**Certificate Renewal process (CI Training Dev and Training Test Environments)**

|  |
| --- |
|  |

**PKI Certificate Request**

**Marriott and IBM Confidential**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Document Id** | |  | |
|  | | **Version** | | **0.1** | |
|  | | **Owner** | | **IBM Siebel Admin Team**  **Pankaj Mishra** | |

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **V. No.** | **Issue Date** | **Modified By** | **Description of Changes** | **Location/Para/Page/Sec. No.** |
| 0.1 |  | PANKAJ MISHRA | Initial Draft |  |

Contents

[Email notification for certificate renewal 3](#_Toc503344939)

[Raising request for new certificates 4](#_Toc503344940)

[Pre-Requisites 6](#_Toc503344941)

[Invoking the Oracle Wallet Manager: 6](#_Toc503344942)

[Opening a Wallet: 9](#_Toc503344943)

[Add a certificate request 11](#_Toc503344944)

[Downloading the certificate 14](#_Toc503344945)

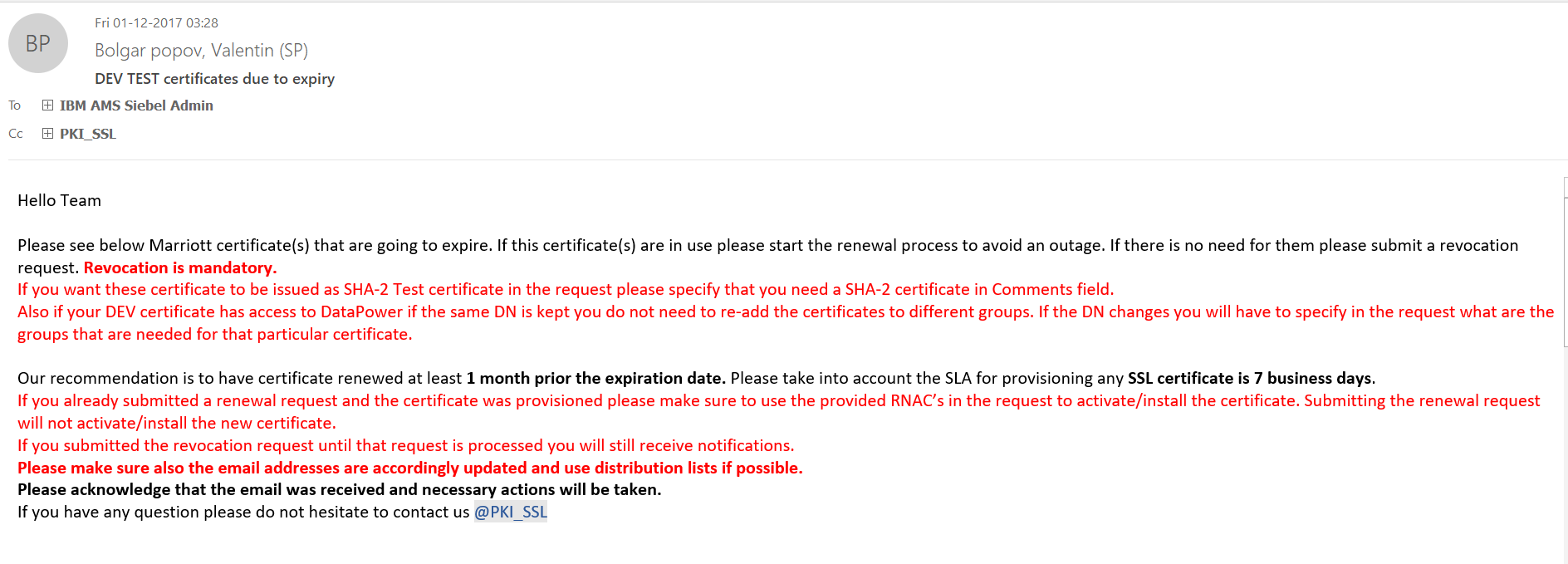
[Removal of old certificate 16](#_Toc503344946)

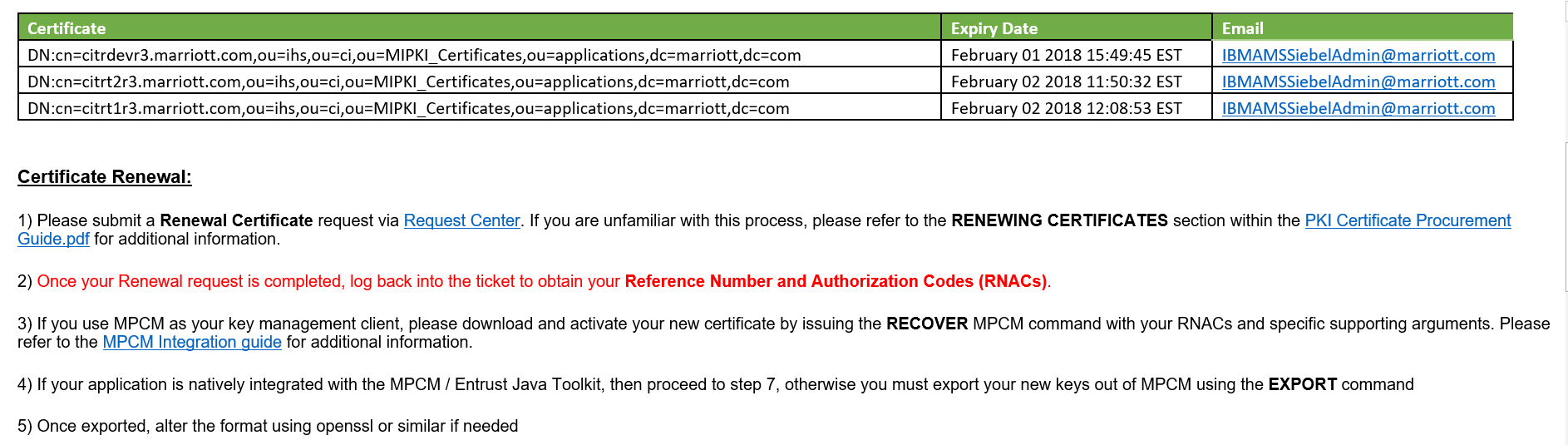
[Recycling the web server 17](#_Toc503344947)

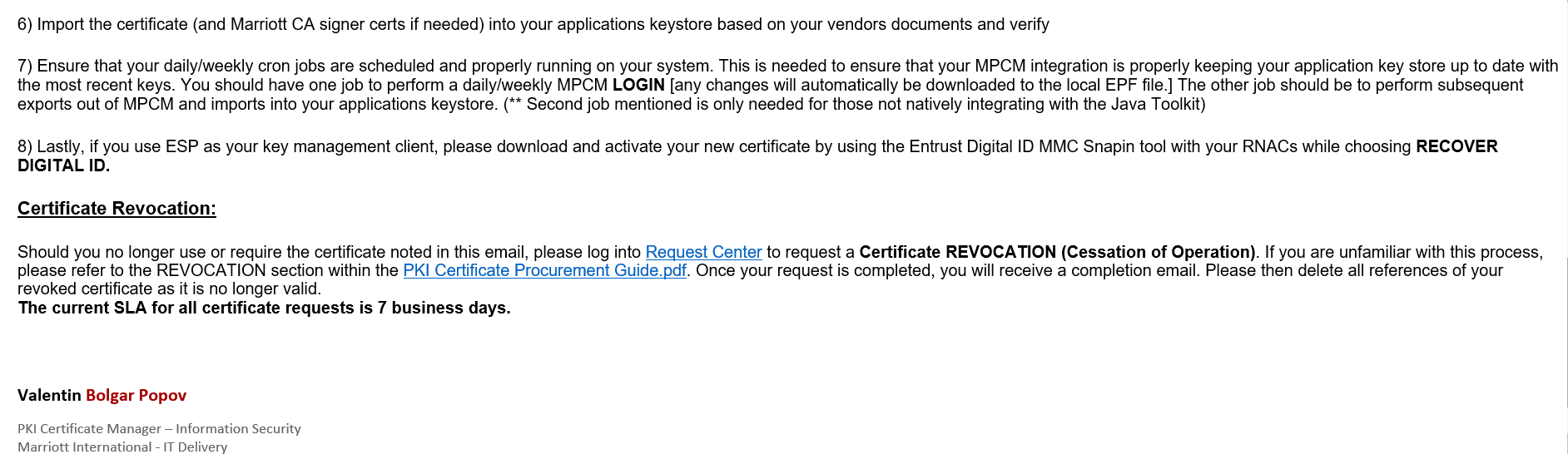
[Verification 18](#_Toc503344948)

# *Email notification for certificate renewal*

Below is the notification we start receiving once the expiry due date for the existing certificates are- round the corner:



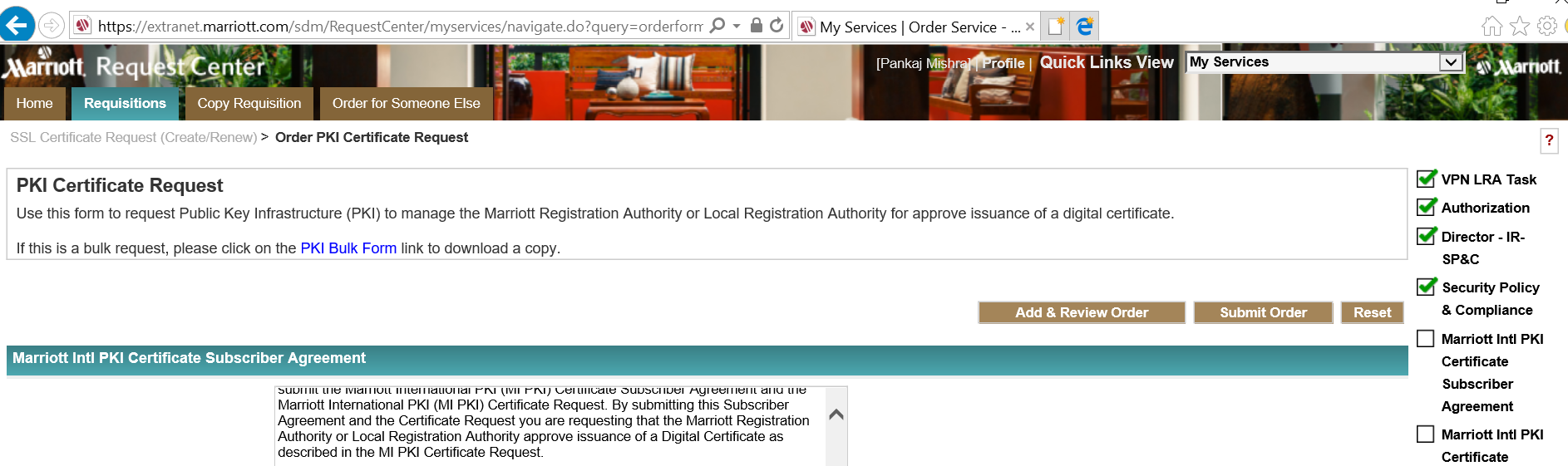




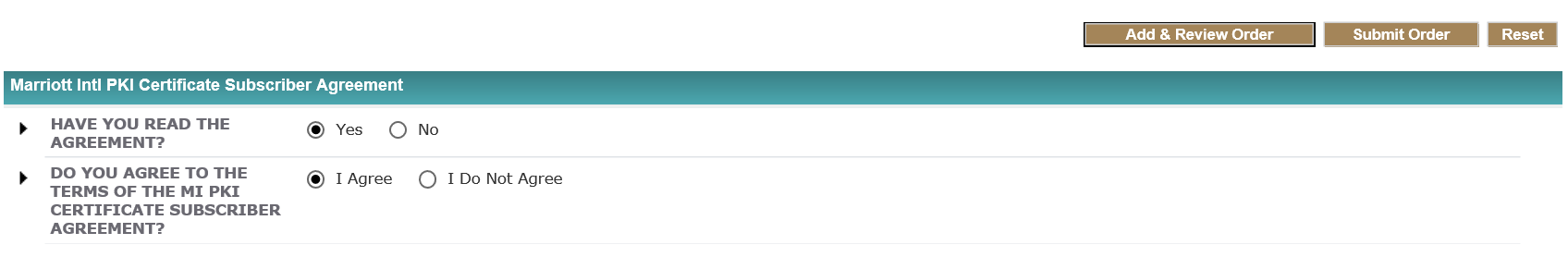
# *Raising request for new certificates*

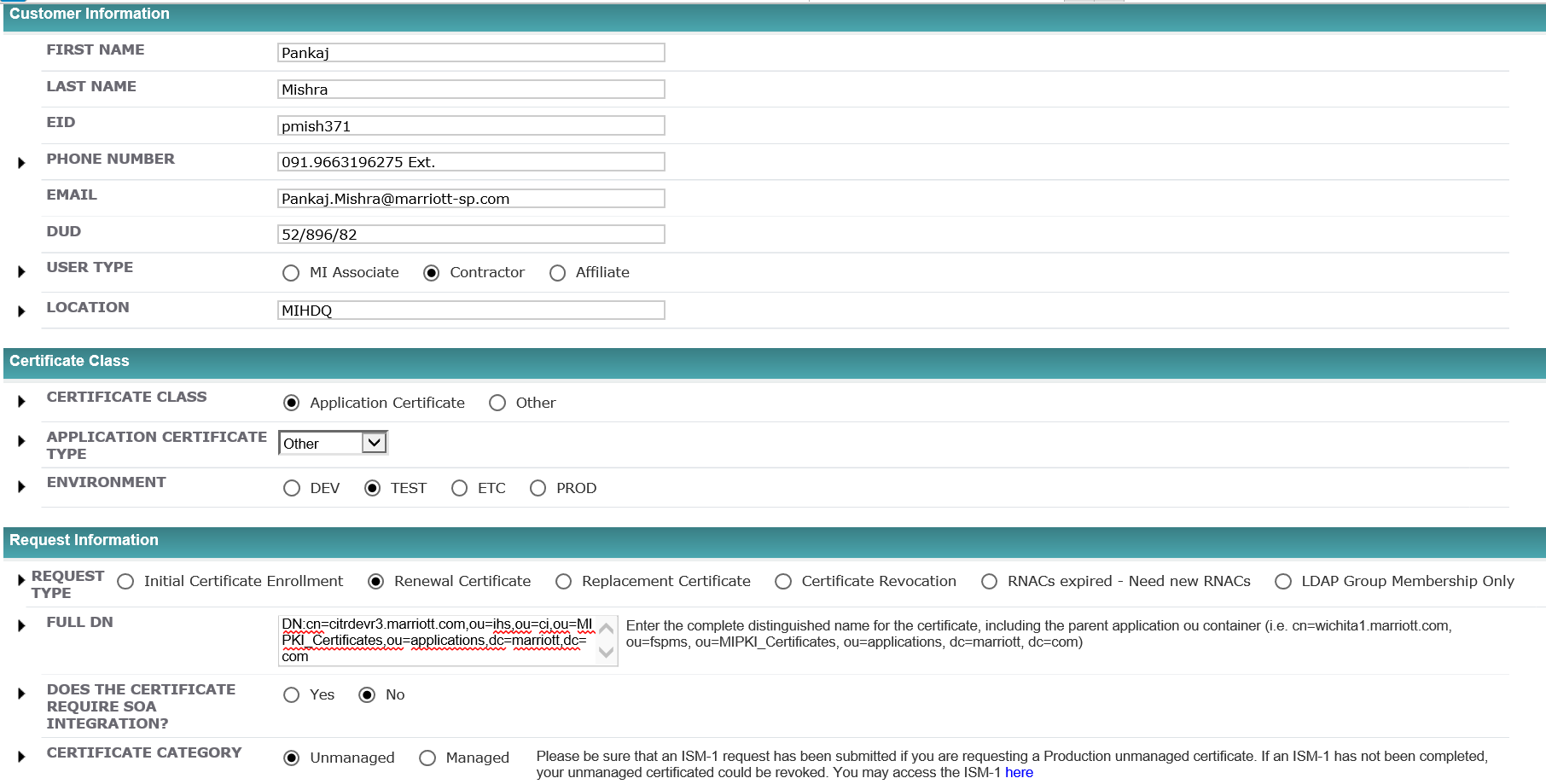
*Access request center:*

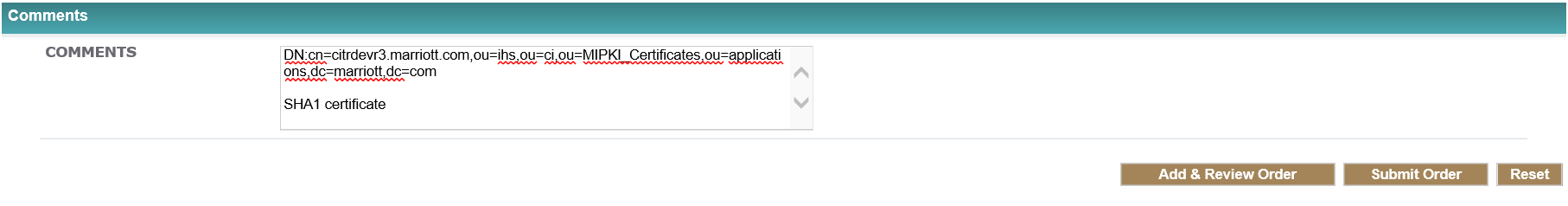
<https://extranet.marriott.com/sdm/RequestCenter/myservices/navigate.do?query=orderform&sid=302&>



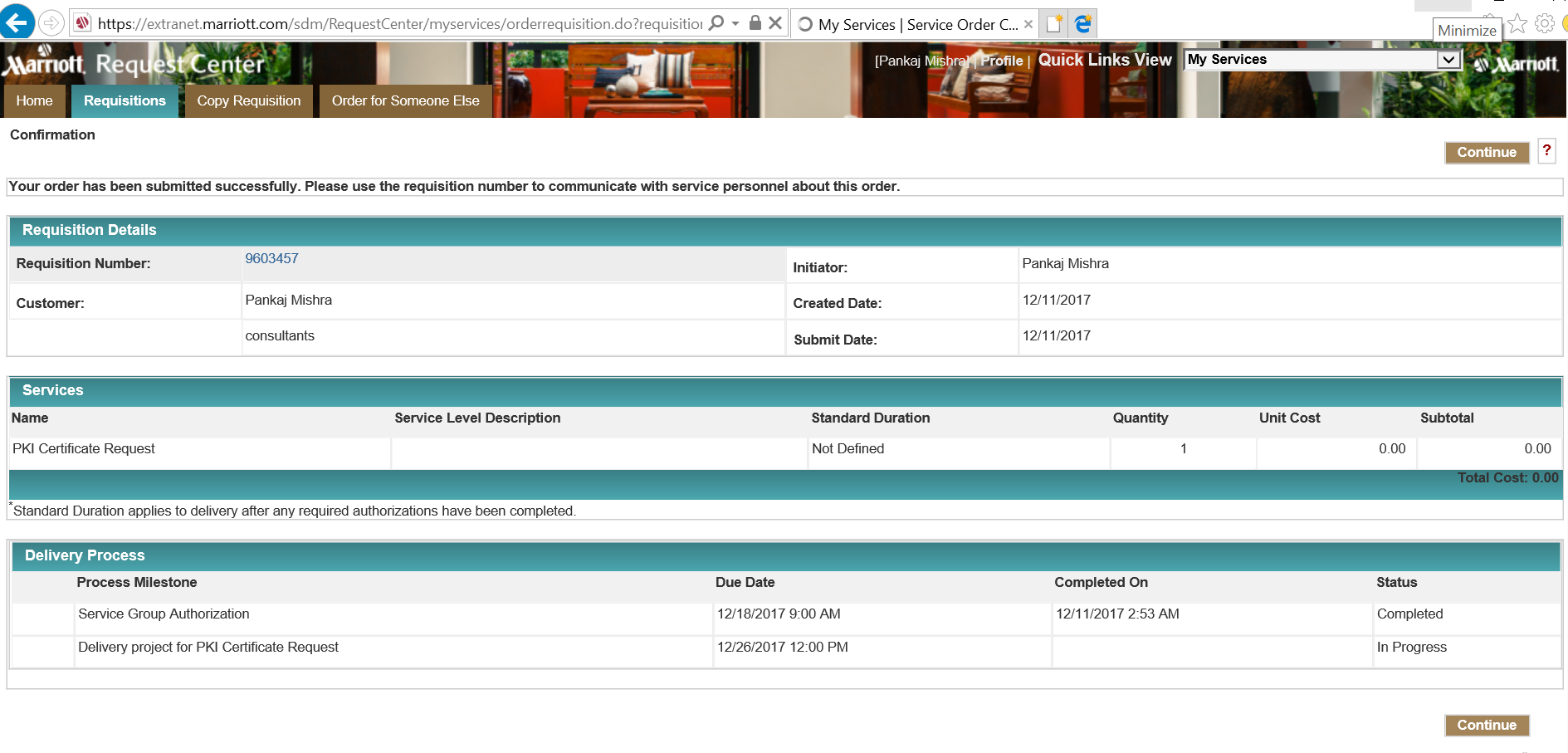
Scroll below and click accept





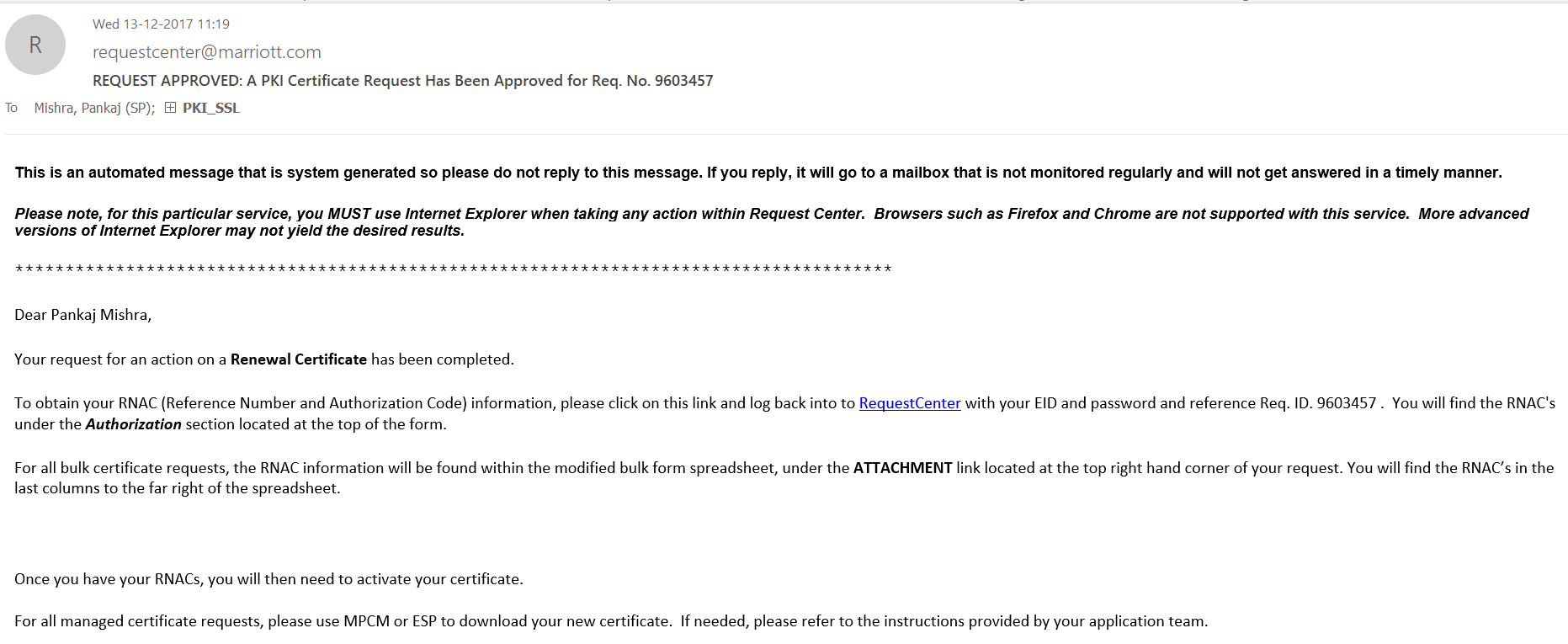


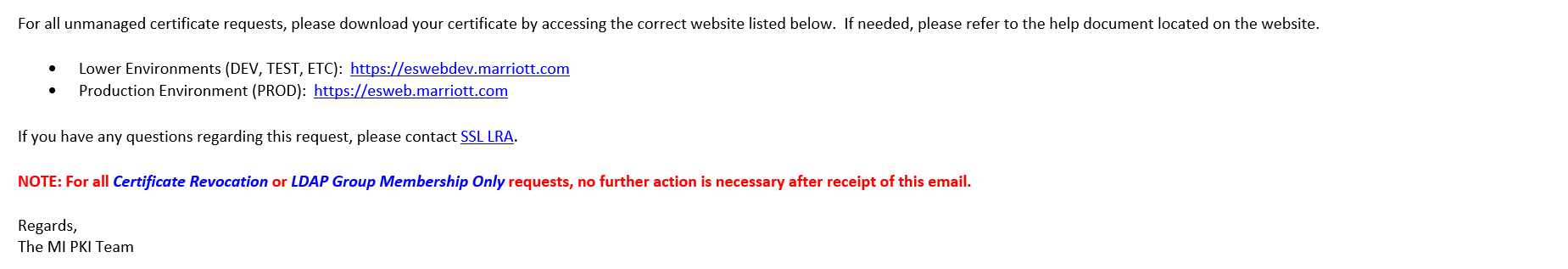
Click on ‘Submit Order’



Click ‘Continue’

*Once the request is approved and completed you would get an email like below:*





Click on the ‘RequestCenter’ link in the email which takes you to the page from where you get the Reference number and the Authorization code.

# Pre-Requisites

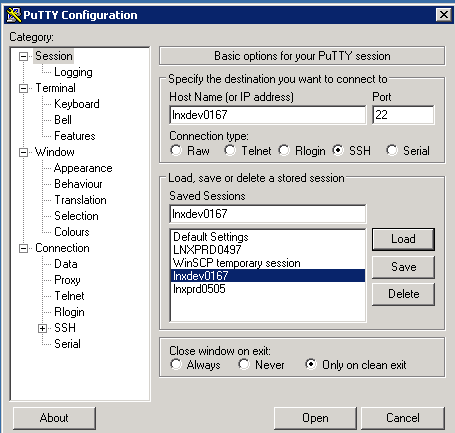
*To do this you would need the below:*

1. **RNAC** which you would receive on the request which you raised on Request Center post approval.
2. **CSR** 🡪 To generate the CSR you need to access the wallet manager the process for which is as below:

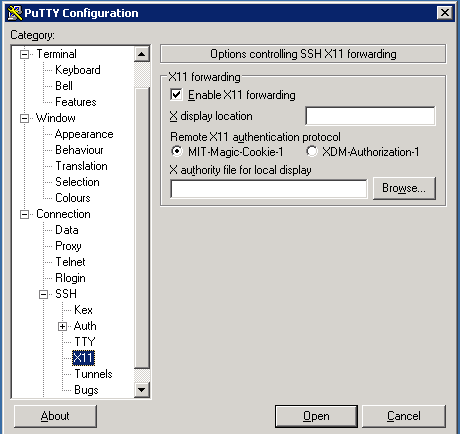
Login to [HDQNCVMCISDSD1-RDP](https://bpa2.marriott.com/Portal/Main) , then mstsc to [HDQNCVMCISDSD2-RDP](https://bpa2.marriott.com/Portal/Main)

# *Invoking the Oracle Wallet Manager:*

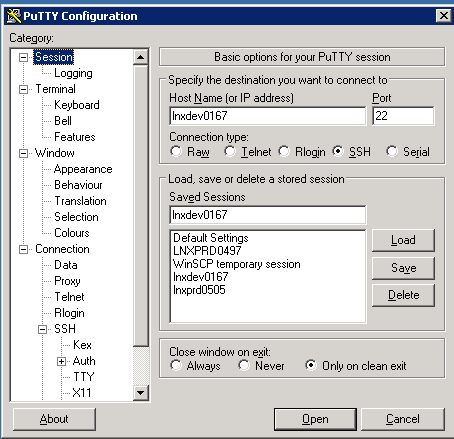
Open a putty session (in our case for this certificate – lnxdev0167) and load the session



Click on ‘SSH’ and then ‘X11’ and Check the box ‘Enable X11 forwarding’



Click on session again



Click ‘Save’

Login as sblweb user

cd /home/sblweb

rename the exisiting .Xauthority file

mv .Xauthority .Xauthority\_BKP\_03Jan2018

Login as root [sudo su -]

rename the exisiting .Xauthority file

mv .Xauthority .Xauthority\_BKP\_03Jan2018

exit from the session

login back to session as sblweb

switch to root user

sudo su -

cd /root

sudo cp /home/sblweb/.Xauthority .

Start task manager on DSD2 box

kill the processs for Xming under processes tab

Click on the 'Xming' utility on Desktop 

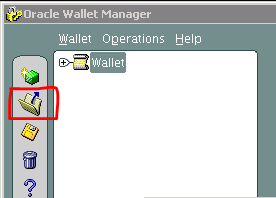
cd /cir5/citrtst2o/Oracle\_OHS/bin

./owm

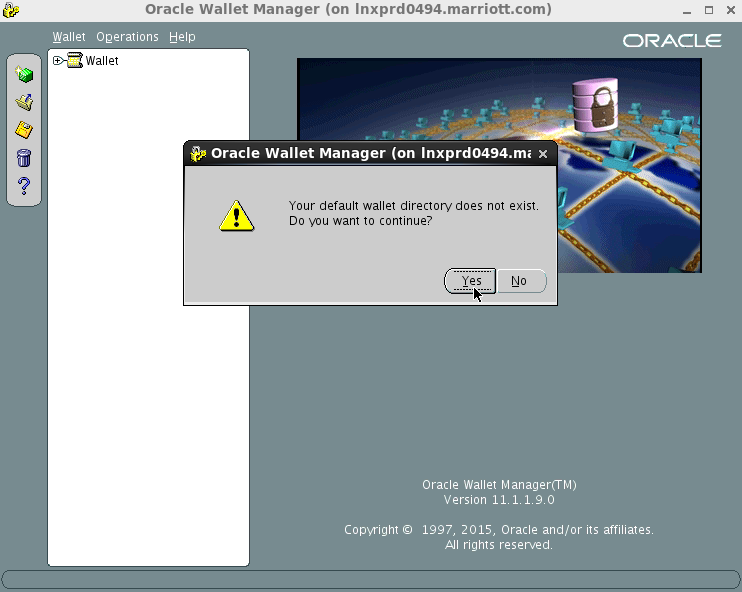
Running this opens the ‘Wallet Manager’ as shown below:



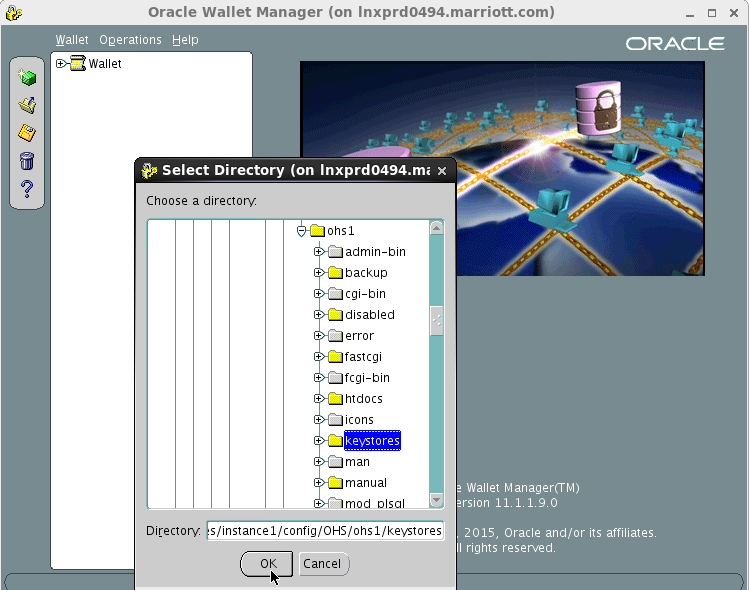
# *Opening a Wallet:*

Click on ‘Open Wallet’ -

Click on Yes to continue:



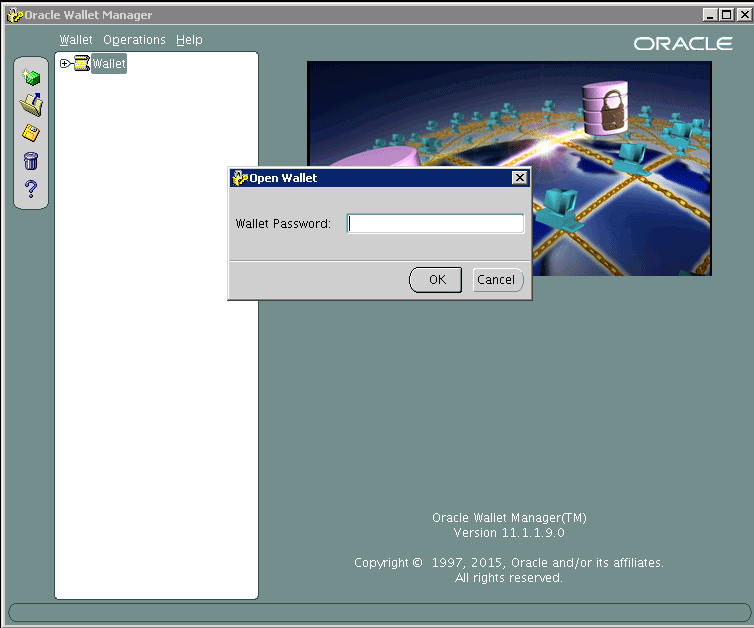
Select the key store location:



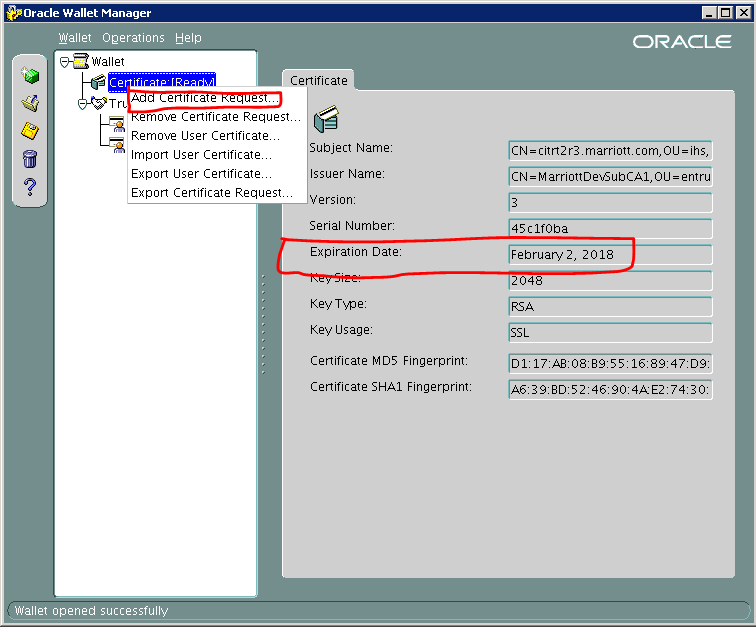
And navigate to the below mentioned location:

/cir5/citrt2o/Oracle\_OHS/instances/instance1/config/OHS/ohs1/keystores *(will vary with environment)*

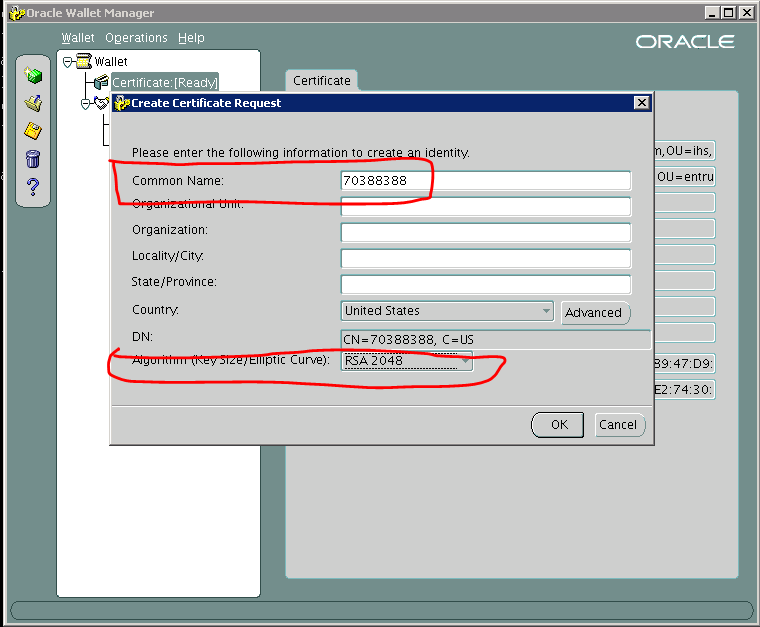
Click Ok where it prompts you for the ‘Wallet password’



# *Add a certificate request*

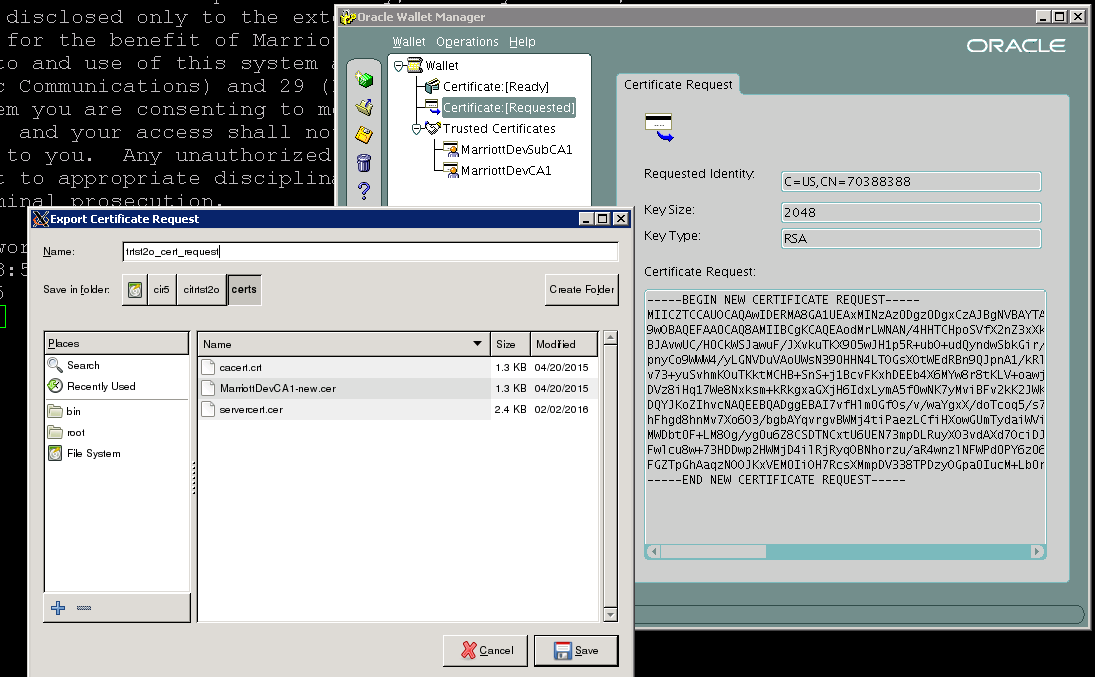


**Enter the ‘Reference number’ which you get from Request Center as shown below and also make sure you select the correct algorithm as shown below:**



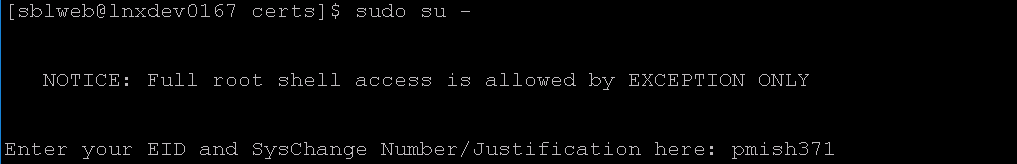
Click ‘OK’ which gets you the below screen. Click OK again

Now right click on Wallet > Certificate (Requested) and click ‘Export Certificate Request’ and enter the path on the server where you want to save the request as show below:



Click ‘Save’

Login to server box as root and copy the content of the files which you saved in the step above

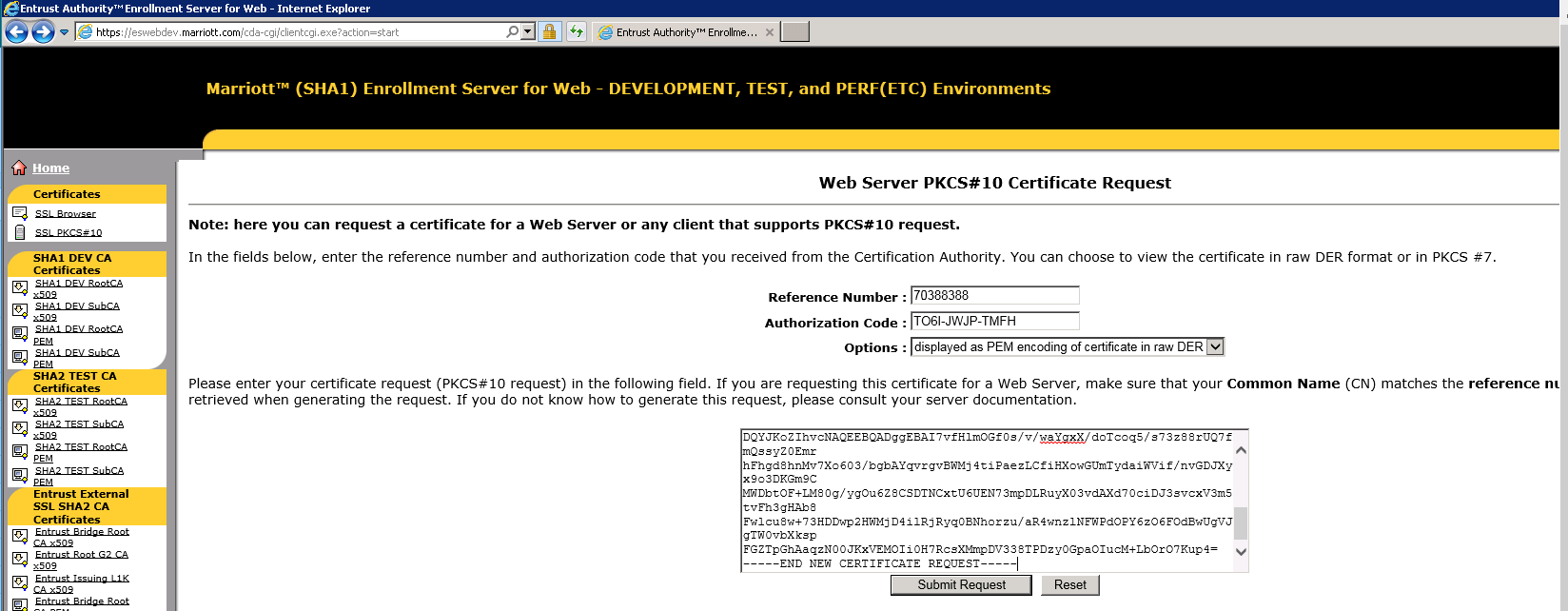




# *Downloading the certificate*

Now login to the website:  [https://eswebdev.marriott.com](https://eswebdev.marriott.com/)

Enter the Reference Number, Authorization Code and the content of certificate request as copied from the step above, show below:



Click on ‘Submit Request’ and then click on Download

Certificate saved on DSD2 RDP machine

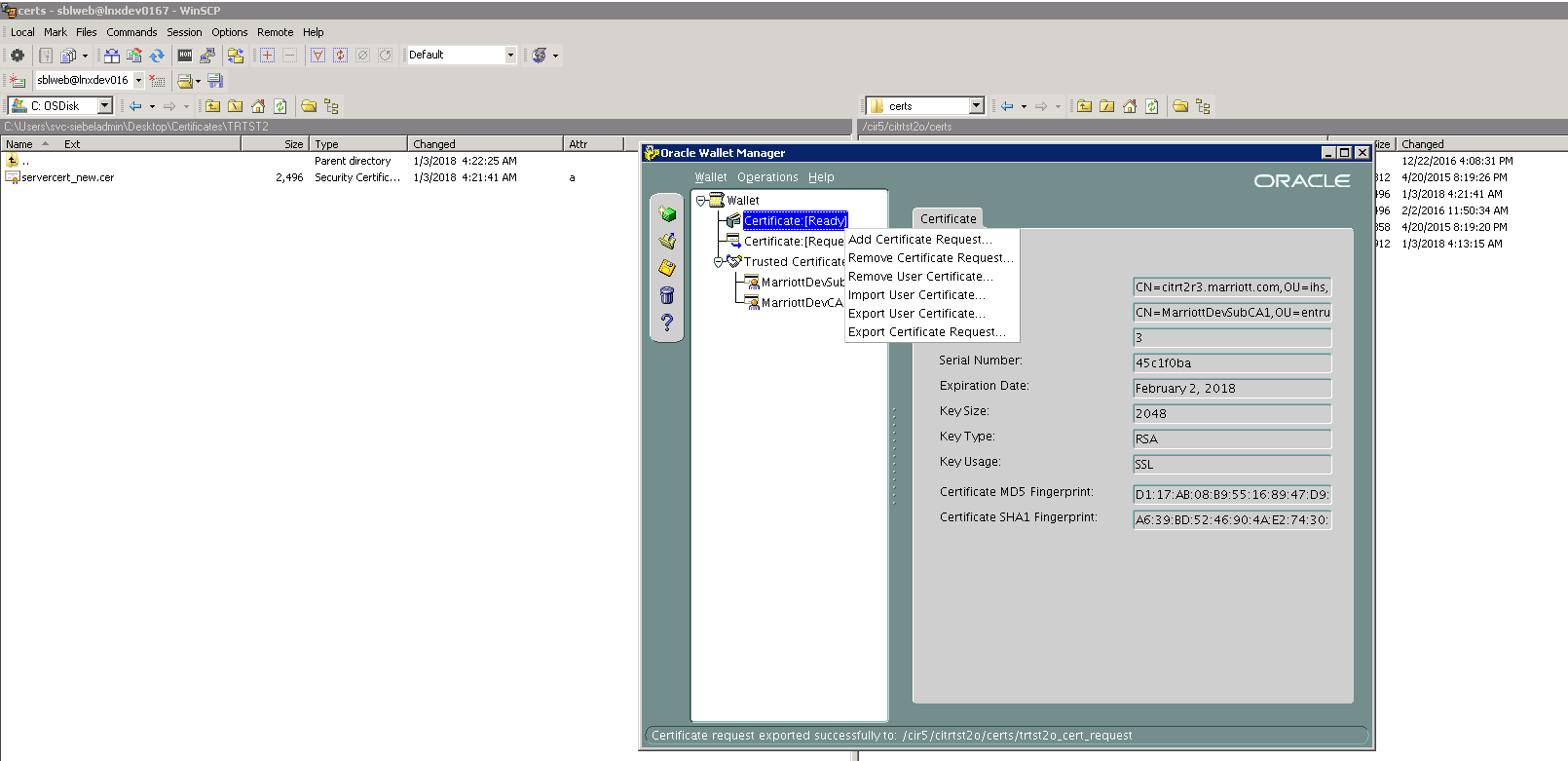
Folder name - C:\Users\svc-siebeladmin\Desktop\Certificates\<env\_name>

File name - servercert\_new.cer

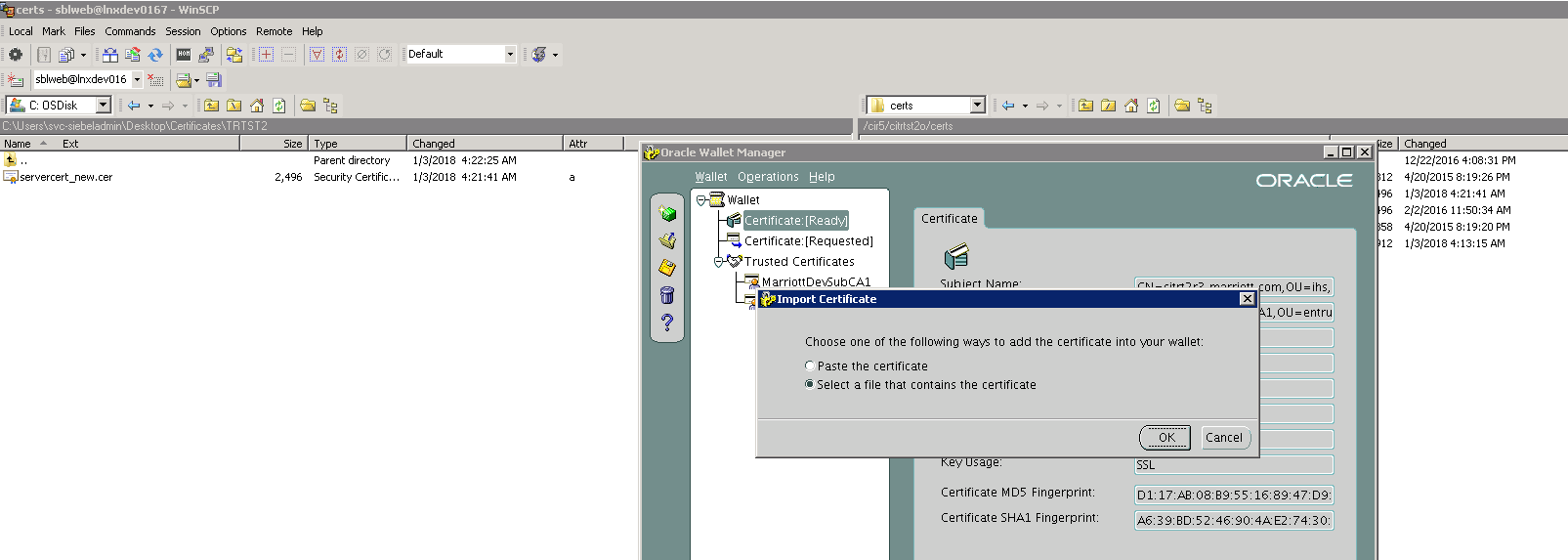
Importing the certificate

Go back to the Oracle Wallet Manager

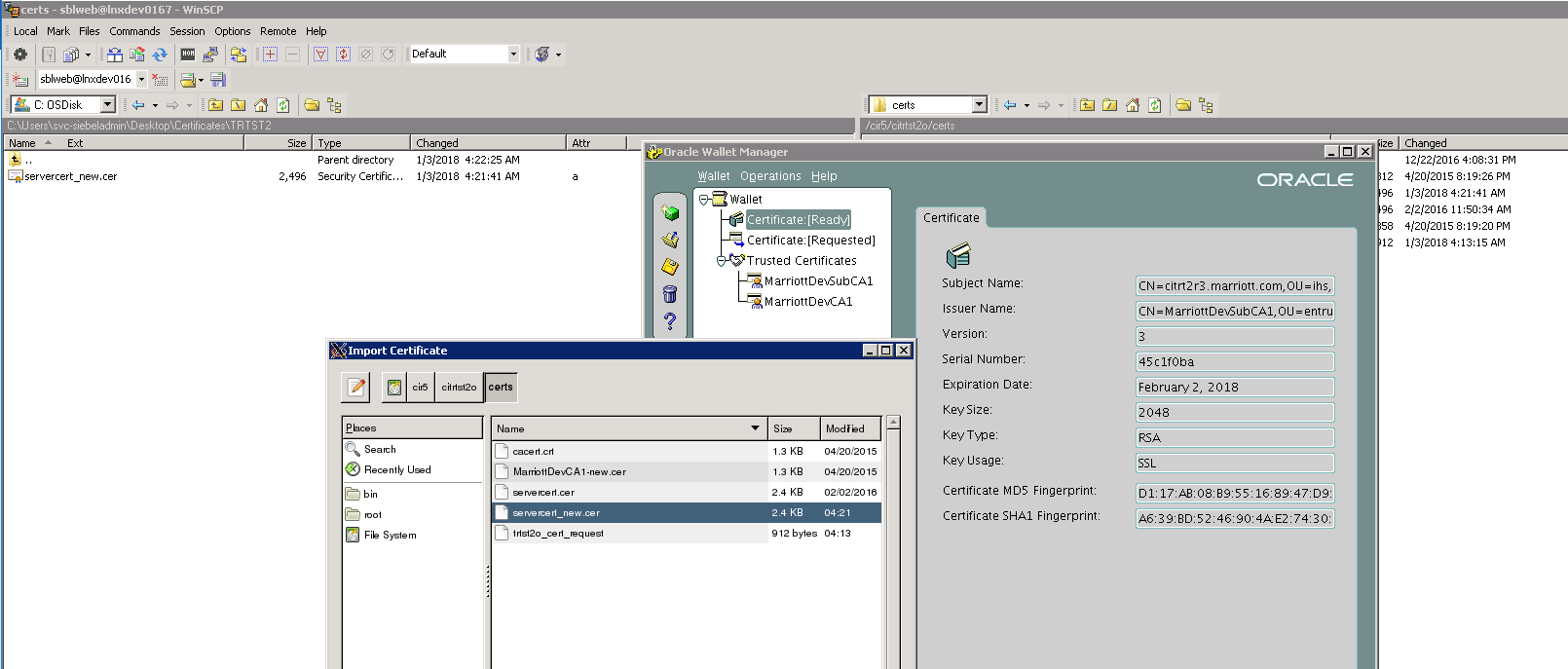
***Wallet > Certificate:[Ready] > right click and click on ‘Import User Certificate’***



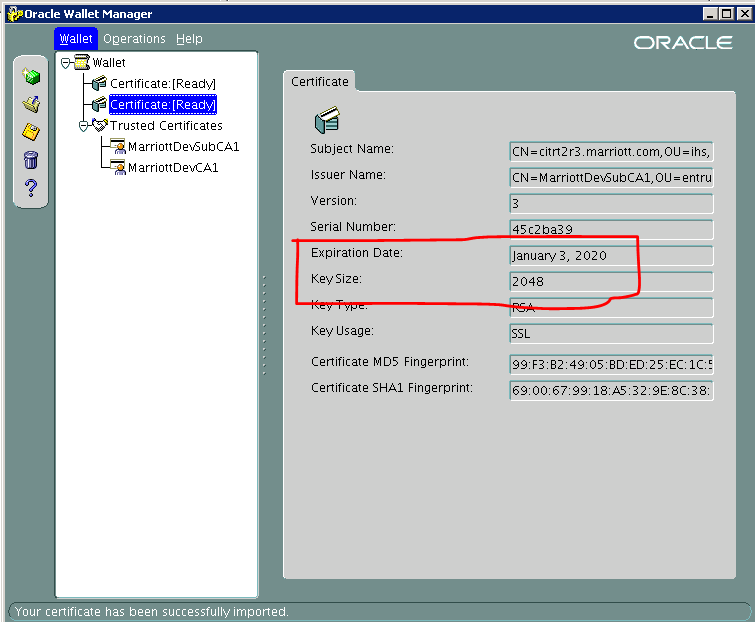
Select the default option and click OK



Select the certificate that was downloaded and placed on the server

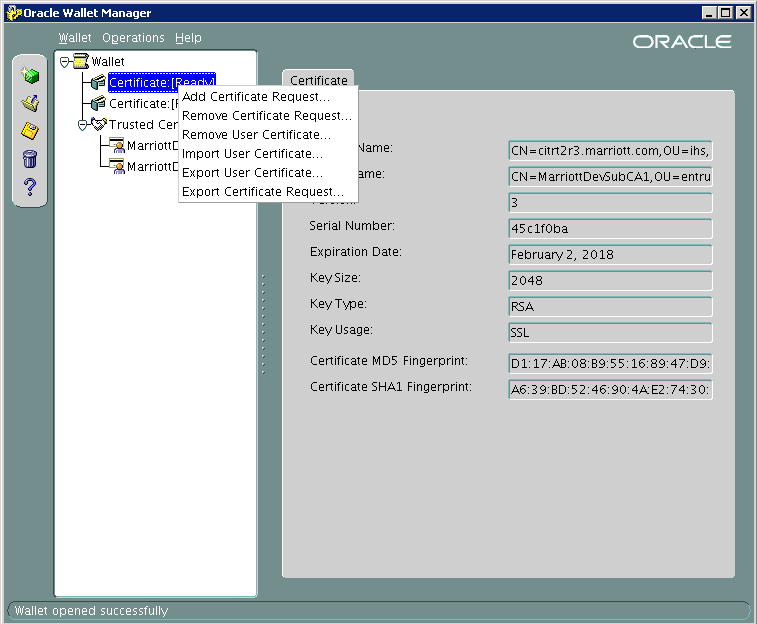


Check the newly imported certificate details as below:

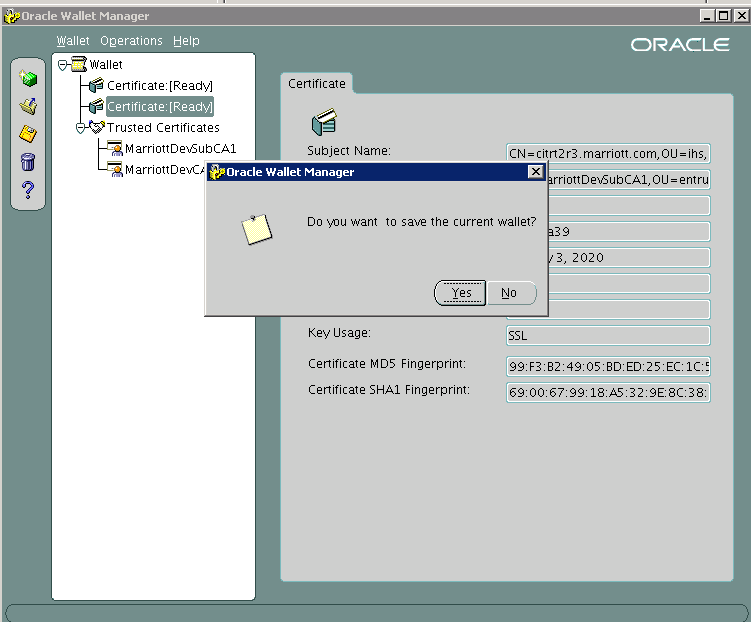


# *Removal of old certificate*

Remove the old certificate from the wallet [Certificate:[Ready] > Remove User Certificate

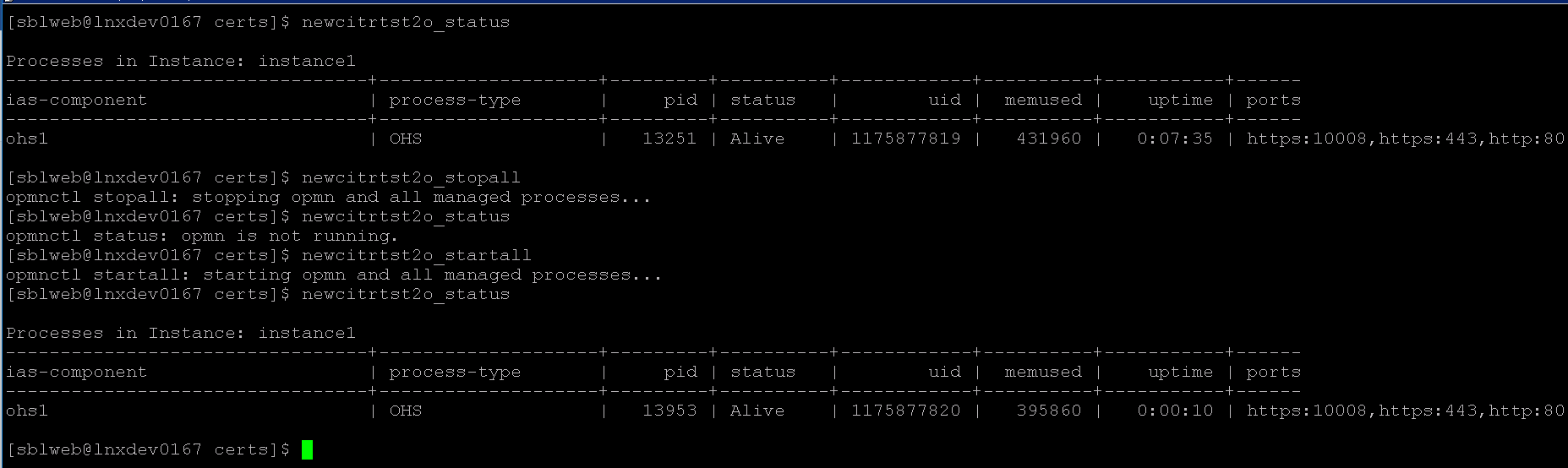


Close the wallet, while closing it will prompt you to save the wallet, click ‘Yes’



# *Recycling the web server*

Recycle the web server as shown below:



# *Verification*

Access the respective application URL and check for certificates as show below: