Generating the CSR file using OPENSSL in Linux:

The following steps are to show you how to create certificate signing request (*.csr) file, so you can upload to RA to generate a request.

Generating the CSR requires a number of shell commands, the location and file name of your newly created key, and a path and file name for your CSR. In addition, some information (e.g. country, state, etc.) is required to populate the CSR.

1) Generate a pair of keys (public and private keys) and save file in path with key file extension, it is imporant to provide the size of keys in this example 2048bit:

   ```
   openssl genrsa -des3 -out /path/to/www_server_com.key 2048
   ```

2) Then, create the csr file by running:

   ```
   openssl req -new -key /path/to/www_server_com.key -out /path/to/www_server_com.csr
   ```

Note that a certificate-signing request always should a file name ending with .csr extension. During executing of previous command, enter your pass phrase will be prompted.

3) At this stage, you will be prompted to provide some information, which will be included into your CSR. This information is also known as the Distinguished Name, or DN. Some fields are required, while others are optional and can be left blank.

- The **Country Name** is mandatory and takes a two-letter country code such as GB.
- The **State or Province Name** field requires a full name – do not use an abbreviation, such as London.
- The **Locality Name** field is for your city or town or device address.
- In the **Organization Name** field, insert your organization or device provider.
- **Organizational Unit** Name is an optional field for your department or section or device type.
- The **Common Name** field is used as a user or device identifier. For a user identifier, enter your name while for a device identifier, it is recommended to use UUDI to have a unique identifier.
- **Email address** is an optional field for this request. (You can press Enter to skip forward.)
- The **challenge password** and **company name** fields are optional and it is important in this stage to skip these fields. This is because it is decided in this system not to handle these fields. Therefore, please leave them blank.

Note: If you prefer to use other tools to generate your own csr file, the following links provide you with some relevant resources of the other tools such as java keytool, windows MMC , etc.:

- **Java Keytool:**

  https://www.digicert.com/csr-creation-java.htm

- **Windows:**

  http://www.entrust.net/knowledge-base/technote.cfm?tn=8924

  https://documentation.meraki.com/zGeneral_Administration/Other_Topics/Creating_an_Offline_Certificate_Request_in_Windows_Server

- **Mac:**

  https://www.digicert.com/csr-creation-ssl-installation-mac-osx-el-capitan.htm

  https://www.sslsupportdesk.com/certificate-signing-request-csr-instructions-for-apple-mac-os-x-10-11/

If you need any support, please do not hesitate to contact the Security Team at Royal Holloway University of London

(Salaheddin.darwish@rhul.ac.uk ,

I.R.Nouretdinov@cs.rhul.ac.uk ,

Stephen.Wolthusen@rhul.ac.uk)