Domino HTTP Hardware Cryptography Support using iSeries SSL

Copyright and Trademark Information

Disclaimer; No Warranty

Trademarks

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

iSeries	Lotus	Quickplace
iSeries Client Access	Lotus Notes	Notes
Power PC	Domino	
OS/400	Sametime Connect	

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. 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.

MMX is a trademark and Pentium is a registered trademark of Intel Corporation in the United States, other countries, or both.

Other product and company names mentioned herein may be the trademarks or registered trademarks of their respective owners.

Domino HTTP Hardware Cryptography Support using iSeries SSL

This white paper provides an example of configuring Domino HTTP to use iSeries System SSL for the purpose of using a hardware cryptographic accelerator.

Domino is not aware of the cryptographic cards and does not need to be specially configured to use them. All it needs to do is be configured to use iSeries System SSL (referred to hereafter as System SSL). System SSL is in turn configured to use the cryptographic hardware. This configuration will function even if there is no configured cryptographic card in the system.

Important Note: Only Domino HTTP will use System SSL. All other Domino tasks will continue to use Domino's internal SSL function, and will not have access to the cryptographic hardware.

System Requirements

- 5722-SS1 Option 34, Digital Certificate Manager
- 5722-DG1, IBM HTTP Server for iSeries
- 5722-AC2, Crypto Access Provider 56-bit for AS/400 or 5722-AC3, Crypto Access Provider 128-bit for AS/400
- Domino 6.5.2, 6.0.4, or later.
- A hardware cryptographic device. This includes the 4758 Cryptographic Coprocessor, or the 2058 Cryptographic Accelerator at the time of this writing.

Hardware Setup

In order to use hardware cryptography (via System SSL) for the iSeries server, you must have the hardware cryptography cards correctly installed and configured. As of this writing, Domino for iSeries supports the 4758 Cryptographic Coprocessor and the 2058 Cryptographic Accelerator. The latest Cryptographic Hardware documentation can be found in the iSeries Information Center (http://publib.boulder.ibm.com/html/as400/infocenter.html) under Networking->Networking Security. This example only covers the certificate creation for the 2058 Cryptographic Accelerator, or software-only encryption. Please refer to the documentation in the Information Center for installation and configuration of the 4758 Cryptographic Coprocessor.

Step-by-step example scenario:

In this example we will:

1. Enable the DCM (Digital Certificate Management) server.
2. Create a local Certificate Authority (CA).
3. Create a certificate store.
4. Create a certificate for Domino using the 2058 Cryptographic Accelerator or software encryption.
5. Assign a certificate to Domino.
6. Configure Domino to use System SSL.
7. Configure the 2058 Cryptographic Accelerator.
8. Follow links to information on configuring the 4758 Cryptographic Coprocessor.

1. Enable the Digital Certificate Management (DCM) server

DCM is configured using the *ADMIN instance of the iSeries HTTP server. Start the *ADMIN instance of the HTTP server if needed:

STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

The DCM server is accessed through your Web browser using port 2001. Internet Explorer is recommended. (Such as http://youriseries:2001. Figure 1)

Figure 1

2. Create a Local Certificate Authority (CA)

This section illustrates how to create your own Local certificate authority (CA) for issuing a certificate to use with Domino. Creating a local CA is a good way to test your SSL setup before purchasing a certificate from a trusted Internet CA.

From the HTTP Admin screen in the step above, click the “Digital Certificate Manager” link. (Figure 1)

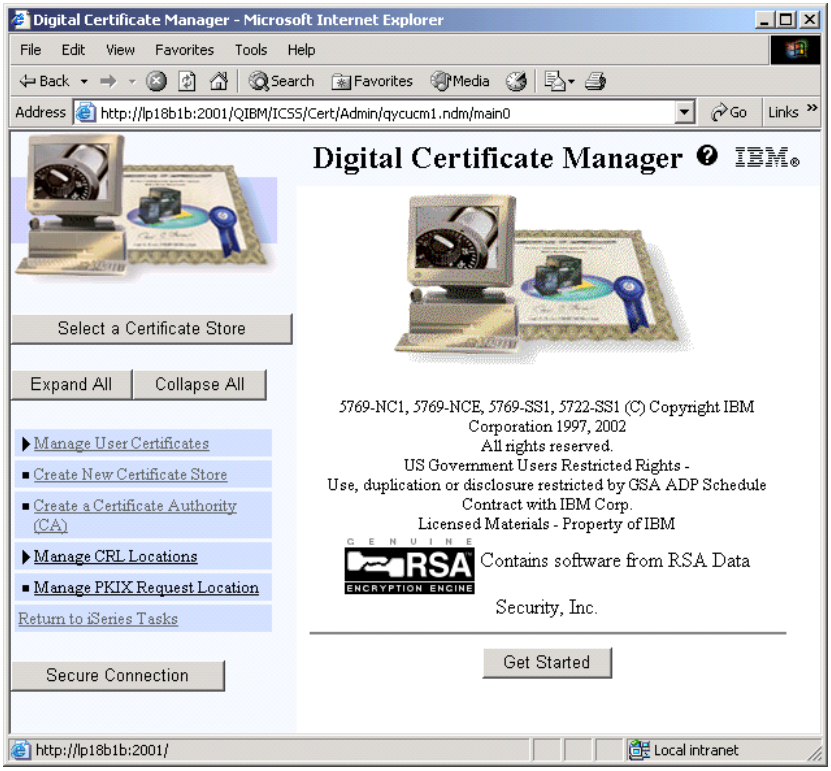

Figure 2

Click “Create a Certificate Authority (CA)” from the left menu pane on Figure 2.

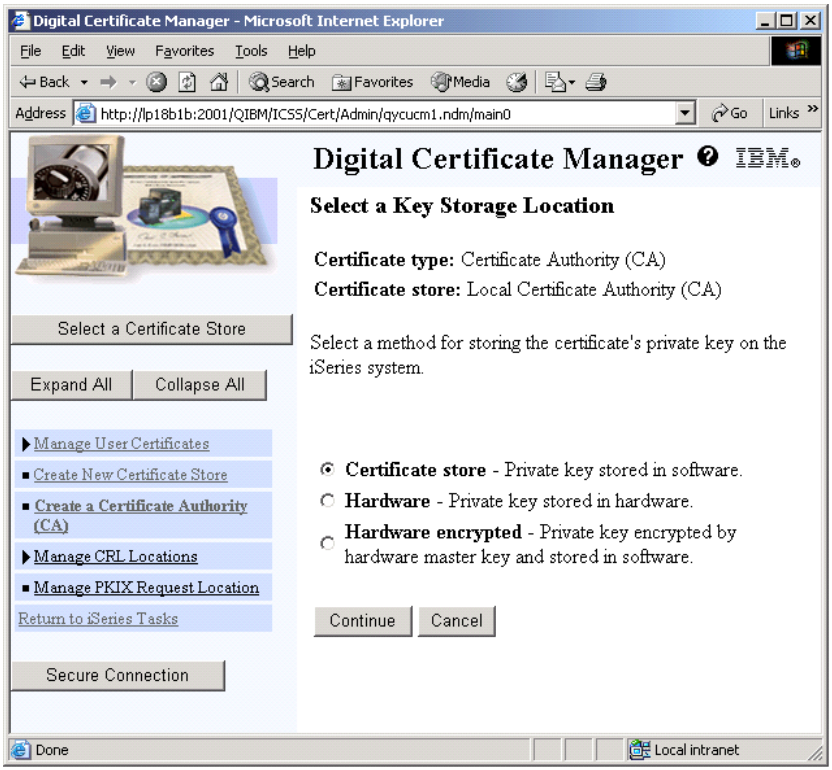

Figure 3

Select “Certificate Store” on Figure 3 and click Continue. Note that if you do not have a 4758 Cryptographic Coprocessor in your system, that you may not see this screen. In that case, skip ahead to the next step.

Figure 4

Fill in the fields on Figure 4 with your system and business information. This certificate will be used as a root certificate for issuing other certificates (such as Domino's certificate). It is a good idea to distinguish in the name that it is a CA. Click Continue when done to bring up Figure 5.

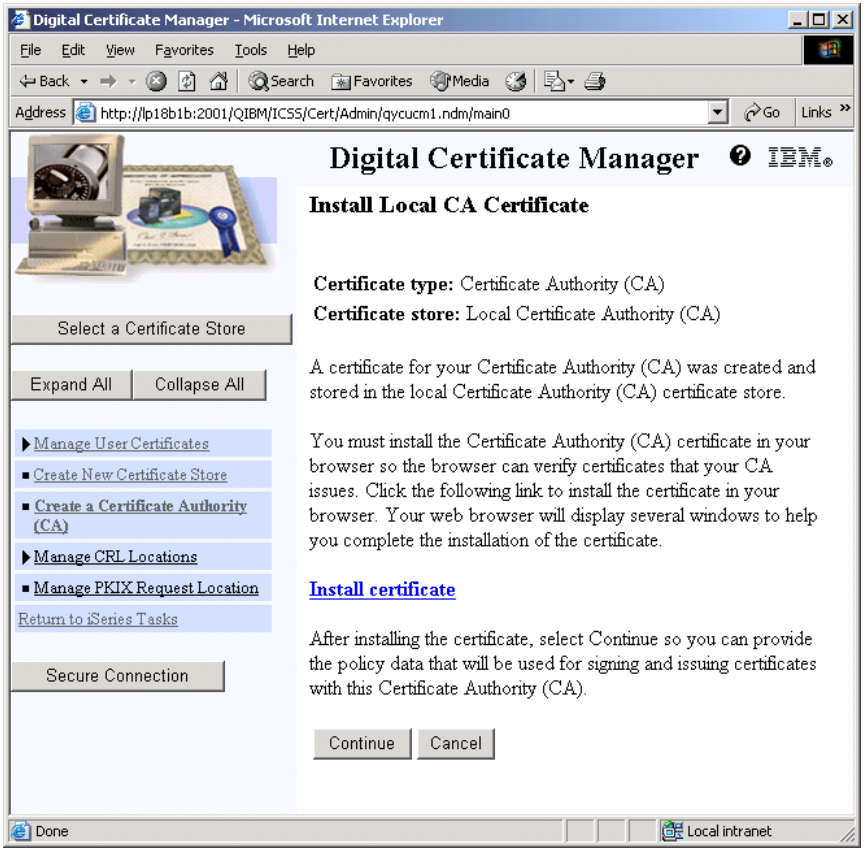

Figure 5

Since you have created your own CA, you need to tell your Web browser that your CA is trusted. Click “Install Certificate.” If you are using Internet Explorer, you should see a box pop up (Figure 6):

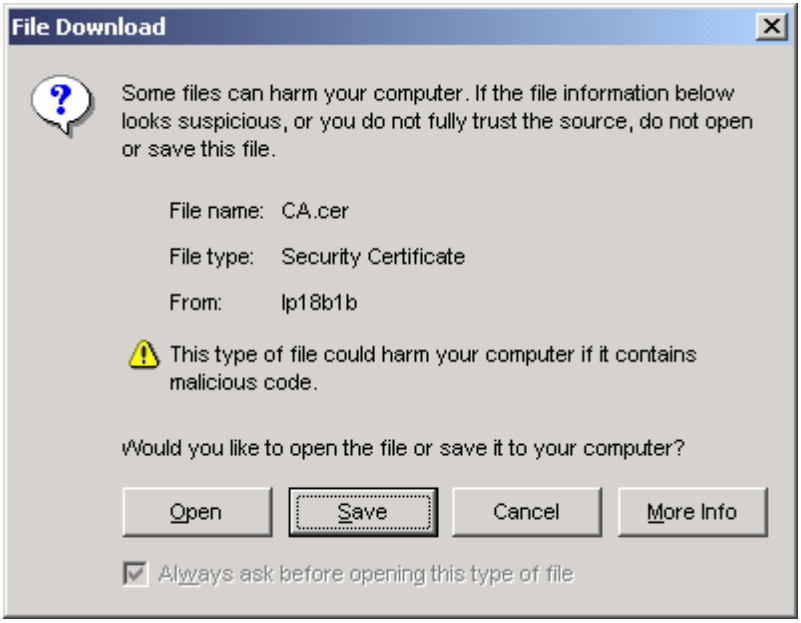

Figure 6

Click Open.

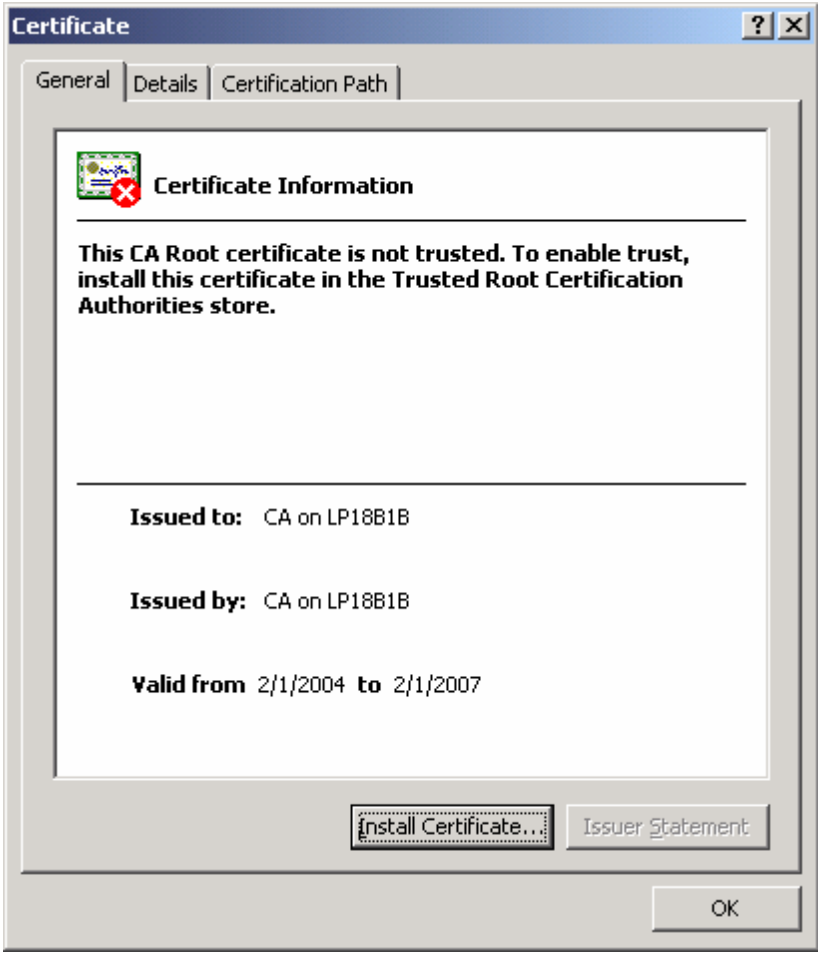

Figure 7

Click “Install Certificate” on Figure 7. This will start a certificate import wizard (Figure 8). The following will guide you through the steps for Internet Explorer. Other browsers will vary.

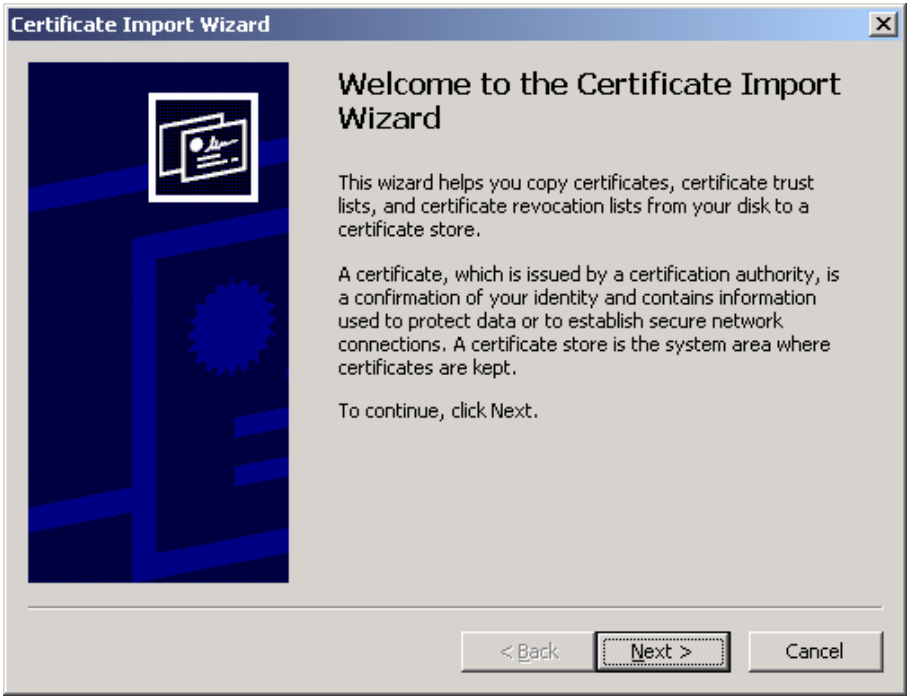

Figure 8

Click Next.

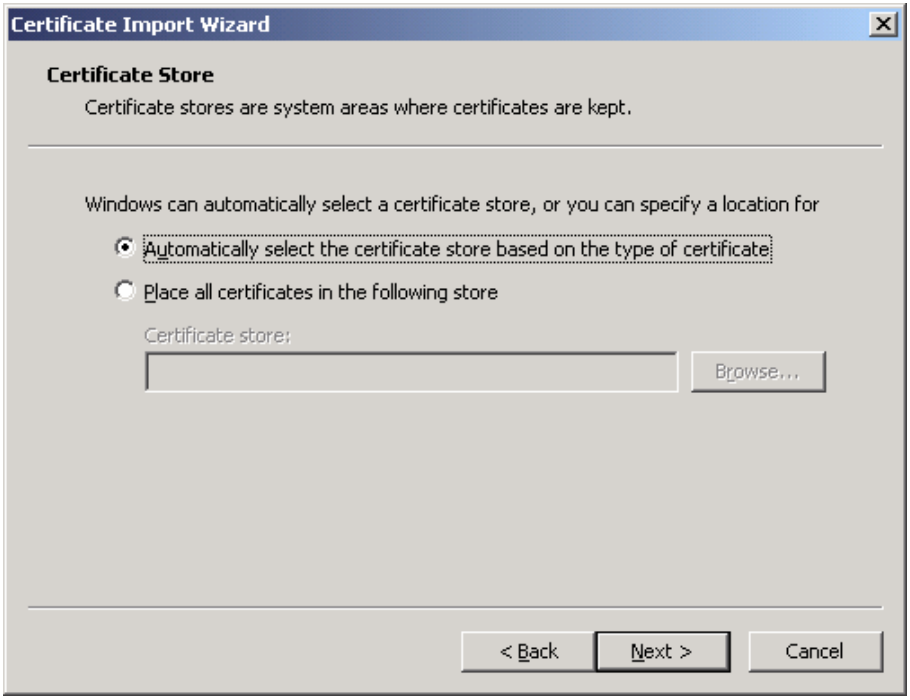

Figure 9

Keep the default at “Automatically select the certificate store based on the type of certificate,” and click Next.

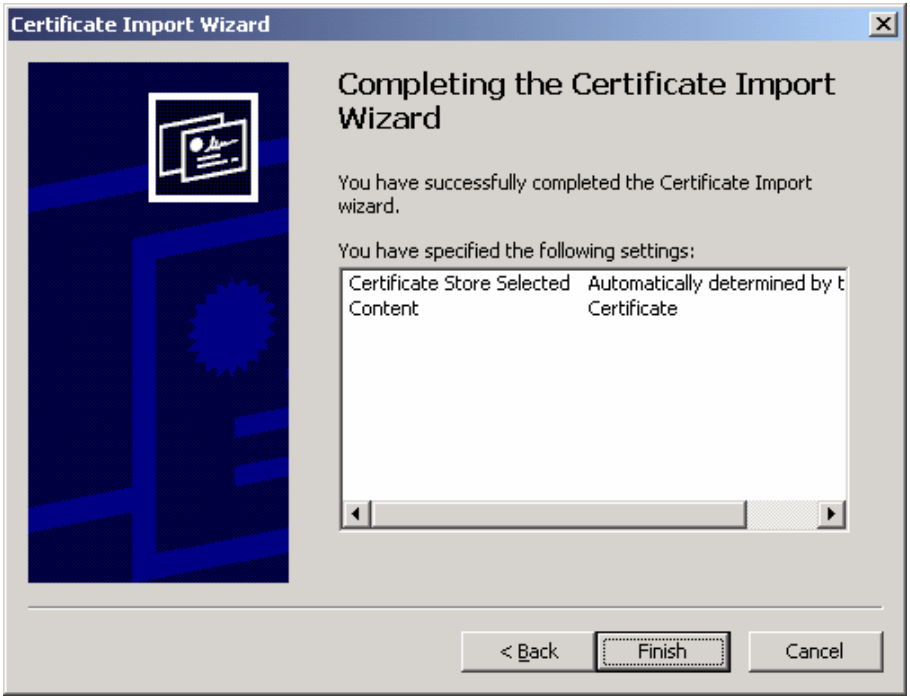

Figure 10

Click Finish.

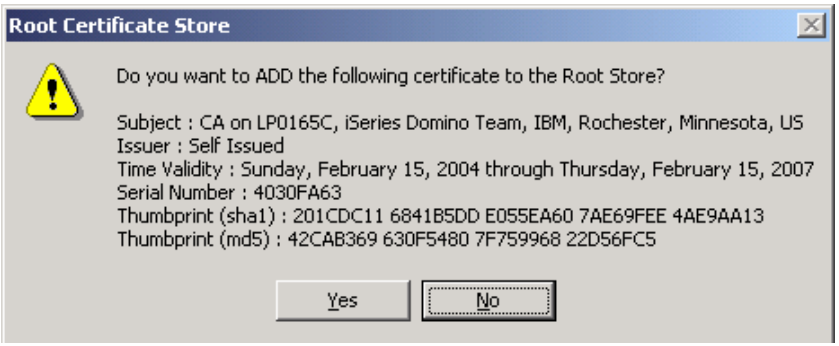

Figure 11

You will see a popup box about adding your certificate to the Root Store (Figure 11). Click Yes.

Figure 12

Another popup box will appear with the message “The import was successful.” Click OK. You’ll then be back at the screen where you started the certificate install. Click OK on Figure 12 to exit the installer.

On the DCM configuration screen that had the “Install Certificate” link, click Continue (Figure 5).

Figure 13

Leave the values as the default on Figure 13. Click Continue.

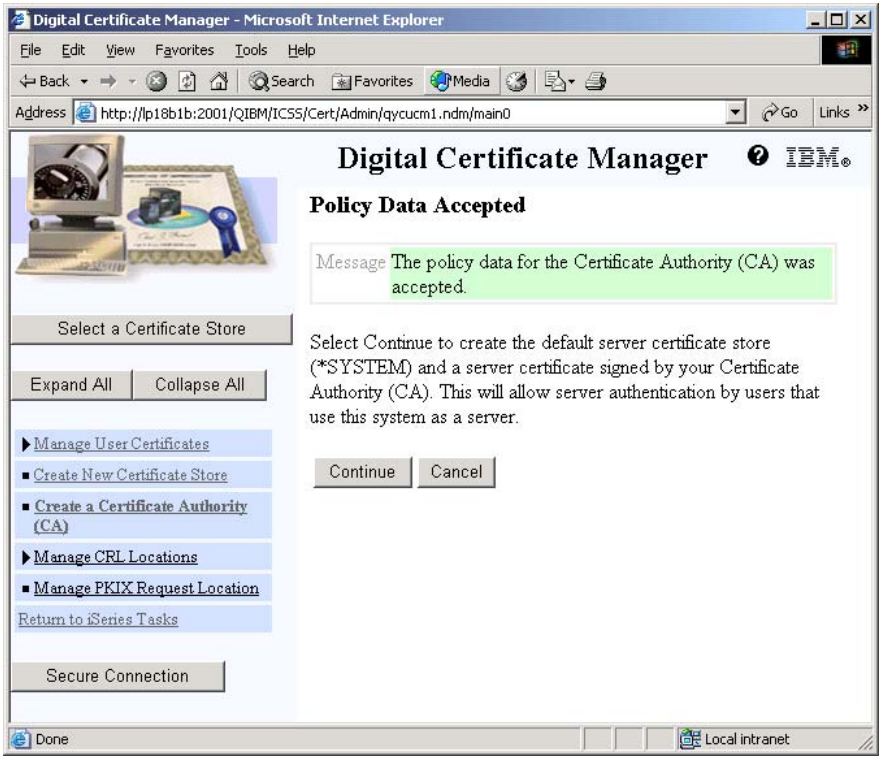

Figure 14

You are done! Click Cancel, as we will not be continuing on from this screen.

3. Create a Certificate Store

On the left menu panel, click “Create New Certificate Store”. (Figure 15)

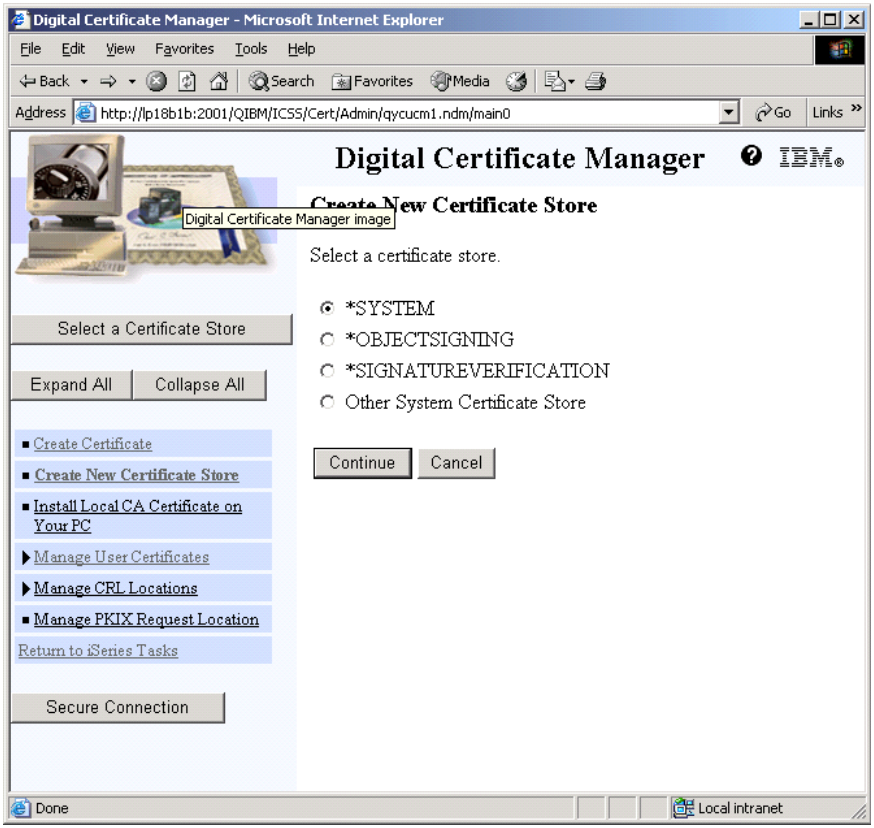

Figure 15

Select *SYSTEM and click Continue. If *SYSTEM does not appear on this screen, then *SYSTEM already exists. In that case, skip ahead to section 4, “Create a certificate for Domino using the 2058 Cryptographic Accelerator or software encryption.”

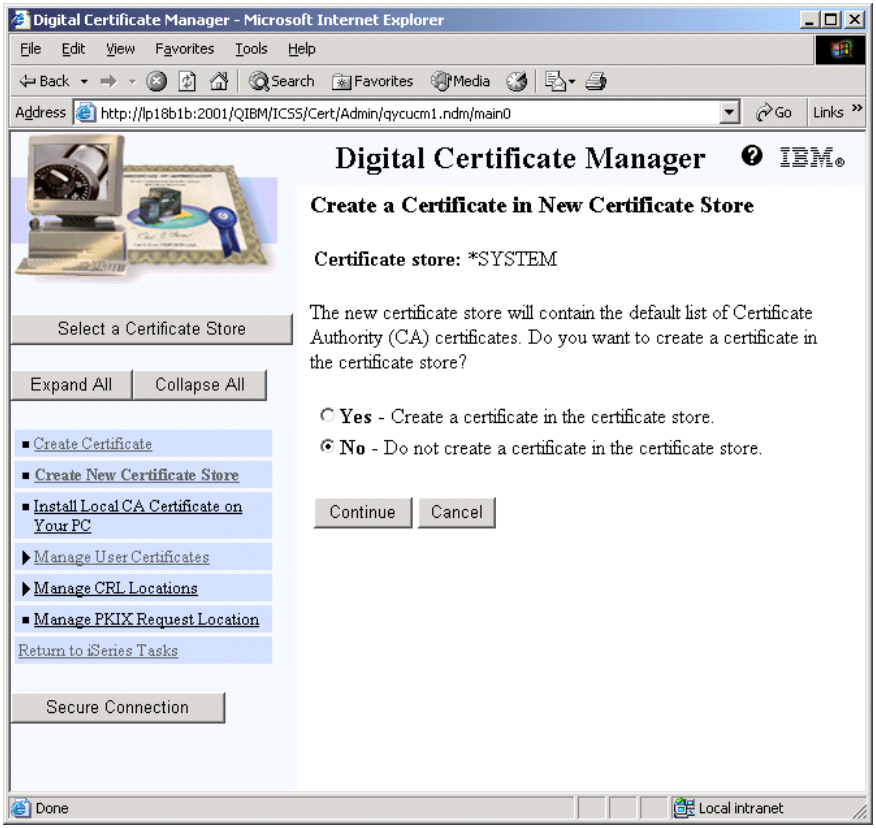

Figure 16

Select “No - Do note create a certificate in the certificate store” on Figure 16, and click Continue.

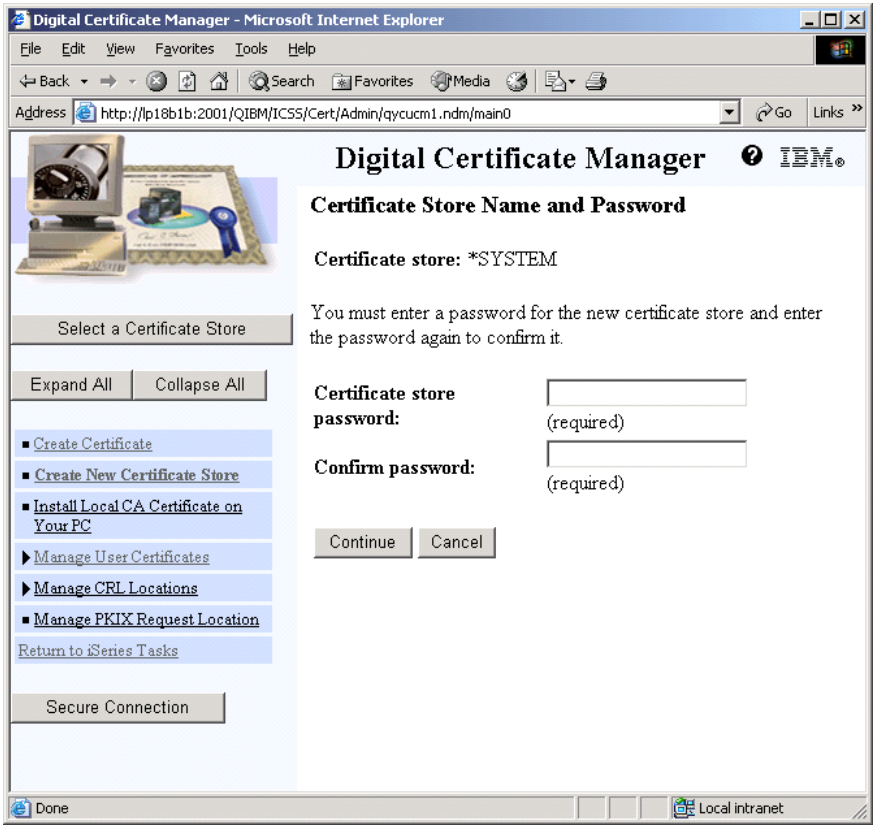

Figure 17

Create a new password for the *SYSTEM certificate store on Figure 17 and click Continue.

You will get a screen that says the certificate store has been created. Click “OK” to proceed. You will be back at the screen titled “Create New Certificate Store.” You are now done creating the *SYSTEM Certificate Store. Click “Cancel”.

4. Create a certificate for Domino using the 2058 Cryptographic Accelerator or software encryption

This section explains how to create a certificate that is used by DCM and Domino. This certificate can be used with either the 2058 Cryptographic Accelerator, or with no cryptographic accelerator. This can be useful for testing on a system without an accelerator. The 2058 Cryptographic Accelerator is transparent to this certificate and will be used if configured and varied on.

Click “Select a Certificate Store” on the left menu panel.

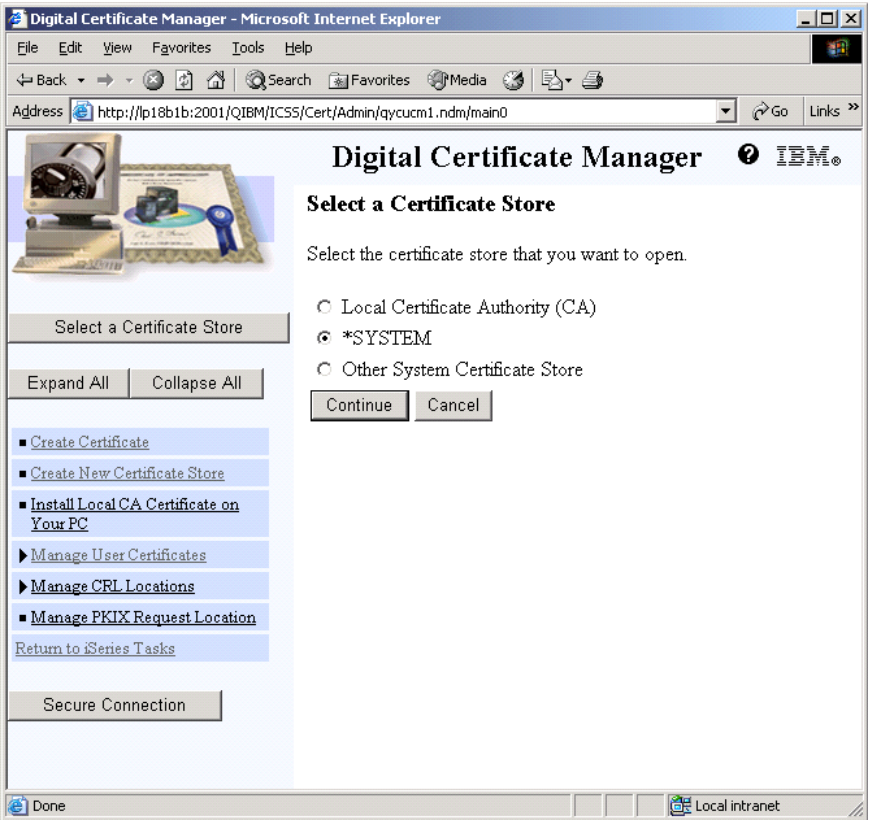

Figure 18

Select “*SYSTEM” for the certificate store on Figure 18 and click Continue.

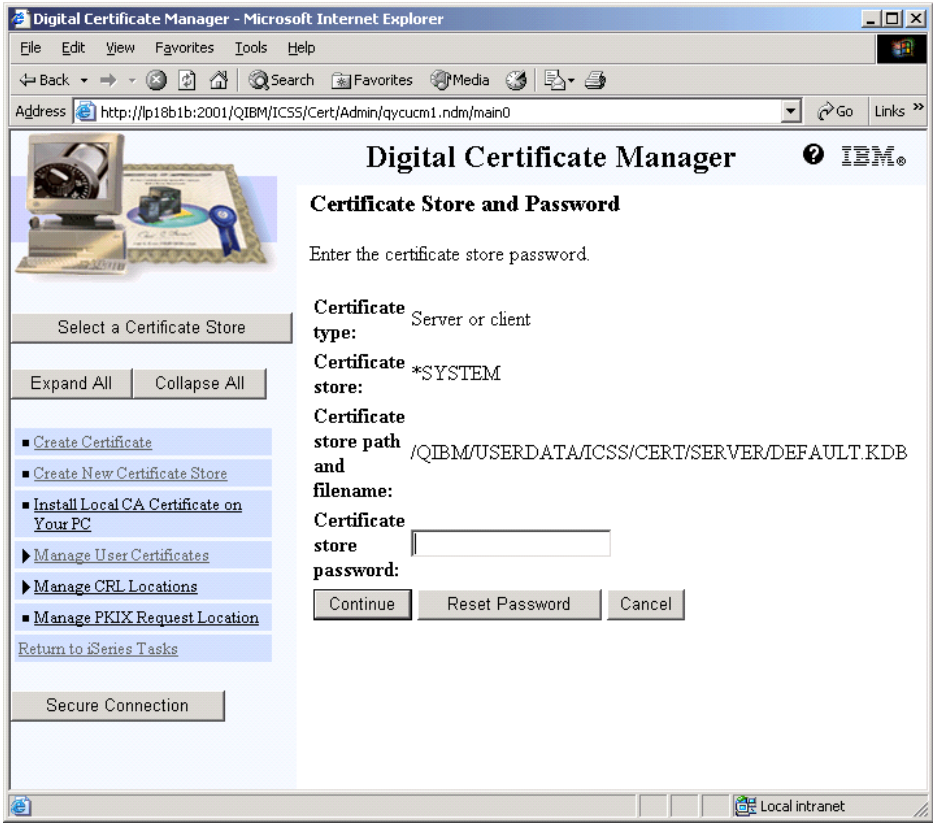

Figure 19

Enter the password for the *SYSTEM certificate store on Figure 19 and click Continue. You now have access to the certificate store.

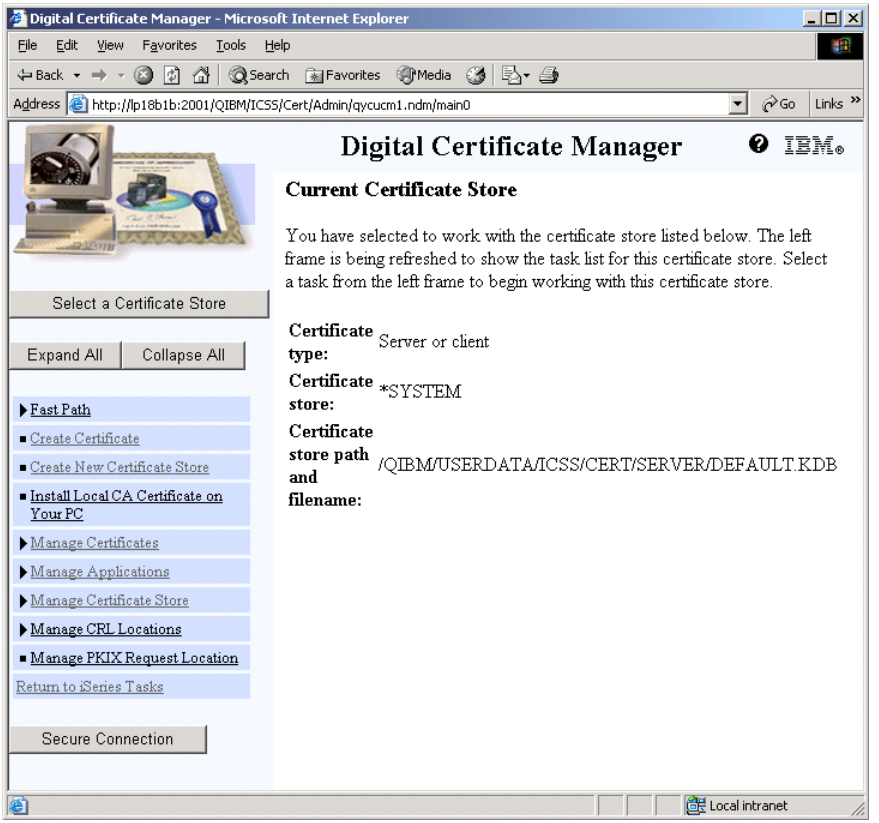

Figure 20

Click “Create Certificate” from the left menu panel on Figure 20.

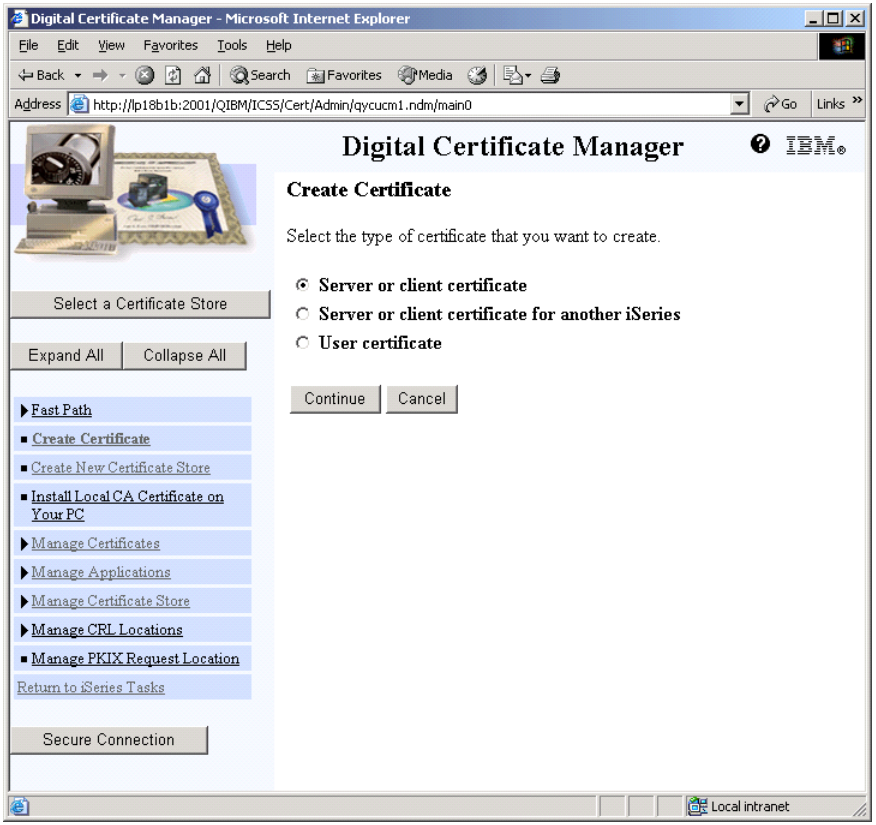

Figure 21

Select “Server or client certificate” on Figure 21 and click Continue

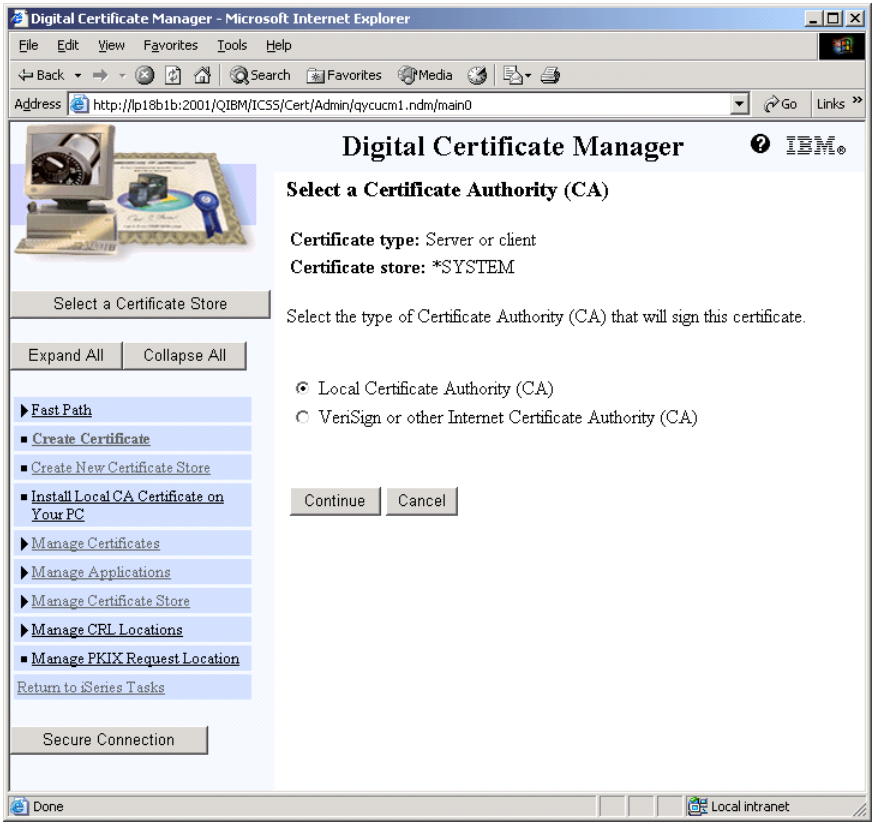

Figure 22

Select “Local Certificate Authority (CA)” on Figure 22 and click Continue. Note that this is where you would select to use a certificate purchased from an Internet Certificate Authority.

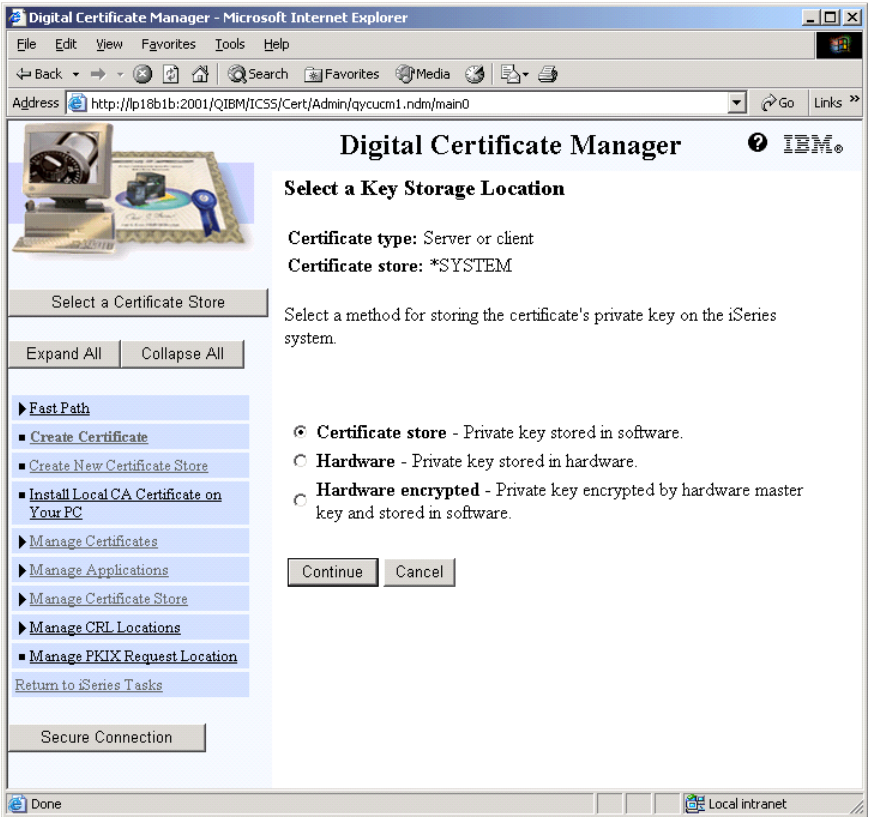

Figure 23

Note If there is no 4758 Cryptographic Coprocessor in your system, you will not see this screen. Continue on to the next step.

Select “Certificate Store - Private Key stored in software” on Figure 23 and click Continue. Note that this is the point where, if you were creating a certificate to use with the 4758, you would select “Hardware” or “Hardware encrypted.” The 2058 does not require this step, as the certificate doesn’t need to be aware of the 2058 existing.

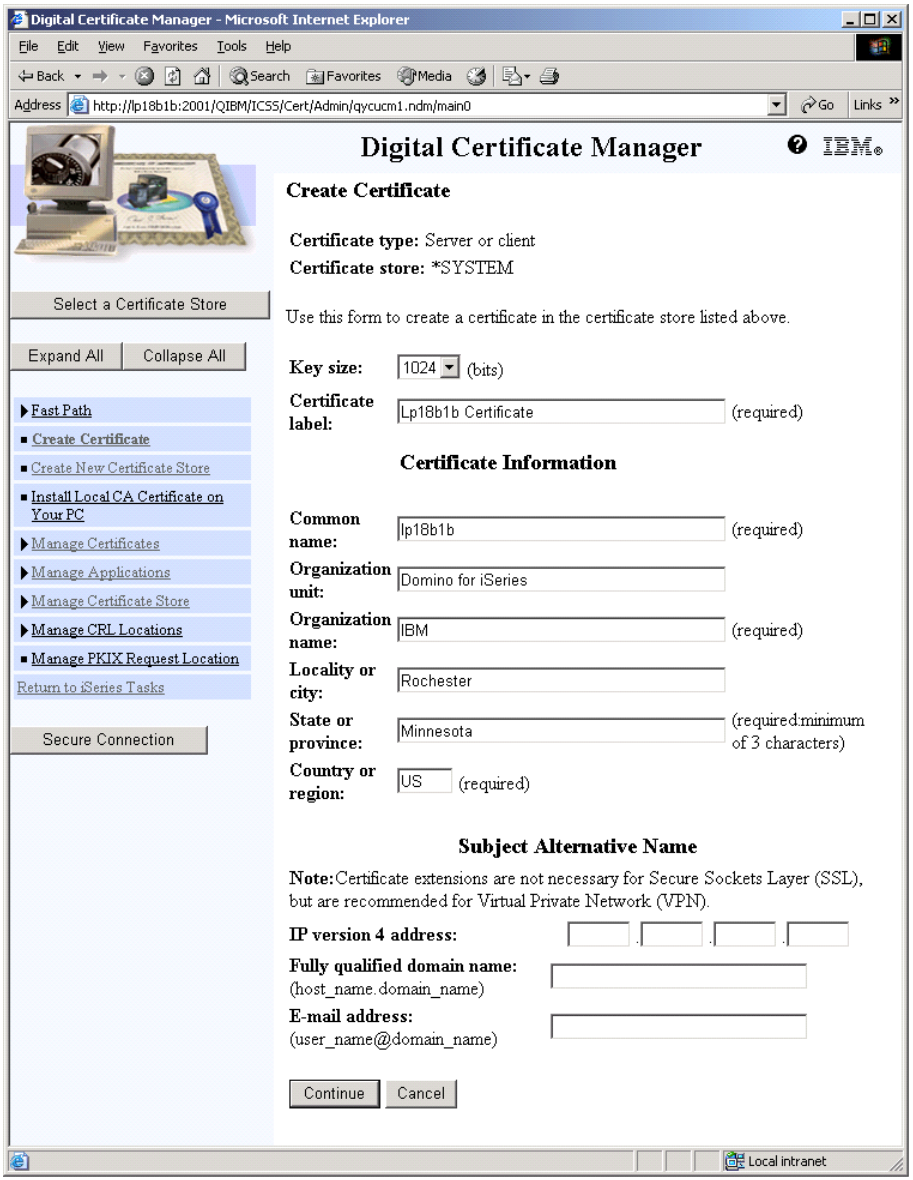

Figure 24

Fill in the screen on Figure 24 with information about your system and company. You can pick a key size of your choice. The “Subject Alternative Name” can be left blank for this example. Click Continue.

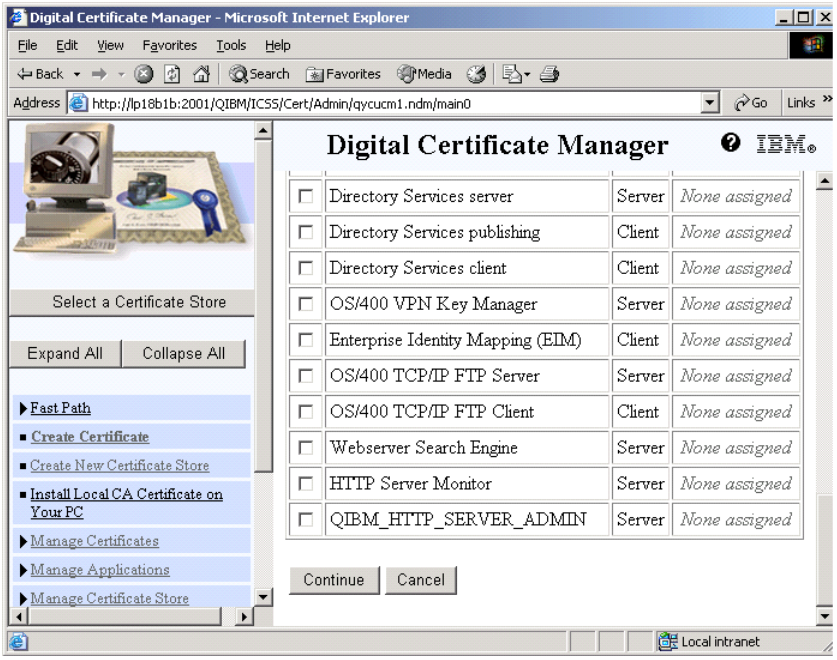

Figure 25

This next screen (Figure 25) is titled “Select Applications.” We will do this after we create an application identifier for Domino. For now, do not check any boxes. Click Continue.

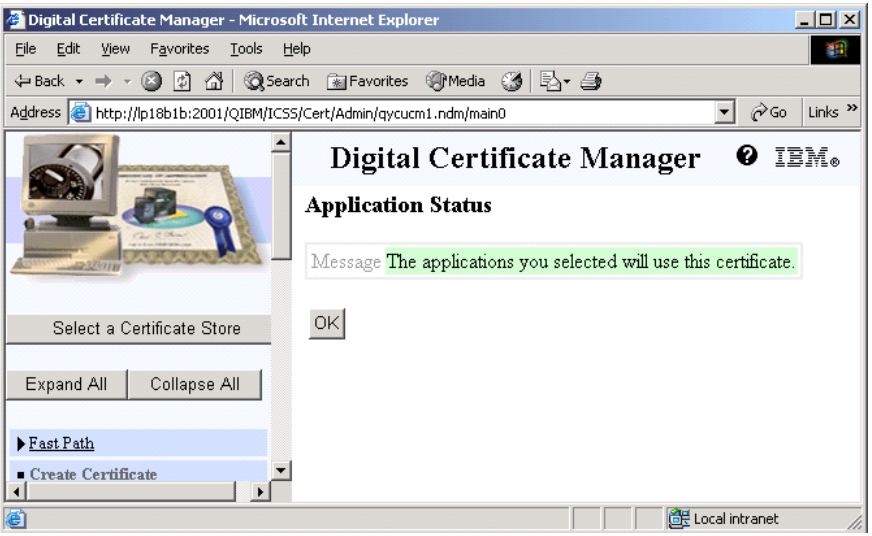

Figure 26

Click OK on Figure 26. You are now done and have a certificate that will work with software encryption or with the 2058 Cryptographic Accelerator. You will be back at the “Create Certificate” screen. Click Cancel to exit.

5. Assign a certificate to Domino

The iSeries DCM uses Applications Identifiers (AppID) to associate a certificate with an application. We will now create a new AppID for Domino.

Click “Manage Applications” from the left menu panel on figure 27.

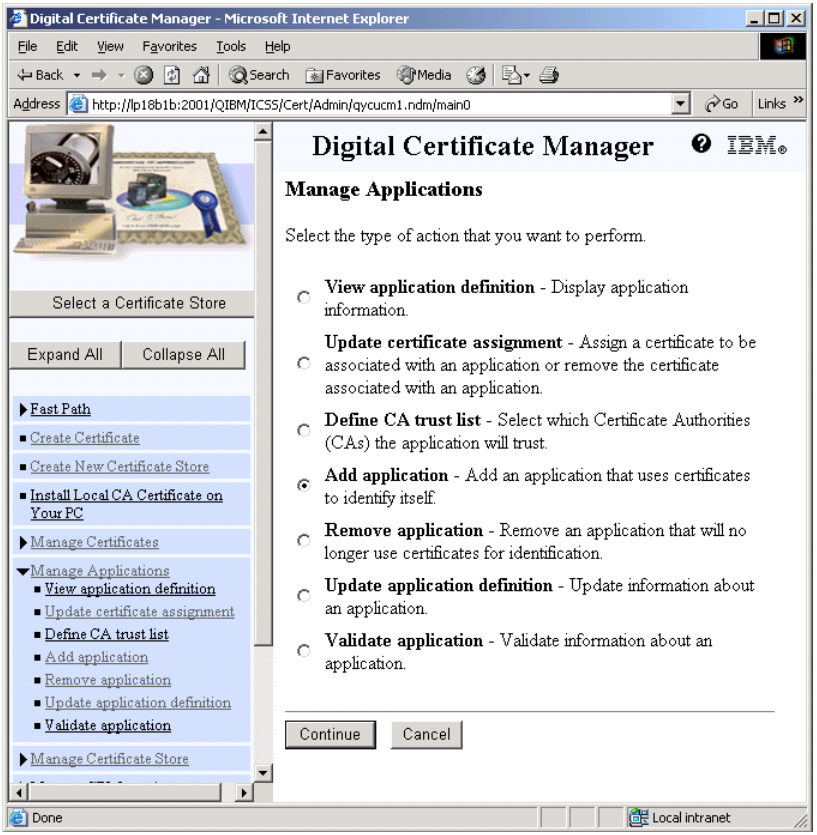

Figure 27

Select “Add application” on Figure 27 and click Continue.

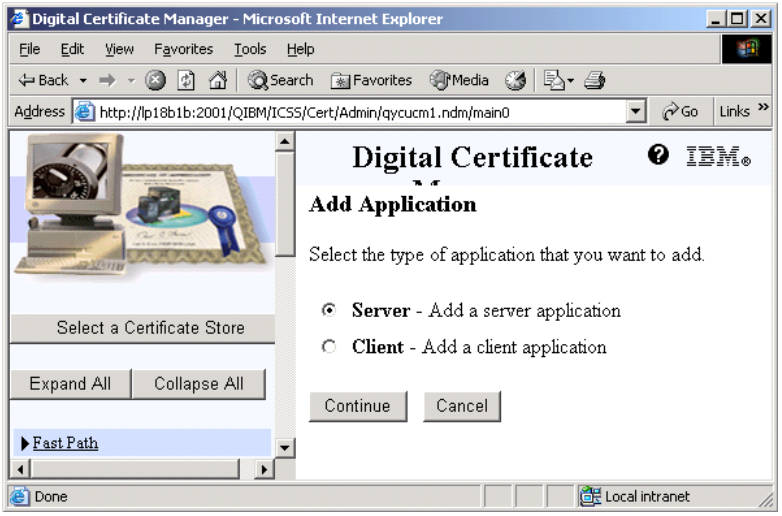

Figure 28

Select “Server” on Figure 28 and click Continue.

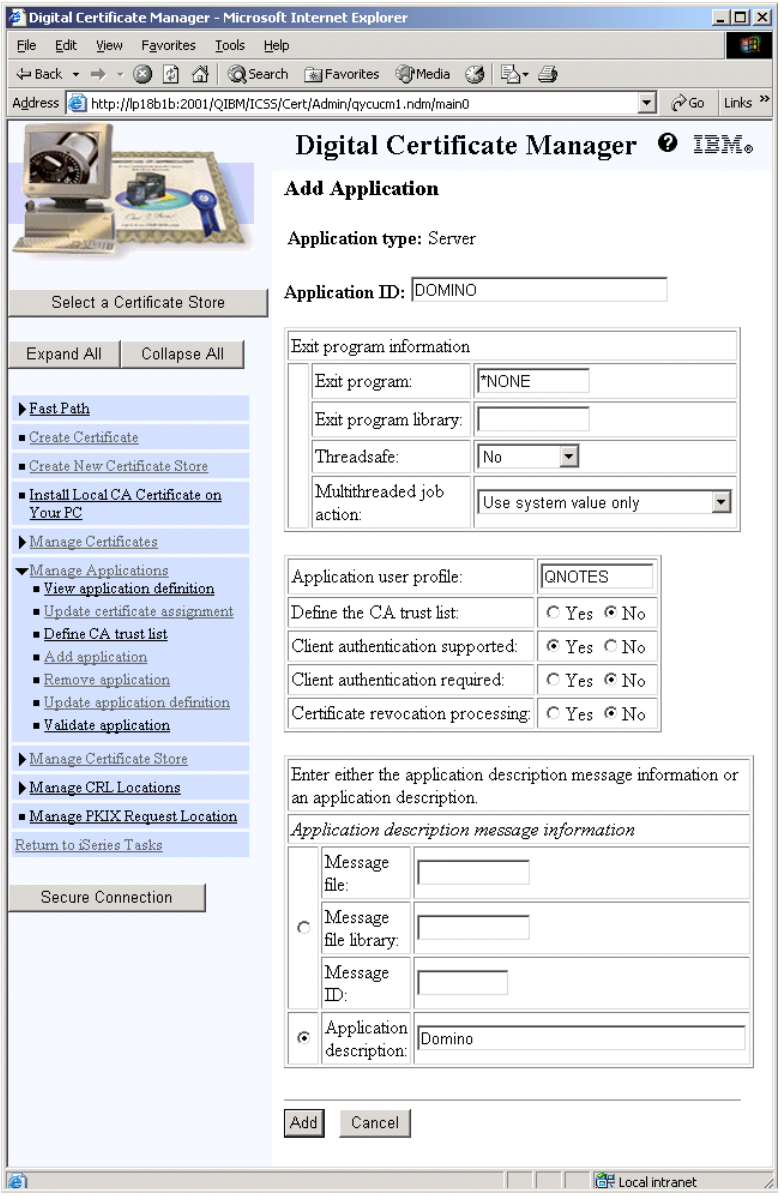

Figure 29

Fill in the fields on Figure 29 as shown above. You can choose to require client authentication if needed. Please note the Application ID specified at the top of the page (DOMINO in our example). You will need this name to configure Domino in a later step. Also note that the “Application User Profile” needs to be set to QNOTES.

This will give Domino access to the *SYSTEM certificate store files. Click Add to continue.

You should receive a message that the application has been added. Click OK.

We are now back at the Manage Applications screen. We need to assign the certificate we created earlier to Domino's AppID that we just created. Select "Update certificate assignment" on Figure 30 and click Continue.

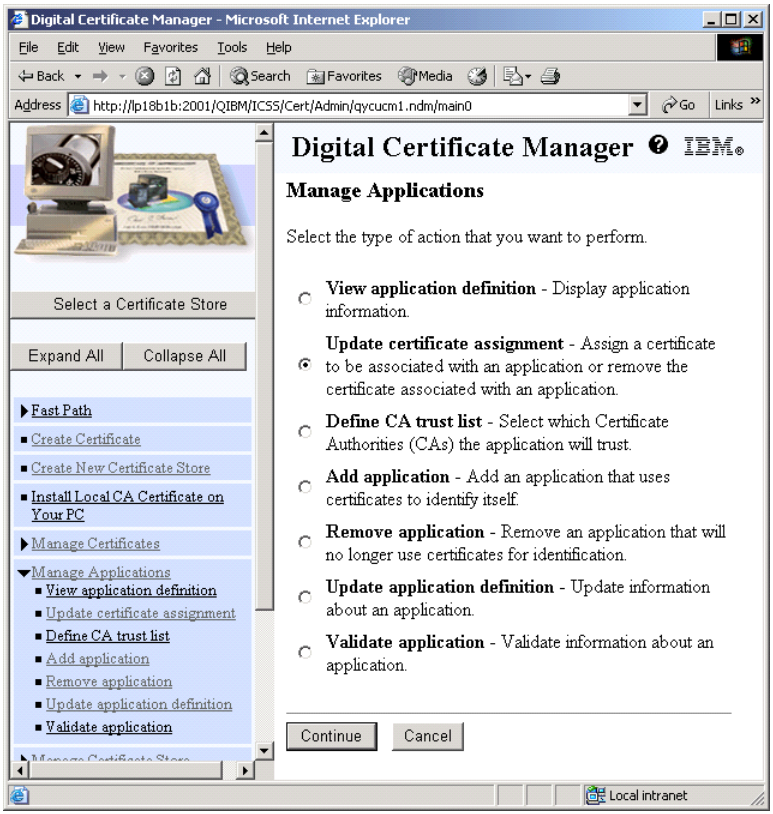

Figure 30

Select the type of application that you want to update on Figure 31. Select “Server” and click Continue.

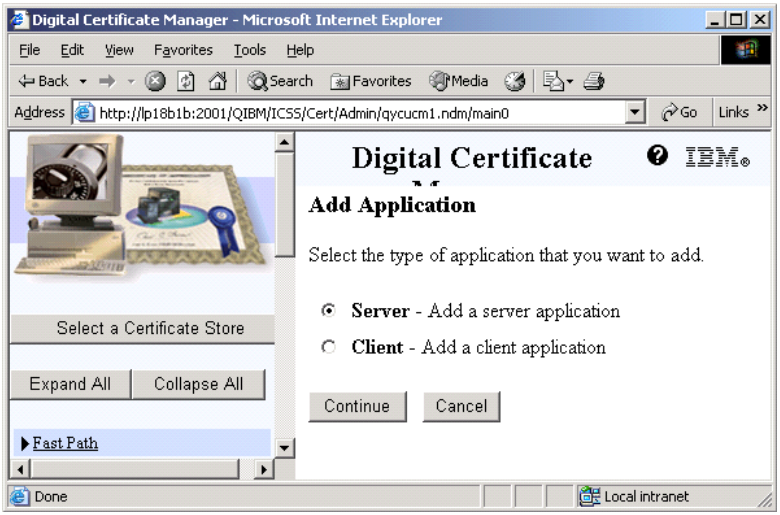

Figure 31

On Figure 32, pick Domino as the Application and click “Update Certificate Assignment.”

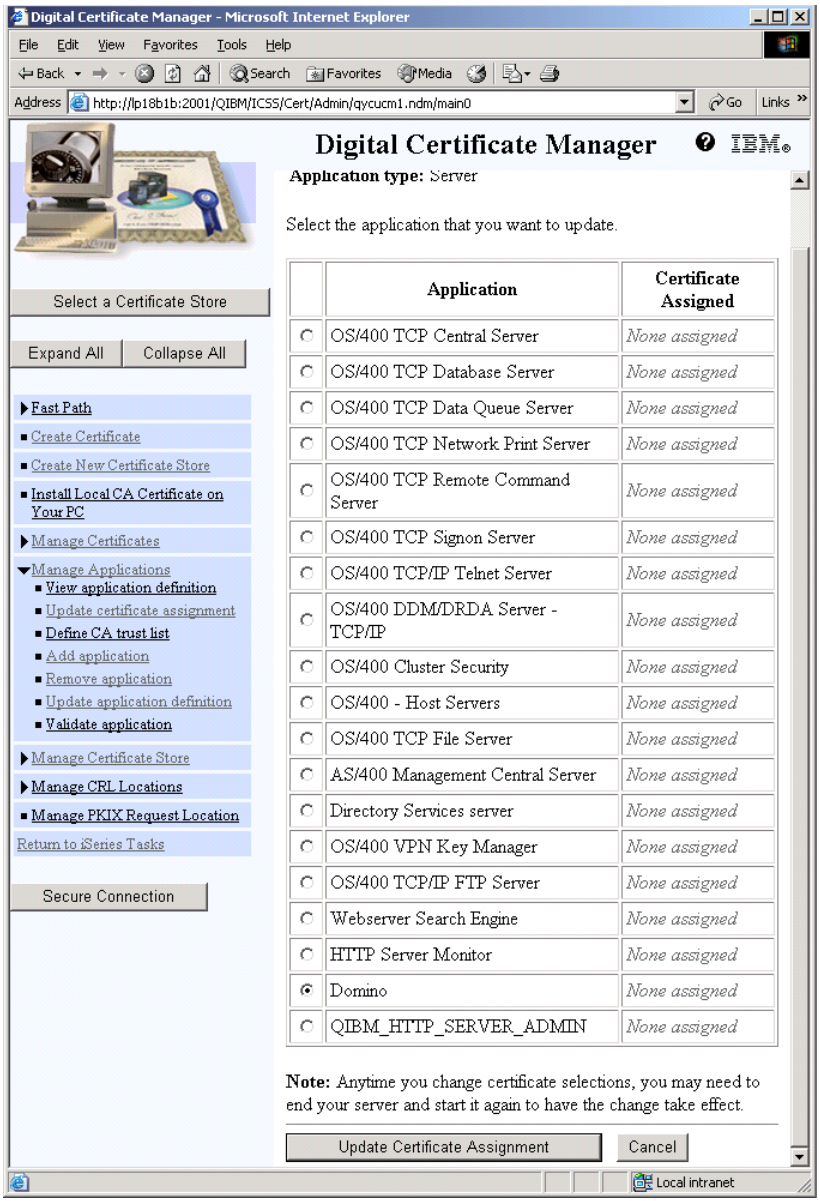

Figure 32

Now select the certificate to assign to Domino on Figure 33 and click “Assign New Certificate”.

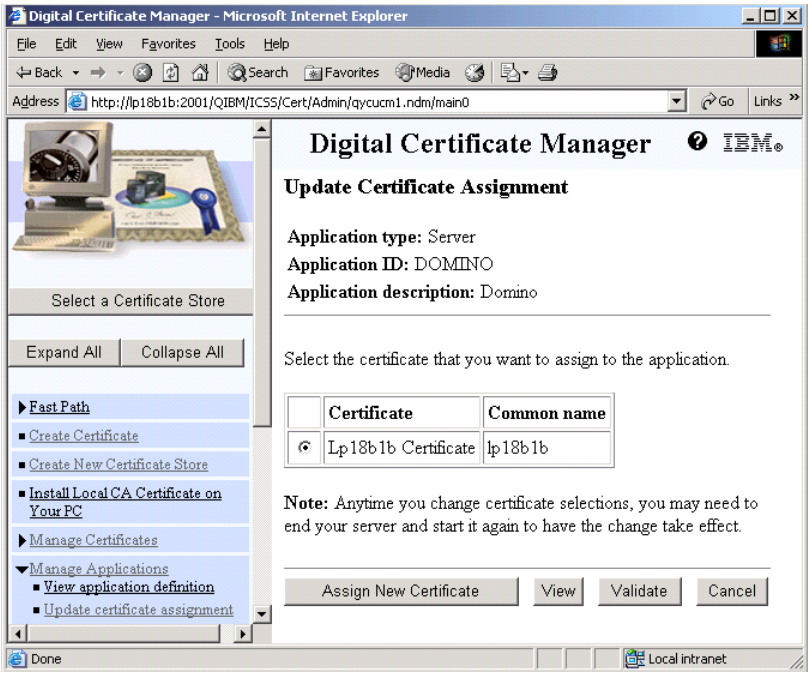

Figure 33

You should see the message “The certificate was assigned to the application.” You are done.

This concludes the configuration of the DCM to use Domino with the 2058 Cryptographic Accelerator, or using software encryption.

Grant access to the *SYSTEM certificate store for Domino

This step is only necessary if you did not create an application definition to use with Domino, meaning you used one that already existed.

When Domino's application definition is created in the example above, the user profile is set to QNOTES. This gives QNOTES (Domino's user profile) access to the *SYSTEM certificate store. We need to do this manually if you did not go through that step. Enter the following commands on an OS/400 command line:

CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QNOTES) DTAAUT(*RX)

CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QNOTES) DTAAUT(*RX)

CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.RDB') USER(QNOTES) DTAAUT(*RX)

If you are unsure if this is needed, go ahead and do it. This step will do no harm if the application definition already gave QNOTES access.

6. Configure Domino to use System SSL

Notes.INI Variables

The following are the Notes.INI variables that can be set for using System SSL. The variables that have ‘Y’ under the "REQ?" column indicate that it is a variable that must be set in order to use System SSL.

Add the following parameters to your Domino server’s Notes.ini file. Add this for each server that will be using the iSeries SSL.

NOTES.INI VARIABLE NAME	*REQ?*	*DESCRIPTION*
SYSTEM_SSL_HTTP=1	Y	Tells Domino to use the iSeries System SSL API instead of Domino’s SSLPlus for HTTP
SYSTEM_SSL_APPLICATION_ID=DOMINO	Y	The Application ID created in DCM for this Domino server
SYSTEM_SSL_TIMEOUT=30000	N	The number of seconds until the SSL V3.0 session identifier expires. The range is 0-86400 (1 day) seconds. System SSL will remember SSL V3.0 session identifiers for up to this amount of time. By remembering these SSL V3.0 session identifiers, the amount of data exchanged during the SSL handshake can be reduced for peer applications where a complete initial handshake has already been performed. The default is 30000 seconds (8 hours)

Configure the Domino Server Document

SSL must be enabled in the Domino server document. At a minimum, the SSL port will need to be enabled. Other options such as the “SSL key file name” are only used for Domino SSL tasks other than HTTP. Remember that only HTTP uses the system SSL and hardware cryptography. (Figure 34)

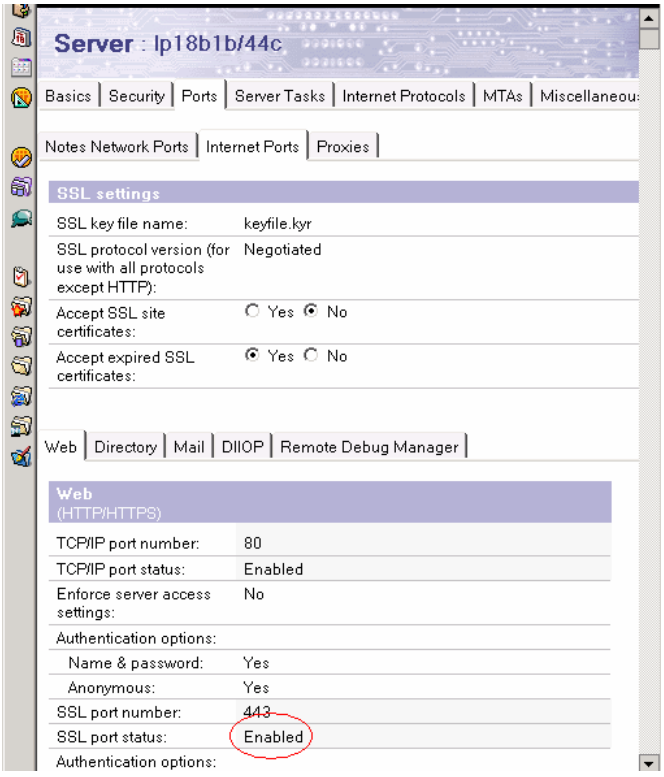

Figure 34

7. Configure the 2058 Cryptographic Accelerator

The 2058 Cryptographic Accelerator is simple to configure. To find the accelerator, enter the following command:

WRKHDWRSC *CRP

In the result below, the 2058 Cryptographic Accelerator is resource CRP01.

```
                    Work with Cryptographic Resources

                                                          System:   LP18B1B

Type options, press Enter.

  5=Work with configuration descriptions   7=Display resource detail


Opt  Resource        Type  Status               Text

     CMB05           2843  Operational          Combined function IOP

       CRPCTL03      4758  Operational          Cryptographic IOA
        CRP03        4758  Operational          Cryptographic Device

       CRPCTL01      2058  Operational          Cryptographic IOA

         CRP01       2058  Operational          Cryptographic Device
```

We need to create a device description for the accelerator. Enter the following command (Substituting CRP01 for your 2058 Cryptographic Accelerator's resource name):

CRTDEVCRP DEVD(CRP01) RSRCNAME(CRP01)

To vary on (enable) the accelerator, enter the following command:

WRKCFGSTS *DEV

```
                        Work with Configuration Status                LP18B1B
                                                              02/02/04  15:28:40
Position to  . . . . .               Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...

Opt  Description       Status                -------------Job--------------
1    CRP01             ACTIVE
     CRP03             ACTIVE
     DSP01             ACTIVE
     LANTAP            VARIED OFF
     OPT01             VARIED OFF
     OPT02             VARIED OFF
     QCONSOLE          VARIED OFF
     QESPAP            VARIED OFF
     QIADSP            VARIED OFF
                                                                      More...
Parameters or command
===>
               F3=Exit   F4=Prompt   F12=Cancel   F23=More options   F24=More
               keys
```

Select a 1 for ‘Vary On’ next to your device description, and press Enter. The device will go to ACTIVE status and you are done. All requests to the iSeries SSL will now use the 2058 Cryptographic Accelerator.

8. Configure the 4758 Cryptographic Coprocessor

The 4758 Cryptographic Coprocessor is a more involved configuration process than the 2058 Cryptographic Accelerator. This document will not cover this process. The main different steps required are:

1. Coprocessor initialization requires the *ADMIN HTTP server to be in SSL mode.
2. You must initialize the 4758 using the *ADMIN HTTP server if not previously done.
3. You must create a new certificate for Domino that uses ‘hardware’ or ‘hardware encryption’ for key storage rather than software (selected during certificate creation).

Under V5R2, see the topic e-business and Web serving->Web Serving->Set up->Set up SSL for the ADMIN Server (powered by Apache) in the iSeries Information Center for information on configuring the *ADMIN HTTP server to use SSL.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzaie/rzaieconfigssladmin.htm

See chapters 3.2.4 to 3.2.6 for information on configuring the 4758 Cryptographic Coprocessor in the Redbook "iNotes Web Access on the IBM eServer iSeries Server." This Redbook was written for Domino usage of the coprocessor and is recommended.

http://www.redbooks.ibm.com/redbooks/pdfs/sg246553.pdf

See the topic Security->4758 PCI Cryptographic Coprocessor for iSeries in the iSeries Information Center for information on configuring and using the 4758 Cryptographic Coprocessor.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzajc/rzajcco4758.htm

The Redbook “IBM ~ iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptography Enhancements” contains step-by-step instructions of configuring the 4758, as well as creating a certificate that will use it. See Chapter 4 of the Redbook for details. Appendix C also contains information on configuring the *ADMIN HTTP server for SSL.

http://www.redbooks.ibm.com/redbooks/pdfs/sg246168.pdf

Additional Information:

iSeries Information Center: V5R2->Networking->Networking security->Cryptographic hardware

Contains links to configuration information of the 4758 and 2058 accelerators.

http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzajc/rzajcoverview.htm