



Session: 406152 / 25CS

iSeries. mySeries.

Configuring the iSeries Access Servers to Use SSL

David Boutcher, Jeff Van Heuklon, Carol Woodbury

© Copyright IBM Corporation, 2004. 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.

iSeries. mySeries.



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

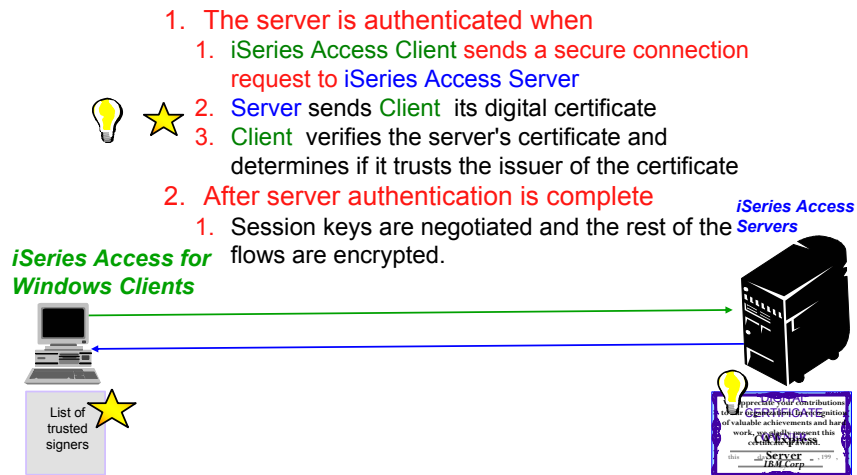
© 2004 IBM Corporation

iSeries. mySeries.

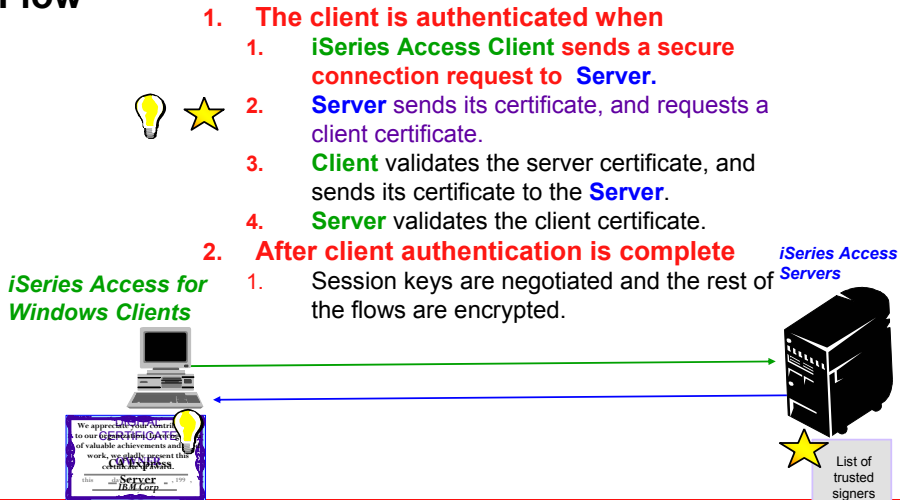
Objectives (continued)

- 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

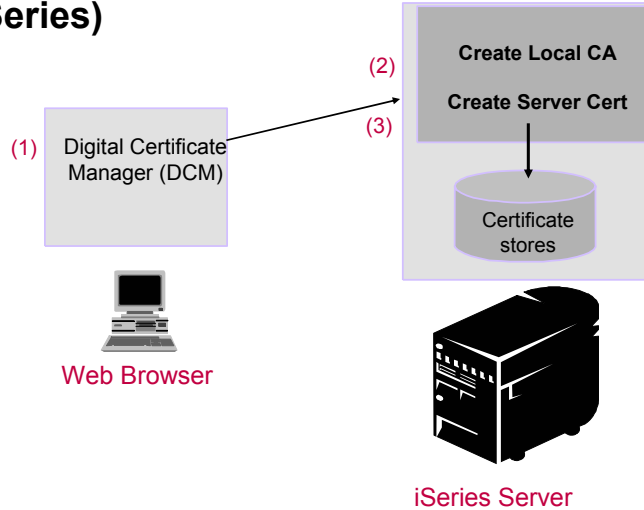


Client Authentication Secure Sockets Layer (SSL) Flow



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

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



iSeries Tasks - Microsoft Internet Explorer

File Edit View Favorites Tools Help

← Back → Search Favorites History

Address <http://System1:2001>

IBM
(C) IBM Corporation 2000

iSeries Tasks

System1 RCHLAND.IBM.COM

[IBM HTTP Server for iSeries](#)

Configure the iSeries HTTP Server and SSL

[IBM WebSphere Application Server - Express for iSeries](#)

Configure application servers and deploy applications

[Digital Certificate Manager](#)

Create, distribute, and manage Digital Certificates

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

© 2004 IBM Corporation

iSeries. mySeries.

Bookmarks Location http://System1:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

IBM Instant Message Internet Lookup New&Cool

Digital Certificate Manager

Select a Certificate Store

Expand All Collapse All

- ▶ Manage User Certificates
- Create New Certificate Store
- Create a Certificate Authority (CA)
- ▶ Manage CRL Locations
- Manage PKIX Request Location

[Return to AS/400 Tasks](#)

Secure Connection

5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1 (C) Copyright IBM Corporation 1997, 2000
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

Contains software from RSA Data Security, Inc.

Getting Started

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

Digital Certificate Manager

Certificate store: Local Certificate Authority (CA)

The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.

Select a Certificate Store

Expand All Collapse All

- ▶ Manage User Certificates
- Create New Certificate Store
- Create a Certificate Authority (CA)
- ▶ Manage CRL Locations
- Manage PKIX Request Location

[Return to AS/400 Tasks](#)

Secure Connection

Key size: 1024 (bits)

Certificate store password: ***** (required)

Confirm password: ***** (required)

Certificate Information

Certificate Authority (CA) name: COMMON 2001 (required)

Organization unit: Client Access

Organization name: IBM (required)

Locality or city: Rochester

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

Country: US (required)

- 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).

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

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

© 2004 IBM Corporation

iSeries. mySeries.



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) (I-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!!!

© 2004 IBM Corporation

iSeries. mySeries.



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 signed by your Certificate Authority (CA). This will allow server authentication by users that use this system as a server.

Select a Certificate Store

- ▶ 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

© 2004 IBM Corporation

iSeries. mySeries.



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 (*SY

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 charac

Country: (required)

Select a Certificate Store

- ▶ 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

© 2004 IBM Corporation

iSeries. mySeries.



Configuring an Application to Use a Server Certificate ...

© 2004 IBM Corporation

iSeries. mySeries.

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.
- Click OK



Series. mySeries.



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.

Continue

Cancel

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

© 2004 IBM Corporation

iSeries. mySeries.

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

© 2004 IBM Corporation

iSeries. mySeries.

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.
- List of port numbers is in I112227 at:



Getting a CA certificate into the iSeries Access for Windows Client's list of trusted signers ...

© 2004 IBM Corporation

iSeries. mySeries.



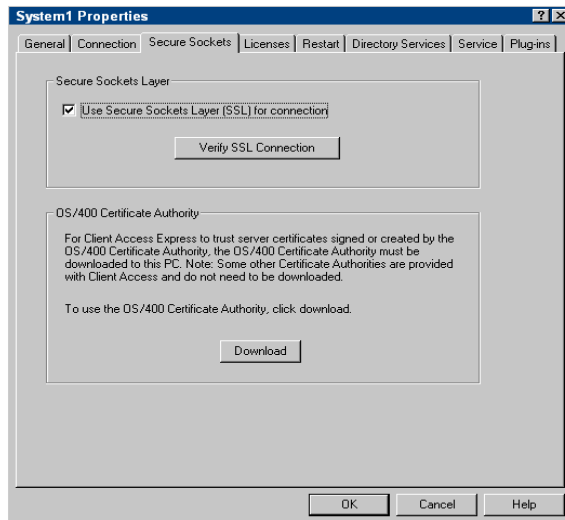
Installing SSL on your Client

- 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 in V5R2 and earlier.
 - For V5R3, the SSL component is shipped on that 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.

© 2004 IBM Corporation

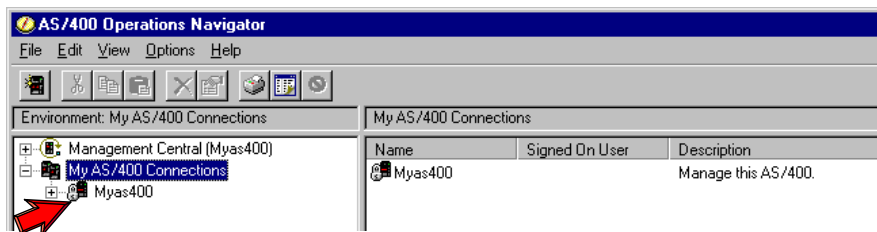
iSeries. mySeries.

Installing CA onto client PC



- A download button is available in 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.)



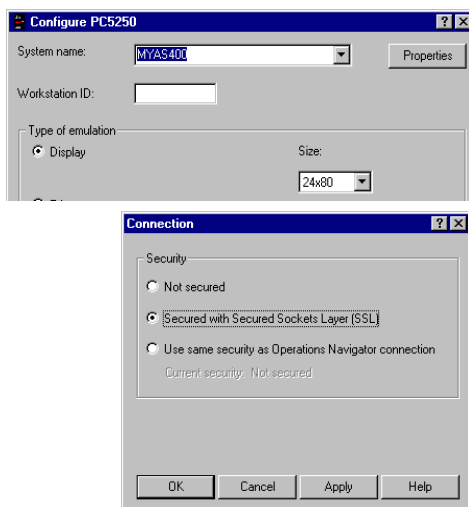
Enabling SSL on iSeries Access functions

© 2004 IBM Corporation

iSeries. mySeries.



Enabling PC5250 Sessions for SSL...

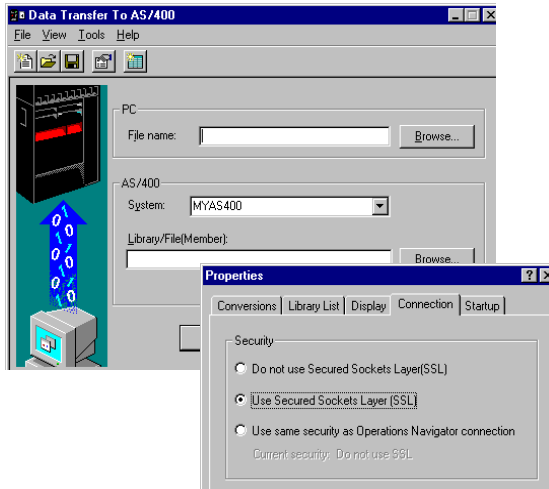


- Open your 5250 session. From the menu bar, click *Communication*, then select *Configure*
- Select *Properties*
- Click on *Secured with SSL*
- Click on *Apply* or *OK*.

© 2004 IBM Corporation

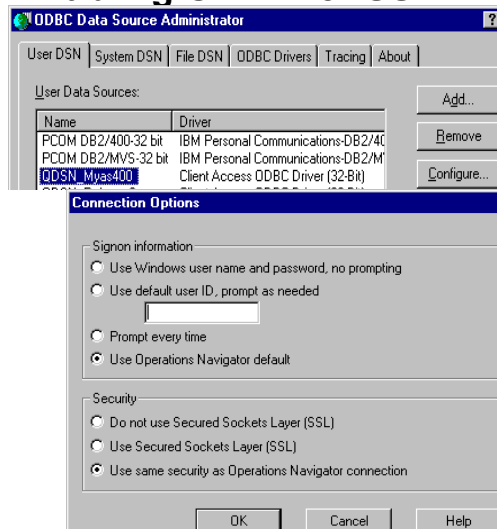
iSeries. mySeries.

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

Enabling ODBC for SSL



- 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

© 2004 IBM Corporation

iSeries. mySeries.



Enabling Client Authentication in DCM

- Client Authentication of the telnet server is available on V5R1 and later
- Start with the main DCM screen below, and click on "Create Certificate" in the left navigation pane.



Digital Certificate Manager



5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1 (C) Copyright IBM C
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADF Schedule (C)
Licensed Materials - Property of IBM



Contains software from RSA Data Security, Inc.

Getting Started

© 2004 IBM Corporation

iSeries. mySeries.

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

Expand All Collapse All

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

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

Certificate Information

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

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
- With Internet Explorer, this screen will not appear



Create User Certificate

Message A user certificate was created for you.

Select a Certificate Store

Expand All Collapse All

Create Certificate

Create New Certificate Store

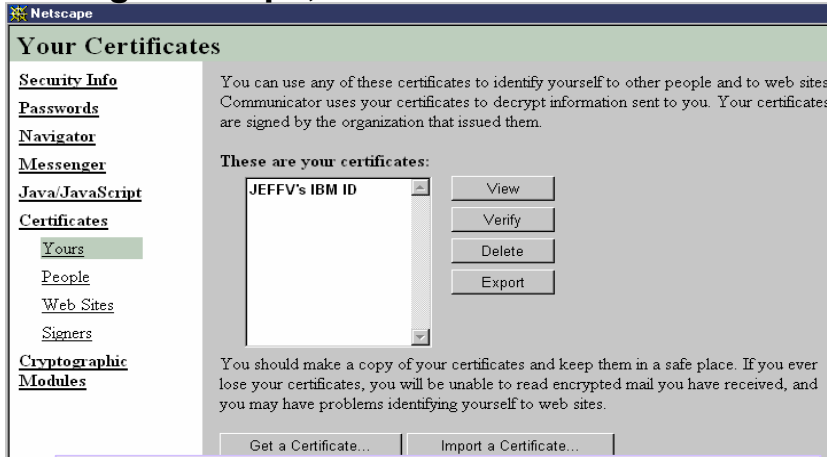
Click the following link to install the certificate in your browser. Your web browser may display several windows to help you complete the installation of the certificate.

[Install certificate](#)

Done

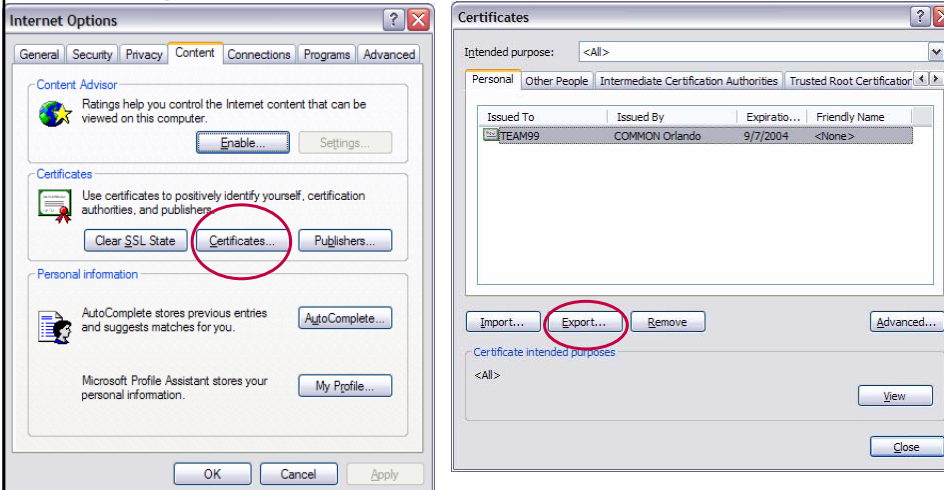
Click on the Install Certificate link

If using Netscape, then...



- 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.

If using Internet Explorer, then...



- From the toolbar, select Tools->Internet Options
- From the Content page, click on Certificates
- Highlight the certificate and select Export

Exporting a certificate with IE continued...

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
- Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)**
 - Include all certificates in the certification path if possible
 - Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
 - Delete the private key if the export is successful

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

- The certificate export wizard starts. Select **Next**
 - Then select **Yes, export the private key** and then **Next**
 - Then select the **Personal Information Exchange** button and then **Next**
- iSeries. mySeries.**

Exporting a certificate with IE continued...

File to Export

Specify the name of the file you want to export

File name:

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Cer
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

- Next you will be prompted for a password to protect the file. Enter a password and confirmation.
- Select a location to save the file, and select Next
- Select Finish to complete the export

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

Continue Cancel

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



Select a Certificate Store

Expand All Collapse All

- ▶ **Fast Path**
 - Create Certificate
 - Create New Certificate Store
 - Install Local CA Certificate on Your PC
- ▶ **Manage Certificates**
- ▼ **Manage Applications**
 - View application definition
 - Update certificate assignment
 - Define CA trust list
 - Add application
 - Remove application
 - Update application definition
 - Validate application

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 DDMDRDA 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)



Select a Certificate Store

Expand All Collapse All

- ▶ **Fast Path**
 - Create Certificate
 - Create New Certificate Store
 - Install Local CA Certificate on Your PC
- ▶ **Manage Certificates**
- ▼ **Manage Applications**
 - View application definition
 - Update certificate assignment
 - Define CA trust list
 - Add application
 - Remove application
 - Update application definition
 - Validate application

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.



Select a Certificate Store

Expand All Collapse All

- ▶ **Fast Path**
 - [Create Certificate](#)
 - [Create New Certificate Store](#)
 - [Install Local CA Certificate on Your PC](#)
- ▶ **Manage Certificates**
- ▼ **Manage Applications**
 - [View application definition](#)
 - [Update certificate assignment](#)
 - [Define CA trust list](#)
 - [Add application](#)
 - [Remove application](#)
 - [Update application definition](#)
 - [Validate application](#)

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:

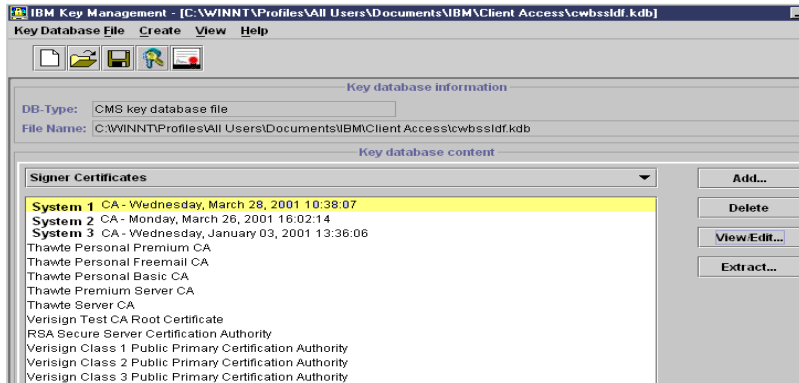
Client authentication required:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Define the CA trust list:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Certificate Revocation List (CRL) checking:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

Click the Apply button

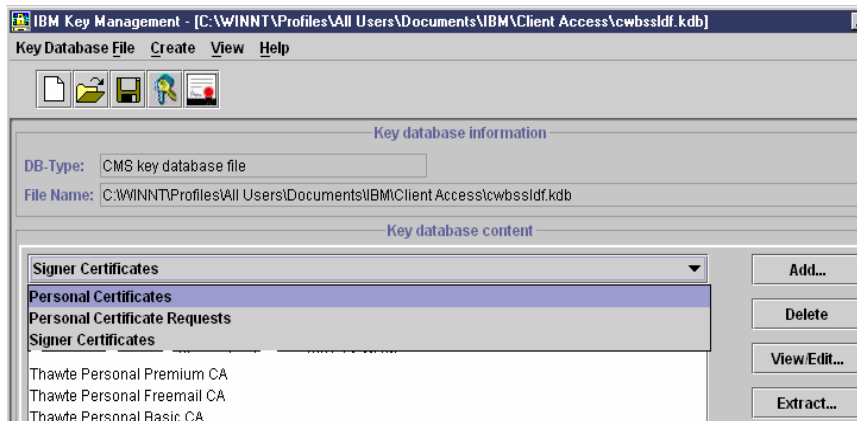
Application Information: Note that this will take effect immediately. Telnet does not have to be restarted.

Configuring Client Authentication on the PC



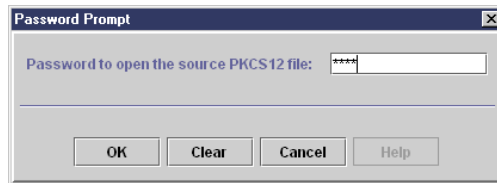
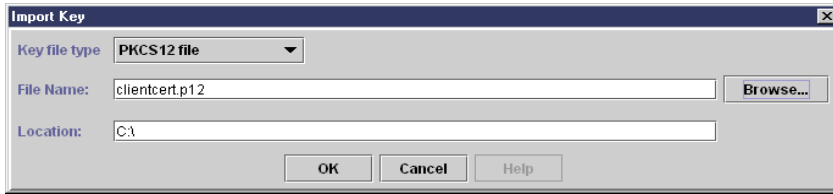
- Once the client certificate is stored in a PKCS12 file, it must be imported into the iSeries Access key database.
- The preferred way to start the IBM Key Database Management program is through Control Panel
 - Start->Settings->Control Panel, then double-click on "iSeries Access". Select the "Secure 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

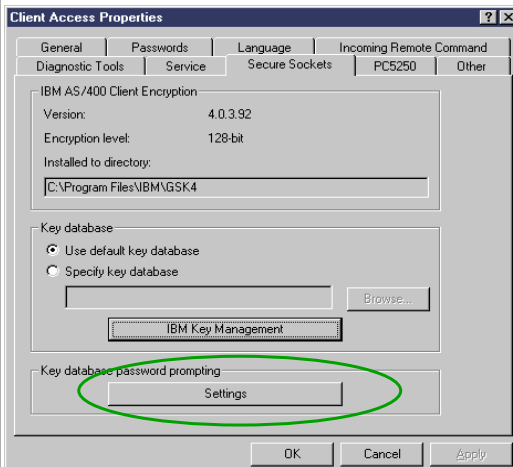
Importing Personal Certificate (continued)



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

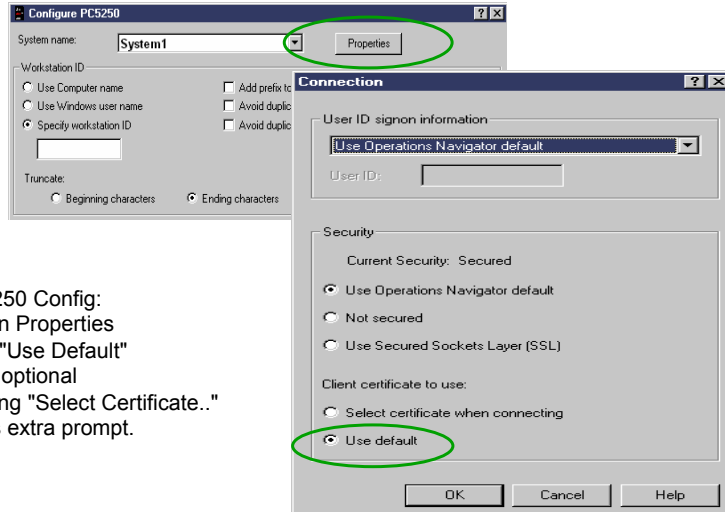
Setting Prompting for Key Database Password

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



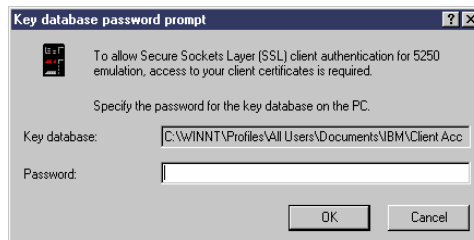
Specify how often you want to be prompted.

Enabling Client Authentication on PC



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

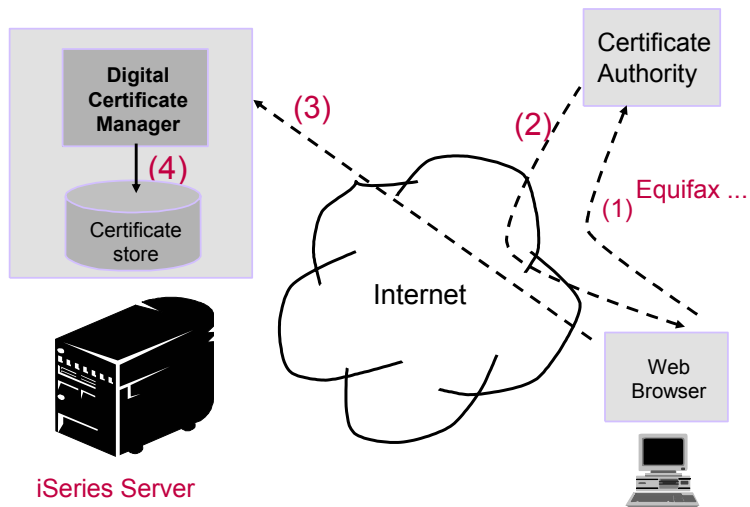
Connecting with Client Authentication



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

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

Obtaining a server certificate from a well-known CA





Select a Certificate Store

Expand All Collapse All

Fast Path

- **Create Certificate**
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- ▼ Manage Certificates
 - View certificate

Digital Certificate Manager

Create Certificate

Select the type of certificate that you want to create.

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

Continue Cancel

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



Select a Certificate Store

Expand All Collapse All

Fast Path

- **Create Certificate**
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- ▼ Manage Certificates

Digital Certificate Manager

Select a Certificate Authority (CA)

Certificate type: Server or client

Certificate store: *SYSTEM

Select the type of Certificate Authority (CA) that will sign this certificate.

- Local Certificate Authority (CA)
- VeriSign or other Internet Certificate Authority (CA)

Continue Cancel

- 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: ITS0

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 appropriate Certificate Authority that will sign your certificate request.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICrDCCA2QCAQAwZzELMAkGA1UEBhMCVVMxDDAKBgNVBAGTA01JTjESMBAGA1UE
BxMJUm9jaGVzdGVyM0wvCgYDVQKEwNjQkOxDTALBgNVBAsTBTE1U008xGTAXBgNV
BAMTEGFPzNDwLmRvbWVUFpb15jb20wgqE1MAOGCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCuy8tBLmRRo9GeDMuXVzoc5OnacZOTKA2w5FYJyKgw9Fq71eaWrdEmc71
aehBb/ukr06xCe731phpXmGcfdC63kP1nOVy8dZsnyjY9gbXR1D2dZBUEWHR8uSt
T5jUfOjdpU1ewKhirZ5UDD+11wQ/0+qaQ3o28TVISy+47U8O5KBRzNjMkcpR7106
eQL9x1yYonDEDA1yxkzu6W43Zh02oPXGOvp1762Dya7kU5oUW6NTQgHOYx1Ph6z
t6jYq9a73WUUB5r21y9e6NzOR2t0o9Z7p0zFLKht1HV335c2jH6J01EsRCDUQ1jL
7AEUtr7rCt5SMB4dstjyF7LX9P1mDAgMBAAAGADANBgkqhkiG9w0BAQQAQAAQAA
j17U1F1K5y0zcbKvOGHz8TBoPbcJNBvBUe1b6TX644G/fvGY/BA4rYraEdv8MN1v
ZyRNe7TG2JIMwXbHJHJNMePICzoq71JvcGtQIA/ZmyyhTOU7tCsk9u5LO10tjMu
Go3K1zBFLUcXQ6s4x6QMFyWvayKfr8WN8tVa7ZXtgQhHhv60T7RNsPh0UmzMQ+e1
8J9p31DYwRgBUUDLSeYgsur821RH1QxOGW5qdgUXdWSdpmxcrJswHcOU9dWBNhM
BQ3vcKevggbnkz24DBHj28114CUygp9VPnSjh1hcBMDm1Zr348gtRNs/XV/LQCG1
rWpJG2hSxaus5bpIBnx4pQ==
-----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 signing request as Certificate Signing Request (CSR).



Select a Certificate Store

Expand All Collapse All

- Fact Path
- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- Manage Certificates
 - ▼ Manage Applications
 - View application definition
 - **Update certificate assignment**
 - Define CA trust list
 - Add application
 - Remove application
 - Update application definition
 - Validate application
 - Manage Certificate Store
 - Manage CRL Locations
 - Manage PKIX Request Location

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 iSeries Access 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)
- iSeries Client Encryption (5722-CE2 or CE3)



For More Information

- AS/400 Client Access Express for Windows: Implementing V4R4, SG24-5191 (redbook)
- 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
- www.as400.ibm.com/http
- www.software.ibm.com/network/hostondemand
- www.software.ibm.com/network/pcomm
- www.as400.ibm.com/tcpip
- www.as400.ibm.com/ebusiness/security
- www.rsa.com
- www.verisign.com
- www.entrust.com
- 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](#)

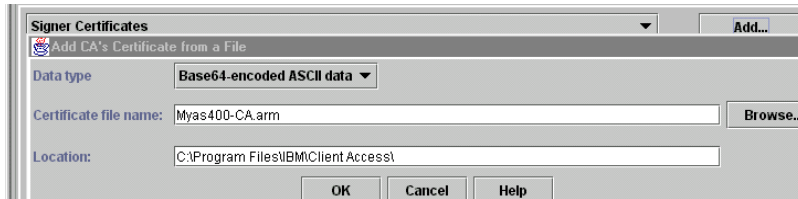
To copy and paste the certificate to a file on your PC:

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 to return to the main page.

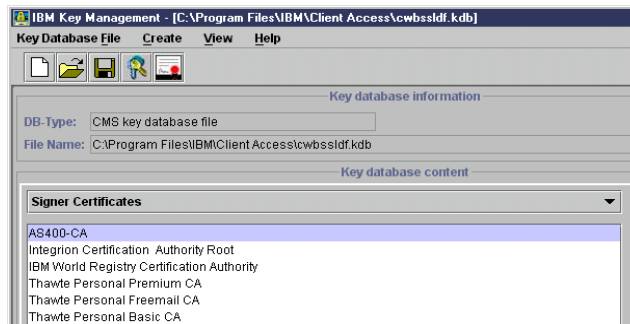
[Copy and paste certificate](#)

[Done](#)

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



- 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 1994-2004. 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 of International Business Machines Corporation in the United States, other countries, or both:
Instruction: Refer to the following URL: <http://www.ibm.com/legal/copytrade.shtml>. Edit the list below, IBM subsidiary statement, and special attribution companies which follow so they coincide with your presentation.

AS/400	e-business on demand	i5/OS
AS/400e	IBM	OS/400
	IBM (logo)	
	iSeries	

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are 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.
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 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 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. Changes may be incorporated in production models.

© 2004 IBM Corporation

iSeries. mySeries.