

**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>

Digital Certificate Manager IBM®

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 LDAP Location
- Manage PKIX Request Location

Return to IBM i Tasks

Secure Connection

5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1, 5761-SS1, 5770-SS1 (C) Copyright IBM Corporation 1997, 2014
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

GENUINE RSA ENCRYPTION ENGINE Contains software from RSA Data Security, Inc.

Get Started

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”).

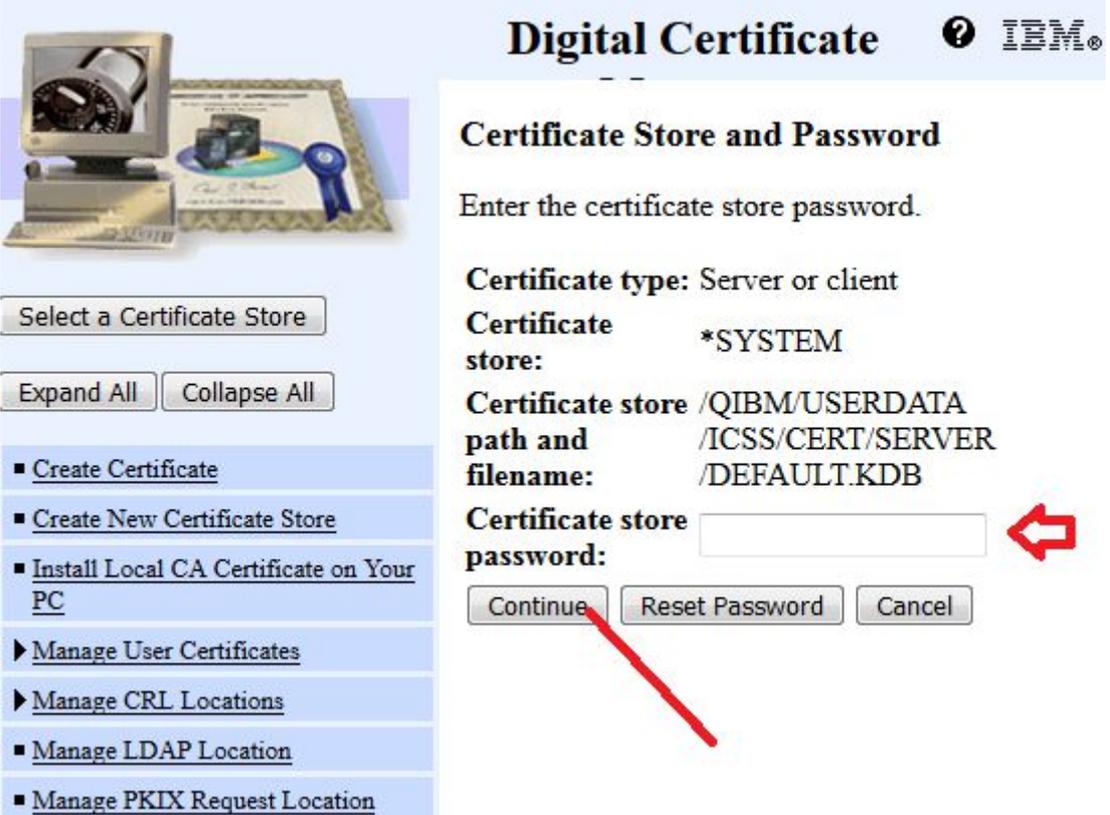
This you do by running the following commands:

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



The screenshot shows the 'Digital Certificate' dialog box with the title bar 'Digital Certificate' and the IBM logo. The main heading is 'Select a Certificate Store'. Below it, the instruction reads 'Select the certificate store that you want to open.' There are four radio button options: 'Local Certificate Authority (CA)', '*SYSTEM' (which is selected and circled in red), '*OBJECTSIGNING', and 'Other System Certificate Store'. At the bottom, there are 'Continue' and 'Cancel' buttons. A red arrow points from the 'Continue' button to the instruction below. On the left side, there is a navigation pane with a tree view containing several items: 'Create Certificate', 'Create New Certificate Store', 'Install Local CA Certificate on Your PC', 'Manage User Certificates', 'Manage CRL Locations', 'Manage LDAP Location', and 'Manage PKIX Request Location'. There are also buttons for 'Select a Certificate Store', 'Expand All', and 'Collapse All'.

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



The screenshot shows the 'Digital Certificate' dialog box with the title bar 'Digital Certificate' and the IBM logo. The main heading is 'Certificate Store and Password'. Below it, the instruction reads 'Enter the certificate store password.' The 'Certificate type' is set to 'Server or client'. The 'Certificate store' is '*SYSTEM'. The 'Certificate store path and filename' is '/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB'. There is a text input field for the 'Certificate store password:' with a red arrow pointing to it from the right. At the bottom, there are 'Continue', 'Reset Password', and 'Cancel' buttons. A red arrow points from the 'Continue' button to the instruction below. The left navigation pane and buttons are identical to the previous screenshot.

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



Digital Certificate ? IBM®

Current Certificate Store

You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.

Certificate type: Server or client

Certificate store: *SYSTEM

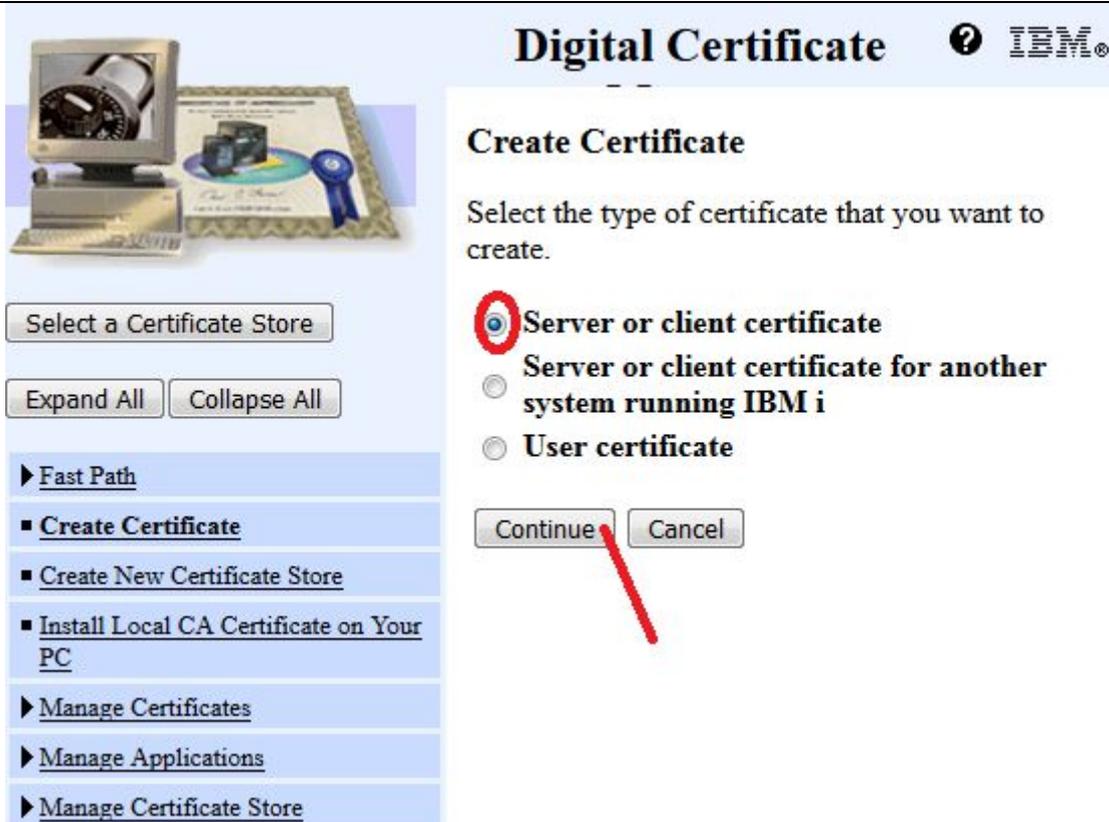
Certificate store path and filename: /QIBM/USERDATA /ICSS/CERT/SERVER /DEFAULT.KDB

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](#)
- ▶ [Manage Certificate Store](#)

6. Press **Create Certificate**



Digital Certificate ? IBM®

Create Certificate

Select the type of certificate that you want to create.

Server or client certificate

Server or client certificate for another system running IBM i

User certificate

Continue Cancel

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](#)
- ▶ [Manage Certificate Store](#)

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



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

Digital Certificate Manager

Certificate store: *SYSTEM

Use this form to create a certificate in the certificate store listed above.

Key algorithm: RSA
Key size: 2048 (bits)
Certificate label: easy400 (required)

Certificate Information

Common name: easy400.net (required)
Organization unit:
Organization name: easy400 (required)
Locality or city: Milano
State or province: Milano (required: minimum of 3 characters)
Country or region: IT (required)

Subject Alternative Name

IP version 4 address:
Fully qualified domain name: (host_name.domain_name)
E-mail address: (user_name@domain_name)

Continue Cancel

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



Digital Certificate Manager



Certificate Request Created

The certificate request data is shown below. Copy and paste the request data, including both the Begin request and End request lines, into the form that the Certificate Authority (CA) provided.

Warning: If you exit this page, the certificate request data is lost. Therefore, make sure you carefully copy and paste the data into the Certificate Authority (CA) form or into a file for later use.

Select a Certificate Store

Expand All Collapse All

- ▼ Fast Path
 - Work with server and client certificates
 - Work with CA certificates
 - Work with user certificates
 - Work with certificate requests
 - Work with server applications
 - Work with client applications
 - Work with CRL locations
 - Create Certificate
 - Create New Certificate Store
 - Install Local CA Certificate on Your PC
 - Manage Certificates
 - Manage Applications
 - Manage Certificate Store
 - Manage CRL Locations

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC8DCCAdgCAQAwaTElMAkGA1UEBhMCSVQxDzANBgNVBAgTBk1pbGFubzEPMA0G
A1UEBxMGTW1sYW5vMRAwDgYDVQQKEwd1YXN5NDAwMRAwDgYDVQQLEwd1YXN5NDAw
MRQwEgYDVQQDEwt1YXN5NDAwLm5ldDCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALh/iJddxWttW6RP14TJ2fJhXQSHE7mjHOBMXAIGviOtl2oPLSyuCIp
Vdxrx54fIoTJszecQ6YtydkMHWGemzhwxQ1IdHiNvOatgTZErkhvx/kgt403iosU
E5BeE0VK1g9gHP1C0E8HYM6BYIFTphh8nxW0TcKmcN+4TuPiUkQhoe/ZxrYtC7Fc
8ylh+w9Wbqb23tjHVoctMsdF8e3h3jswNTHS7uLXd+liMYqJsuJVLd3+MZ/6A8px
KKomN9w+ITVbi/VOqc/yqpZX6au8Q2R9IYSjyGAoRPsCbWxov+w+1FzT8i2P51kf
TjJ0eIp2TrQ2eacxFz8YzhKDTwJM2gMCAwEAAaBCMEAGCSqGS1b3DQEJDjEzMDew
LwYDVR0RBCgwJocEuXEEN4ILZWFzeTQwMC5uZXSBEWFkbWluQGVC3k0MDAubmV0
MA0GCSqGS1b3DQEBCwUAA4IBAQByp1QRxMbH+7YZtNsolPbB4888JhtS3A9+xfAX
zYNwf/3rq1CUxbq/bTho2pAlIbR0m/a5sGa3vefd8sArOcMwMfqsFMHm9S0s+FRq
ceVyZHFRTWOUJPfrRQtKHiRnNsb7aZabefbuIQ6WQZMxX0HVxTUwT5IL/txvAYSe
3HBQAFdAdu7jSZEa3zTOiW78N9hBxU2EKrkjKBoOTNC1oz65RBvpHF/zc++P2kQM0
jSks54VDuvCAP+Cernh3MH0X0rLuK63T7WWFJD0czW3xinSoWfK/mj9cvaAK3ouo
p0tJlXoMS6L4scRgROyV3Bxp4hHa2Uic8+sLJMgtcJths9Ro
-----END NEW CERTIFICATE REQUEST-----

```

OK

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
A1UEBxMGTW1sYW5vMRAwDgYDVQQKEwd1YXN5NDAwMRAwDgYDVQQLEwd1YXN5NDAw
MRQwEgYDVQQDEwt1YXN5NDAwLm5ldDCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALh/iJddxWttW6RP14TJ2fJhXQSHE7mjHOBMXAIGviOtl2oPLSyuCIp
Vdxrx54fIoTJszecQ6YtydkMHWGemzhwxQ1IdHiNvOatgTZErkhvx/kgt403iosU
E5BeE0VK1g9gHP1C0E8HYM6BYIFTphh8nxW0TcKmcN+4TuPiUkQhoe/ZxrYtC7Fc
8ylh+w9Wbqb23tjHVoctMsdF8e3h3jswNTHS7uLXd+liMYqJsuJVLd3+MZ/6A8px
KKomN9w+ITVbi/VOqc/yqpZX6au8Q2R9IYSjyGAoRPsCbWxov+w+1FzT8i2P51kf
TjJ0eIp2TrQ2eacxFz8YzhKDTwJM2gMCAwEAAaBCMEAGCSqGS1b3DQEJDjEzMDew
LwYDVR0RBCgwJocEuXEEN4ILZWFzeTQwMC5uZXSBEWFkbWluQGVC3k0MDAubmV0
MA0GCSqGS1b3DQEBCwUAA4IBAQByp1QRxMbH+7YZtNsolPbB4888JhtS3A9+xfAX
zYNwf/3rq1CUxbq/bTho2pAlIbR0m/a5sGa3vefd8sArOcMwMfqsFMHm9S0s+FRq
ceVyZHFRTWOUJPfrRQtKHiRnNsb7aZabefbuIQ6WQZMxX0HVxTUwT5IL/txvAYSe
3HBQAFdAdu7jSZEa3zTOiW78N9hBxU2EKrkjKBoOTNC1oz65RBvpHF/zc++P2kQM0
jSks54VDuvCAP+Cernh3MH0X0rLuK63T7WWFJD0czW3xinSoWfK/mj9cvaAK3ouo
p0tJlXoMS6L4scRgROyV3Bxp4hHa2Uic8+sLJMgtcJths9Ro
-----END NEW CERTIFICATE REQUEST-----

```

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

Digital Certificate Manager ? IBM®

Work with Certificate Requests

Certificate type: Server or client
Certificate store: *SYSTEM

Select a certificate request from the list, then select a button to perform an action on the certificate request.

	Certificate	Common name
<input checked="" type="radio"/>	easy400	easy400.net

Then press the **View** button.

Digital Certificate Manager

View Certificate Request

Certificate type: Server or client
 Certificate store: *SYSTEM
 Certificate label: easy400

Certificate request information:

Common name	easy400.net
Organization unit	easy400
Organization name	easy400
Locality or city	Milano
State or province	Milano
Zip or postal code	
Country or region	IT

Additional information:

Private key	Yes
Signed certificate request	Yes

Private key information:

Key algorithm	RSA
Key length	2048
Storage location	Stored in software

OK

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 what 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 CA root.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>

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

1

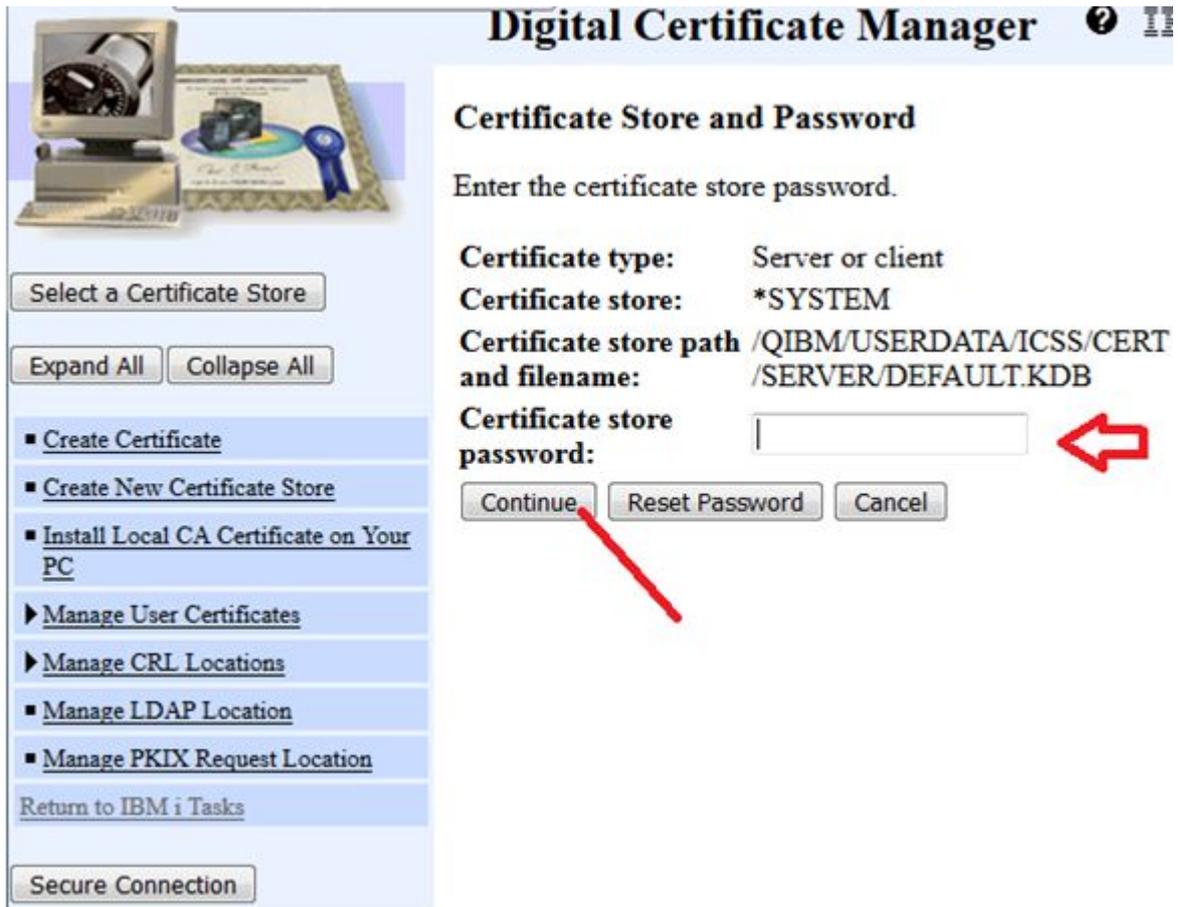
2

3

- [Create Certificate](#)
- [Create New Certificate Store](#)
- [Install Local CA Certificate on Your PC](#)
- ▶ [Manage User Certificates](#)
- ▶ [Manage CRL Locations](#)
- [Manage LDAP Location](#)
- [Manage PKIX Request Location](#)

[Return to IBM i Tasks](#)

4. Enter the Certificate Store Password:



Digital Certificate Manager

Certificate Store and Password

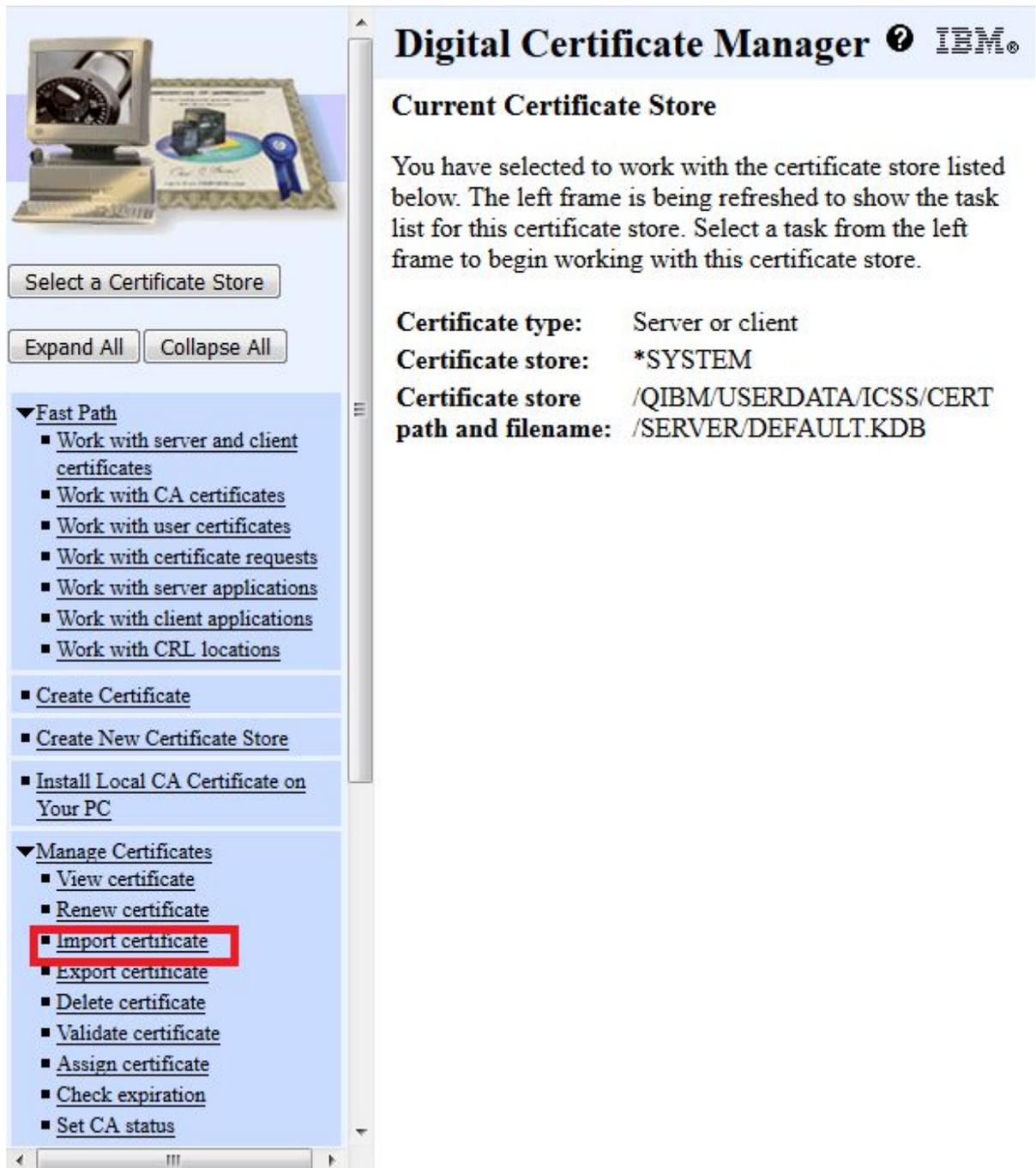
Enter the certificate store password.

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate store path and filename: /QIBM/USERDATA/ICSS/CERT /SERVER/DEFAULT.KDB
Certificate store password:

Left Panel:

- 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 LDAP Location](#)
- [Manage PKIX Request Location](#)
- [Return to IBM i Tasks](#)
-

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



Digital Certificate Manager 

Current Certificate Store

You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate store path and filename: /QIBM/USERDATA/ICSS/CERT /SERVER/DEFAULT.KDB

Select a Certificate Store

Expand All Collapse All

- ▼ **Fast Path**
 - Work with server and client certificates
 - Work with CA certificates
 - Work with user certificates
 - Work with certificate requests
 - Work with server applications
 - Work with client applications
 - Work with CRL locations
- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- ▼ **Manage Certificates**
 - View certificate
 - Renew certificate
 - Import certificate**
 - Export certificate
 - Delete certificate
 - Validate certificate
 - Assign certificate
 - Check expiration
 - Set CA status

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

Digital Certificate ? IBM®

Import Certificate

Certificate store: *SYSTEM

Select the type of certificate that you want to import.

Server or client

Certificate Authority (CA)

Continue Cancel

Select a Certificate Store

Expand All Collapse All

- ▼ **Fast Path**
 - [Work with server and client certificates](#)
 - [Work with CA certificates](#)
 - [Work with user certificates](#)
 - [Work with certificate requests](#)
 - [Work with server applications](#)
 - [Work with client applications](#)
 - [Work with CRL locations](#)
- [Create Certificate](#)
- [Create New Certificate Store](#)
- [Install Local CA Certificate on Your PC](#)
- ▼ **Manage Certificates**
 - [View certificate](#)
 - [Renew certificate](#)
 - **Import certificate**
 - [Export certificate](#)
 - [Delete certificate](#)
 - [Validate certificate](#)
 - [Assign certificate](#)
 - [Check expiration](#)
 - [Set CA status](#)

7. Import, one at a time,
 - a. First, the **CA Root certificate**
(example: /cert/AddTrustExternalCARoot.crt)
 - b. Then, one at a time the **CA Intermediate CA certificates** (any importing sequence is OK)
(example: /cert/USERTrustRSAAddTrustCA.crt
then /cert/SectigoRSADomainValidationSecureServerCA.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
AddTrustExternalCARoot.crt	Sectigo Root CA Certificate
USERTrustRSAAddTrustCA.crt	Sectigo User Trust Intermediate Certificate
SectigoRSADomainValidationSecureServerCA.crt	Sectigo Domain Validation Intermediate Certificate

Digital Certificate

Import Certificate Authority (CA) Certificate

Certificate type: Certificate Authority (CA)
Certificate store: *SYSTEM

Specify the fully qualified path and file name of the certificate that you want to import.

Example path and file name: /MYDIRECTORY /MYFILE.EXT

Import file:

- ▼ **Fast Path**
 - [Work with server and client certificates](#)
 - [Work with CA certificates](#)
 - [Work with user certificates](#)
 - [Work with certificate requests](#)
 - [Work with server applications](#)
 - [Work with client applications](#)
 - [Work with CRL locations](#)
- [Create Certificate](#)
- [Create New Certificate Store](#)
- [Install Local CA Certificate on Your PC](#)
- ▼ **Manage Certificates**
 - [View certificate](#)
 - [Renew certificate](#)
 - **[Import certificate](#)**
 - [Export certificate](#)
 - [Delete certificate](#)
 - [Validate certificate](#)
 - [Assign certificate](#)
 - [Check expiration](#)
 - [Set CA status](#)

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)**:

Digital Certificate ? [List Icon]

Import Certificate

Certificate store: *SYSTEM

Select the type of certificate that you want to import.

Server or client

Certificate Authority (CA)

Continue Cancel

Fast Path

- Work with server and client certificates
- Work with CA certificates
- Work with user certificates
- Work with certificate requests
- Work with server applications
- Work with client applications
- Work with CRL locations

Create Certificate

Create New Certificate Store

Install Local CA Certificate on Your PC

Manage Certificates

- View certificate
- Renew certificate
- Import certificate**
- Export certificate
- Delete certificate
- Validate certificate
- Assign certificate
- Check expiration
- Set CA status

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

Digital Certificate IBM®

Import Server or Client Certificate

Certificate type: Server or client
Certificate store: *SYSTEM

Specify the fully qualified path and file name of the certificate that you want to import.

Example path and file name:
`/MYDIRECTORY/MYFILE.EXT`

Import file:

Fast Path

- Work with server and client certificates
- Work with CA certificates
- Work with user certificates
- Work with certificate requests
- Work with server applications
- Work with client applications
- Work with CRL locations

Create Certificate

- Create New Certificate Store
- Install Local CA Certificate on Your PC

Manage Certificates

- View certificate
- Renew certificate
- Import certificate**
- Export certificate
- Delete certificate
- Validate certificate
- Assign certificate
- Check expiration
- Set CA status

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:

Digital Certificate Manager

Work with Server and Client Certificates

Certificate type: Server or client
Certificate store: *SYSTEM
Default certificate label: No default certificate found in certificate store.

Select a certificate, then select a button to perform an action on the certificate.

	Certificate	Common name
<input checked="" type="radio"/>	easy400	easy400.net

1

2

The screenshot shows the IBM Digital Certificate Manager interface. On the left is a navigation pane with a 'Fast Path' section where 'Work with server and client certificates' is highlighted with a red box. Below it are sections for 'Create Certificate', 'Create New Certificate Store', 'Install Local CA Certificate on Your PC', and 'Manage Certificates'. The main content area shows the 'Work with Server and Client Certificates' page. It displays certificate details for 'easy400' with common name 'easy400.net'. A row of buttons includes 'View', 'Delete', 'Renew', 'Export', 'Set Default', and 'Validate'. A red arrow labeled '1' points to the 'Validate' button. Another red arrow labeled '2' points to the 'View' button. At the bottom of the main area are buttons for 'Import', 'Create', 'Check Expiration', and 'Cancel'.

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

The screenshot shows the IBM Digital Certificate Manager interface. On the left is a navigation pane with a 'Fast Path' section where 'Work with server and client certificates' is highlighted with a red box. The main area displays a message: 'Message The certificate has been successfully validated.' Below this, it shows details for a certificate: 'Certificate type: Server or client', 'Certificate store: *SYSTEM', and 'Default certificate label: No default certificate found in certificate store.' A table lists certificates with columns for 'Certificate' and 'Common name'. The first entry is 'easy400' with 'easy400.net'. Below the table are buttons for 'View', 'Delete', 'Renew', 'Export', 'Set Default', and 'Validate'. A red arrow points from the 'Validate' button to a red number '2'.

Digital Certificate Manager IBM

Work with Server and Client Certificates

Message The certificate has been successfully validated.

Certificate type: Server or client
Certificate store: *SYSTEM
Default certificate label: No default certificate found in certificate store.

Select a certificate, then select a button to perform an action on the certificate.

	Certificate	Common name
<input checked="" type="radio"/>	easy400	easy400.net

Buttons: View, Delete, Renew, Export, Set Default, Validate

Assign to Applications

Buttons: Import, Create, Check Expiration, Cancel

2

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

Digital Certificate Manager



Select a Certificate Store

Expand All Collapse All

- ▼ Fast Path
 - Work with server and client certificates
 - Work with CA certificates
 - Work with user certificates
 - Work with certificate requests
 - Work with server applications
 - Work with client applications
 - Work with CRL locations
- Create Certificate
- Create New Certificate Store
- Install Local CA Certificate on Your PC
- ▼ Manage Certificates
 - View certificate
 - Renew certificate
 - Import certificate
 - Export certificate
 - Delete certificate
 - Validate certificate
 - Assign certificate
 - Check expiration
 - Set CA status
 - Update CRL location assignment
 - Assign a user certificate
- ▶ Manage Applications
- ▶ Manage Certificate Store
- ▶ Manage CRL Locations
- Manage LDAP Location
- Manage PKIX Request Location
- [Return to IBM i Tasks](#)

Secure Connection

View Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: easy400

Subject:

Common name	easy400.net
Organization unit	COMODO SSL, OU=Domain Control Validated
Organization name	
Locality or city	
State or province	
Zip or postal code	
Country or region	

Additional information:

Private key	Yes
Signed certificate	Yes
Signature Algorithm	SHA256 with RSA
Serial number	0099A28C630D877D63C38B097501DC5F34
Validity period	2019-02-13 00:00:00 - 2020-02-13 23:59:59

Private key information:

Key length	2048
Key algorithm	RSA
Storage location	Stored in software

Issuer:

Common name	Sectigo RSA Domain Validation Secure Server CA
Organization unit	
Organization name	Sectigo Limited
Locality or city	Salford
State or province	Greater Manchester
Zip or postal code	
Country or region	GB

View the extensions for this certificate:

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:

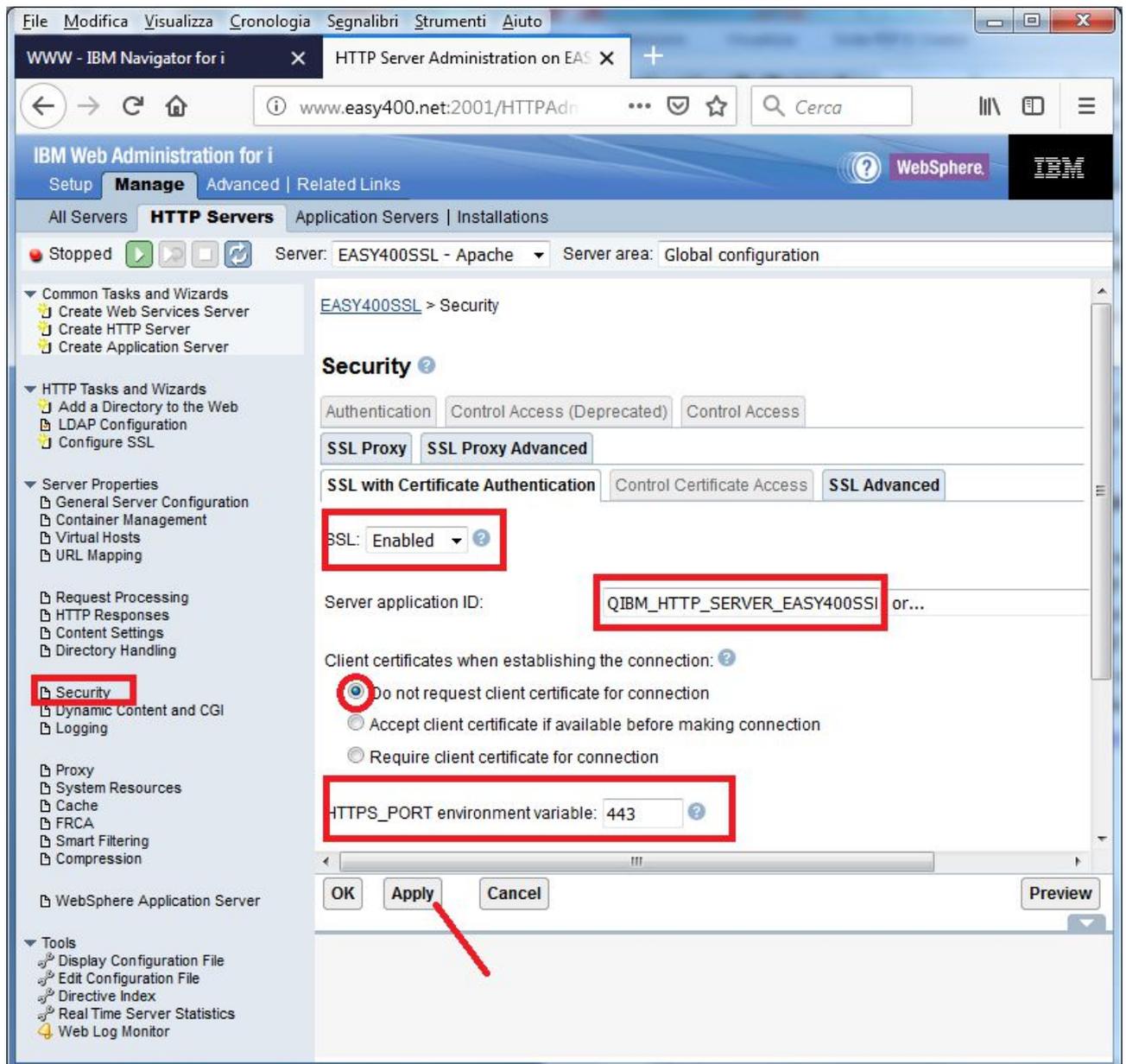
```
Listen 443
NameVirtualHost 185.113.4.55:443
    ... ..
<VirtualHost 185.113.4.55:443>
    ServerName www.easy400.net:443
    ... ..
    ... ..
</VirtualHost>
```

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/QHTTSPVR.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.