Generating the CSR file using OPENSSL in Linux:

The following steps are to demonstrate how to create Certificate Signing Request (*.csr) file using a Linux terminal, 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 important to provide the size of keys in this example 2048bit:

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

2) Then, create a configuration file (*.txt file) which includes all the information and properties required for generate a correct certificate request for CA. in

cat > csr_details.txt <<-EOF

[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[dn]
C=GB # The **Country** Name is mandatory and takes a two-letter country code such as GB.
ST=Surrey # The **State or Province Name** field requires a full name – do not use an abbreviation, such as London.
L=Egham # The **Locality Name** field is for your city or town or device address.
O= RHUL # The **Organization Name** field, insert your organization or device provider
OU=ISG # The **Organizational Unit** Name is an optional field for your department or section or device type
CN = www.your-new-domain.com # 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.
emailAddress=your-administrative-address@your- domain.com # An optional filed

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = your-new-domain.com # alternative Name for CN
DNS.2 = www.your-new-domain.com # alternative Name for CN
EOF

After performing the previous command, please check if the configuration file has been created by looking into the current directory.

3) Finally, create Certificate Signing Request (*.csr) file by using the following OpenSSL command:

   openssl req -new -key -out /path/to/www.your-new-domain.com.csr **-key** /path/to/www_server_com.key **-config** <(**cat** csr_details.txt)

Note that a certificate-signing request always should a file name ending with a *csr* file extension. During executing of the previous command, enter your passphrase will be prompted for the key.

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)