SSL Configuration in local AEM instance

Before configuring the SSL in our local AEM instance, we need to have a valid private key and certificate files.

Go to bin location, where you have openssl installed.

Ex: C:\Users\vthalla\Downloads\openssl-0.9.8k\_X64\bin

Execute the below listed commands in the same order to create both private key and certificate files.

1. Create a private key –

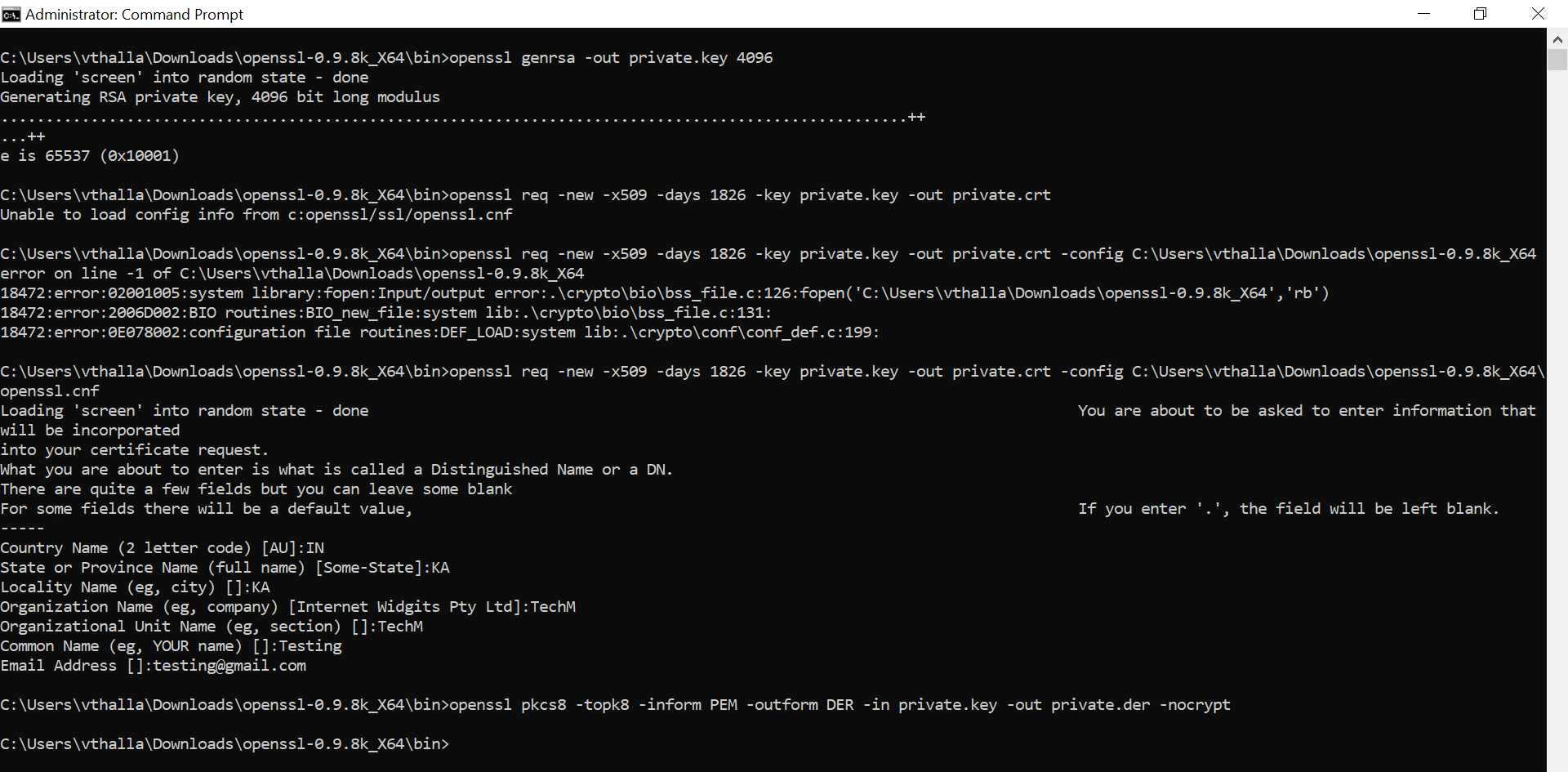
openssl genrsa -out private.key 4096

1. Create a certificate

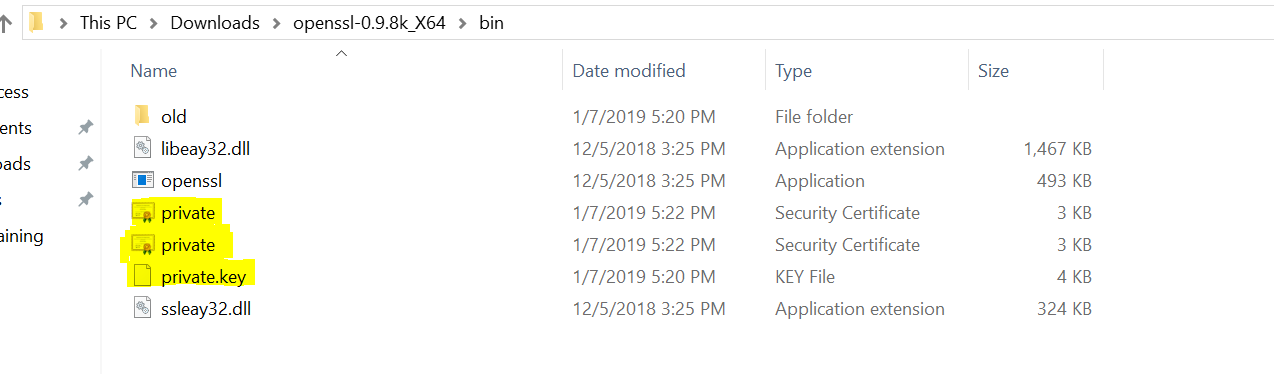
openssl req -new -x509 -days 1826 -key private.key -out private.crt -config C:\Users\vthalla\Downloads\openssl-0.9.8k\_X64\openssl.cnf

1. Convert the private key format from .key to .der

openssl pkcs8 -topk8 -inform PEM -outform DER -in private.key -out private.der -nocrypt



After executing these list of commands mentioned above, you will see the private key, certificate create inside bin folder.

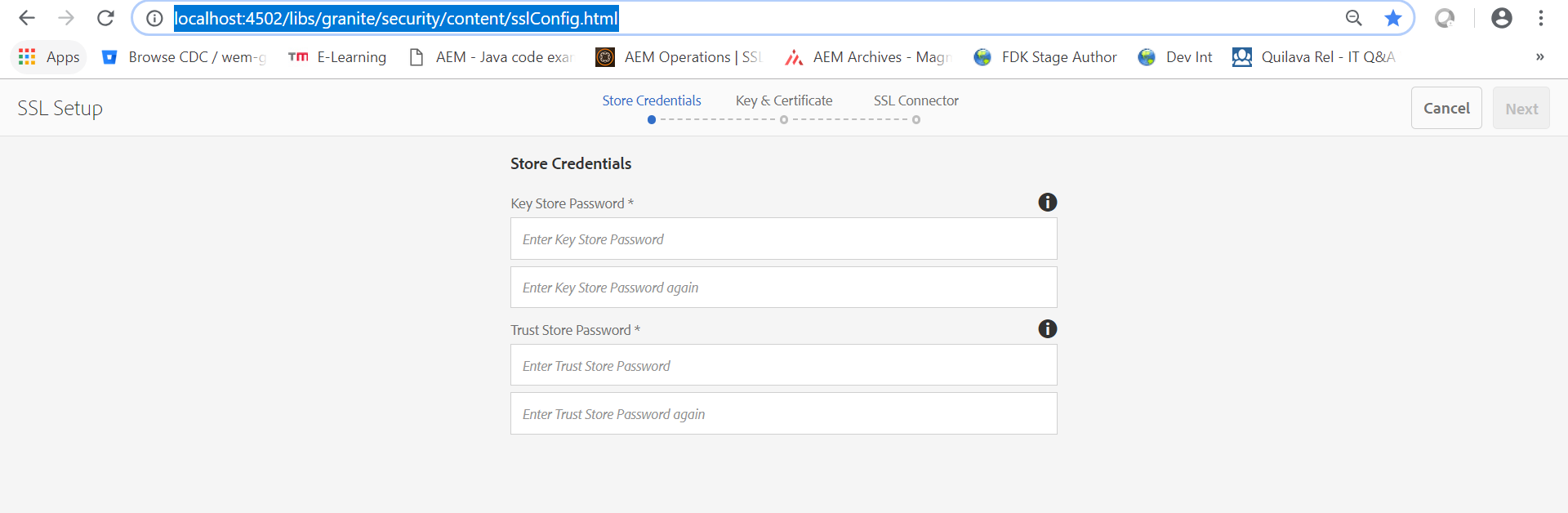


Once we have all these things created, we need to configure SSL under the following location.

<http://localhost:4502/libs/granite/security/content/sslConfig.html>

Follow the below steps to finish the configuration.

Step1: Provide store credentials

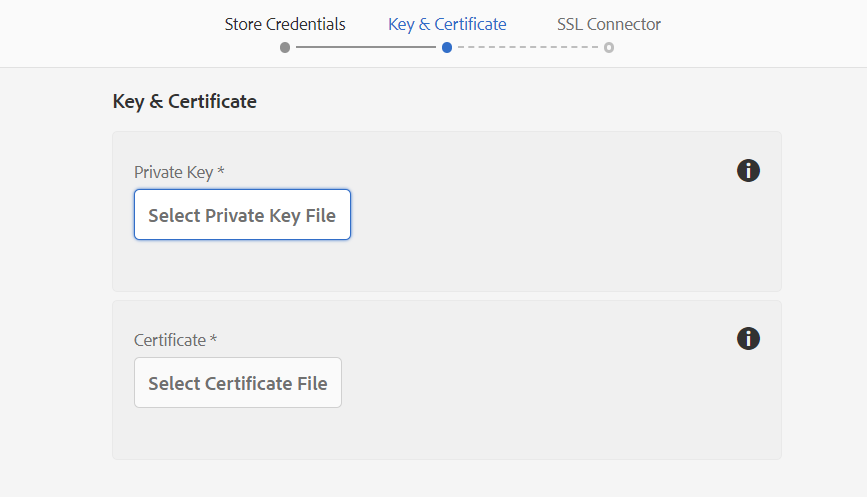


Provide the password details here (as it is just for local instance, you can give any simple passwords).

Step2: Uploading key and certificates created earlier.

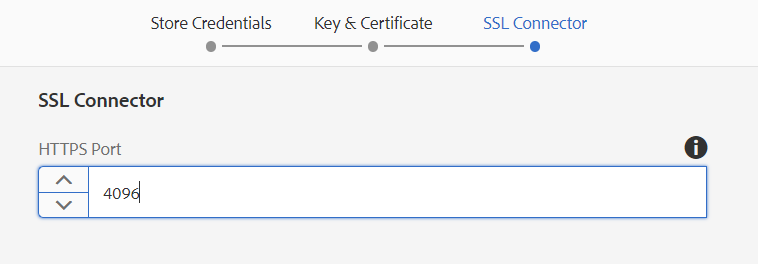
We need to upload the private key and certificates created in our earlier steps. As we are setting up SSL for local instance, a self-certificate is enough for testing purposes. But for production environments, we need a certificate from certified authorities.

Select the private key, which is created in .der format and certificate in .crt format.

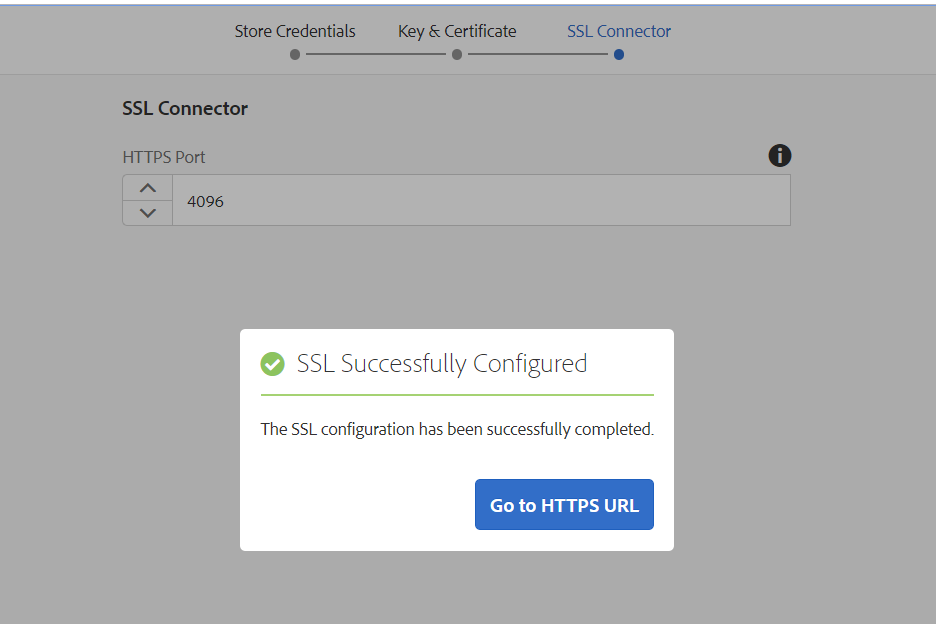


Step3: Provide the SSL connector value

This is the port number on which this SSL is going to work. Provide the port value of your choice and click on “Done”.



You will see a success message as shown below, after successful SSL configuration.

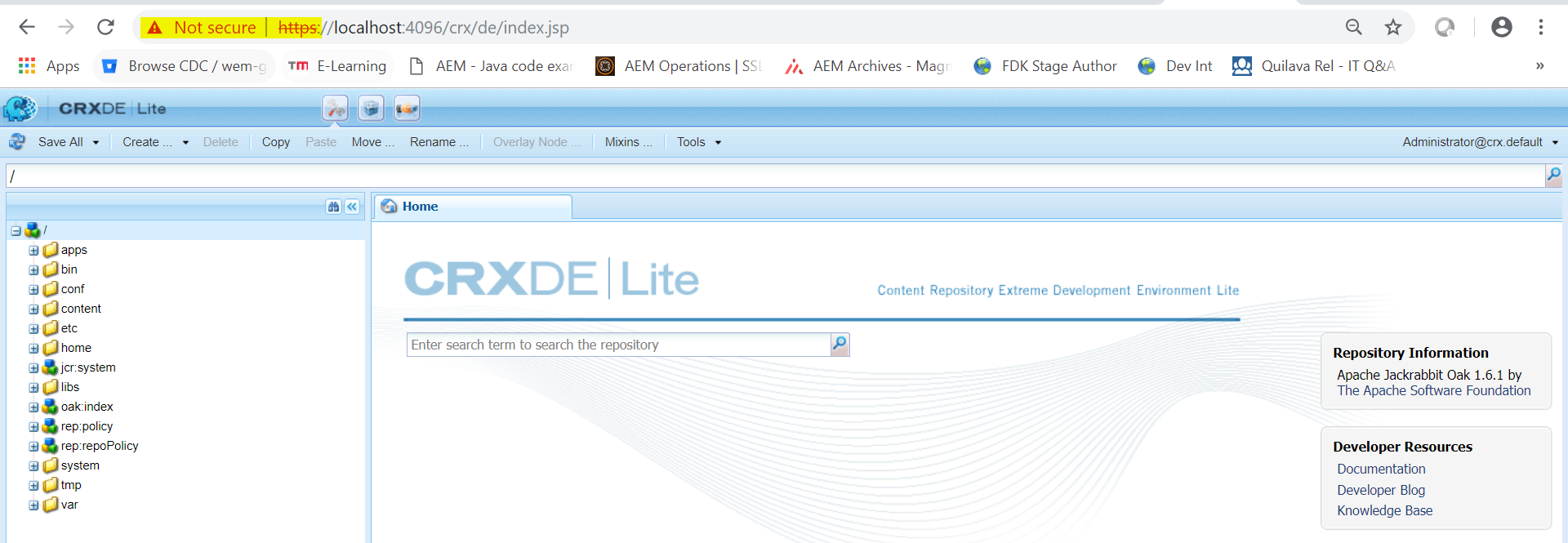


**Verification steps:**

We are good to go now. Access the instance URL on SSL port and verify if it’s working.

<https://localhost:4096/crx/de/index.jsp>

After accessing the crx de, we should be able to see the instance as shown below.



As we don’t have a trusted certificate from certified authorities, URL is showing the message “Not secure”.