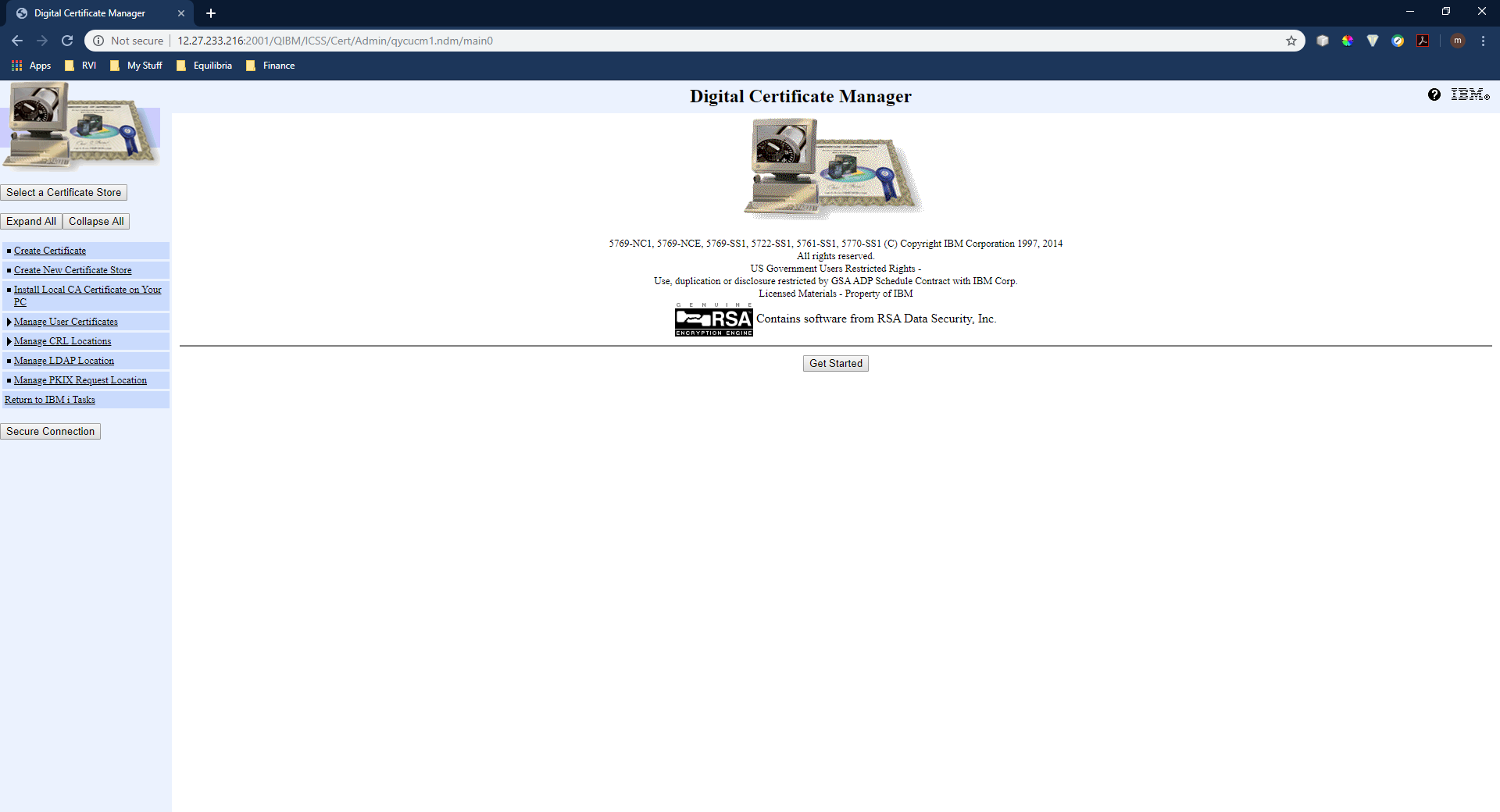
**WSS SSL CONFIGURATION FOR IBM I**

**(Note: If you just installed HTTPS and have the “SSLKEY.txt” file and downloaded files from your certificate provider then skip to Step – 9)**

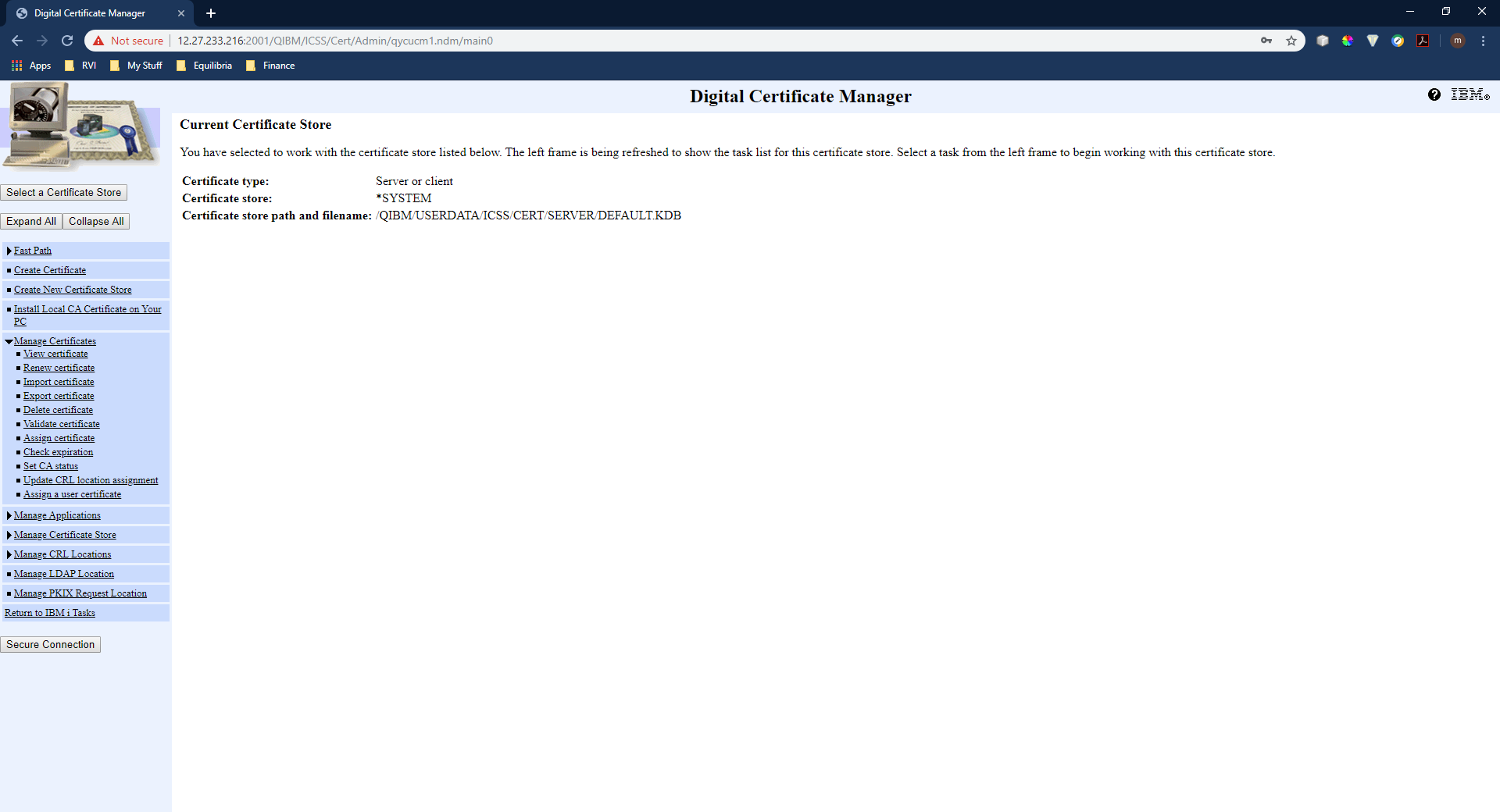
Step 1 - First go to your Hosts DCM (Digital Certificate Manager)

Ex. <http://12.27.233.216:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0>

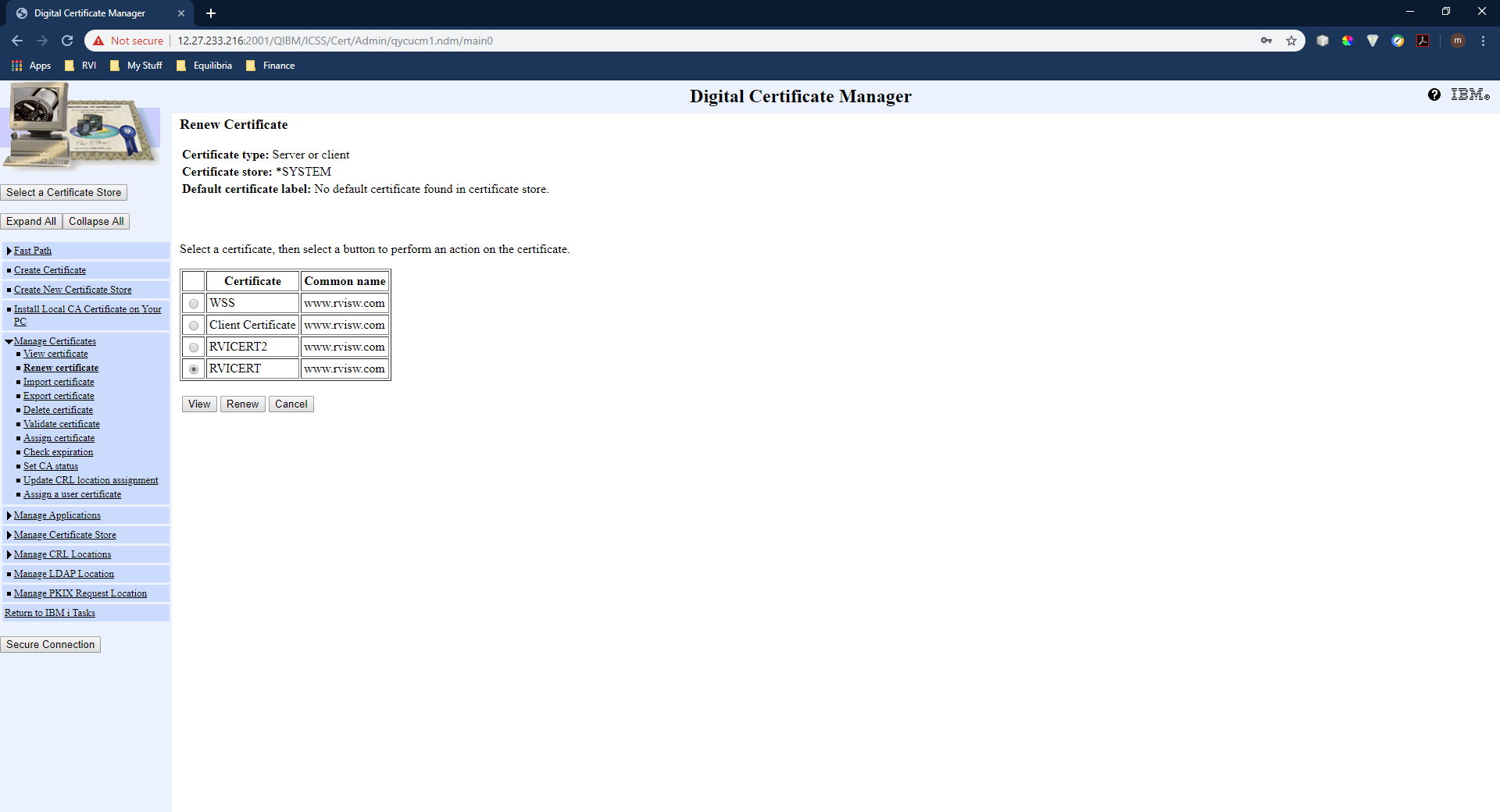


Step - 2 Click the “Select a Certificate Store” button and select the \*SYSTEM store. (This is if the \*System Store has already been created. Click Continue.

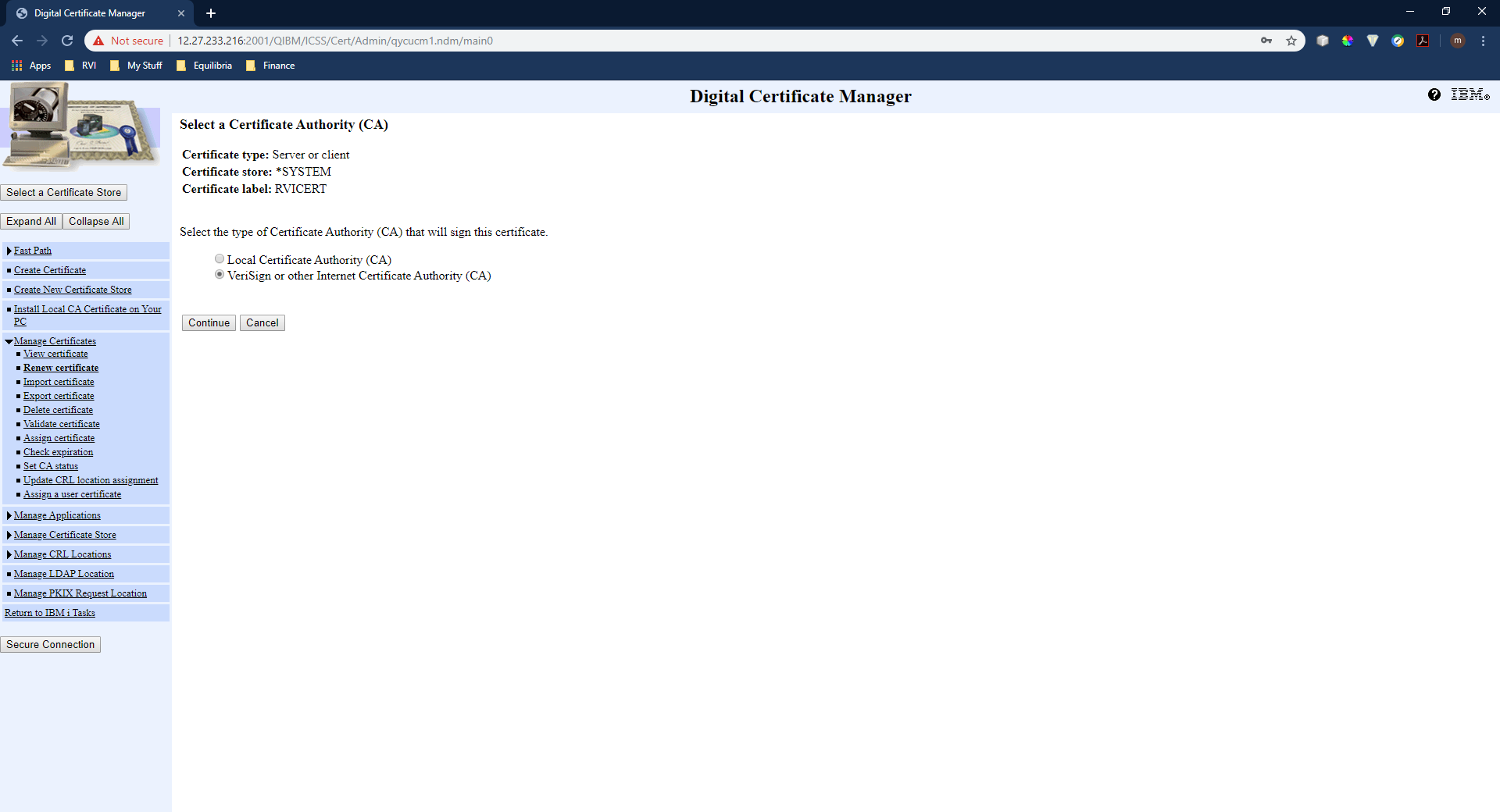
Step - 3 Enter the password for the certificate Store when prompted. Click Continue.

Step - 4 Click the “Manage Certificates” drop down and select “Renew certificate”.

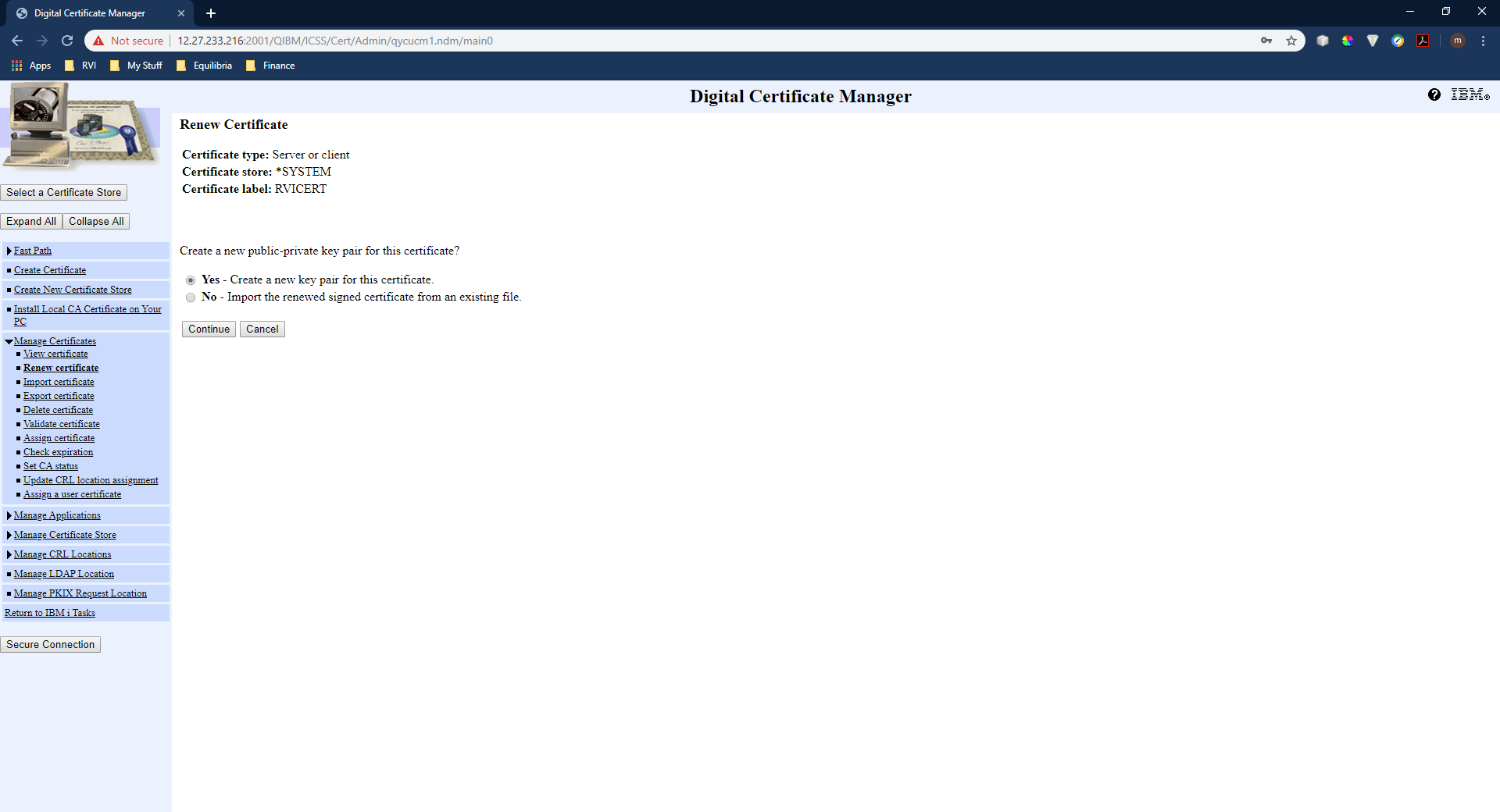
Step - 5 Select the certificate pertaining to the HTTPS instance you are working with and click “Renew”.

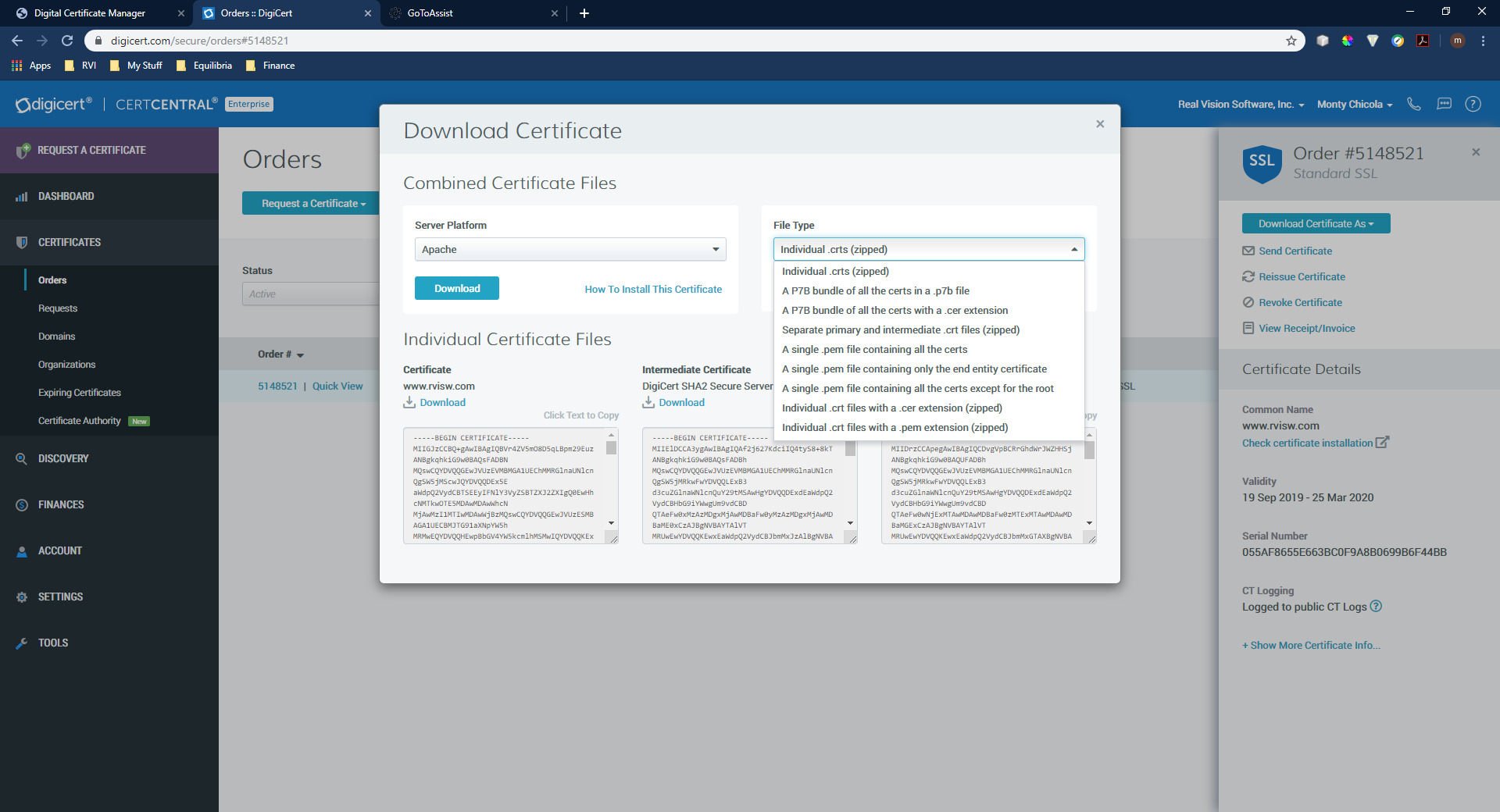


Step - 6 Select “VeriSign or other Internet Certificate Authority (CA)” and click Continue.



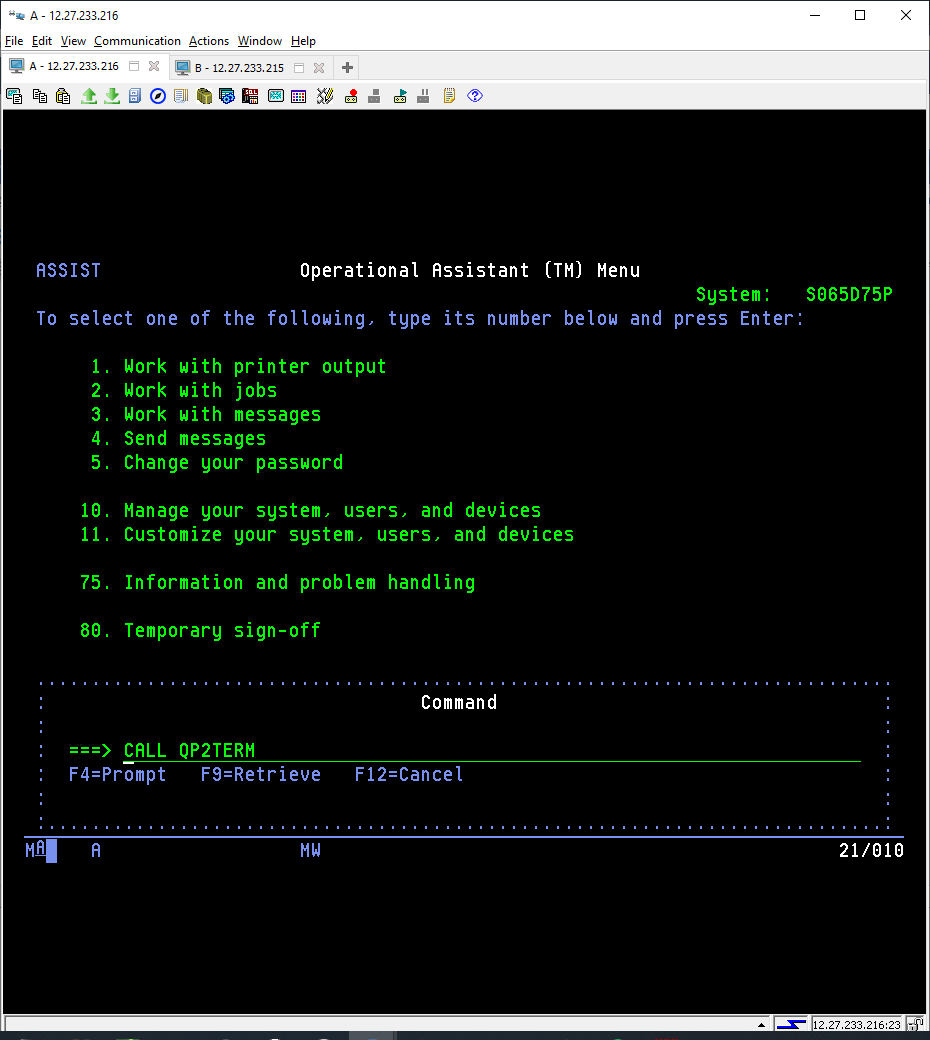
Step - 7 When prompted to create a new public-private key pair select “Yes” and click Continue.



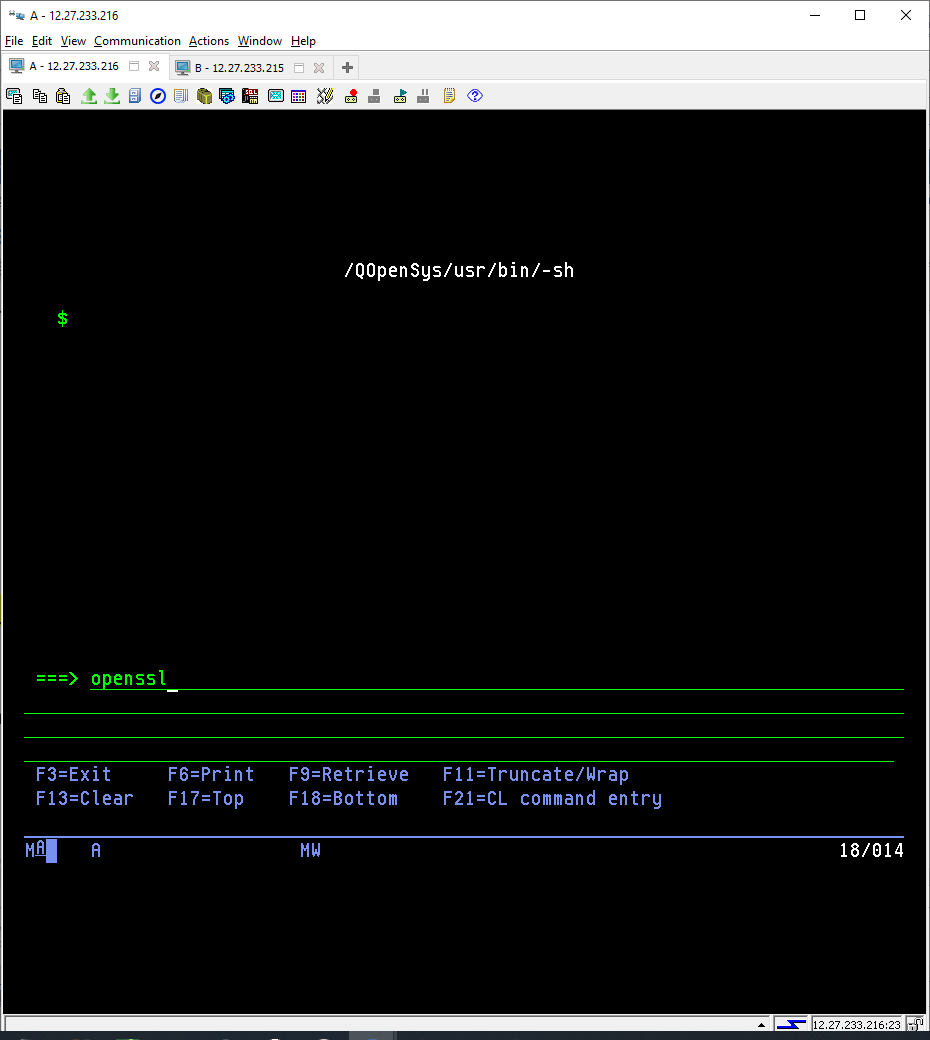
Step - 8 You will then fill out the information accordingly. Once finished, this process will produce a Base64 key. You will take this key and go to [www.digicert.com](http://www.digicert.com) to renew the certificate(make sure to save the key data in a text file named “SSLKEY” for later use. Also make sure to include “-----BEGIN NEW CERTIFICATE REQUEST-----” and “-----END NEW CERTIFICATE REQUEST-----" in the file). To renew your ssl certificate you will then use this key as your “CSR” which is the key used to generate your new certificate. Once the process is complete you want to download your certificates.(Make sure to select the options “Individual .crt files with a .cer extension (zipped)” and “A single .pem file containing all the certs”) 

Step - 9 Unzip the .zip file and put the .cer files on the server in the “/cgibin” directory. Next take the “SSLKEY.txt” file and change the extension on it to “.key” and move it on the server in the “/cgibin” directory as well.

Step - 10 Now on the IBM I we will run a few commands to create a java keystore for the secured websocket to connect to. First enter “Call QP2TERM” on the command line to enter Qshell.



Step - 11 Now enter “openssl” on the Qshell command line.



Step - 12 Next we will create a .p12 file by running the following command in OpenSSL. (pkcs12 -export -in "/cgibin/www\_rvisw\_com.cer" -inkey "/cgibin/SSLKEY.key" -name "www.rvisw.com" -out "/cgibin/keystore.p12”). (Make sure to replace “www\_rvisw\_com” and “www.rvisw.com” with your servers domain name.) This will create a keystore.p12 file in “/cgibin” directory. Once this is complete enter “exit” on the command line.

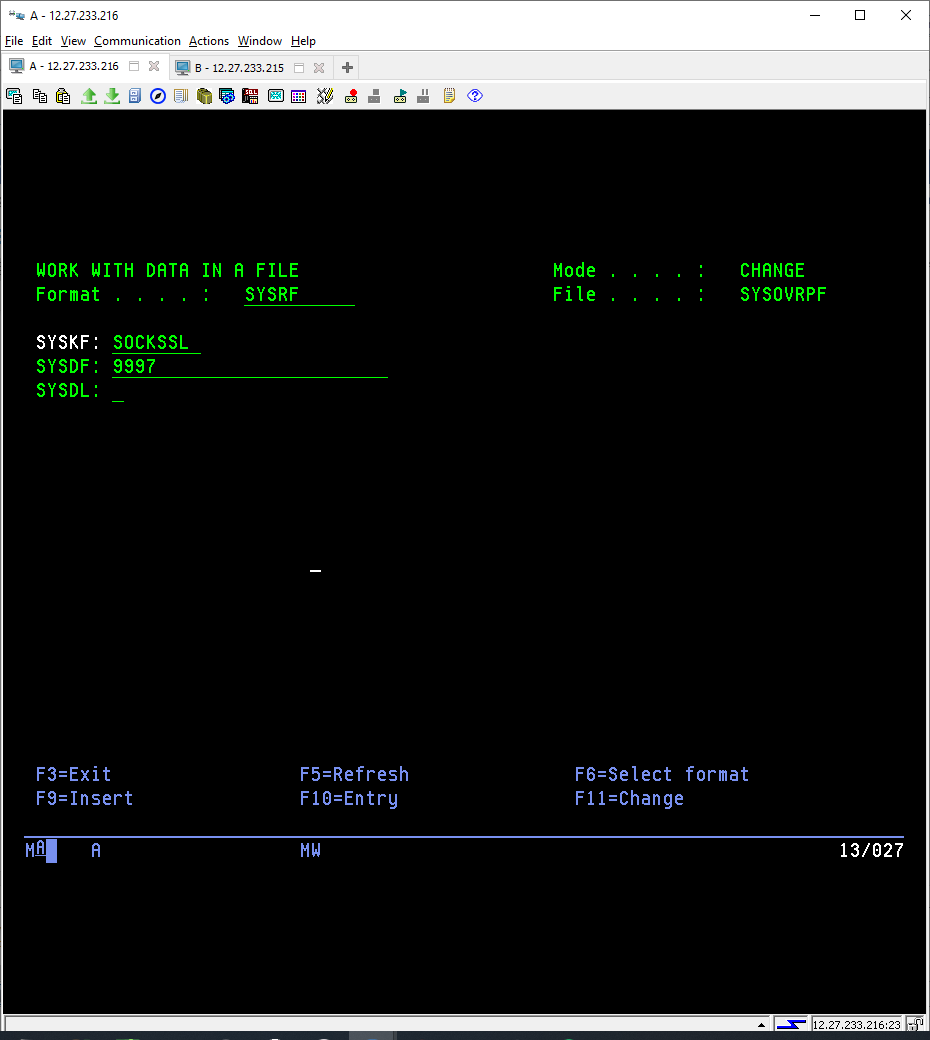
Step - 13 Next we will create a keystore by running the following command in Qshell. (keytool -genkey -keystore "/cgibin/keystore.jks" -storepass "remote" -keypass "remote" -alias "default" -dname "CN=www.rvisw.com, OU=MyOrgUnit, O=RVI, L=Alexandria, S=LA, C=US"). (Make sure to replace all the highlighted items with values for your company. Do not replace storepass and keypass values because they are used in the socket program.) This will create a keystore.jks file in “/cgibin” directory.

Step - 14 Next we will import the .p12 file into the keystore by running the following command in Qshell. (keytool -importkeystore -deststorepass "remote" -destkeystore "/cgibin/keystore.jks" -srckeystore "/cgibin/keystore.p12" -srcstoretype PKCS12)

Step - 15 Next we will import the trusted root certificate into the keystore by running the following command in Qshell (keytool -import -alias firstCA -file "/cgibin/trustedroot.cer" -keystore "/cgibin/keystore.jks")

Step – 16 Lastly we will import the main CA files into the CAroot file on your IBM i. We can do this by running the following command. (keytool -import -alias bundle -trustcacerts -file "/cgibin/www\_rvisw\_com.pem" -keystore "/QOpenSys/QIBM/ProdData/JavaVM/jdk80/32bit/jre/lib/security/cacerts") (Make sure to replace “www\_rvisw\_com” with the correct name of your .pem file. Also check to make sure this path above exists on your machine. If it doesn’t you may be running an older version of Java which means you will need to change the path accordingly.) You will be prompted for a password on the cacerts keystore. If you have never used with this file before the password is “changeit”.

Step - 17 Now to start the socket. Check to make sure “/cgibin/java/RVISOCKETSSL.jar” exists. Also, check to make sure program RVSTRSSLSK exists in RVILIB. If you don’t not have either of these contact RVI Support. Next we will make sure to add SOCKSSL to RVILIB/SYSOVRPF file with a value of the desired port to run the secured websocket on. With everything set up correctly you can now run this command to start the Secured websocket “CALL RVSTRSSLSK”.





This will display in active jobs when socket is running.