you create more certificates or import them from well-known CAs, you will probably want to store them in the \*SYSTEM certificate store.

## Servers to enable for iSeries Access Functions

iSeries Access Function	Servers to Enable
5250 Display & Print	Sign-on, Central, Telnet
Data Transfer	Sign-on, Central, Database
Base Ops Nav	Sign-on, Remote Command
All Ops Nav Function	Signon, Remote Command, File, Print, Database, Web Admin, Mgmt Central, Directory, Data Queue
ODBC	Sign-on, Database
OLE DB	Sign-on, Database, DDM, Remote Command, Data Queue
AFP Viewer	Sign-on, Print

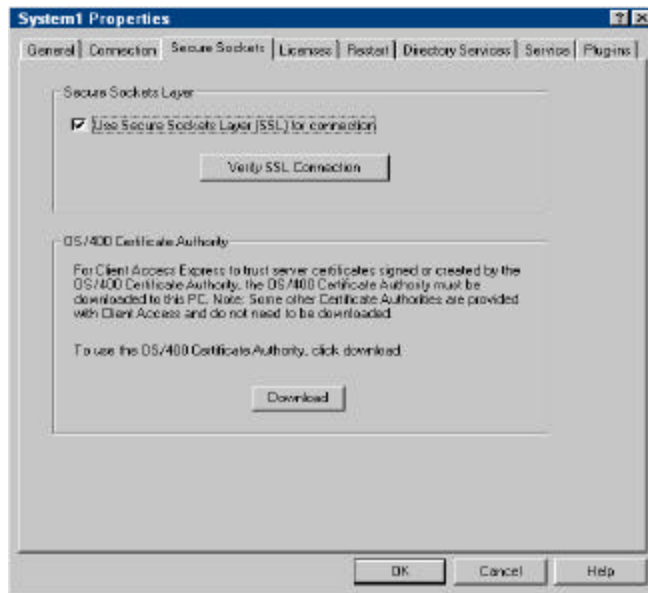
- If Application Administration is being used, then always enable Remote Command. Also, Central may be required if translation tables need to be downloaded for other languages.
- There is no harm in using the same certificate for all applications
- There is no harm in assigning a certificate to applications even if you do not intend to enable them to use SSL.

## *Getting a CA certificate into the Client Access Express Client's list of trusted signers ...*

## Installing SSL on your Client

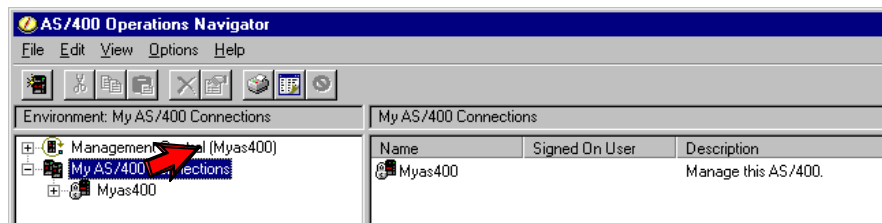
- Click on Selective Setup in the IBM iSeries Access for Windows folder.
- Follow the wizard - specify where you are going to install from
- Look for, then expand the SSL choices. Choose the encryption strength to install.
  - ▶ Hints: if SSL does not show up in the list of choices, you are either not authorized to the directory \QIBM\ProdData\CA400\Express\SSL or you need to install one of the encryption products (CE2 or CE3)
  - ▶ The encryption products must be installed from an AS/400 directory - they are not on the iSeries Access install CD.
- Verify that Secure Sockets Layer (SSL) is under the "Added components" heading
- In the iSeries Access for Windows folder you will see a new IBM Key Management icon as well as a new tab Secure Sockets in the iSeries Access for Windows Properties dialog.

## Installing CA onto client PC



- New in V5R1, a download button has been added to iSeries Navigator to easily move the CA into the 2 key databases used by iSeries Access:
  - ▶ iSeries Access key database
  - ▶ Java key database (used by Java components of iSeries Navigator)
- Right-click on system name in iSeries Navigator, and choose "Properties".
- From "Secure Sockets" tab, check box to enable SSL.
- Click on "Download" button.
- Restart iSeries Navigator for SSL to take effect for iSeries Navigator

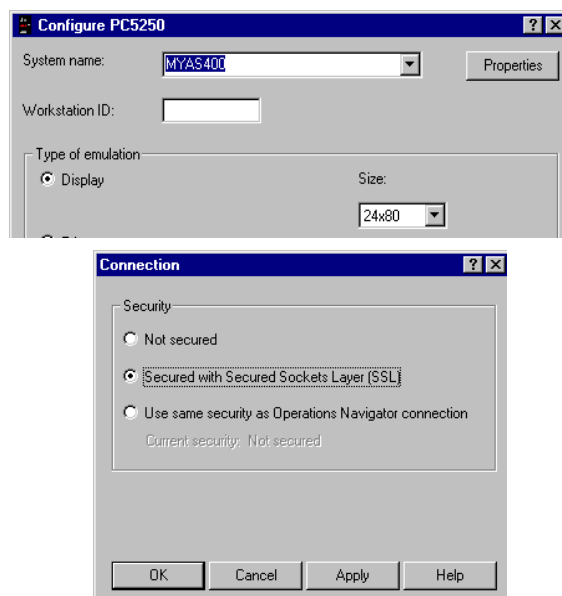
## Enabling iSeries Navigator for SSL...



- After restarting iSeries, notice the padlock on the iSeries you just configured to use SSL
- Also, once SSL is turned on in iSeries, all other iSeries Access applications that are started from that point on will also get SSL as the default (including 3rd-party apps that use iSeries Access APIs.)

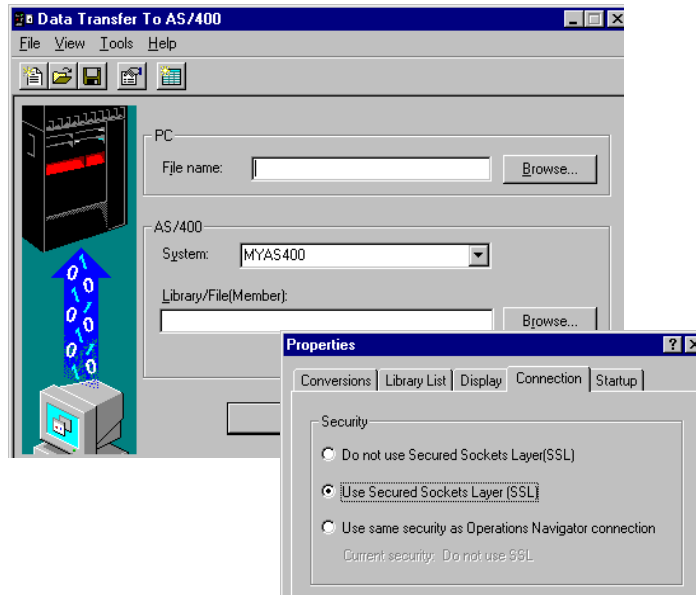
## Enabling SSL on iSeries Access functions

## Enabling PC5250 Sessions for SSL...

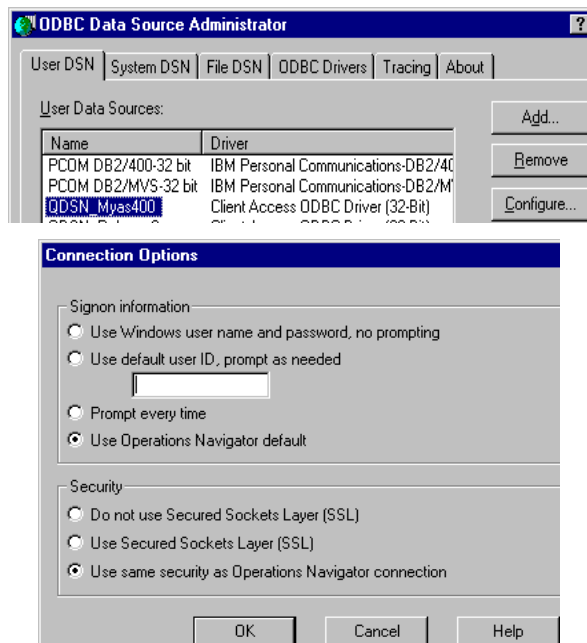


- Open your 5250 session. From the menu bar, click *Communication*, then select *Configure*
- Select *Properties*
- Click on *Secured with SSL*
- Click on *Apply* or *OK*

## Enabling Data Transfer for SSL



- Open the *Data Transfer* you want to configure to use SSL. From the menu bar, click File->Properties
- From *Properties*, click the *Connection* tab.
- From *Connection*, choose which option you want.
- Click *OK*
- You can save this data transfer by using File->Save



- Launch ODBC Administration
- Click on the *User DSN* tab
- Double-click on the user *Data Source* you want to configure to use SSL.
- Click on *Connection Options* in the *General* tab.
- Select *Use Secured Sockets Layer (SSL)* under the *Security* heading
- Click *OK*
- Close the ODBC Setup.
- Current connections must be closed and re-opened to take effect

## Creating Client Certificate for Client Authentication

## Enabling Client Authentication in DCM

- Client Authentication of the telnet server is new in V5R1
  - ▶ Enablement via commands is available with V4R4 and V4R5 PTFs.
- To enable in V5R1, start with the main DCM screen below, and click on "Create Certificate" in the left navigation pane.

## Creating User Certificate



### Digital Certificate Manager

#### Create Certificate

Select the type of certificate that you want to create.

- Server or client certificate for another AS/400  
 Object signing certificate for another AS/400  
 User certificate

Select a Certificate Store

- **Create Certificate**
- Create New Certificate Store

- Select "User Certificate" as the type of certificate.
- Click on the Continue button.

## Certificate Information

Select a Certificate Store

Expand All Collapse All

- **Create Certificate**
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- ▶ Manage User Certificates
- ▶ Manage CRL Locations
- Manage PKIX Request Location
- Return to AS/400 Tasks

Secure Connection

### Certificate Information

User name: JEFFV

Organization unit:

Organization name:  (required)

Locality or city:

State or province:  (required minimum of 3)

Country:  (required)

If you want to use this certificate for secure e-mail, enter your e-mail address.

E-mail address: (user\_name@domain\_name)

Select the key size for your web browser to use when generating the private key for your certificate.

Key size:  (bits)

- Fill out the Certificate Information. The Email address is not used by iSeries Access for Windows.
- ▶ Bottom section will only be displayed to Netscape users
- ▶ Click on Continue



## Private Key Generation



- If using Netscape, this screen is shown
- Click on OK

Select a Certificate Store

Expand All Collapse All

Create Certificate

Create New Certificate Store

### Create User Certificate

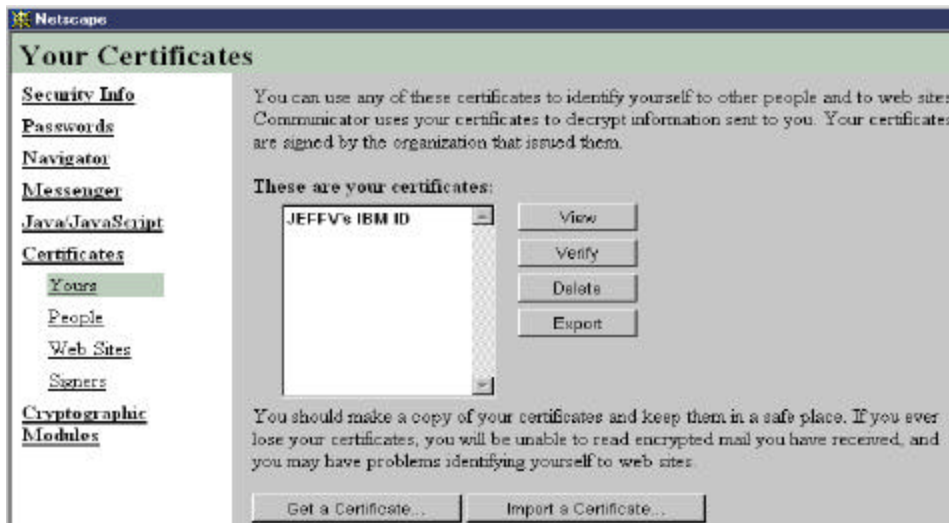
Message A user certificate was created for you.

Click the following link to install the certificate in your browser. Your web browser may display several windows to help you complete the installation of the certificate.

[Install certificate](#)

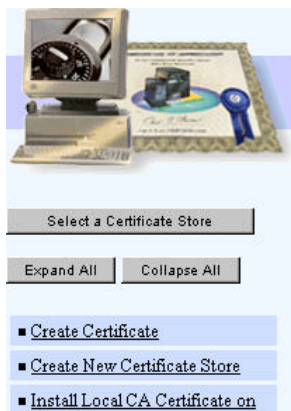
Done

Click on the Install Certificate link



- With Netscape, click on Communicator->Tools-> Security Info. Netscape will prompt for key database password too.
  - ▶ Click on the certificate, then on the Export button
  - ▶ When prompted, save the certificate as a PKCS12 file.
  - ▶ Password protect the file.

## Enabling Telnet Server for Client Authentication



### Digital Certificate Manager

#### Select a Certificate Store

Select the certificate store that you want to open.

- Local Certificate Authority (CA)
- \*SYSTEM
- \*OBJECTSIGNING
- Other System Certificate Store

Continue Cancel

- Click on "Select a Certificate Store"
- Select \*System
- Click on Continue

**Digital Certificate Manager**

**Update Application Definition**

Select the type of application that you want to update.

**Server** - Add, change, or remove certificate assignment for a server application.  
 **Client** - Add, change, or remove certificate assignment for a client application.

- Under "Manage Applications", select "Update Application Definition"
- Select "Server" in the right pane.

**Digital Certificate Manager**

**Update Application Definition**

Application type: Server

Select the application that you want to update.

	Application	Certificate Assigned
<input type="radio"/>	OS/400 TCP Central Server	System certificate
<input type="radio"/>	OS/400 TCP Database Server	System certificate
<input type="radio"/>	OS/400 TCP Data Queue Server	System certificate
<input type="radio"/>	OS/400 TCP Network Print Server	System certificate
<input type="radio"/>	OS/400 TCP Remote Command Server	System certificate
<input type="radio"/>	OS/400 TCP Signon Server	System certificate
<input checked="" type="radio"/>	OS/400 TCP/IP Telnet Server	System certificate
<input type="radio"/>	OS/400 DDM/DRDA Server - TCP/IP	System certificate
<input type="radio"/>	OS/400 Cluster Security	None assigned
<input type="radio"/>	OS/400 - Host Servers	None assigned

- Select OS/400 TCP/IP Server
- Click on "Update Application Definition" (bottom of dialog)

**Digital Certificate Manager**

Application type: Server  
 Application ID: QIBM\_QTV\_TELNET\_SERVER  
 Application description: OS/400 TCP/IP Telnet Server  
 Certificate Assigned: System certificate

**Information that can be updated:**

Client authentication required:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Define the CA trust list:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Certificate Revocation List (CRL) checking:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

---

**Application Information:**

Exit program information	
Exit program:	QTVSSL
Exit program library:	QSYS

Select "Yes" for Client Authentication Required.

**Digital Certificate Manager**

**Update Application Definition**

Message: The application was updated successfully.

Application type: Server  
 Application ID: QIBM\_QTV\_TELNET\_SERVER  
 Application description: OS/400 TCP/IP Telnet Server  
 Certificate Assigned: System certificate

**Information that can be updated:**

Client authentication required:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Define the CA trust list:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Certificate Revocation List (CRL) checking:	<input type="radio"/> Yes <input checked="" type="radio"/> No

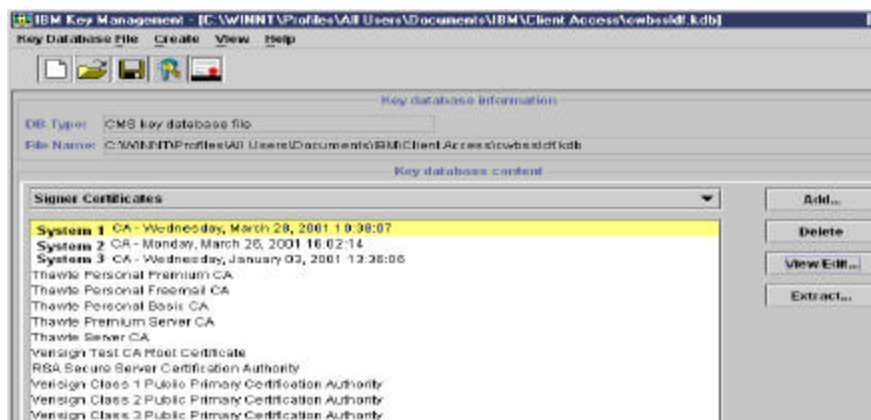
Apply

---

Application Information: Note that this will take effect immediately. Telnet does not have to be restarted.

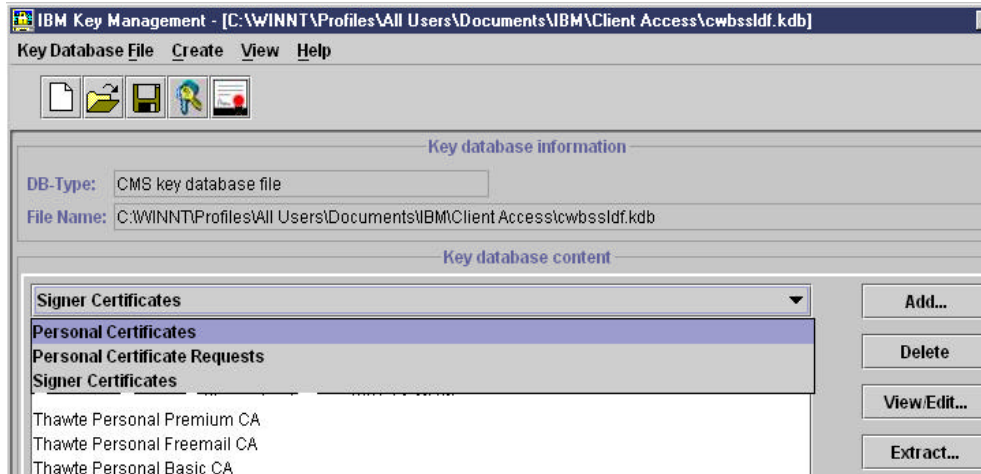
Click the Apply button

## Configuring Client Authentication on the PC



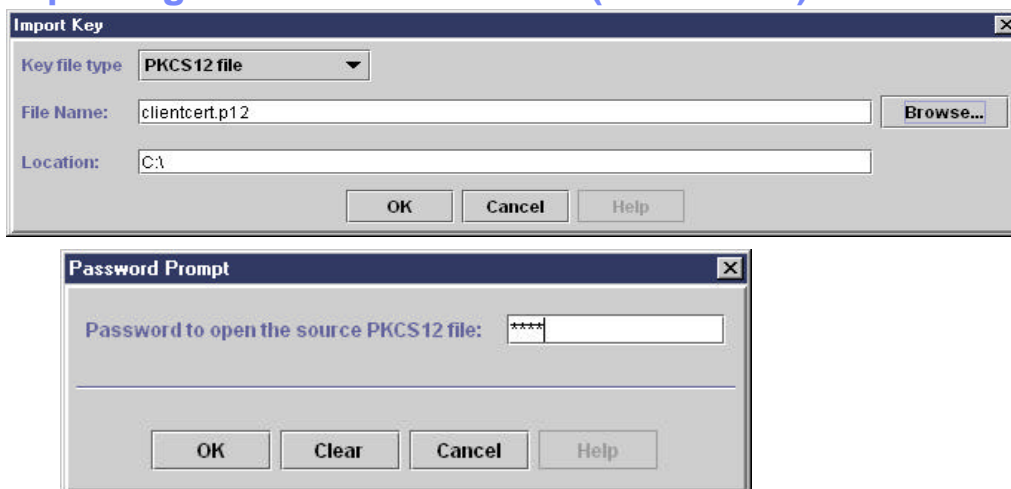
- Once the client certificate is stored in a PKCS12 file, it must be imported into the iSeries Access key database.
- The preferred way to start the IBM Key Database Management program is through Control Panel
  - ▶ Start->Settings->Control Panel, then double-click on "Client Access". Select the "Secure Sockets" tab, and then click on the IBM Key Management button
  - ▶ If you start this program an alternate way, the key database name won't be filled in by default, and you will have to browse for it.

## Importing Personal Certificate



- From the pull-down, choose "Personal Certificates"
- Then click on the "Import" button on the right

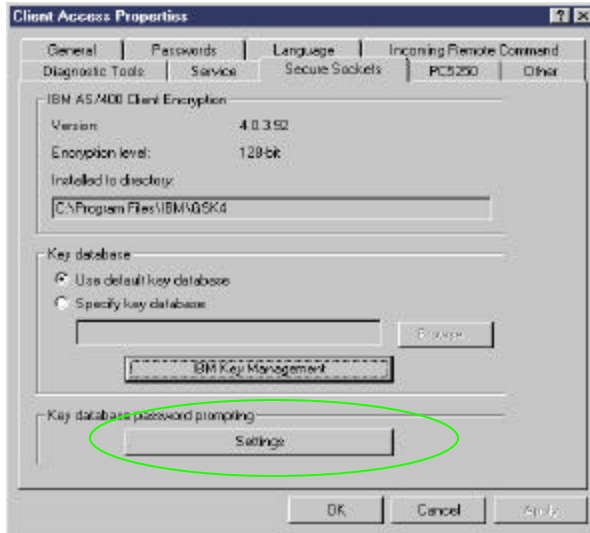
## Importing Personal Certificate (continued)



- Specify the PKCS file you saved earlier
- Enter the password you saved for it.

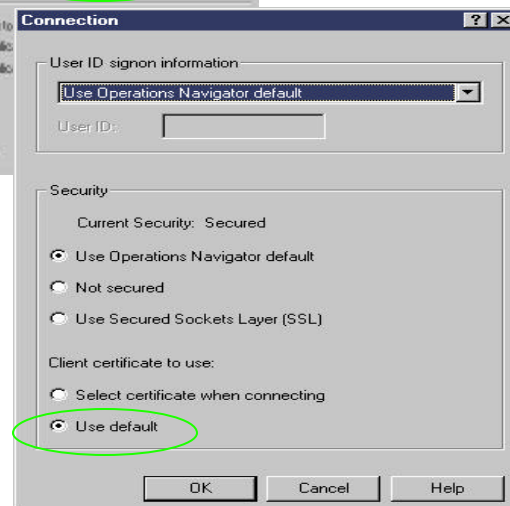
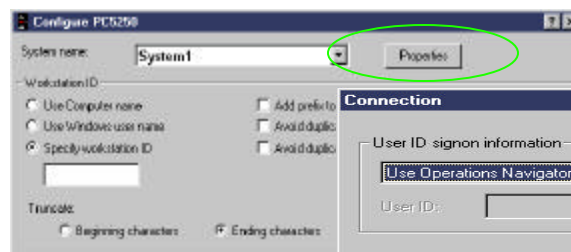
## Setting Prompting for Key Database Password

- Set the prompting mode for the key database password (optional)



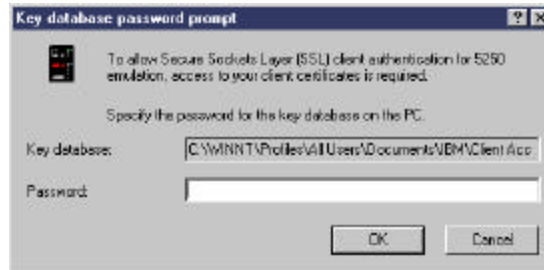
Specify how often you want to be prompted.

## Enabling Client Authentication on PC



- From PC5250 Config:
  - Click on Properties
  - Select "Use Default"
  - This is optional
  - Selecting "Select Certificate.." causes extra prompt.

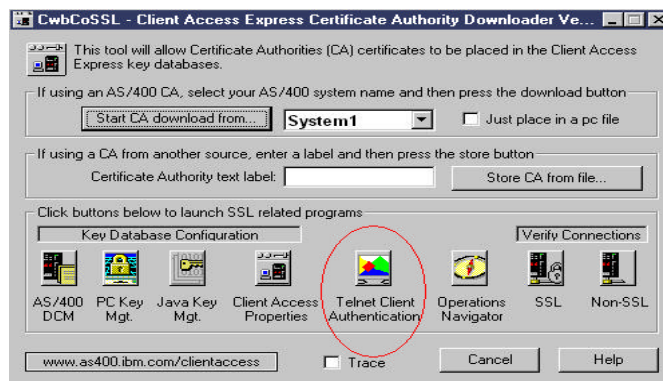
## Connecting with Client Authentication



When attempting a PC5250 connection, the above dialog appears. Enter your key database password (default password is "ca400").

## Client Authentication for V4R4/V4R5 Servers

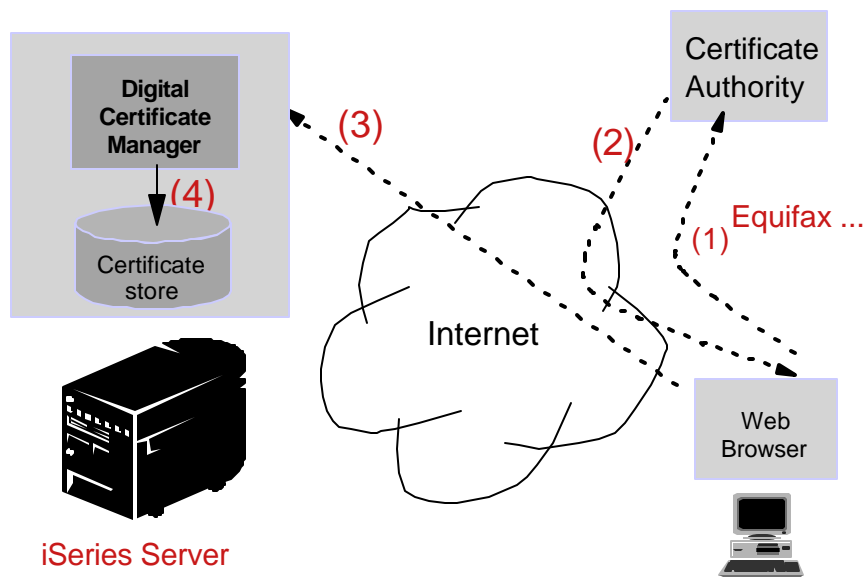
- To turn on Client Authentication on a V4R4 or V4R5 server, a command is needed to enable or disable it (no support in DCM).
  - ▶ enable: CALL PGM(QSYS/QTVSRV) PARM(\*SSLCERT)
  - ▶ disable: CALL PGM(QSYS/QTVSRV) PARM(\*NOSSLCERT)
- Alternatively, the CWBCOSSL tool can be used to enable/disable.

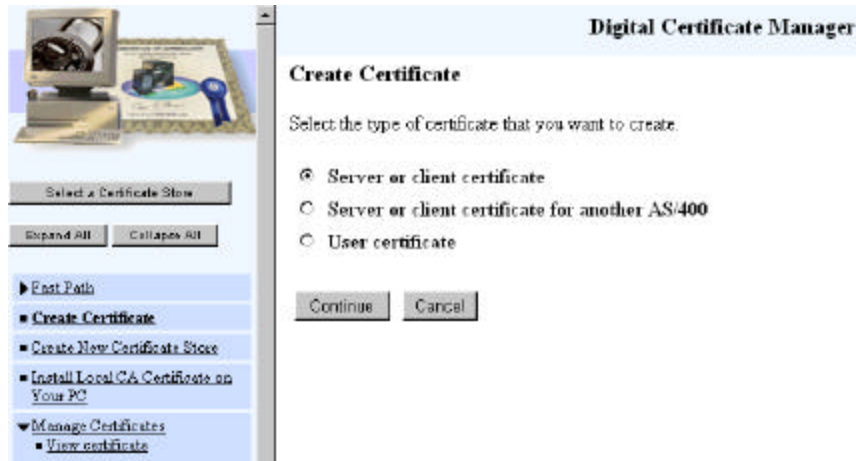




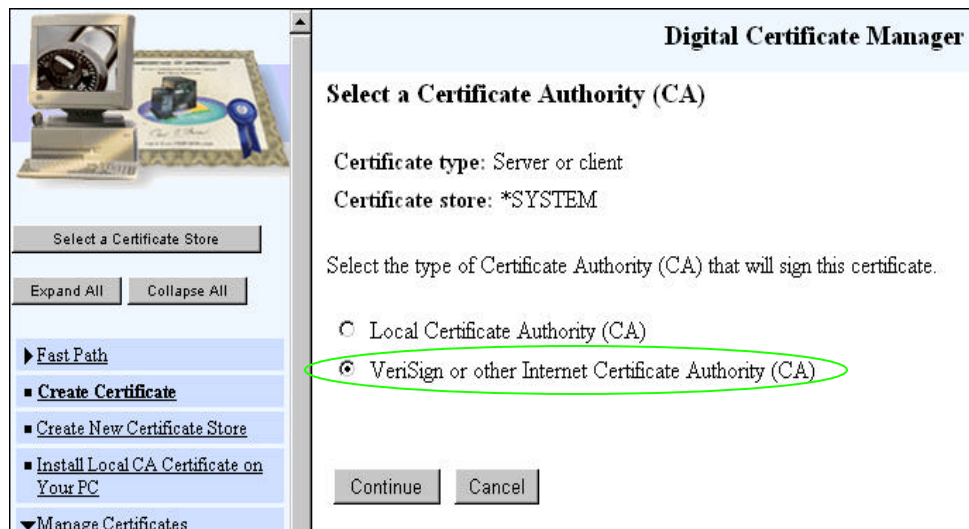
## Obtaining a certificate from a well-known CA ...

## Obtaining a server certificate from a well-known CA





- Click on "Select a Certificate Store"
- Select "\*\*System"
- Select "Create Certificate" on left
- Select "Server or client certificate"
- Click *Continue*



- Select "Verisign or other Internet Certificate Authority"
- Click on Continue

## Digital Certificate Manager

## Create a System Certificate

The system will create a public-private key pair and store the key pair in the certificate store listed below.

Certificate store: \*SYSTEM

Key size: 2048 (bits)

Key label: VeriSignCert (required)

## Certificate Information

Server name: as400.domain.com (required)

Organization unit: ITSO

Organization name: IBM (required)

Locality or city: Rochester

State or province: MIN (required: minimum of 3 characters)

Country: US (required)

Zip or postal code:

- Fill out form. Hints:
  - ▶ Server name is the TCP/IP host\_name.domain\_name of your iSeries.
  - ▶ Spell out your state
  - ▶ Don't specify the zip code
- Click OK

## Digital Certificate Manager

## System Certificate Request Created

Your certificate request data is shown below. Copy and paste the request data into the Certificate Authority that will sign your certificate request.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICrDCCA2QCAQAwZzELMAkGA1UEBhMCVVMxDTALBgNVBAsTBTE1UU08xGTAXBgNV
BANTEPGFZNDwLmRvbnR1b3R5b20wggE1MAOGCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCuyWtBLmR9Ge0MuXVzoc5OncZOTKA2w5FYJyKgw9Fq7lsaWrdEmt71
arhR3/uKr06xCe73lphpXmGcfdC63kP1nOVy8dZsnyjY9gbXR1D2dZBUEWMR8uSt
TSjWfOjdpU1ewKh1RZ5UDD+11uQ/O+gaQ3o2SYVIsy+47U8O5KBRzNjNkcpB7106
eQL9x1yYonOBD1yxkzu6W43ZhO2oPXGOvp176ZDya7kJSouW86NTQgMOYx1Ph6z
t6JYq9a73WUUB5r21y9e6NzORZtOo9Z7p0zfLKhT1HV335c2jM8J01EsRCDUQ1jL
7AEWr7rCt5SMb4dstjyf7LX9P1mDAgMBAAGgADANBgkqhkiG9w0BAQQAOCQAQEA
j17W1f1R5y0zcbKv0GHZ8TBoPBeJNbVBJE1b6TX644G/fvGY/BA4rYraEdv8NN1v
ZyKNt7TG2JIMwXbHJHJNMePICzoq71JvcGtQIA/ZmyyhTOU7tCsk9u5LO110tjMu
Go3K1zBFLUtXQ6s4x6QMFyWvayKFR8WNS8tVa72XtgQhHv60T7RNspH0UmzMQ+e1
8J9p31DYwRgBuUDL5eygsur821RH1QxOGW5qdgUXdWSdpnxcRjSwnHcOU9dWBNhM
BO3vCKevggnkz24DBHj28114CwYgp9VPhSjh1hcBMDmIZr348gtRNs/XV/LQCC1
rWpJGZhSxaus5bpIBnx4pQ=
-----END NEW CERTIFICATE REQUEST-----
```

Done

- Copy the certificate request to the clipboard.
- MAKE SURE you select the area that includes "BEGIN NEW CERTIFICATE REQUEST" through the area that ends with "END NEW CERTIFICATE REQUEST -----"
- Some Internet CAs refer to this certificate request as Certificate Signing Request (CSR).

Back Forward Home Search Help Security Help

Bookmarks Netsite: https://digitalid.verisign.com/server/trial/trialStep2.htm

## Enrollment

---

### Step 2 of 5: Submit CSR

Before you Start

Step 1: Generate CSR

• Step 2: Submit CSR

Step 3: Complete Application

Step 4: Install Test CA Root

Step 5: Install your Test Server ID

---

**Submit CSR**

When you generated the CSR in Step 1: Generate CSR, your server software either e-mailed the CSR to you, or created a request file on your hard disk (such as key.req). Open the CSR file with an ASCII text editor such as NotePad. (Do not use a word processor such as Word that inserts formatting or control characters.)

This is an example CSR file:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBCTCBtAIBADBPHQswCQYDVQQGEwJVUzEQMA4GA1UECBMRmxvcmlkYTEYMBYG
A1UEChMPRXI1lcyBvb1BUaGUgV2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm51dDBeMAOG
CSqGSIb3DQEBAQUAAQsAMEgCQQCojtjnHqg0GTxp+XZ56RaSe11ZWpumXjU6Sx7
v1FdXzsY1oLQoa090Jtnu1UsQRHh0yDS+45oncjKmlzCG/IZAgMBAAAGgADANBgkq
hk1G9w0BAQQFAANBAFBj9g+N1Uh8YWPFGntgf4mlUd/wqUshptjJy4PjdsD3ugy
5avvuh3G//PpGh2aYXIjHpJXTUBQyzxSEIINytc=
-----END NEW CERTIFICATE REQUEST-----
                
```

- Example of requesting a certificate from VeriSign at [www.verisign.com](http://www.verisign.com)

Description	
<p><b>Enter CSR Information:</b> Copy the entire contents of the CSR file including the lines that contain the begin and end statements into the field on the right.</p>	<pre style="font-family: monospace; font-size: x-small;"> -----BEGIN NEW CERTIFICATE REQUEST----- MIICrDCCAZQCAQAwZzELMakGA1UEBhMCVVMxDDAKBgNVB ExMJU9jaGVzdGVyMQwwCgYDVQQKEwNJKkOxDTALBgNVB EAMTEGFZNDAwLmRvbWVpb15jb20wgGEiMAOGCSqGSIB3D AoIBAQCuyWtBLLmRRo9Ge0MuXVzoc5OnaCzOTKA2w5FYJ arhKb/uKr06xCe73lphpXmGcfDC63kPinOVy8dZsnyjY9 T5jWf0jdpU1ewKhirZ5UDD+11uQ/0+gaQ3o2SYVISy+47 eQL9x1yYon0BD&amp;1yxkzu6W43ZhO2oPXGOvp176ZDya7kK t6JYq9a73WUUB5r21y9e6NzORZtOo927p0zfLKhT1HV33 7AEWr7rCt5SMb4dstjyf7LX9P lmdAgMBAAAGgADANBgkqh                 </pre>



Click the CONTINUE button to submit the CSR and proceed with the Test Server ID enrollment.



- Paste the certificate request from DCM into the box.

## Hints to this point ...

```
VeriSign Digital ID Services

-----BEGIN CERTIFICATE-----
MIICYDCCAgwCEQumleUwZE+x/7E01ofUDCwDQYJKoZIhvcNAQEEBQAwgaxxFjAU
BgNVBAsTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52Zkxpc2lnb15jb20w
cmVwb3NpdG9yeS9SUZKN0Q1BTIE1uY29ycC4gQmVzUmVhLiBhMAwFIlIEMVEQuHUYw
RAYDVQQLZ21Gb3IyYmVyaVNoZ24gYXV0aG9yaXplZCB0ZXR0aW50aW50aW50aW50
IGFzc3VyYW5jZXN0aG9yaXplZCB0ZXR0aW50aW50aW50aW50aW50aW50aW50aW50
NlRk10VGVwcm90aG9yaXplZCB0ZXR0aW50aW50aW50aW50aW50aW50aW50aW50
EzQJUn9jaGVzIG9yaXplZCB0ZXR0aW50aW50aW50aW50aW50aW50aW50aW50aW50
HrYDQDEPb3QhBU1JDMi5SQ0hN0U5ELk1CT55DT00wgZ8wDQYJKoZIhvcNAQEE
EQADgYQAMIGIAoGBAKsn+sRqW9ByVK1PZaQ89to/VdB0808wmIvIdbHREC0cFwI6
g9OLK2UK1fUTIEzcy+p9hy641buZS4DYTWOKH12rJjuMkC/E2mKCOu+rE8igsW7l
501C6pgSkujwQQGBCvcQt0F7AisDTrGaw1rAltENO7NA2eaCPAzSCrml1frAgME
AAEwDQYJKoZIhvcNAQEEBQADQOBiB1HDPaw5pc+gQ4v1ssYb66gGoFxsaeT8xHv4
VW2yEaxMVLzj5YVf3liYG2eJA8MdfUmLInoEQHwXSgv2ZJQN
-----END CERTIFICATE-----
```

- You will be sent a certificate to the e-mail address you specified in the server certificate request.
- Cut and paste the certificate into a .txt file on your PC.
- ftp or map a drive to your iSeries to store the file in IFS

ne Search Netscape Print Security Stop

/as400:2001/QIBM/ICSS/Cert/Admin/qycum1.ndm/main0

### Digital Certificate Manager

**Receive a System Certificate**

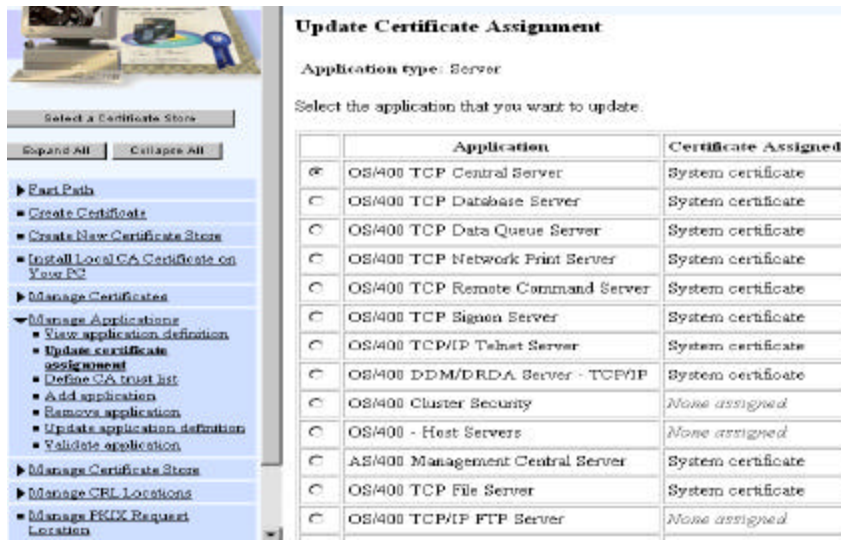
Use this form to receive a system certificate into a certificate store after the certificate has been signed by a Certificate Authority. Before using this form, you must copy the signed certificate into a file which you specify below.

Certificate store: \*SYSTEM

Signed certificate path and file name:  (required)

OK Cancel

- Back in DCM, click on "Select a Certificate Store", and select \*System
- In the left panel, select "Manage Certificates", then *Import Certificate*
- On the *Import Certificate* form, specify the path name of the IFS file name where you placed the certificate sent back to you by the well-known CA
- Click *OK*
- Now DCM takes the VeriSign certificate and puts it in the \*SYSTEM certificate store



**Update Certificate Assignment**

Application type: Server

Select the application that you want to update.

	Application	Certificate Assigned
<input checked="" type="radio"/>	OS/400 TCP Central Server	System certificate
<input type="radio"/>	OS/400 TCP Database Server	System certificate
<input type="radio"/>	OS/400 TCP Data Queue Server	System certificate
<input type="radio"/>	OS/400 TCP Network Print Server	System certificate
<input type="radio"/>	OS/400 TCP Remote Command Server	System certificate
<input type="radio"/>	OS/400 TCP Signon Server	System certificate
<input type="radio"/>	OS/400 TCP/IP Telnet Server	System certificate
<input type="radio"/>	OS/400 DDM/DRDA Server - TCP/IP	System certificate
<input type="radio"/>	OS/400 Cluster Security	None assigned
<input type="radio"/>	OS/400 - Host Servers	None assigned
<input type="radio"/>	AS/400 Management Central Server	System certificate
<input type="radio"/>	OS/400 TCP File Server	System certificate
<input type="radio"/>	OS/400 TCP/IP FTP Server	None assigned

- Click on *Update certificate assignment* under "Manage Applications"
- Select the Client Access Express Servers that you need.
- Click on *Update certificate assignment* button at the bottom

***If you are using a well-known CA, configuration is complete and you are ready to go!!!***

## Software Requirements

- OS/400 release V4R4 or later
- IBM HTTP Server for AS/400 (5769-DG1)
- Digital Certificate Manager (5769-SS1, option 34)
- IBM Cryptographic Access Provider (5722-AC2 or AC3)
- AS/400 Client Encryption (5722-CE2 or CE3)

Note: If using V4R4 or V4R5, then there will also be AC1 and CE1 products available. Also the product numbers will be 5769 instead of 5722. 5722 is new for V5R1.

## For More Information

- **AS/400 Client Access Express for Windows: Implementing V4R4, SG24-5191 (redbook)**
- [www.as400.ibm.com/clientaccess](http://www.as400.ibm.com/clientaccess)
- Webmaster's Guide, GC41-543
- Tips and Tools for Securing Your AS/400, SC41-5300
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure, SC24-5659 (redbook)**
- [www.as400.ibm.com/infocenter](http://www.as400.ibm.com/infocenter)
- [www.as400.ibm.com/http](http://www.as400.ibm.com/http)
- [www.software.ibm.com/network/hostondemand](http://www.software.ibm.com/network/hostondemand)
- [www.software.ibm.com/network/pcomm](http://www.software.ibm.com/network/pcomm)
- [www.as400.ibm.com/tcpip](http://www.as400.ibm.com/tcpip)
- [www.as400.ibm.com/ebusiness/security](http://www.as400.ibm.com/ebusiness/security)
- [www.rsa.com](http://www.rsa.com)
- [www.verisign.com](http://www.verisign.com)
- [www.entrust.com](http://www.entrust.com)
- [www.thawte.com](http://www.thawte.com)

## *Appendix: How to manually copy CA to PC (Alternative to using "Download" button)*

Digital Certificate Manager



### Install Local CA Certificate on Your PC

**To install (receive) the certificate on your browser:**

Click the following link to install the certificate in your browser. Your web browser will complete the installation of the certificate.

[Install certificate](#)

**To copy and paste the certificate to a file on your PC:**

If you need the Certificate Authority (CA) certificate for a non-browser application such as Personal Communications, choose the Copy and paste certificate link. Use the online help application for information about working with your certificate file. Click the following link on your PC.

[Copy and paste certificate](#)

Select a Certificate Store

Expand All Collapse All

- Create Certificate
- Create New Certificate Store
- **Install Local CA Certificate on Your PC**
- ▶ Manage User Certificates
- ▶ Manage CRL Locations
- Manage PKIX Request Location

[Return to AS2900 Task](#)

- Select "Copy and Paste certificate" from DCM.
- "Install Certificate" link will not work for Client Access



## Digital Certificate Manager

### Copy and Paste CA Certificate

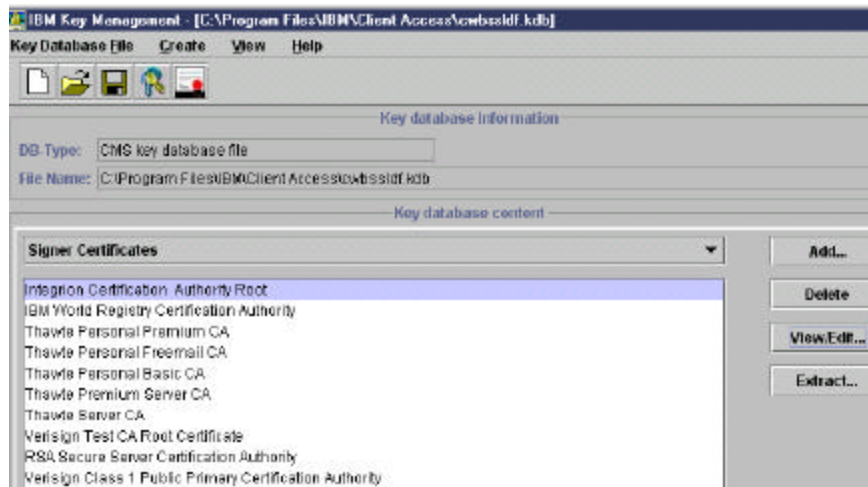
Copy and paste the CA certificate into a file on your PC. The certificate is in Base64-encoded ASCII data format.

```
-----BEGIN CERTIFICATE-----
MIICSTCCAbRgAwIBAgII06hfaVa7/s8wDQYJKoZIhvcNAQEEBQAwwZELMAkGA1UE
BhMCVVMxDDAKBgNVBAsTAA1JTjESMBAGA1UEBxMJUme9jaGVzdGVyMQwwCgYDVQQK
EwNjQ0OxETAPBgNVBAsTCFNIY3VyaXR5MRUwEwYDVQQDEwxxXb29kYnVyeVR1c3Qw
HhcNOTkwOTA2MTYzNTQ3WhcNMDIwOTA3MTYzNTQ3WjBnMQswCQYDVQQGEwJVUzEM
MAoGA1UECjBMDTU1OMRIwEAYDVQQHEw1Sb2NoZ2NoZXIyLmN0ZXIwDzAKBgNVBAsTAA1CTTER
MASGA1UECjBMTU2VjdXJpdHkxFTATBgNVBAMTDFdvb2RidXJ5SVZvZndkCnZANBgkq
hk1G9wOBAQEFAAOBjQAwGykCYEAv3G2TgtptPK65HHuWbmafcOW8bogHmEV9Ho
21kZP4PZ1qykfVdgVKp/cyWAoDbDZPcv9OJ9b3kssLDjjY1QcCbsaL21zdjfs0/
CkQFQdYVVK31tyC1cZBfa1wMbr26s3hsISsOY5yq+5eHfPnV34hTdSj9Kx6q12gHx
Cf6XdbUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQANHgm1rNzq3xhGuNaZTnDs4H6X
NDVEEZYzG899Xcx6U5wdZbh3Tp1qCQHseJ4o1Pt u9r AhQmEcx11Z2PYamTw5Y1Q
3L4E+dr r idf jLp2MFG4mRqqJEAPyBnOf rDXzNJP+EEhz17tMM68+zw4D5Pfxu5g
f1V0QL+oKg+F+hNyAg==
-----END CERTIFICATE-----
```

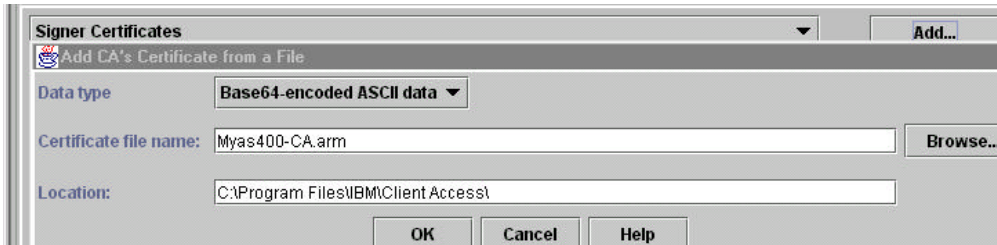


Done

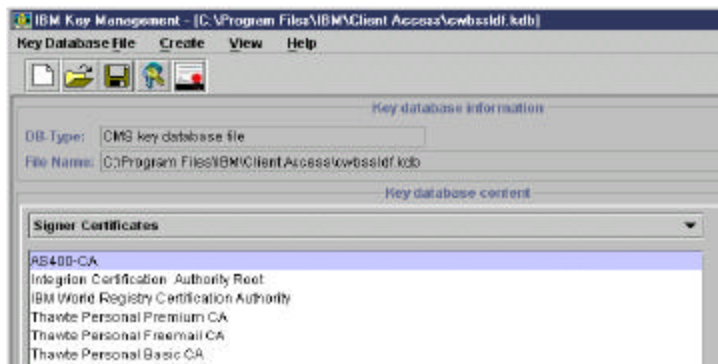
- Copy certificate from the ---BEGIN through CERTIFICATE---
- In the menu bar, click Edit->Copy
- In the task bar, click Start->Programs->Accessories->Notepad
- On the menu bar, click Edit->Paste
- On the menu bar, click File->Save As. Call the file your\_AS400\_name-CA.arm. Save in C:\Program Files\IBM\Client Access



- Go to the Client Access Express window
- Double click on the IBM Key Management shortcut (this may take a few minutes)
- Choose *Signer Certificates* from the drop down
- Click on *Add*



- In the *Location* field, enter the pathname of the CA certificate you stored earlier
- Hint: If you use the *Browse* button to find the location and click *Open*, it will fill in the pathname for you.
- Click *OK*
- Now you will be asked to provide a name (label) for the certificate
- Click *OK*



- ★ ■ The iSeries CA certificate now is in iSeries Access's list of trusted signers.
- ★ ■ Note: These steps do not put the certificate into the Java Toolbox key database, so parts of iSeries Navigator will not work over SSL.


## Trademarks and Disclaimers

© IBM Corporation 1994-2003. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

*Instruction: Refer to the following URL: <http://w3.ibm.com/legal/ipl/wtts>. Edit the list below, IBM subsidiary statement, and special attribution companies which follow so they coincide with your presentation.*

AS/400	IBM
AS/400e	IBM (logo)
eServer	iSeries
	OS/400

Lotus and SmartSuite are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

*Instruction: For a complete list of Lotus/IBM trademarks, see [www.lotus.com/lotus/information.nsf/firstpages/copyright](http://www.lotus.com/lotus/information.nsf/firstpages/copyright) and edit the above statements to coincide with your presentation.*

MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes and may be incorporated in production models.