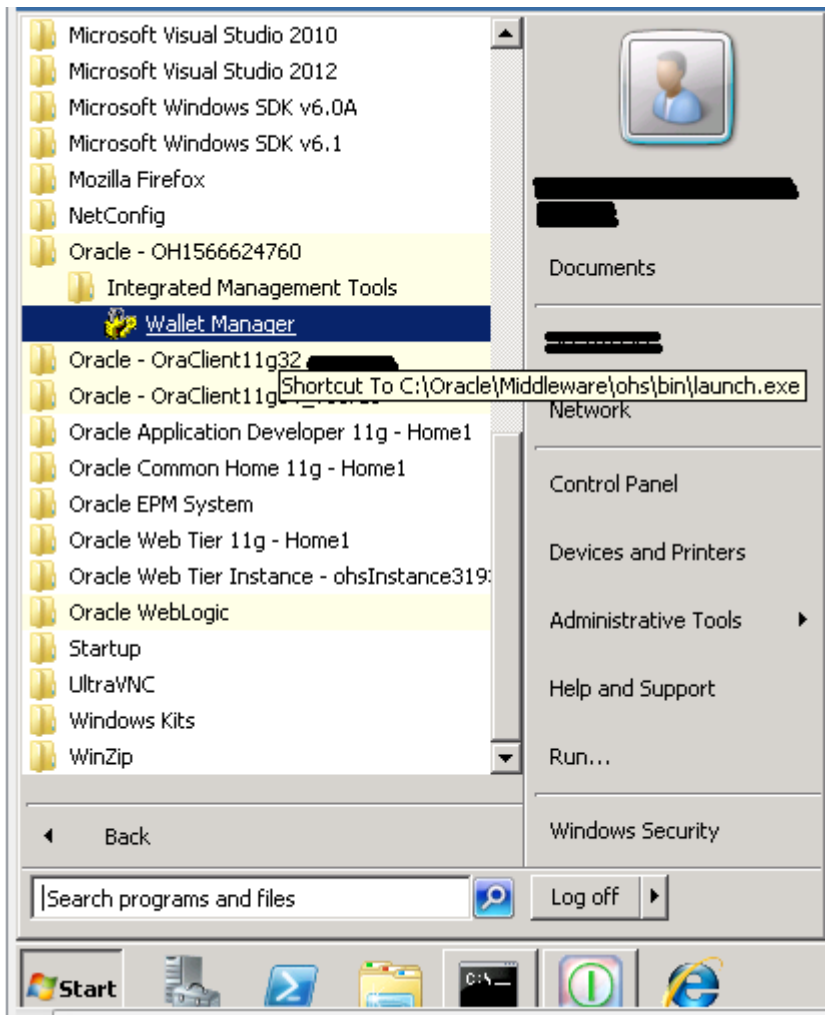
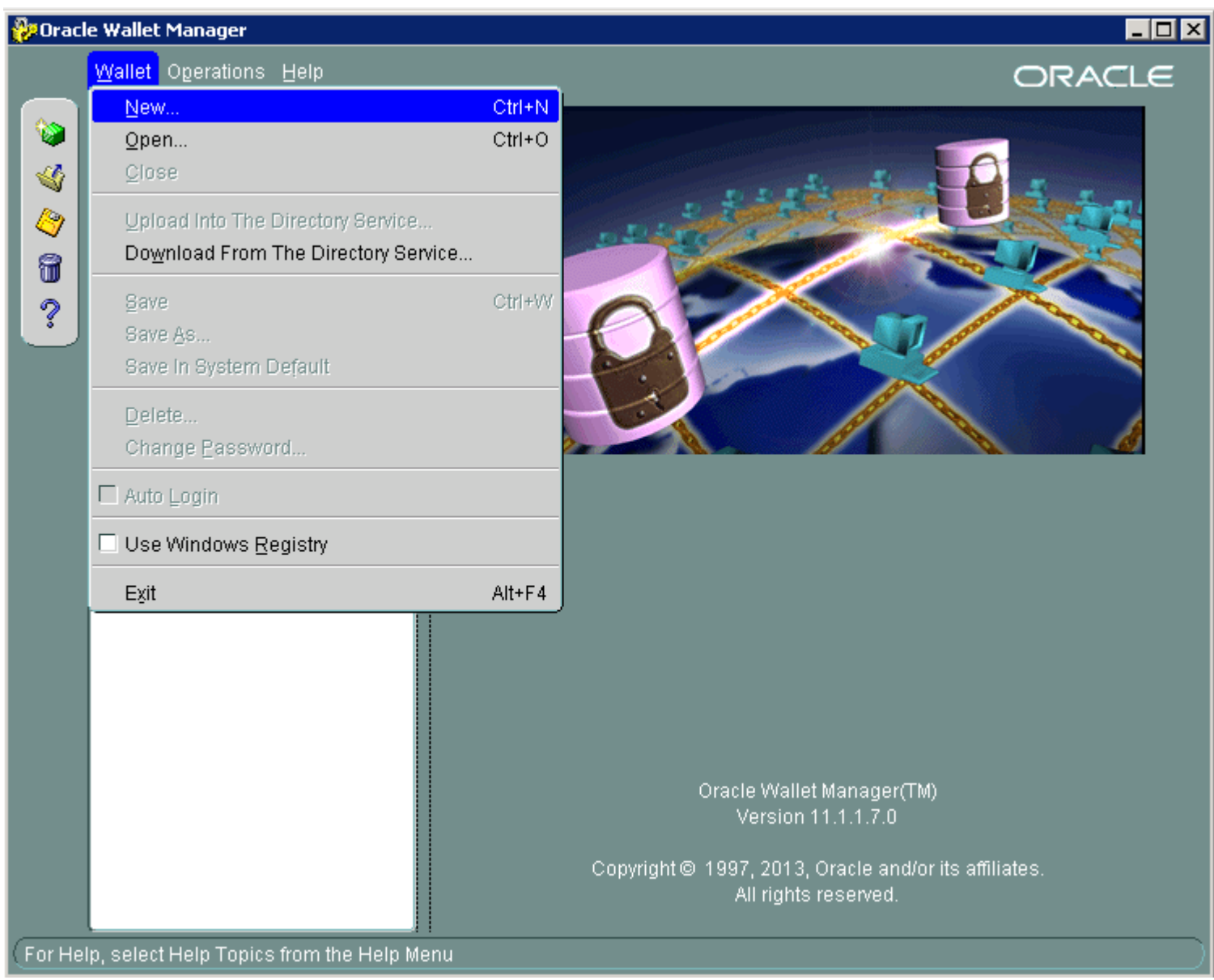
Configure SSL to Oracle Http Server (OHS) to be the Web Server for OBIEE 11g and Essbase shipped in along with OBIEE 11g

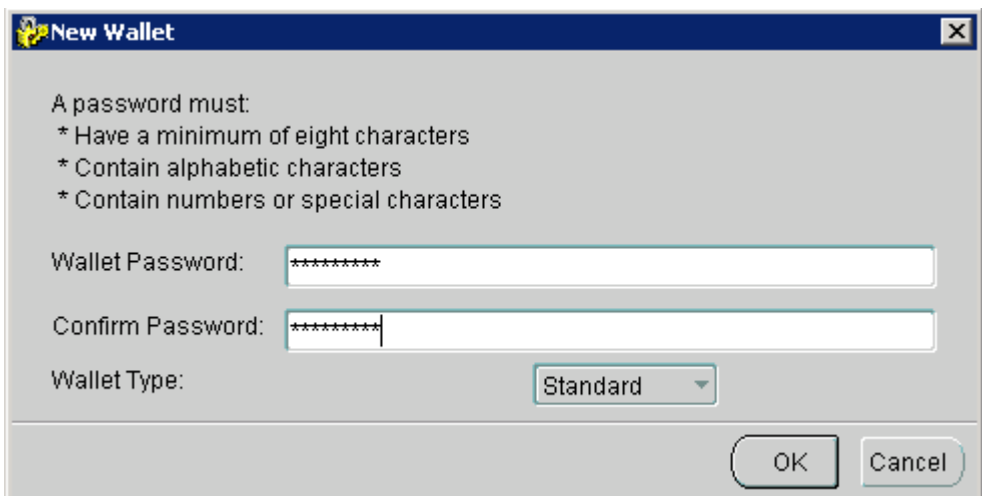
What do we need?

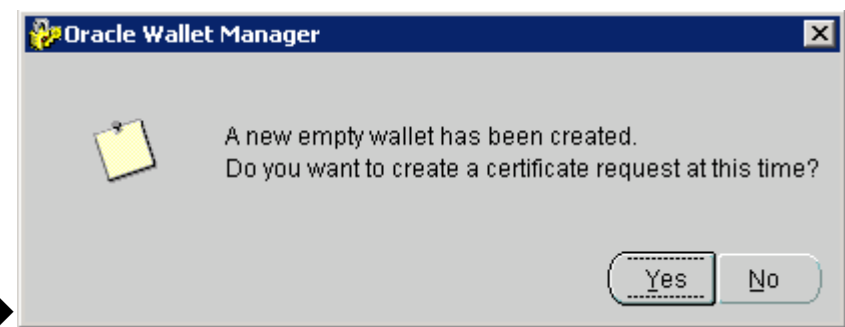
1. SSL Certificates
    - CA Root Certificate
    - CA Intermediate Certificate
    - CA Signed OHS Server Certificate
2. Create an Oracle Wallet
    - Using Oracle Wallet Manager (GUI mode)
    - Using orapki command line tool (cmd line interface)
    - Convert jks Keystore to Oracle Wallet
3. OHS Configuration Steps for OBIEE Full SSL Deployment
    - httpd.conf
    - ssl.conf
    - mod_wl_ohs.conf
4. Configuration Steps for OBIEE SSL termination at Web Server (OHS)
    - httpd.conf
    - ssl.conf
    - mod_wl_ohs.conf
5. Configuring Essbase Server in SSL Mode
    - Creating Oracle Wallet (created by converting jks Keystore file to wallet)
    - Configuring Essbase Server

Creating Oracle Wallet for OHS Using Wallet Manager

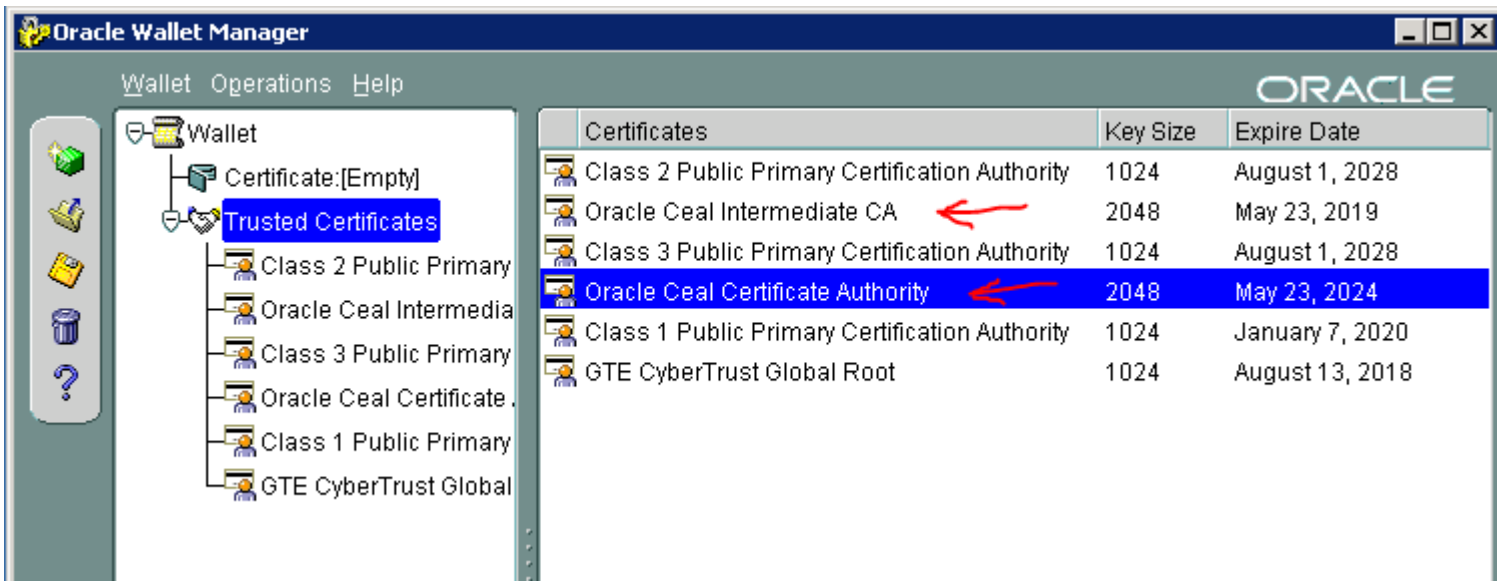


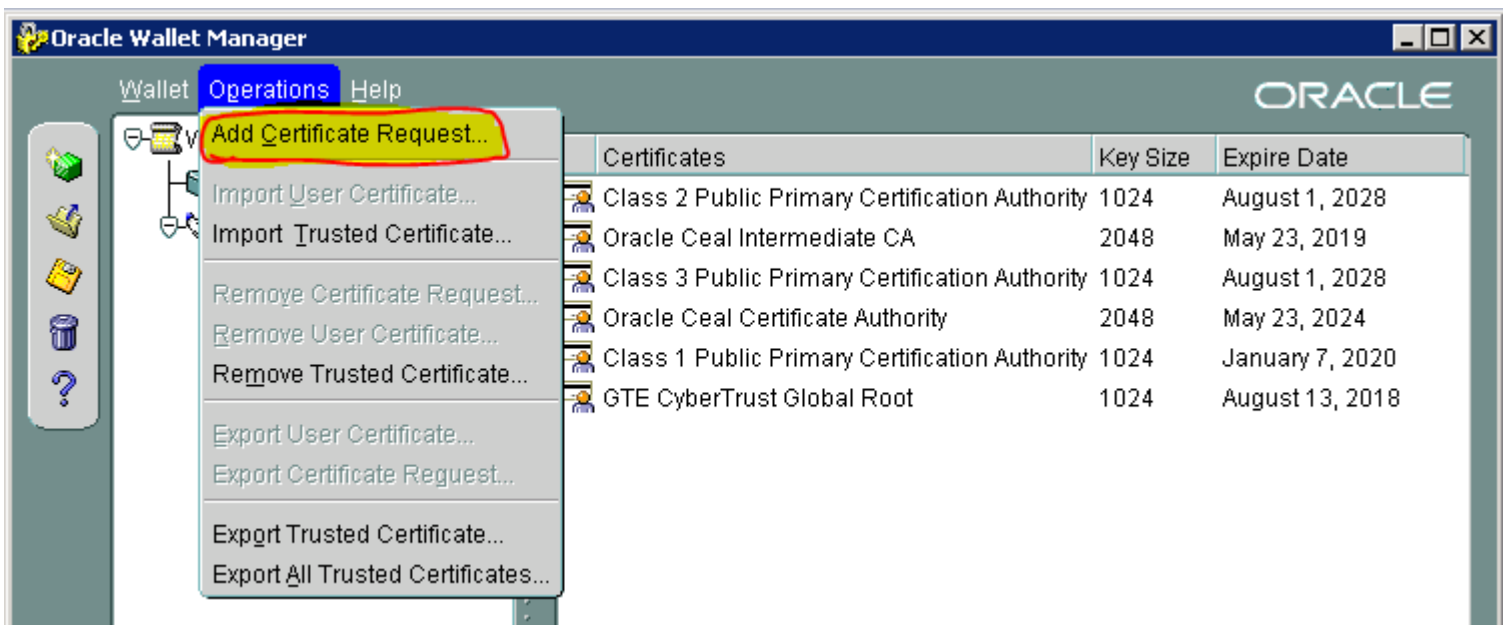




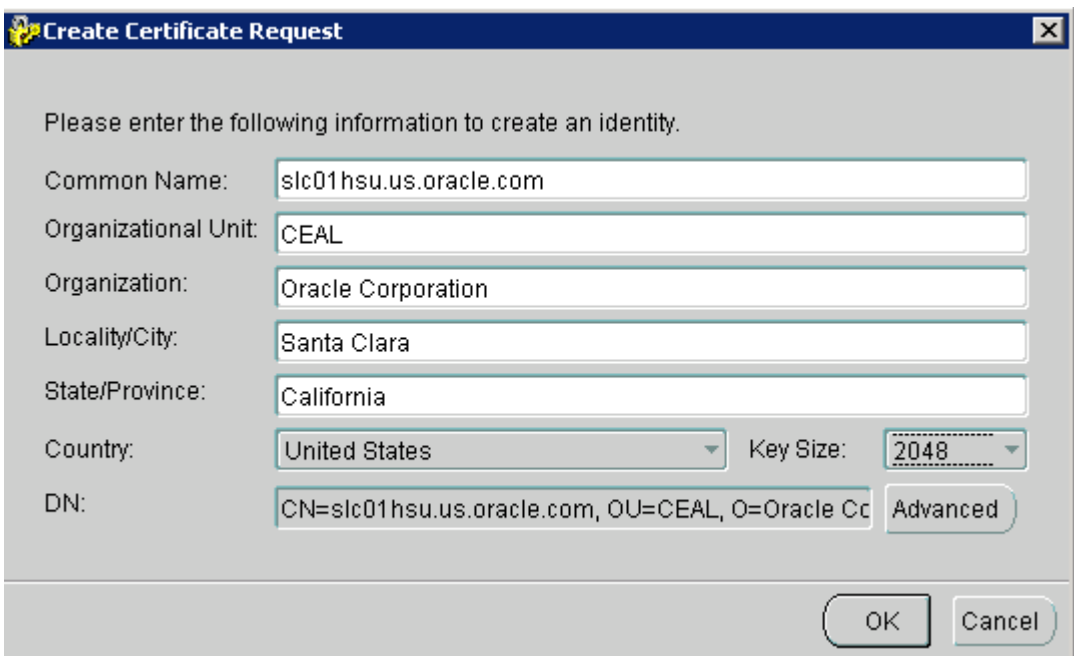


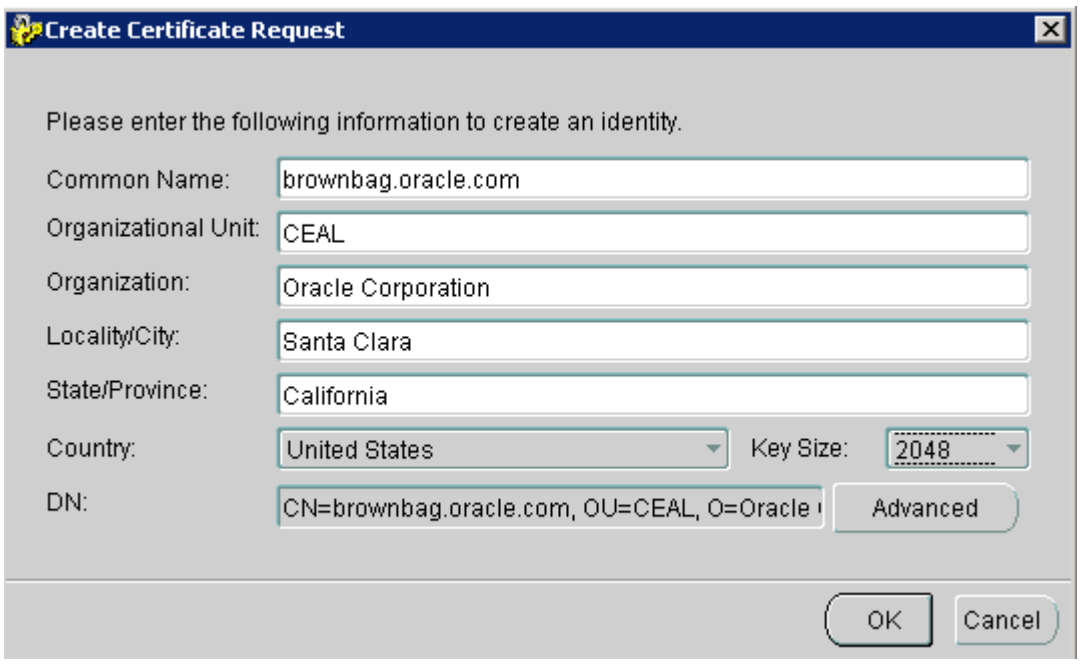
➔ Click No ➔ Right Click Trusted Certificates and add your CA intermediate and root certificates

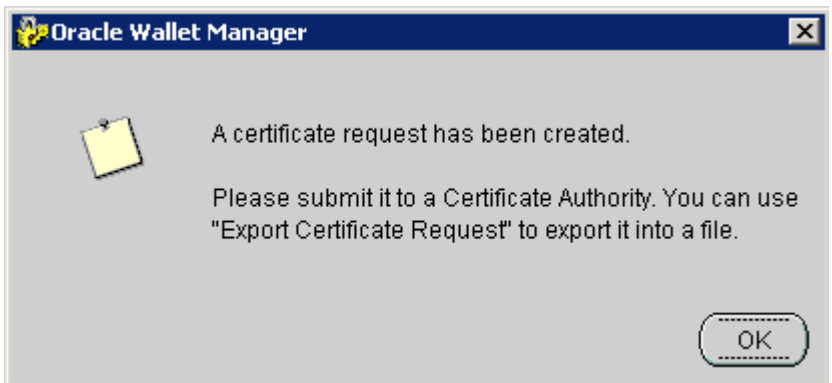


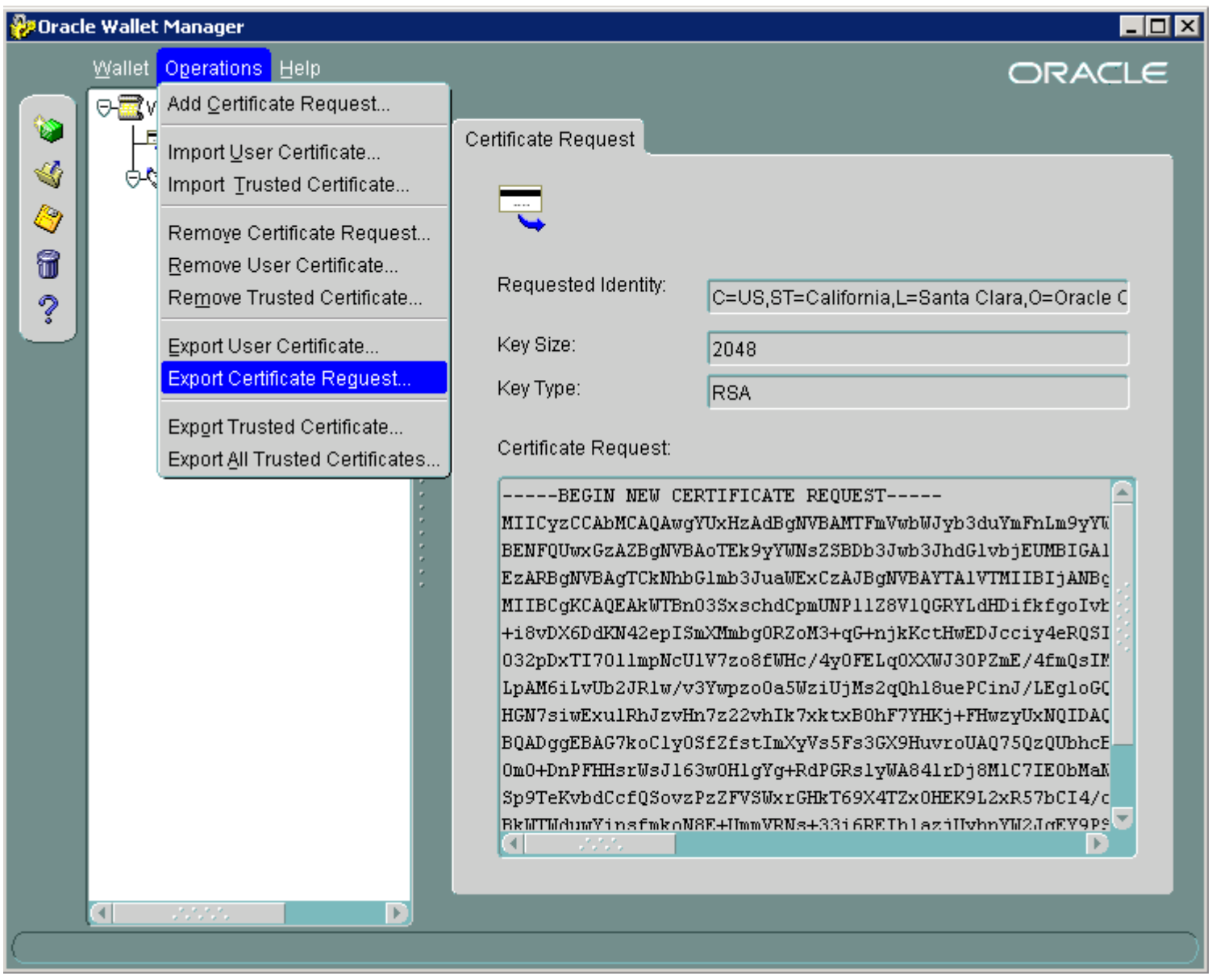


Create the Certificate Request either for the ohs server name or for the website name



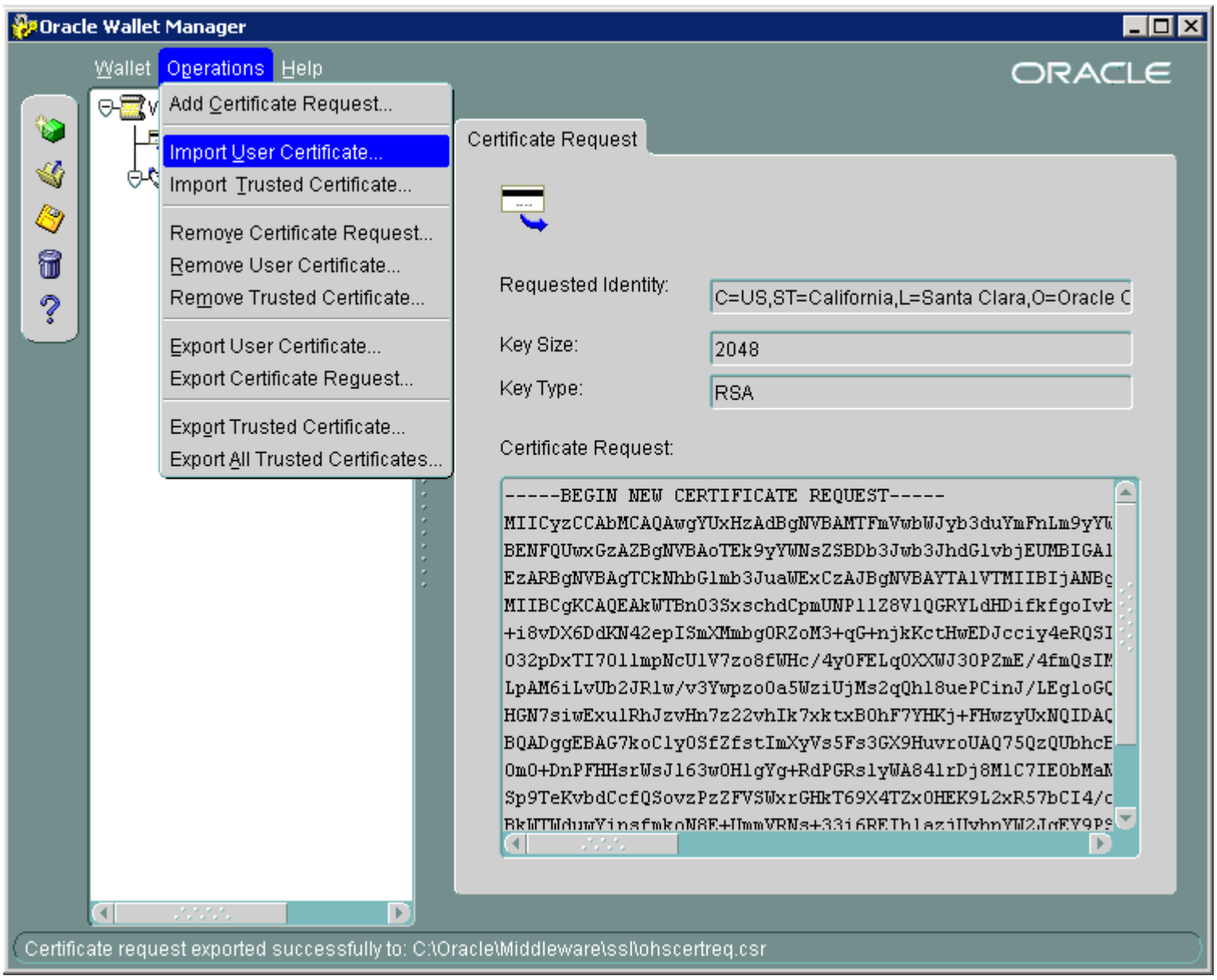


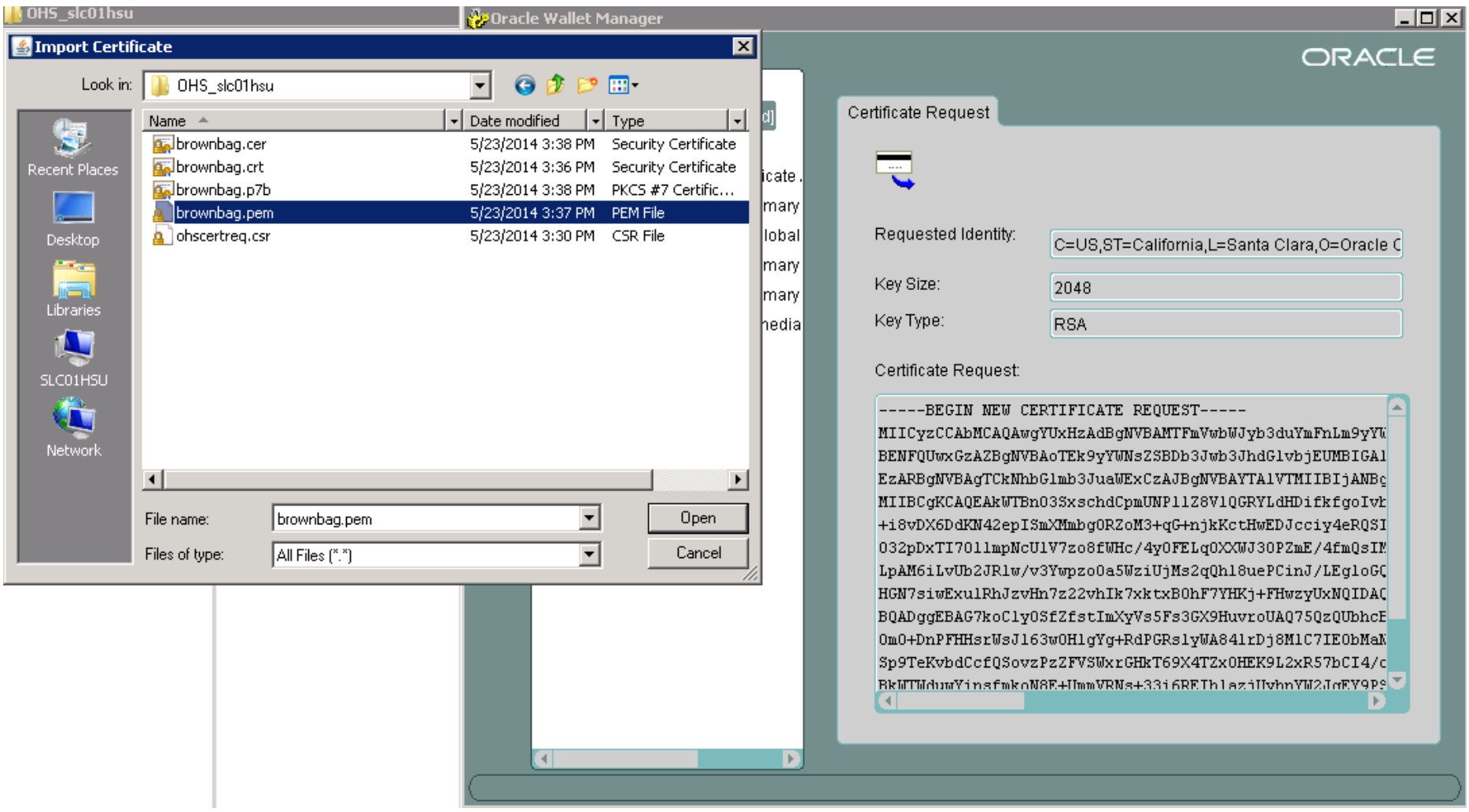


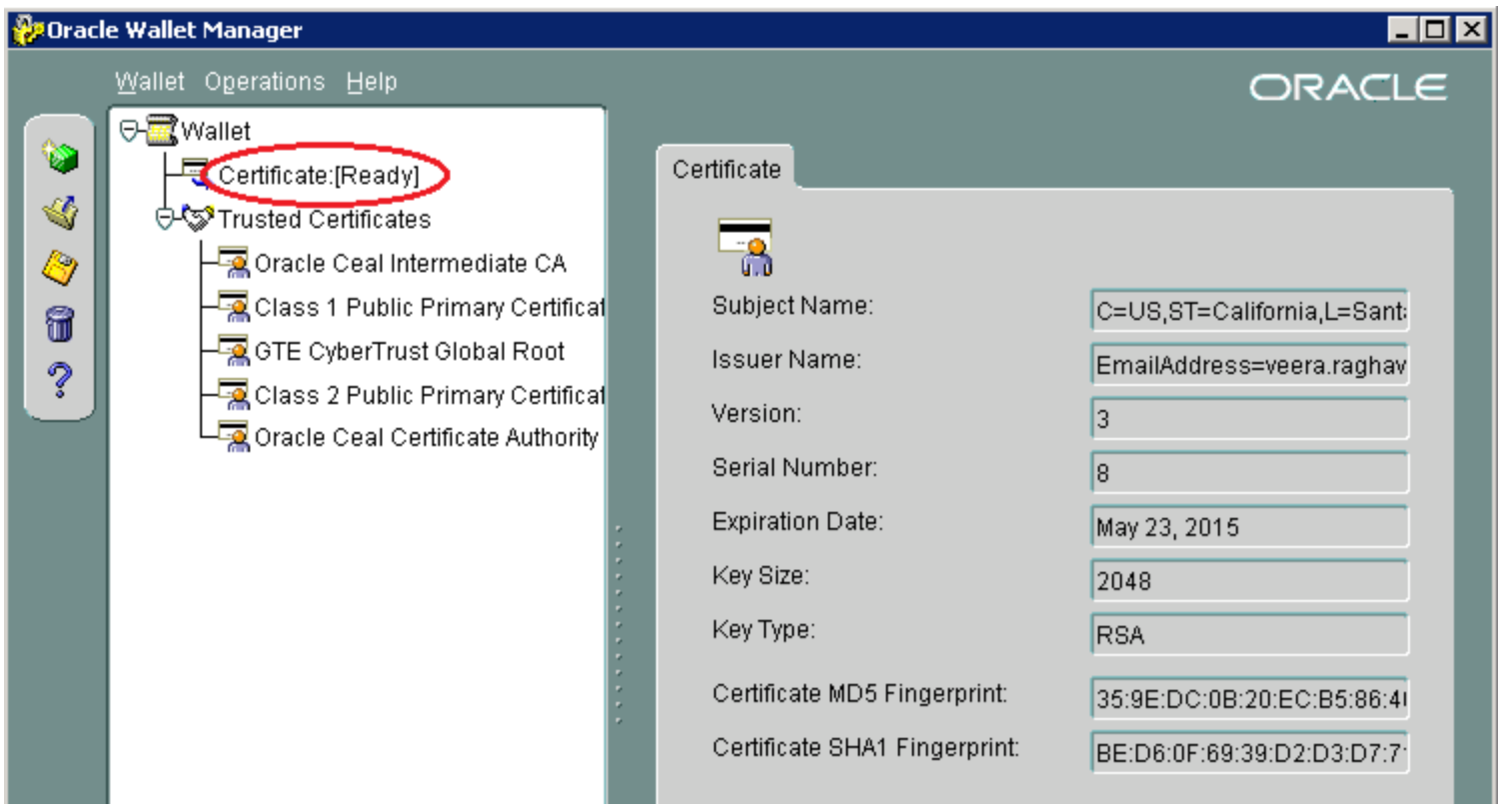


Send the CSR to the Certification Authority and get it signed.

Import the CA Signed OHS Server Certificate into the OHS Wallet.

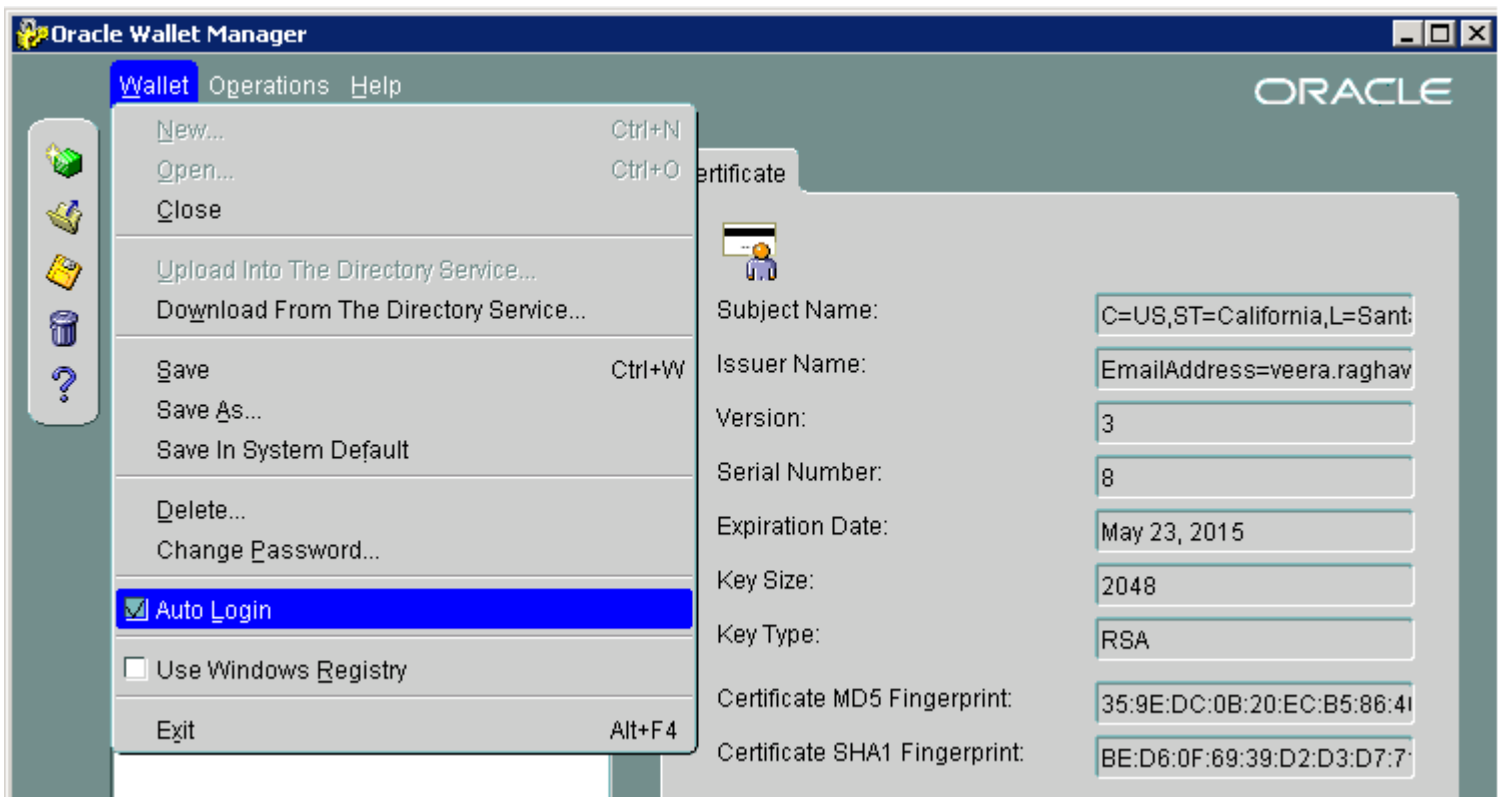

Oracle Wallet Manager
Wallet
Operations
Help
ORACLE
Add Certificate Request...
Import User Certificate...
Import Trusted Certificate...
Remove Certificate Request...
Remove User Certificate...
Remove Trusted Certificate...
Export User Certificate...
Export Certificate Request...
Export Trusted Certificate...
Export All Trusted Certificates...
Certificate Request
Requested Identity:
C=US,ST=California,L=Santa Clara,O=Oracle C
Key Size:
2048
Key Type:
RSA
Certificate Request:
-----BEGIN NEW CERTIFICATE REQUEST-----
Certificate request exported successfully to: C:\Oracle\Middleware\ssl\ohscertreq.csr


OHS_slc01hsu
Oracle Wallet Manager
Import Certificate
Look in:
OHS_slc01hsu
Name
Date modified
Type
brownbag.cer
5/23/2014 3:38 PM
Security Certificate
brownbag.crt
5/23/2014 3:36 PM
Security Certificate
brownbag.p7b
5/23/2014 3:38 PM
PKCS #7 Certific...
brownbag.pem
5/23/2014 3:37 PM
PEM File
ohscertreq.csr
5/23/2014 3:30 PM
CSR File
Recent Places
Desktop
Libraries
SLC01HSU
Network
File name:
brownbag.pem
Files of type:
All Files (*.*)
Open
Cancel
ORACLE
Certificate Request
Requested Identity:
C=US,ST=California,L=Santa Clara,O=Oracle C
Key Size:
2048
Key Type:
RSA
Certificate Request:
-----BEGIN NEW CERTIFICATE REQUEST-----

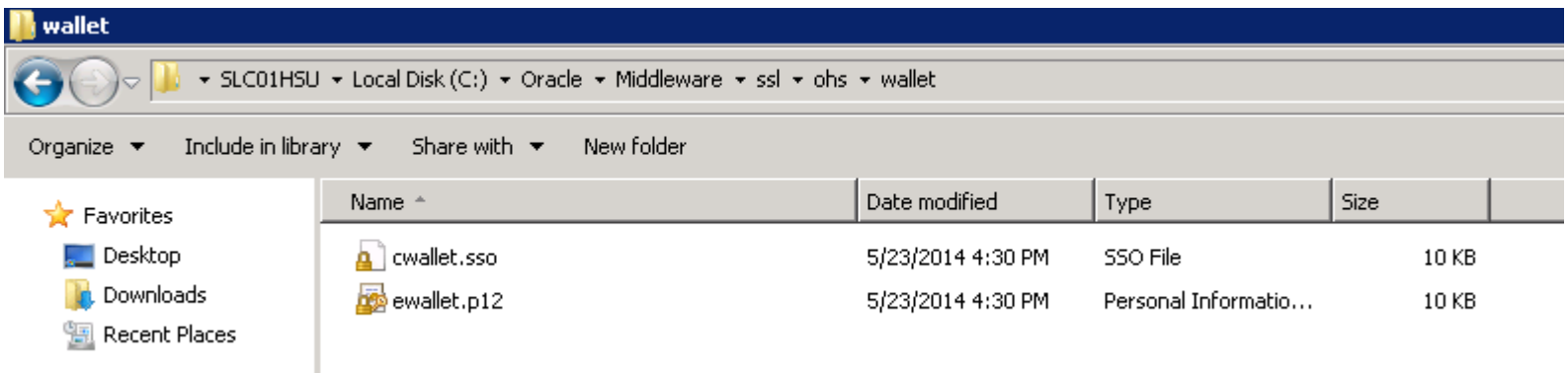


Select Save As, and save the certificate to *Oracle_home>\Middleware\user_projects\epmsystem1\httpConfig\ohs\config\OHS\ohs_component\keystores\default*

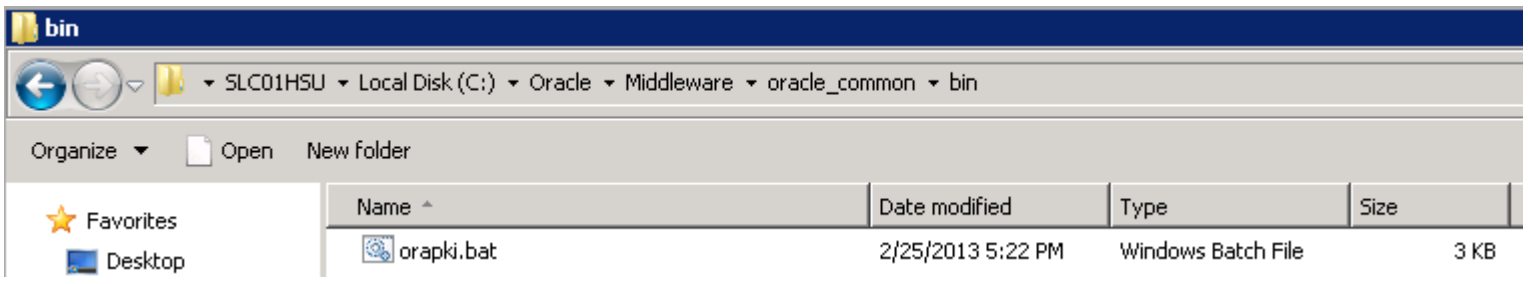
Saved to C:\Oracle\Middleware\ssl\ohs\wallet & created the certificate for **brownbag.oracle.com**



Once Auto Login is checked cwallet.sso file is created.

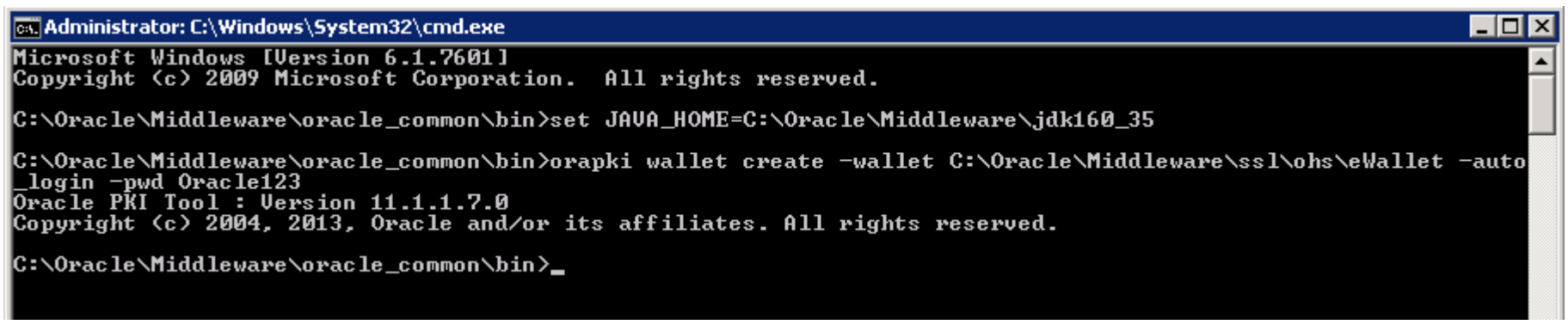


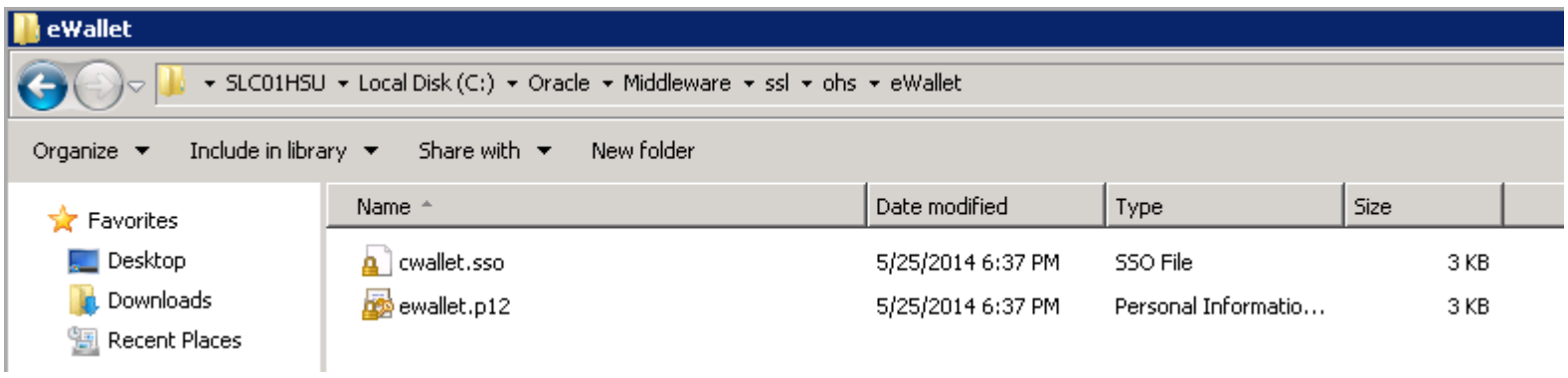
Creating Oracle Wallet for OHS using orapki command line tool



Create an auto-login wallet and use the wallet:

orapki wallet create -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -auto_login -pwd Oracle123





We need a key pair for the Server Certificate Signing Request:

Unfortunately we will fail validating the java key store if we use anything other than orapki.

So we have to use the wallet. The signing request will be created along:

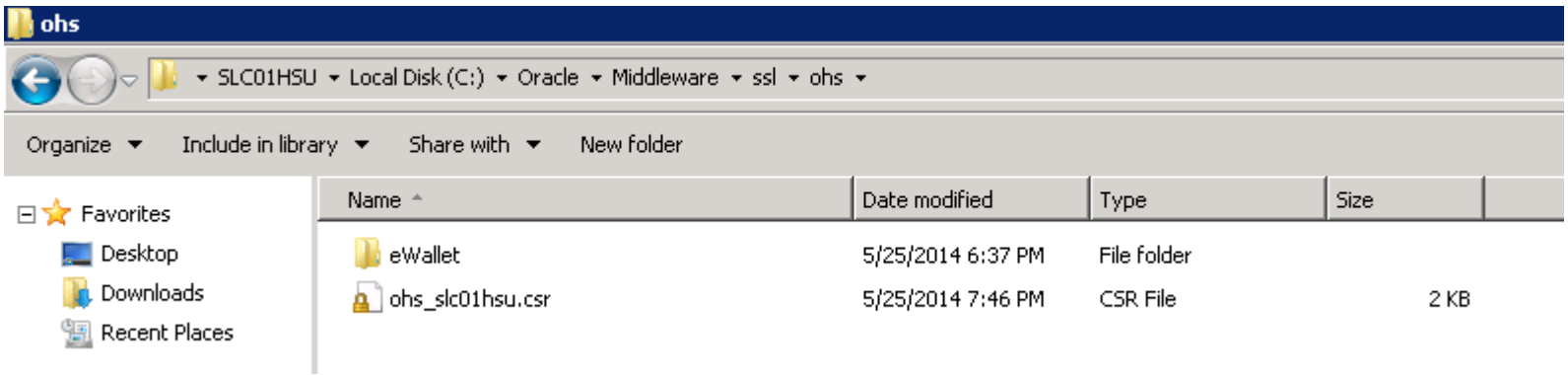
Command: orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -dn "CN= brownbag.oracle.com, OU=CEAL, O=Oracle Corporation, L=Santa Clara, ST=California, C=US" -keysize 2048 -pwd Oracle123 -validity 365

Export the CSR from the wallet:

Command: orapki wallet export -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -dn "CN= brownbag.oracle.com, OU=CEAL, O=Oracle Corporation, L=Santa Clara, ST=California, C=US" -request C:\Oracle\Middleware\ssl\ohs\ohs_slc01hsu.csr

```
C:\Oracle\Middleware\oracle_common\bin>orapki wallet export -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -dn "
CN=brownbag.oracle.com, OU=CEAL, O=Oracle Corporation, L=Santa Clara, ST=California, C=US" -request C:\Oracle\
Middleware\ssl\ohs\ohs_slc01hsu.csr
Oracle PKI Tool : Version 11.1.1.7.0
Copyright (c) 2004, 2013, Oracle and/or its affiliates. All rights reserved.

C:\Oracle\Middleware\oracle_common\bin>_
```



Send the CSR to the Certification Authority and get it signed.

Import the CA Signed OHS Server Certificate into the OHS Wallet.

Import CA Inter, CA Root, brownbag (ohs) certificates into the wallet

Command: orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -pwd Oracle123 -trusted_cert -cert C:\Oracle\Middleware\ssl\CAInter.pem

Command: orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -pwd Oracle123 -trusted_cert -cert C:\Oracle\Middleware\ssl\CARoot.pem

Command: orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -pwd Oracle123 -user_cert -cert C:\Oracle\Middleware\ssl\ohs\brownbag.pem

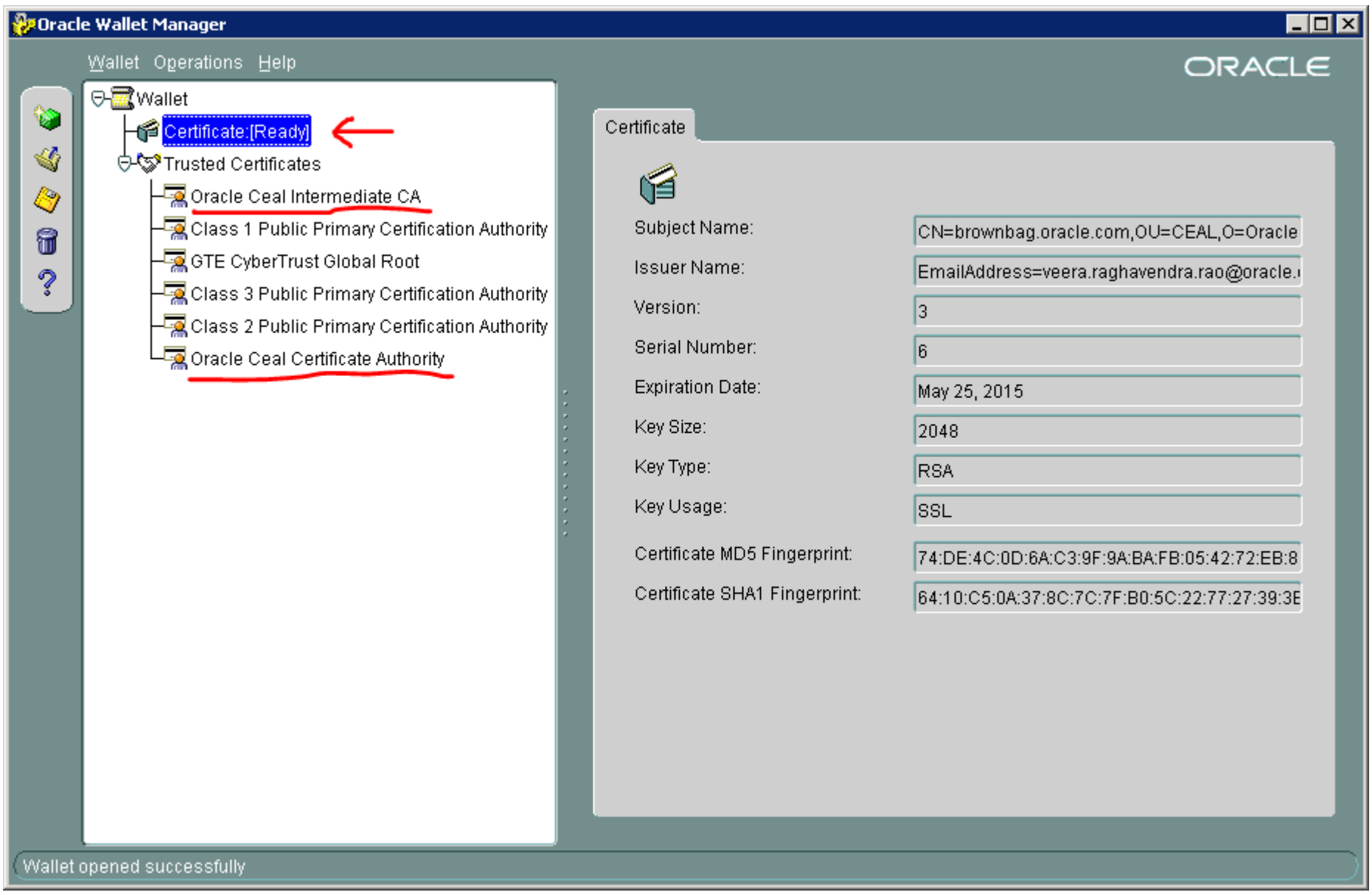
```
C:\Oracle\Middleware\oracle_common\bin>orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -pwd Ora
cle123 -trusted_cert -cert C:\Oracle\Middleware\ssl\CAInter.pem
Oracle PKI Tool : Version 11.1.1.7.0
Copyright (c) 2004, 2013, Oracle and/or its affiliates. All rights reserved.

C:\Oracle\Middleware\oracle_common\bin>orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -pwd Ora
cle123 -trusted_cert -cert C:\Oracle\Middleware\ssl\CARoot.pem
Oracle PKI Tool : Version 11.1.1.7.0
Copyright (c) 2004, 2013, Oracle and/or its affiliates. All rights reserved.

C:\Oracle\Middleware\oracle_common\bin>orapki wallet add -wallet C:\Oracle\Middleware\ssl\ohs\eWallet -pwd Ora
cle123 -user_cert -cert C:\Oracle\Middleware\ssl\ohs\brownbag.pem
Oracle PKI Tool : Version 11.1.1.7.0
Copyright (c) 2004, 2013, Oracle and/or its affiliates. All rights reserved.

C:\Oracle\Middleware\oracle_common\bin>_
```

Open the wallet in Oracle Wallet Manager and validate it



Creating a Oracle Wallet by converting jks Keystore

You want to create a wallet containing your server cert and private key provided by your PKI administrator as a yourcert.p12 file.

Let's assume the password for the private key is "mypassword".

One way is to convert this p12 to jks

keytool -v -importkeystore -srckeystore yourcert.p12 -srcstoretype PKCS12 -destkeystore yournewkeystore.jks -deststoretype JKS

You must use the same password for the new jks and the private key = "mypassword"

Import in this keystore, the intermediate and root certs for your server cert. This is required to create a valid wallet.

keytool -import -alias Root -keystore yournewkeystore.jks -trustcacerts -file root.cer

keytool -import -alias Intermediate -keystore yournewkeystore.jks -trustcacerts -file intermediate.cer

Validate all entries are there using keytool -list -keystore yournewkeystore.jks

Since we already have a jks file which is created in the Config SSL for OBIEE Steps, let us ignore the above steps.

https://blogs.oracle.com/pa/resource/Configuring_OBIEE_with_Ful_End_to_End_SSL.pdf

Using the jks file let us create a wallet:

Create an empty wallet with auto login:

C:\Oracle\Middleware\oracle_common\bin\orapki wallet create -wallet C:\Oracle\Middleware\ssl -auto_login -pwd Oracle123

```
C:\Oracle\Middleware\oracle_common\bin>orapki wallet create -wallet C:\Oracle\Middleware\ssl\eWallet -
auto_login -pwd Oracle123
Oracle PKI Tool : Version 11.1.1.7.0
Copyright (c) 2004, 2013, Oracle and/or its affiliates. All rights reserved.

C:\Oracle\Middleware\oracle_common\bin>_
```

Convert the jks to a wallet:

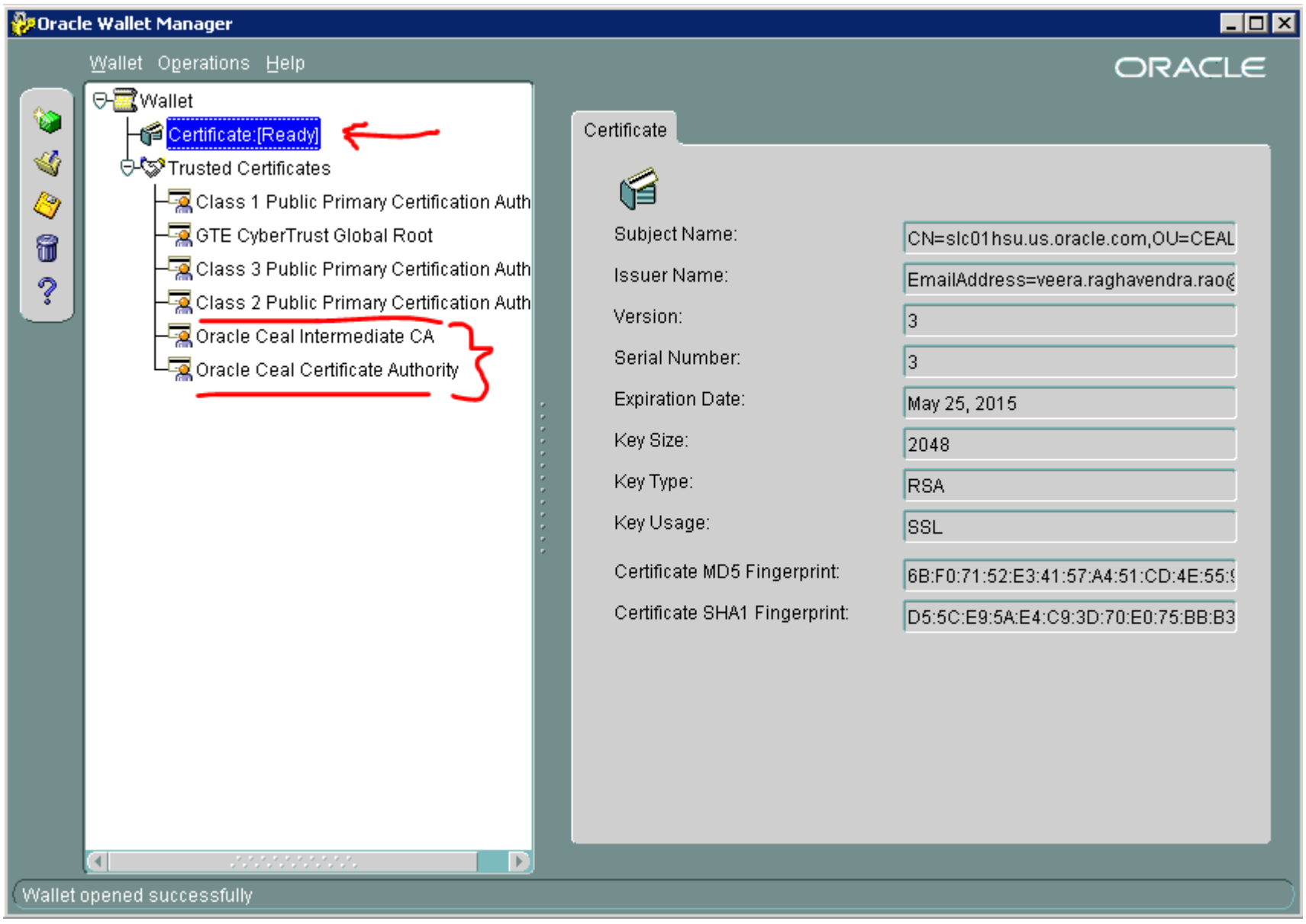
C:\Oracle\Middleware\oracle_common\bin\orapki wallet jks_to_pkcs12 -wallet C:\Oracle\Middleware\ssl\eWallet -pwd Oracle123 -keystore C:\Oracle\Middleware\ssl\myIdentity.jks -jkspwd Oracle123

```
C:\Oracle\Middleware\oracle_common\bin>orapki wallet jks_to_pkcs12 -wallet C:\Oracle\Middleware\ssl\eW
allet -pwd Oracle123 -keystore C:\Oracle\Middleware\ssl\myIdentity.jks -jkspwd Oracle123
Oracle PKI Tool : Version 11.1.1.7.0
Copyright (c) 2004, 2013, Oracle and/or its affiliates. All rights reserved.

C:\Oracle\Middleware\oracle_common\bin>_
```

Make sure the private key password and the wallet password match = Oracle123

Your wallet is ready to be used for OHS and Essbase. But remember this wallet will be having OHS Server Certificate created with OHS Server Name and not the Website Name.



Configure SSL for OHS for OBIEE Full SSL Deployment

httpd.conf:

Add ServerName as brownbag.oracle.com

```
#
# If your host doesn't have a registered DNS name, enter its IP
address here.
#
ServerName brownbag.oracle.com

#
# DocumentRoot: The directory out of which you will serve your
```

```
# Include the configuration files needed for mod_weblogic
include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/
${COMPONENT_NAME}/mod_wl_ohs.conf"

# Include the SSL definitions and Virtual Host container
include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/
${COMPONENT_NAME}/ssl.conf"

# Include the admin virtual host (Proxy Virtual Host) related
configuration
include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/
${COMPONENT_NAME}/admin.conf"

include "moduleconf/*.conf"

Header edit Location ^http://(.*)$ https://$1
# Header set Cache-Control "private,no-cache"
```

ssl.conf:

```
##########################################################################
# Oracle HTTP Server mod_ossl configuration file: ssl.conf        #
##########################################################################


# OHS Listen Port
Listen 443

<IfModule ossl_module>
##
##  SSL Global Context
##
```

```
##
## SSL Virtual Host Context
##

NameVirtualHost brownbag.oracle.com:443

<VirtualHost brownbag.oracle.com:443>
  <IfModule ossl_module>
   #  SSL Engine Switch:
   #  Enable/Disable SSL for this virtual host.
   SSLEngine on
```

```
   ServerName    brownbag.oracle.com:443

   #Path to the wallet
   #SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/default"

   SSLWallet "C:\Oracle\Middleware\ssl\ohs\wallet"

   <FilesMatch "\.(cgi|shtml|phtml|php)$">
      SSLOptions +StdEnvVars
   </FilesMatch>

   <Directory "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/cgi-bin">
      SSLOptions +StdEnvVars
   </Directory>

   BrowserMatch ".*MSIE.*" \
   nokeepalive ssl-unclean-shutdown \
   downgrade-1.0 force-response-1.0

  </IfModule>
</VirtualHost>

</IfModule>
```

mod_wl_ohs.conf

Add (WLProxySSL ON, WLForwardUriUnparsed OFF, KeepAliveEnabled ON)

NOTE: Since its OBIEE Full SSL deployment, the OBIEE WebLogic Port will be SSL port i.e. 9804

NOTE: If OBIEE WebLogic Servers are also running in SSL Mode then add SecureProxy ON

```
# NOTE : This is a template to configure mod_weblogic.

LoadModule weblogic_module   "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

# This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the Base Virtual Host Level

<IfModule weblogic_module>

 WLSSLWallet "C:\Oracle\Middleware\ssl\ohs\wallet"

 WLForwardUriUnparsed OFF

 KeepAliveEnabled ON

 DynamicServerList Off

 WLTempDir C:\tmp

 DEBUG OFF

 WebLogicHost slc01pfz.us.oracle.com

 WebLogicPort 9704      # This port value should be 9804 if OBIEE WebLogic Mqanaged Server is running in SSL Mode

 WLProxySSL ON

 WLProxySSLPassThrough ON

 SecureProxy OFF        # This Value should be ON if OBIEE WebLogic Mqanaged Server is running in SSL Mode

 WLLogFile C:\Oracle\Middleware\Oracle_WT1\instances\instance2\diagnostics\logs\OHS\ohs1\ohs_log.log

 #Configuring Oracle HTTP Server for the BI_SERVERn Managed Servers

 #http://docs.oracle.com/cd/E23943_01/core.1111/e10106/bi.htm#CHDHBAHG

 # BI Office
 <Location /bioffice>
```

```
#http://docs.oracle.com/cd/E23943_01/core.1111/e10106/bi.htm#CHDHBAHG

# BI Office
<Location /bioffice>
   SetHandler weblogic-handler
</Location>

<Location /biofficeclient>
   SetHandler weblogic-handler
</Location>

# WSM-PM
<Location /wsm-pm>
   SetHandler weblogic-handler
</Location>

# BIEE Analytics
<Location /analytics>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

<Location /mapviewer>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

<Location /analytics-ws>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

<Location /bimiddleware>
   SetHandler weblogic-handler
</Location>

# BI Publisher
<Location /xmlpserver>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

</IfModule>
```

mod_wl_ohs.conf:

```
# NOTE : This is a template to configure mod_weblogic.

LoadModule weblogic_module   "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

# This empty block is needed to save mod_wl related configuration from EM to this file when changes are
made at the Base Virtual Host Level

<IfModule weblogic_module>
 WLSSLWallet "C:\Oracle\Middleware\ssl\ohs\wallet"
 WLForwardUriUnparsed OFF
 KeepAliveEnabled ON
 DynamicServerList Off
 WLTempDir C:\tmp
 DEBUG OFF
 WebLogicHost slc01pfz.us.oracle.com
 WebLogicPort 9704      #This port value should be 9804 if OBIEE WebLogic Mqanaged Server is running in SSL Mode
 WLProxySSL ON
 WLProxySSLPassThrough ON
 SecureProxy OFF        #This Value should be ON if OBIEE WebLogic Mqanaged Server is running in SSL Mode
 WLLogFile C:\Oracle\Middleware\Oracle_WT1\instances\instance2\diagnostics\logs\OHS\ohs1\ohs_log.log
 #Configuring Oracle HTTP Server for the BI_SERVERn Managed Servers

 #http://docs.oracle.com/cd/E23943_01/core.1111/e10106/bi.htm#CHDHBAHG

 # BI Office
 <Location /bioffice>
    SetHandler weblogic-handler
 </Location>

 <Location /biofficeclient>
    SetHandler weblogic-handler
 </Location>

 # WSM-PM
 <Location /wsm-pm>
    SetHandler weblogic-handler
 </Location>

 # BIEE Analytics
 <Location /analytics>
```

```
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

<Location /mapviewer>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

<Location /analytics-ws>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
</Location>

<Location /bimiddleware>
   SetHandler weblogic-handler
</Location>

# BI Publisher
<Location /xmlpserver>
   SetHandler weblogic-handler
   WLIOTimeoutSecs 6000
   WLSocketTimeoutSecs 600
 </Location>

</IfModule>
```

OHS SSL URL: https://brownbag.oracle.com/analytics

Configure SSL for OHS (Terminating SSL at Web Server)

Differences between Full SSL and Terminating SSL at Web Server will be only at mod_wl_ohs.conf file

mod_wl_ohs.conf:

Change from ON in Full SSL to OFF in this Config (WLProxySSL OFF, SecureProxy OFF)

NOTE: Since its SSL termination at Web Server, the WebLogic Port will be non-SSL port i.e. 9704

And in httpd.conf file we need to add Header Location to redirect https requests to https only.

Note: In case of https to http fails add in httpd.conf:

Header edit Location ^http://(.*)$ https://$1

****

```
####################

Header edit Location ^http://(.*)$ https://$1
# Header set Cache-Control "private,no-cache"
```

Configure SSL for Essbase Server (Shipped in with OBIEE)

NOTE: From FMW Control we can Configure SSL for all BI Components but we cannot Configure SSL for shipped in Essbase Server Component

Essbase Server to run in SSL needs Oracle Wallet, so create an Oracle Wallet by converting an existing jks Keystore into an Oracle Wallet.

Please refer this section in this document "**Creating an Oracle Wallet by converting jks Keystore**".

Or follow any of the steps used to create a Oracle Wallet for OHS (Web Server)

In essbase.cfg file: add few ssl parameters as below:

Essbase.cfg can be found under
C:\Oracle\Middleware\instances\instance1\Essbase\essbaseserver1\bin

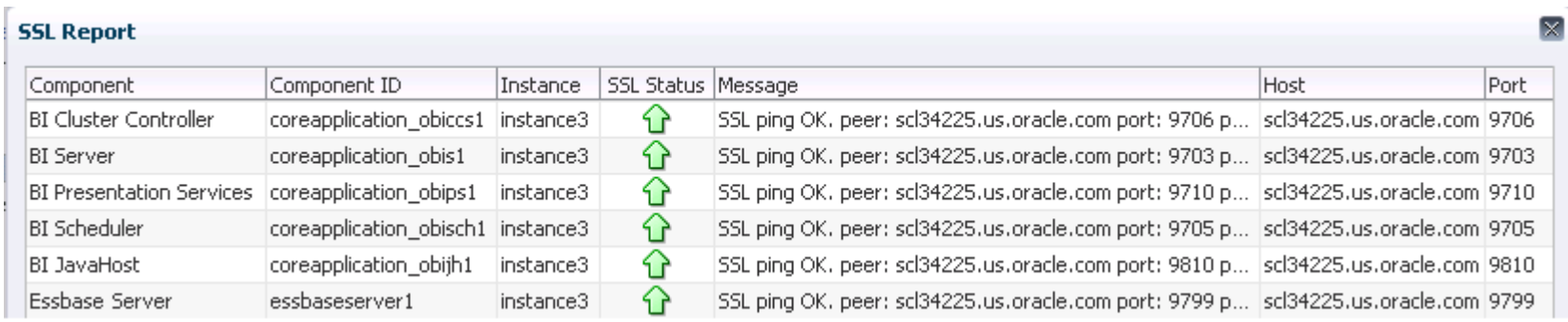
**********Add below line after existing text**********

WalletPath C:\\Oracle\\Middleware\\ssl\\essbase
EnableClearMode FALSE ;deactivates http
EnableSecureMode TRUE ;activates SSL
AgentSecurePort 9799 (*if any port is free use it, if not comment the non-ssl port and use it for ssl)*
ClientPreferredMode SECURE ;always prefer secure communication

****

Restart Essbase Server

Check if Essbase is successfully running in ssl mode at 9799 port in opmnctl status / in EM SSL Report



SSL Report

Component	Component ID	Instance	SSL Status	Message	Host	Port
BI Cluster Controller	coreapplication_obiccs1	instance3	↑	SSL ping OK. peer: scl34225.us.oracle.com port: 9706 p...	scl34225.us.oracle.com	9706
BI Server	coreapplication_obis1	instance3	↑	SSL ping OK. peer: scl34225.us.oracle.com port: 9703 p...	scl34225.us.oracle.com	9703
BI Presentation Services	coreapplication_obips1	instance3	↑	SSL ping OK. peer: scl34225.us.oracle.com port: 9710 p...	scl34225.us.oracle.com	9710
BI Scheduler	coreapplication_obisch1	instance3	↑	SSL ping OK. peer: scl34225.us.oracle.com port: 9705 p...	scl34225.us.oracle.com	9705
BI JavaHost	coreapplication_obijh1	instance3	↑	SSL ping OK. peer: scl34225.us.oracle.com port: 9810 p...	scl34225.us.oracle.com	9810
Essbase Server	essbaseserver1	instance3	↑	SSL ping OK. peer: scl34225.us.oracle.com port: 9799 p...	scl34225.us.oracle.com	9799