Our experience with Digital Certificates to enable SSL on HTTP for IBM i site www.easy400.net

by Giovanni B. Perotti, February 2020

After spending some time to switch our site from HTTP to HTTPS, we thought that some people could perhaps benefit from our experience.

Part 1 - Create a SSL Certificate Request

1. The following documents the work we did to create a Signed Certificate Request to be submitted to a public Certificate Authority (CA).
   This was primarily done to enable HTTPS on our site www.easy400.net .

   The process we went through is documented in IBM i Support Knowledge Center page "*Creating a server or client certificate request*",
   https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzahu/rzahustep2sc.htm .

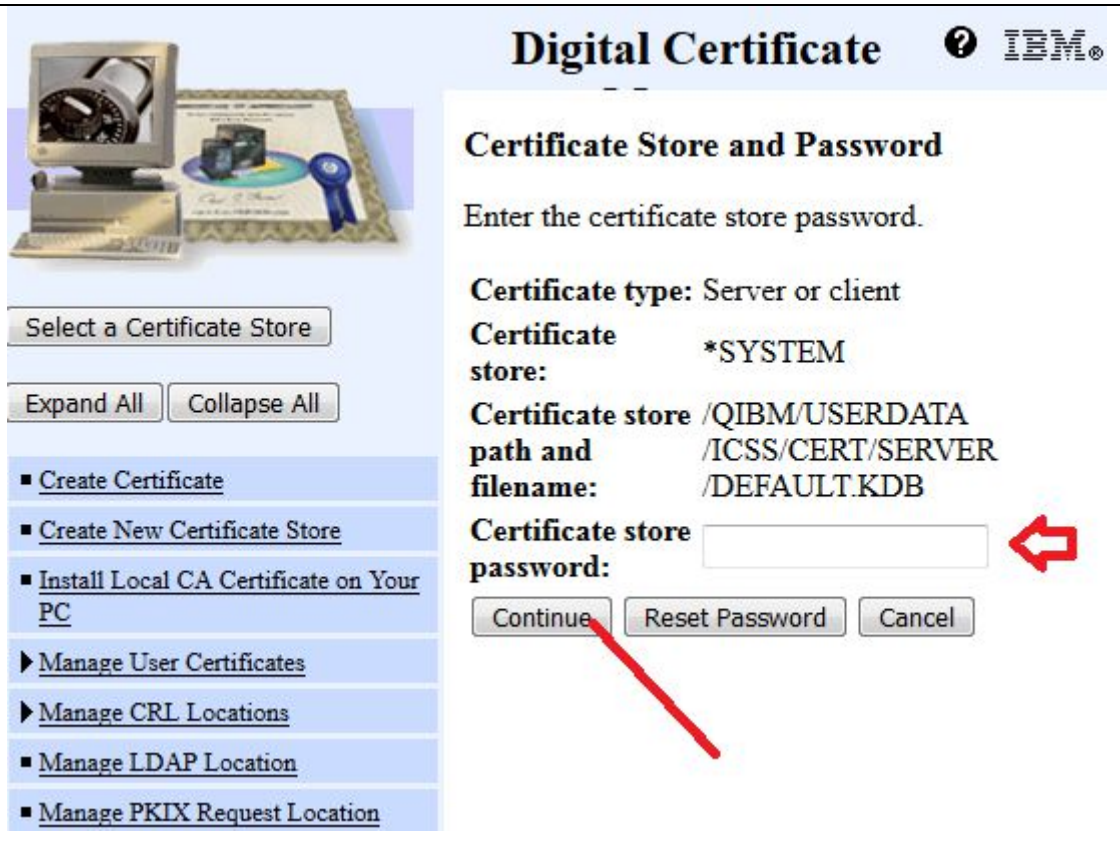
2. If needed, start the HRTTP instance *ADMIN, then open Digital Certificate Manager (DCM):
   http://....net:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0

3. In the navigation leg, press button **Select a Certificate Store**

IMPORTANT NOTE – To enable user *PUBLIC to SSL applications (like HTTPS), you must give to *PUBLIC the access the SYSTEM Certificate Store (in DCM mentioned as "Key Database").
This you do by running the following commands:

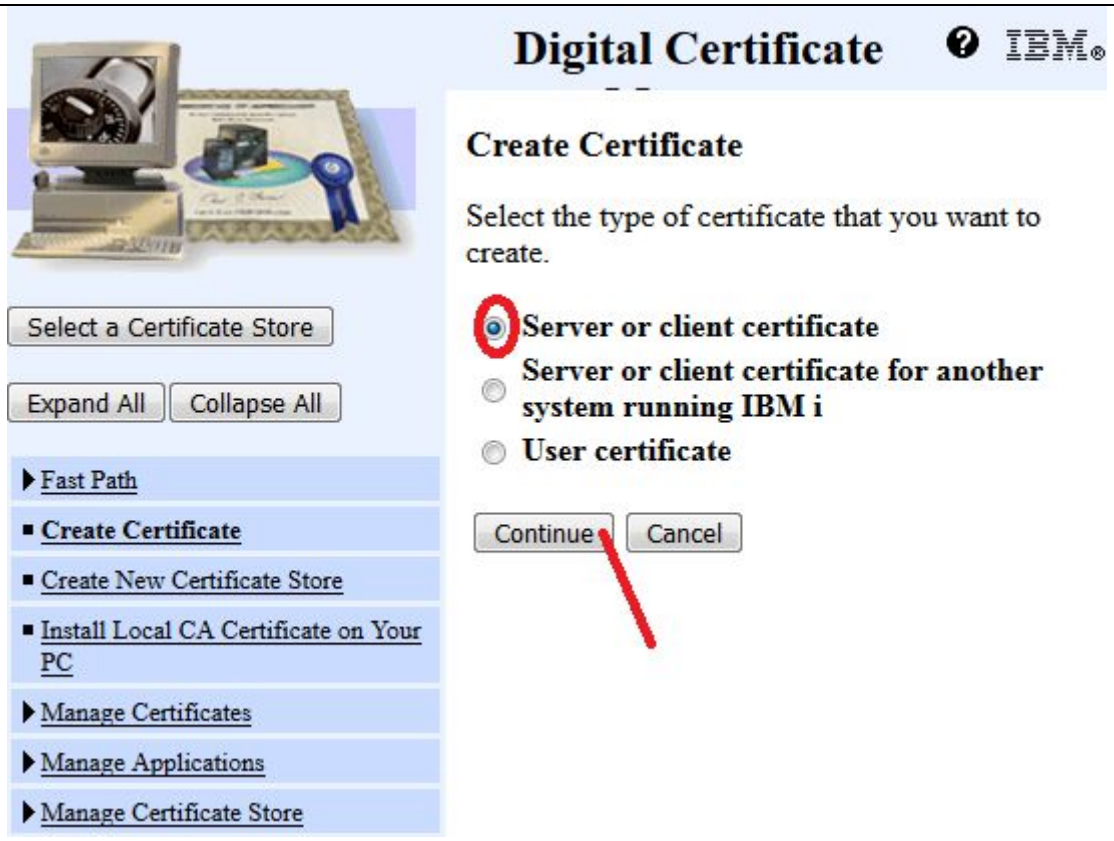
- CHGAUT OBJ('/QIBM/UserData/ICSS/CERT/SERVER/DEFAULT.KDB') USER(*PUBLIC) DTAAUT(*R)
- CHGAUT OBJ('/QIBM/UserData/ICSS/CERT/SERVER/DEFAULT.RDB') USER(*PUBLIC) DTAAUT(*R)

4. Select ***SYSTEM** and press the **Continue** button

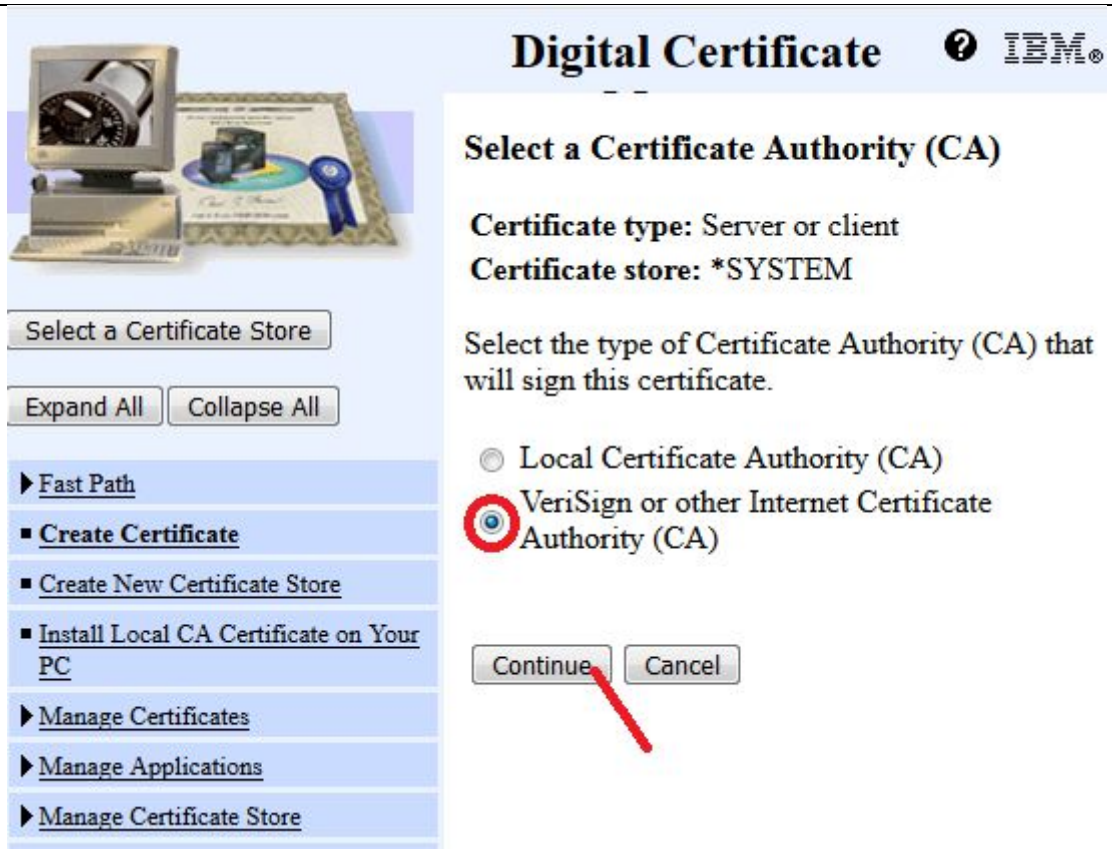


5. Type the **Certificate store password** and press the **Continue** button

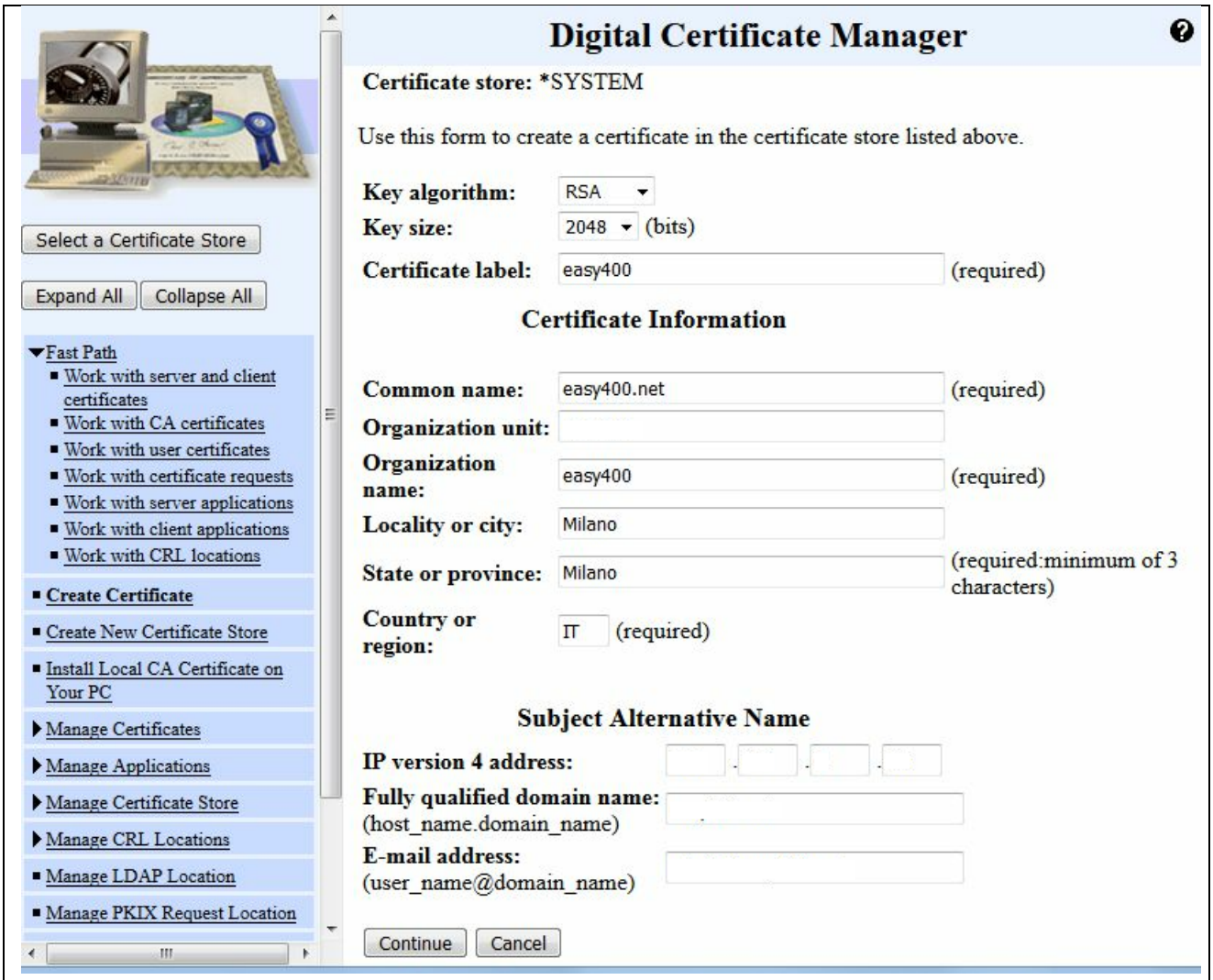
6. Press **Create Certificate**



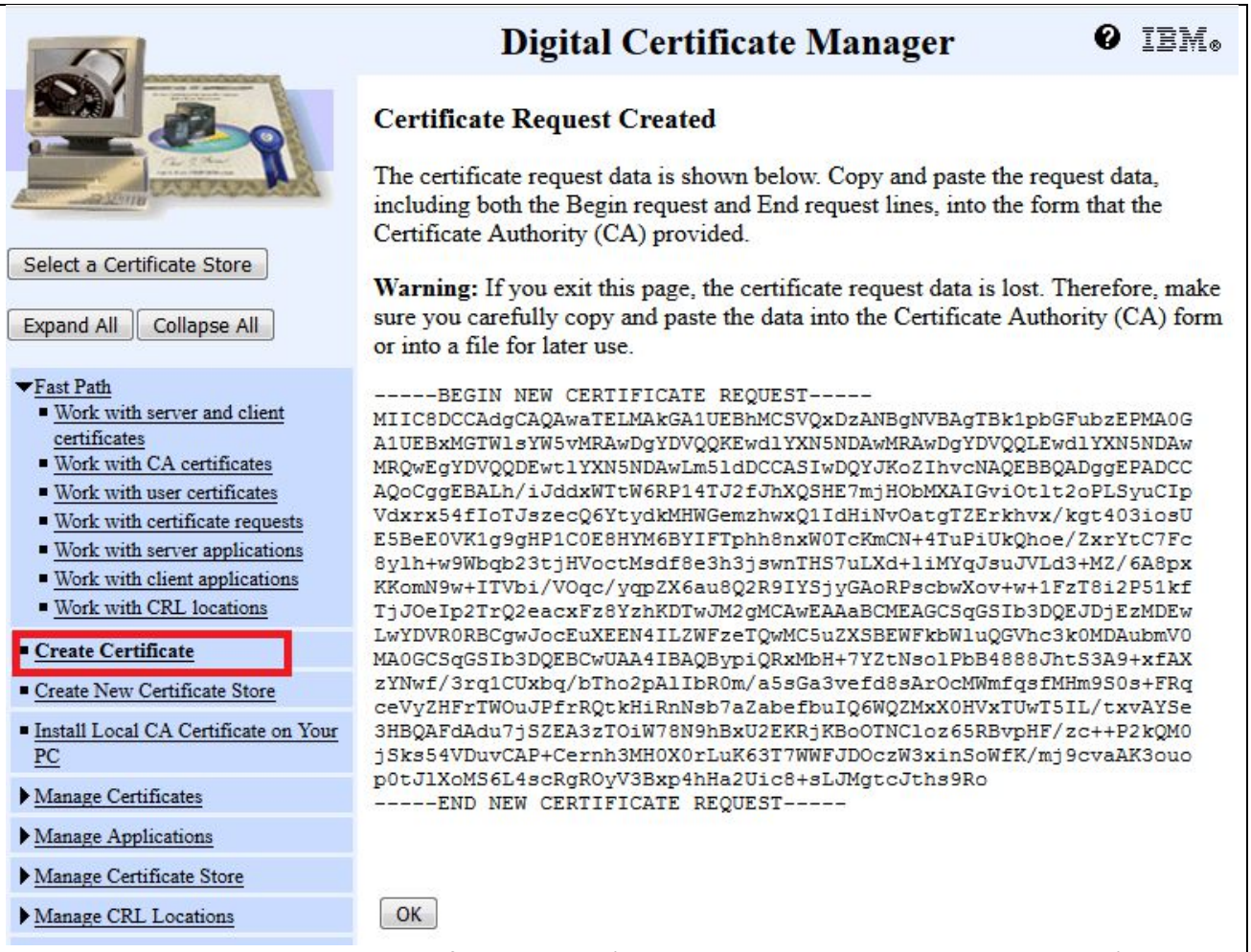
7. Select **Server or client certificate** and the the **Continue** button



8. Select **Verisign or other Internet CA** and press the **Continue** button



9. Fill in the required data and press the **Continue** button

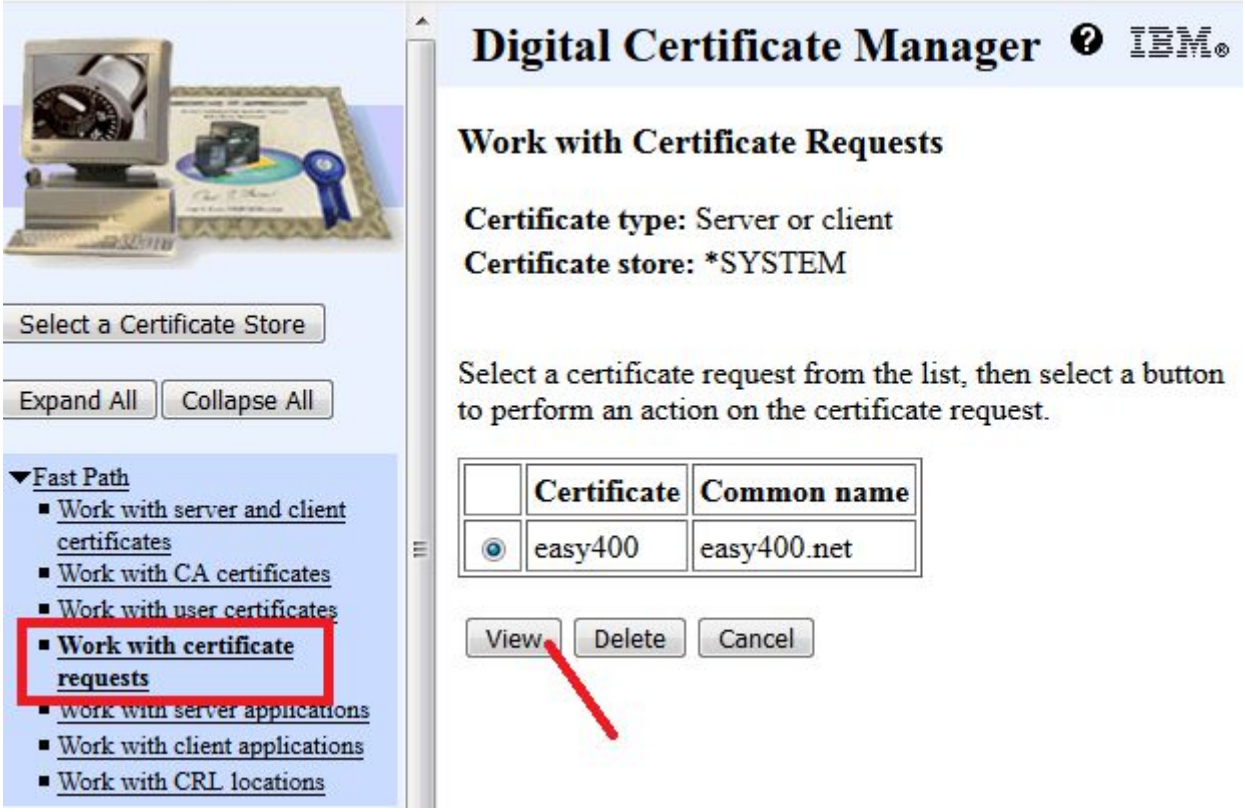


10. Copy and paste the entire certificate request (including the BEGIN and the END delimiters) to a .txt file. This .txt file will be used to generate a Certificate at a Certificate Authority (CA) of your choice. Then press the **OK** button.

11. The following is the CSR text file:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC8DCCAdgCAQAwaTELMAkGA1UEBhMCSVQxDzANBgNVBAgTBk1pbGFubzEPMA0G
A1UEBxMGTWlsYW5vMRAwDgYDVQQKEwdlYXN5NDAwMRAwDgYDVQQLEwdlYXN5NDAw
MRQwEgYDVQQDEwtlYXN5NDAwLm5ldDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALh/iJddxWTtW6RP14TJ2fJhXQSHE7mjHObMXAIGviOtlt2oPLSyuCIp
Vdxrx54fIoTJszecQ6YtydkMHWGemzhwxQ1IdHiNvOatgTZErkhvx/kgt403iosU
E5BeE0VK1g9gHP1C0E8HYM6BYIFTphh8nxW0TcKmCN+4TuPiUkQhoe/ZxrYtC7Fc
8ylh+w9Wbqb23tjHVoctMsdf8e3h3jswnTHS7uLXd+liMYqJsuJVLd3+MZ/6A8px
KKomN9w+ITVbi/VOqc/yqpZX6au8Q2R9IYSjyGAoRPscbwXov+w+1FzT8i2P51kf
TjJOeIp2TrQ2eacxFz8YzhKDTwJM2gMCAwEAAaBCMEAGCSqGSIb3DQEJDjEzMDEw
LwYDVR0RBCgwJocEuXEEN4ILZWFzeTQwMC5uZXSBEWFkbWluQGVhc3k0MDAubmV0
MA0GCSqGSIb3DQEBCwUAA4IBAQBypiQRxMbH+7YZtNsolPbB4888JhtS3A9+xfAX
zYNwf/3rq1CUxbq/bTho2pAlIbR0m/a5sGa3vefd8sArOcMWmfqsfMHm9S0s+FRq
ceVyZHFrTWOuJPfrRQtkHiRnNsb7aZabefbuIQ6WQZMxX0HVxTUwT5IL/txvAYSe
3HBQAFdAdu7jSZEA3zTOiW78N9hBxU2EKRjKBoOTNCloz65RBvpHF/zc++P2kQM0
jSks54VDuvCAP+Cernh3MH0X0rLuK63T7WWFJDOczW3xinSoWfK/mj9cvaAK3ouo
p0tJlXoMS6L4scRgROyV3Bxp4hHa2Uic8+sLJMgtcJths9Ro
-----END NEW CERTIFICATE REQUEST-----
```

12. To view your Certificare Request, in the left navigation leg press **Work with Certificate Request**:



Then press the **View** button.

13. Then press the **OK** button.

This CSR was then submitted to a public certificate Authority (CA) in order to obtain the needed certificate and install it on IBM i.

Note. We happened to submit our CSR to the public *CA Commodo-Sectigo*, ordering a *Sectigo SSL Certificate (DV)* 1 year validity.
Any other public CA could have been used for that.

PART 2 - Install CA SSL Certificates

In this document, we report was was done to install on site www.easy400.net the certificates received from CA Commodo-Sectigo.

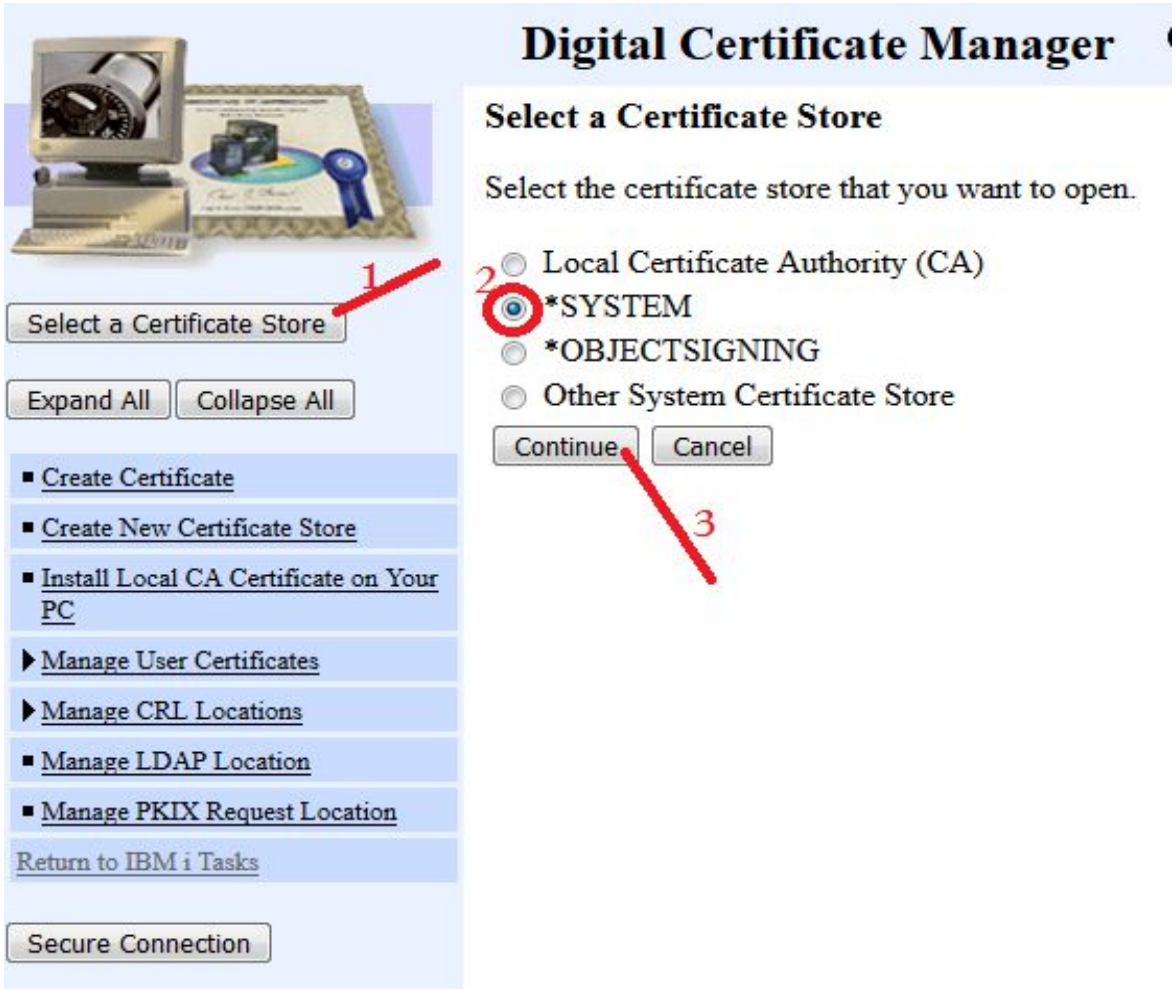
This type of process is documented in IBM i Support Knowledge Center page "*Importing and assigning the signed public certificate*" ,
https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzahu/rzahustep4sc.htm

1. Usually a CA delivers a number of certificates:

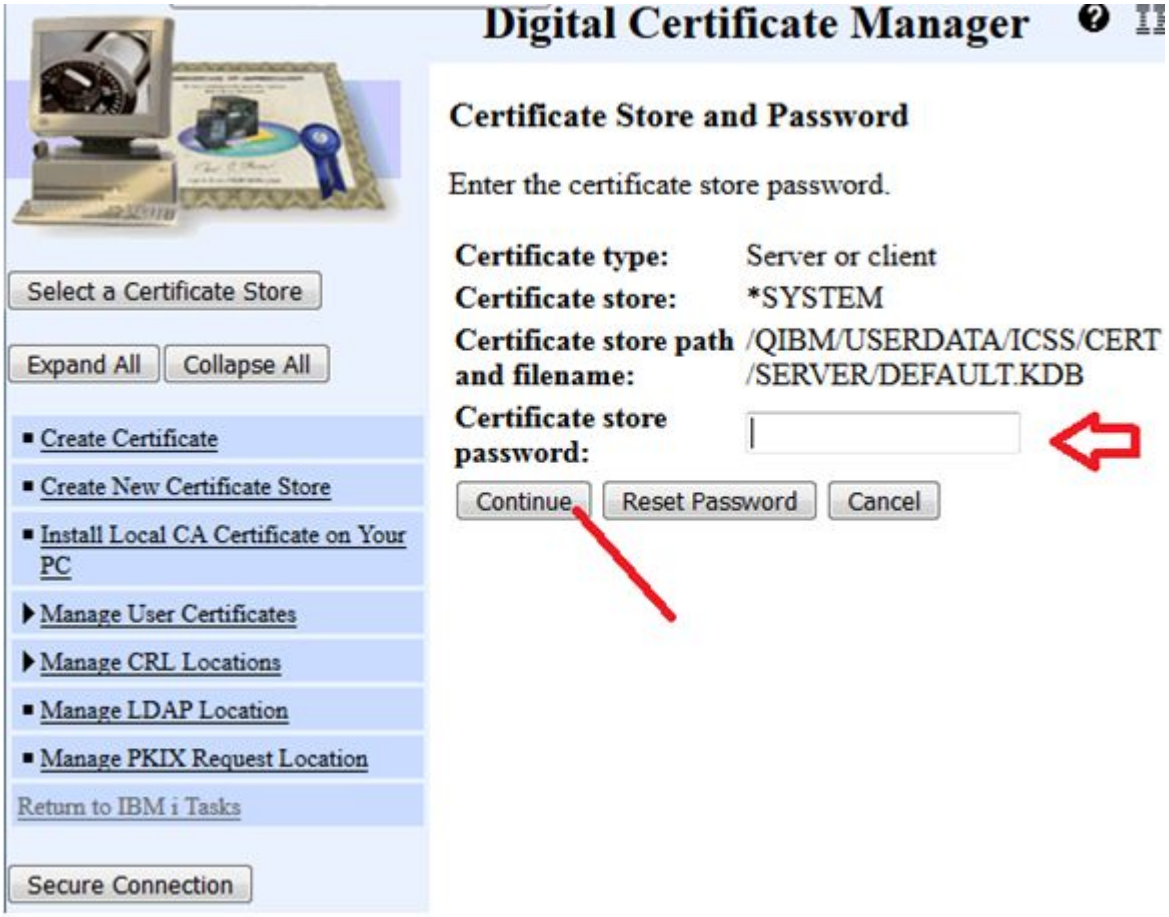
Type of certificates	**Examples of certificate names** (from CA Commodo-Sectigo)
Root	AddTrustExternal**CARoot**.crt
Intermediate (one or more)	USERTrustRSAAddTrust**CA**.crt
	SectigoRSADomainValidationSecureServer**CA**.crt
Domain (SSL certificate)	**easy400_net**.crt

2. You must create an IFS directory
   (Example: *MD DIR('/CERT') DTAAUT(*RX) OBJAUT(*NONE)*)
   and upload to it all the received certificates.

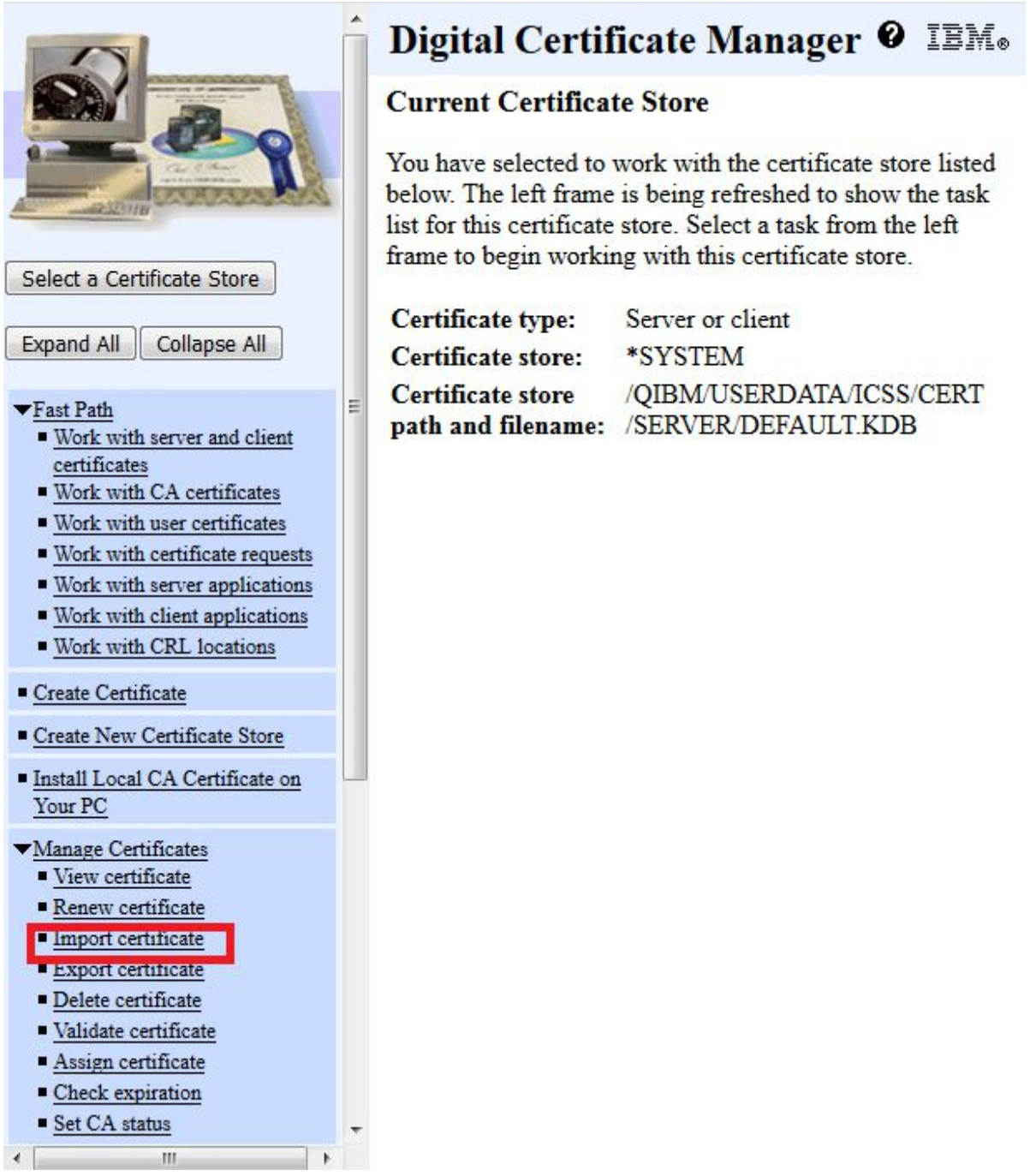
3. If needed, on your IBM i, start the HTTP instance *ADMIN and open the Digital Certificate Manager(DCM), http://...:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0



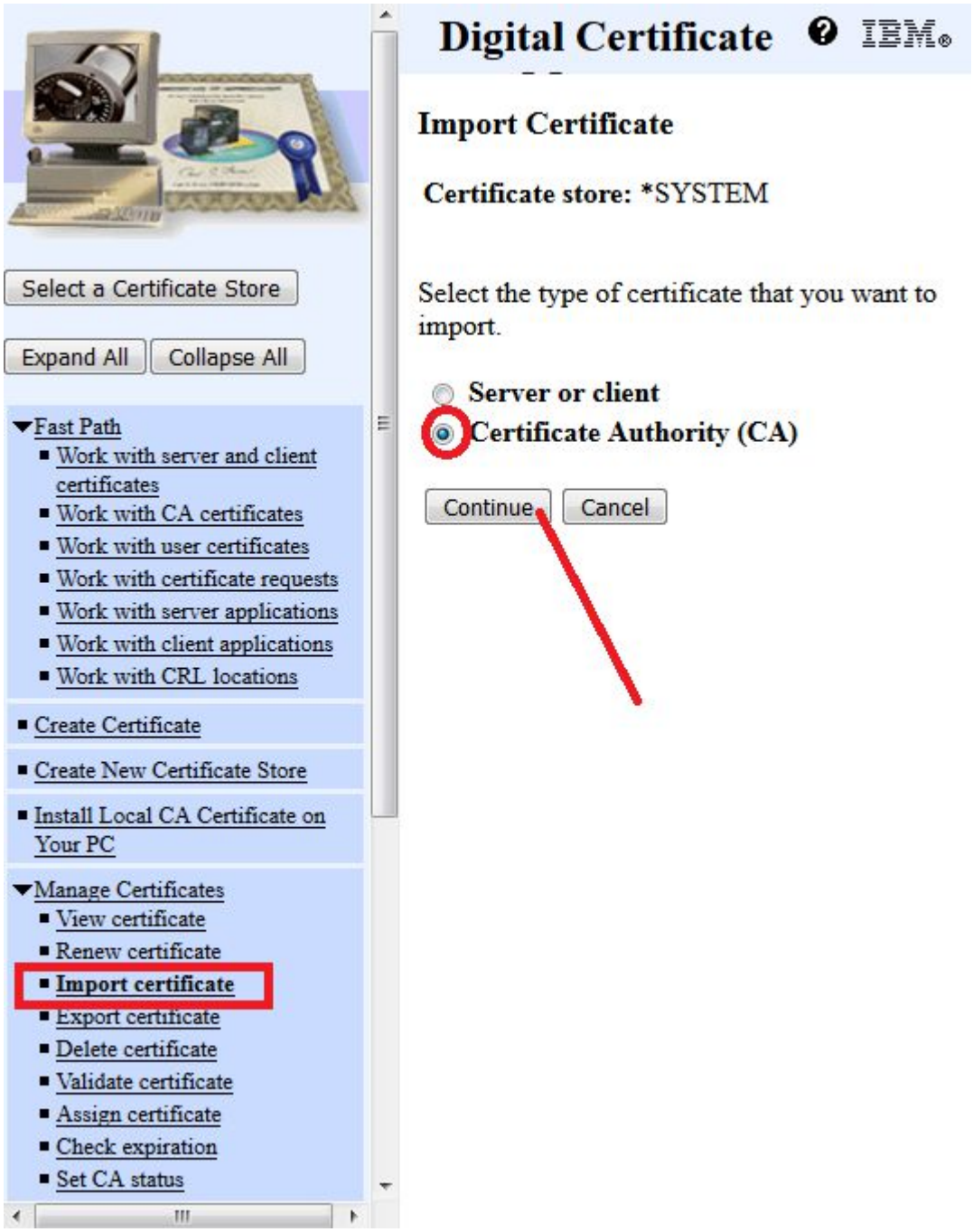
4. Enter the Certificate Store Password:



5. Expand **Manage Certificates** and press **Import Certificate**



6. Select **Certificate Authority (CA)** and press **Continue**



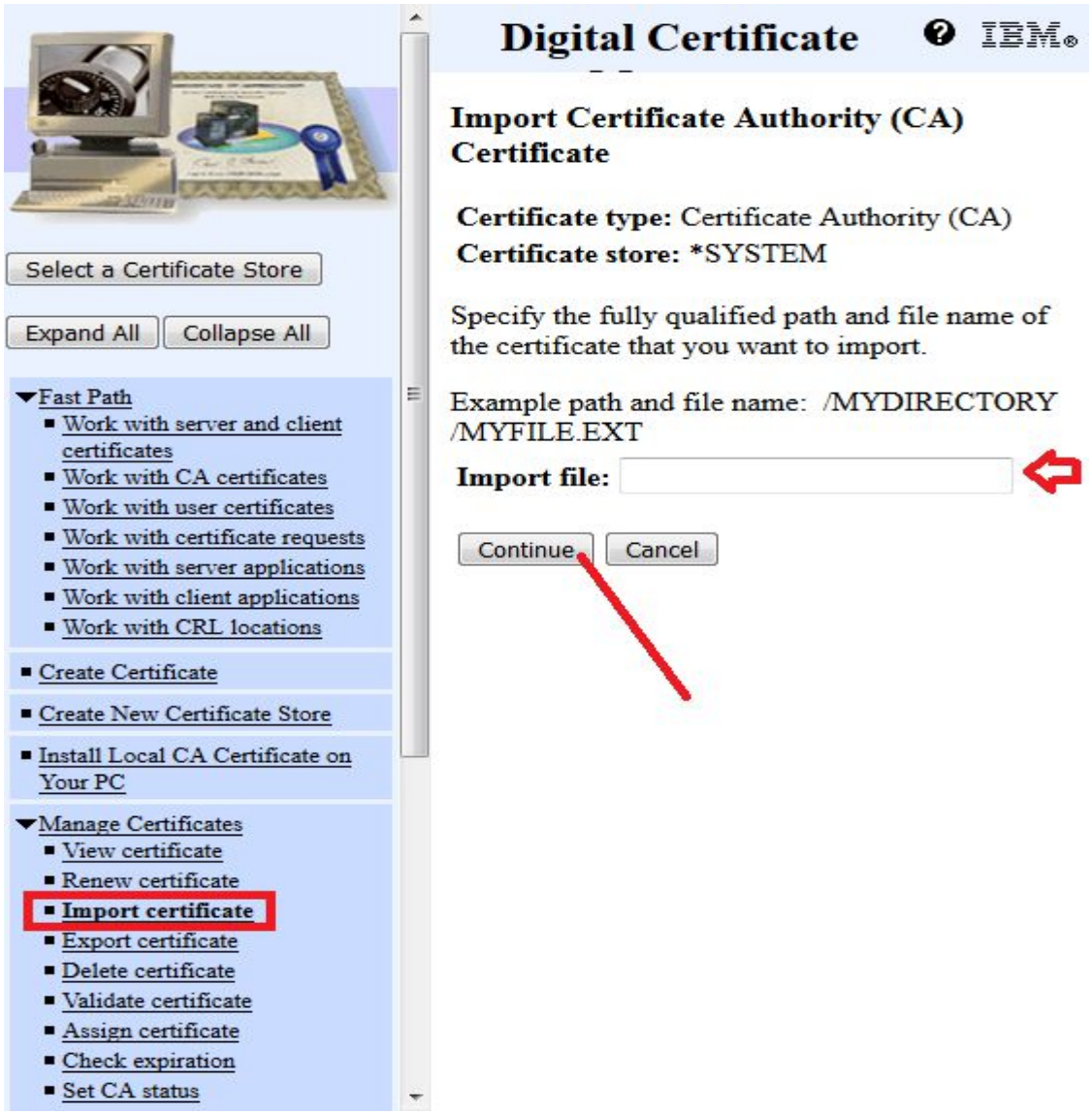
7. Import, one at a time,
   a. First, the CA Root certificate
      (example*: /cert/ AddTrustExternal**CARoot**.crt*)
   b. Then, one at a time the CA Intermediate CA certificates (any importing sequence is OK)
      (example: */cert/ USERTrustRSAAddTrust**CA**.crt*
      then */cert/SectigoRSADomainValidationSecureServer**CA**.crt*)

Note 1 - **DO NOT IMPORT** here the **domain SSL certificate** (example*: easy400_net.crt*). It is not a CA Certificate, it must be imported as "Server or Client" Certificate (*see next page*)

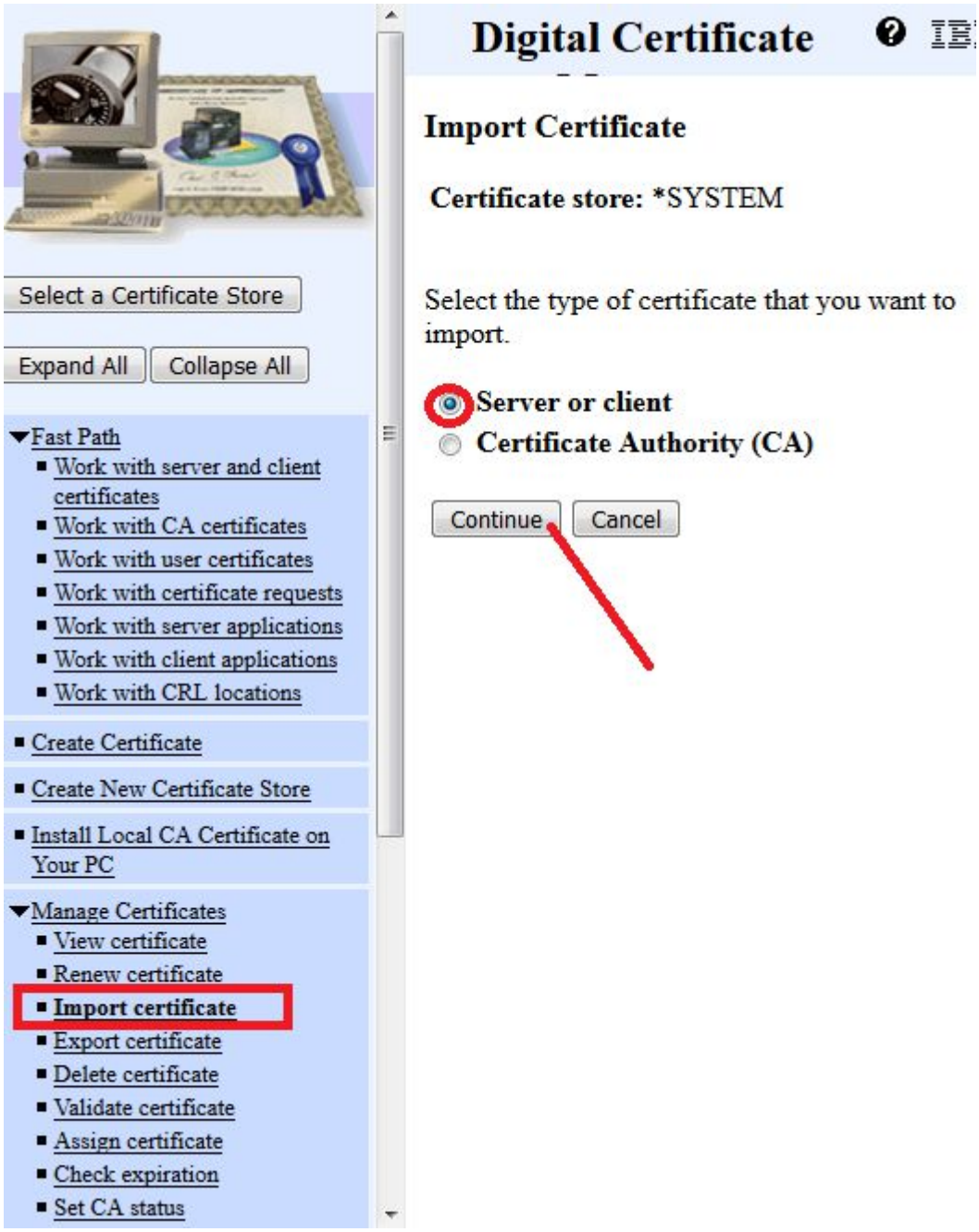
Note 2 – Be very careful in specifying the qualified name of the Import stream file, otherwise you get an error saying that it was not found. In such a case, just go back and fix the Import stream file name.

Note 3 – After pressing Continue, for each imported certificate you are requested to provide a **unique label** name. As an example, we provided the following unique names:

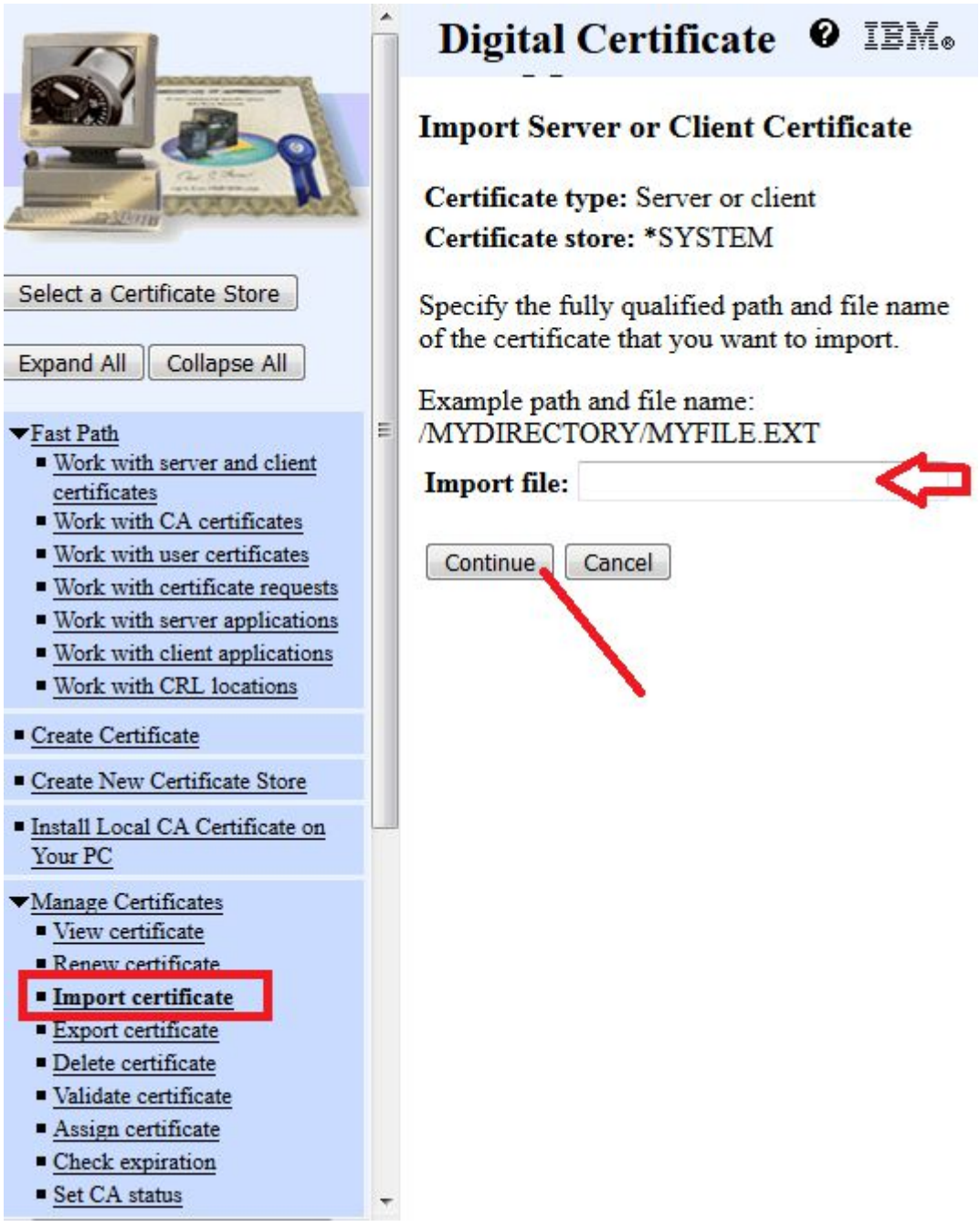
CA certificate	Unique label
*AddTrustExternal**CARoot**.crt*	*Sectigo Root CA Certificate*
*USERTrustRSAAddTrust**CA**.crt*	*Sectigo User Trust Intermediate Certificate*
*SectigoRSADomainValidationSecureServer**CA**.crt*	*Sectigo Domain Validation Intermediate Certificate*



8. Then, to import the **Domain** certificate (example: *easy400_net.crt*), in the navigation leg press again **Import Certificate**, but this time select **Server or Client** instead of **Certificate Authority (CA)**:

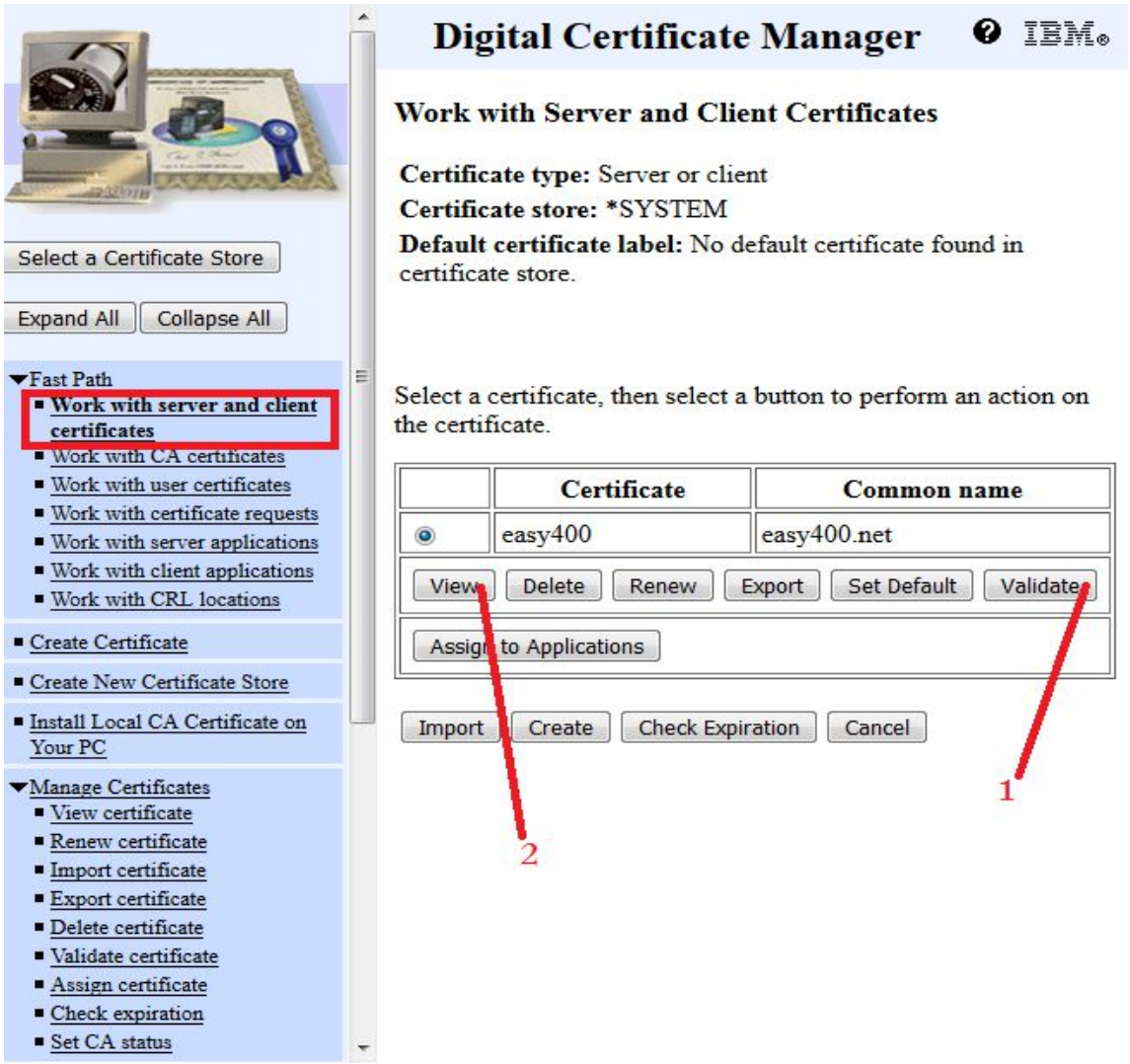


9. Now import the **Domain** certificate (example */cert/ easy400_net.crt*)

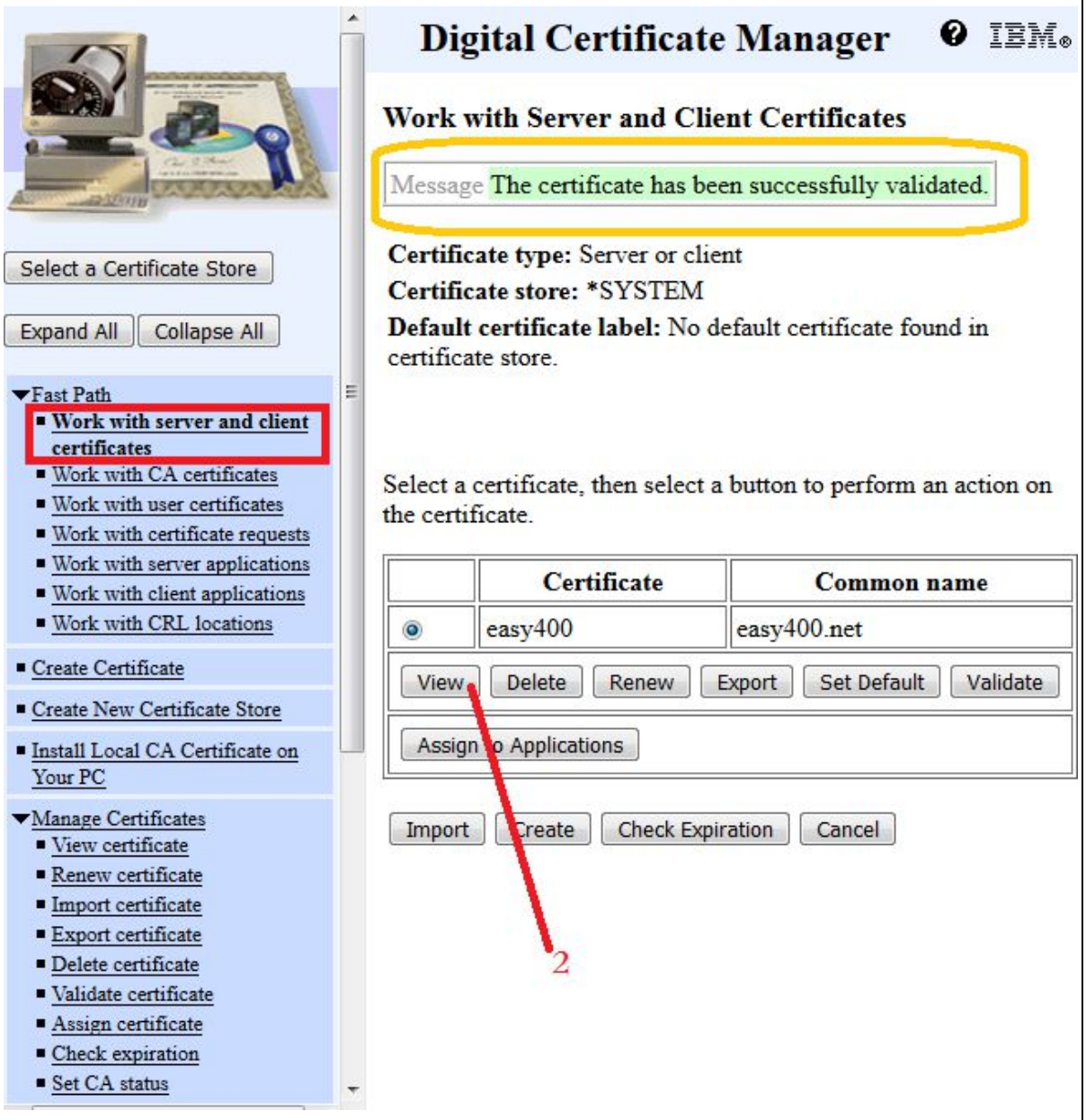


That ends the importing of certificates.

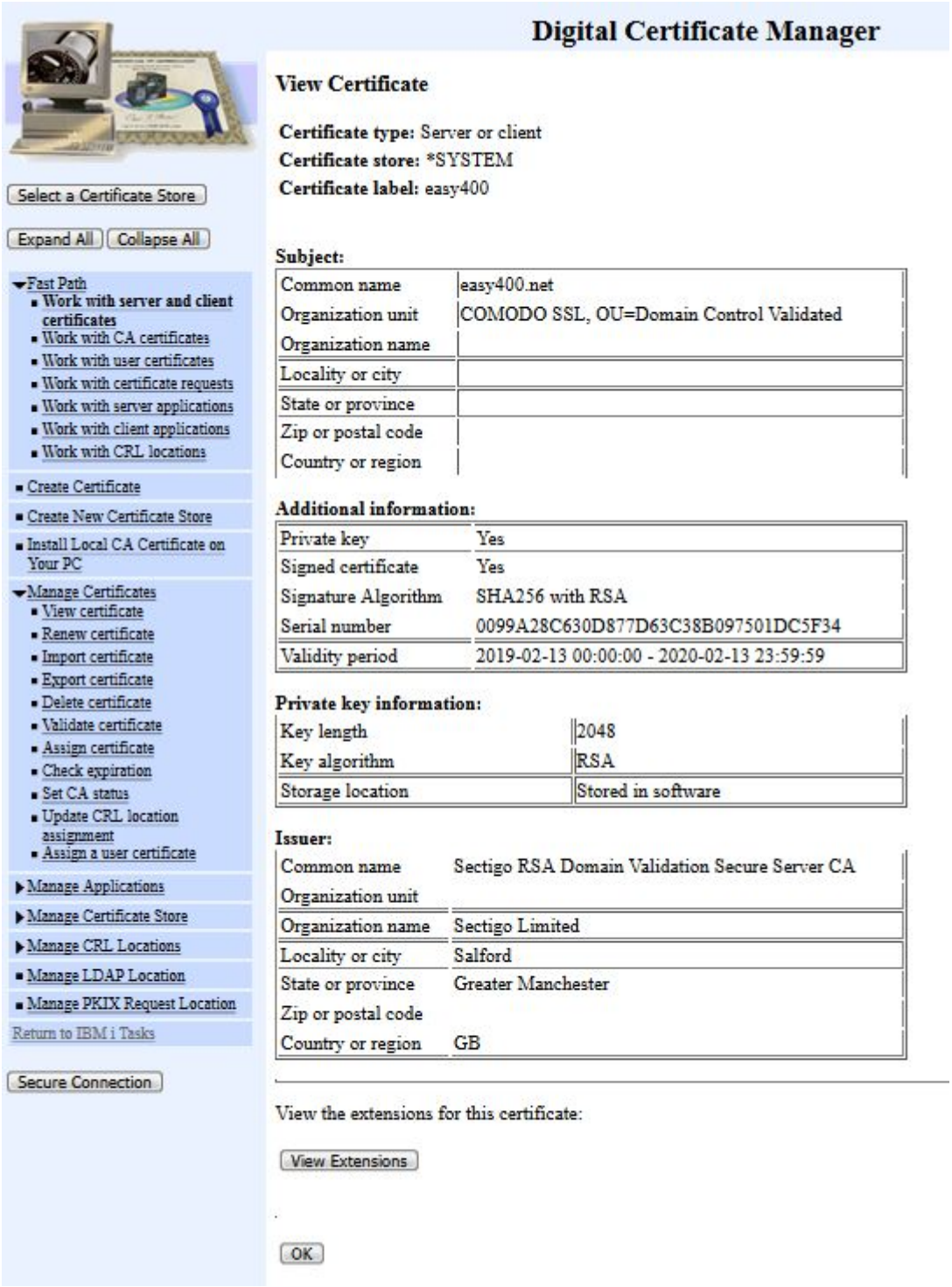
10. It is now time to verify your certificate:
    A. In the navigation leg press **Work with server and client certificates**
    Something like the following shows up:



11. Press the **Validate** button. The following MUST show up:



12. Optionally press button View to display some information about your certificate (e.g. its expiration date)



Press the OK button to end the certificate import.

Part 3 – Enable HTTP to SSL (Converting a HTTP site to HTTPS)

This type of process is documented in IBM i Support Knowledge Center page "*Configuring IBM HTTP Server for SSL on IBM i*" , https://www.ibm.com/support/knowledgecenter/en/SSYGQH_4.5.0/admin/install/t_inst_configure_ibm_http_server_ssl_ibmi.html .

Our HTTP instance is named **EASY400** and listens on the HTTP default port 80.
Our objective was: any request to this HTTP instance must be transferred to an HTTPS instance (named **EASY400SSL**) listening on port 443 (the default HTTPS port).

The schema of the original HTTP directives for the **EASY400** HTTP instance was:

```
Listen 80
NameVirtualHost 185.113.4.55:80
     … … …
<VirtualHost 185.113.4.55:80>
   ServerName www.easy400.net:80
     … … …
     … … …
</VirtualHost>
```

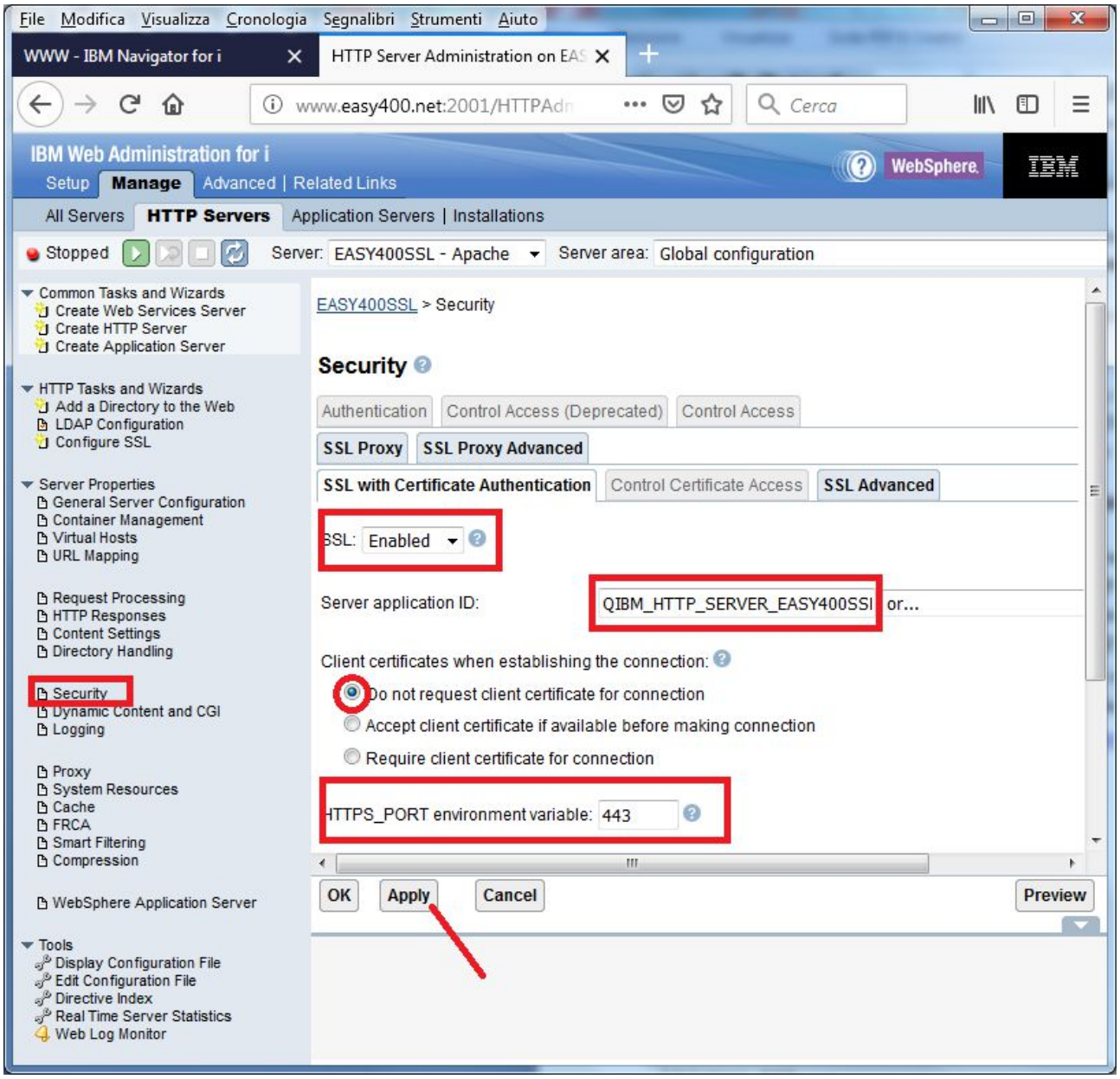
We created another HTTP instance named **EASY400SSL** with the same directives as instance **EASY400**, but listening on port 443:

```
Listen 443
NameVirtualHost 185.113.4.55:443
     … … …
<VirtualHost 185.113.4.55:443>
   ServerName www.easy400.net:443
     … … …
     … … …
</VirtualHost>
```

We shall see later on how these two configuration files had to be changed.

1. Configure HTTP Server for SSL using the IBM Web Administration for IBM i as follow:

i. Open a browser to the URL http://<system_hostname>:2001
ii. Get into **IBM Navigator for i**
iii. Under **IBM i Management**, select **Internet configurations** and get into **IBM WEB Administrator for i**
iv. From the **Server list** select your HTTP instance candidate for SSL (in our case that was HTTP instance EASY400SSL), then click button **Manage Details**
v. Click **Security** in the **Server Properties** list
vi. Click the **SSL with Certificate Authentication** tab in the form
vii. For **SSL** select **Enabled**
viii. On row **Server Application ID,** click the **"or…"** dropdown list and select the item select **"**QIBM_HTTP_SERVER_*<server_name>*"
(In our case it was QIBM_HTTP_SERVER_GIOVANNI)
Remember the name of this server certificate. You will need to select it again in the Digital Certificate Manager.
ix. Under **Client certificates when establishing the connection,** select **Do not request client certificate for connection** .
x. In the input field **HTTPS_PORT environment variable** usually nothing is specified.
However, if this HTTP instance runs CGI programs, some CGI program may need to know if it is running under HTTPS or not. In such a case you need to enter in this field the port number (443). This will cause the directive SETENV HTTPS_PORT be set in the configuration file. In this way a CGI program would be able to know if running under HTTPS by retrieving the environment variable HTTPS. Check out page https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzaie/rzaiemod_ibm_ssl.htm .
See the following picture:



xi. Click the **Apply** button to update the HTTP instance configuration file, then the **OK** button.

xii. As a result, The HTTP instance configuration file is added some SSL directives (the red ones):

```
Listen 443
LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
SSLEngine On
SSLAppName QIBM_HTTP_SERVER_EASY400SSL
SetEnv HTTPS_PORT 443
NameVirtualHost 185.113.4.55:443
     … … …
<VirtualHost 185.113.4.55:443>
   ServerName www.easy400.net:443
     … … …
     … … …
</VirtualHost>
```

2. Assigning the SSL certificate to application HTTP

If needed, on your IBM i, start the HTTP instance *ADMIN and open the Digital Certificate Manager (DCM), http://<system hostname>:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0 .

i. **Select a Certificate Store**
ii. Select ***SYSTEM** and press **Continue** button
iii. Type the **Certificate Store password** and press **Continue** button
iv. Select **Manage Applications**
v. Select **Update certificate assignment** and press **Continue** button
vi. Select **Server** and press **Continue** button
vii. Select the HTTP instance name (example: QIBM_HTTP_SERVER_EASY400SSL) and press the **Update Certificate Assignment** button
viii. Select the certificated to be assigned to the "http instance" Application ID, press **Validate** to check validation, press **Update Certificate Assignment** button. You should get the message *The certificate was assigned to the application* .
ix. You may then start the updated HTTPS instance (in our case EASY400SSL)

3. Transferring requests from the HTTP instance to the HTTPS instance

The last thing you need is that any http request coming to the HTTP instance on port 80 (in our case the instance EASY400) is sent to the HTTPS instance on port 443.
You do this by adding two directives (the red ones in the following example) to the HTTP instance.
Example:

```
Listen 80
NameVirtualHost 185.113.4.55:80
     … … …
<VirtualHost 185.113.4.55:80>
   ServerName www.easy400.net:80
   RewriteEngine On
   RewriteRule ^(.*)$ https://www.easy400.net:443$1 [R,L]
     … … …
     … … …
</VirtualHost>
```

Just restart the HTTP instance on port 80 and start sending requests to it.