Generar manualmente una solicitud de firma de certificado (CSR) Usando OpenSSL

¿Qué es OpenSSL?
OpenSSL es un conjunto de herramientas de línea de comandos de código abierto muy útil para trabajar con solicitudes de firma de certificados (CSRs) y claves criptográficas. Si está utilizando una variante de UNIX como Linux o macOS, es probable que OpenSSL ya esté instalado en su computadora.

En estas instrucciones, usaremos OpenSSL para generar la clave privada como CSR en un comando. Generar la clave privada de esta manera garantizará que se le solicite una contraseña para proteger la clave privada. En los comandos que se muestran, los nombres de archivo que aparecen en MAYÚSCULAS reemplácelos con las rutas y nombres de archivo reales que desea usar. Por ejemplo, puede reemplazar PRIVATEKEY.key con /private/etc/apache2/server.key en un entorno macOS Apache.

RSA

El siguiente comando OpenSSL generará una clave privada RSA de 2048 bits y CSR:

```
[root@localhost ~]# openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr_
```

openssl req -newkey rsa: 2048 -keyout PRIVATEKEY.key -out MYCSR.csr

Analicemos el comando:

- openssl: Es el comando para ejecutar OpenSSL.
- req: Es la utilidad OpenSSL para generar un CSR.
- -newkey rsa:2048:
  Le indica a OpenSSL que genere una nueva clave privada RSA de 2048 bits.
  Si prefiere una clave de 4096 bits, puede cambiar este número a 4096.
- -keyout PRIVATEKEY.key : Especifica dónde guardar el archivo de clave privada.
- -out MYCSR.csr: Especifica dónde guardar el CSR archivo.
    - Con estos dos últimos elementos, recuerde utilizar sus propias rutas y nombres de archivo para la clave privada y CSR.

Después de escribir el comando, presione entrar. Se le presentará una serie de indicaciones:

- Primero cree una contraseña. Recuerde esta contraseña porque la necesitará nuevamente para acceder a su clave privada.

```
Generating a 2048 bit RSA private key
.....................................................................+++
.....................................................+++
writing new private key to 'PRIVATEKEY.key'
Enter PEM pass phrase:
```

- Ahora se le pedirá que ingrese la información que se incluirá en su CSR. Esta información también se conoce como Nombre distinguido DN:
    - El Nombre del país (opcional) toma dos letras código de país.
    - El Nombre de localidad campo (opcional) es para su ciudad o pueblo.
    - El Nombre de la organización El campo (opcional) corresponde al nombre de su empresa u organización.
    - El Nombre común campo (requerido) se utiliza para el Nombre de dominio completo (FQDN) del sitio web que protegerá este certificado.
    - Correo electrónico (opcional)
    - El campo Contraseña de desafío. Es opcional y se puede omitir también.

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:UY
State or Province Name (full name) []:Montevideo
Locality Name (eg, city) [Default City]:Montevideo
Organization Name (eg, company) [Default Company Ltd]:Montevideo Comm
Organizational Unit Name (eg, section) []:Operaciones
Common Name (eg, your name or your server's hostname) []:www.montevideocomm.uy
Email Address []:dominios@m.uy

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@localhost ~]#
```

Al finalizar este proceso, volverá a un símbolo del sistema. No recibirá ninguna notificación de que su CSR fue creado con éxito.
Enviar el archivo .csr a dominios@m.uy para generar el certificado SSL.