

Geranção da CSR - OpenSSL

São Paulo, 7 de Dezembro de 2021

Solicitação de Assinatura de Certificado no OpenSSL

1. Para criar um CSR , você precisa do utilitário de linha de comando OpenSSL instalado em seu sistema, caso contrário, execute o seguinte comando para instalá-lo.

```
$ sudo apt install openssl [On Debian/Ubuntu]
```

```
$ sudo yum install openssl [On CentOS/RHEL]
```

```
$ sudo dnf install openssl [On Fedora]
```

2. Em seguida, emita o seguinte comando para gerar um CSR e a chave que protegerá seu certificado.

```
$ openssl req -new -newkey rsa:2048 -nodes -keyout example.com.key -out example.com.csr
```

3. Onde:

`req` enables the part of OpenSSL that handles certificate requests signing.

`-newkey rsa:2048` creates a 2048-bit RSA key.

`-nodes` means “don’t encrypt the key”.

`-keyout example.com.key` specifies the filename to write on the created private key.

`-out example.com.csr` specifies the filename to write the CSR to.

4. Responda corretamente, as perguntas que você será perguntado. Observe que suas respostas devem corresponder às informações em documentos legais referentes ao registro de sua empresa. Essas informações são verificadas criticamente pela CA antes de emitir seu certificado.

```
[admin@wserver ~]$ openssl req -new -newkey rsa:2048 -nodes -keyout example.com.key -out example.com.csr
Generating a 2048 bit RSA private key
...+++
...+++
writing new private key to 'example.com.key'
-----
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]:UG
State or Province Name (full name) []:Central
Locality Name (eg, city) [Default City]:Kampala
Organization Name (eg, company) [Default Company Ltd]:Example.com LTD
Organizational Unit Name (eg, section) []:Internet and Software
Common Name (eg, your name or your server's hostname) []:server1.example.com
Email Address []:admin@example.com

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

+55 11 2872 7004

Rua Estela, 515 – 7º andar | Vila Mariana
São Paulo, SP

www.arsaopaulo.com.br

5. Depois de criar seu CSR , visualize o conteúdo do arquivo usando um utilitário cat, selecione-o e copie-o.

```
$ cat example.com.csr
```

```
[admin@wserver ~]$ ls example.com.  
example.com.csr example.com.key  
[admin@wserver ~]$  
[admin@wserver ~]$ cat example.com.csr  
-----BEGIN CERTIFICATE REQUEST-----  
MIIC8TCCAdkCAQAwgasxCzAJBgNVBAYTALVHMRAwDgYDVQQIDAdDZW50cmFzMRAw  
DgYDVQQHDAcL7aAhL2EWJ5WpxC60g2HSIXAh1G5Gr1QRpWTrh8pfBZZiP0xZsSeg  
/QKiWA7BlxHXrvh5VW2EGXqyQQHMNsW0ymzWbL/fB8L84zQ3HhZKReyhcb+s2lTy  
Rds0RB4SYiocv6zPE1WXTYe8Ww0PkNh4A8i3EZAV0X0PpK5HxhUKTSxAgMBAAGg  
ADANBgkqhkiG9w0BAQsFAAOCQAQEAZJVPd+4ZpdIJD6vs4QMCRXoJJFgEIZGPPqYA  
+sg94IWpXJTNX0wh0i0gXqpoCKFNrHN90Yh9GZic8imDGM7ihXu64NaJ/sV/kH02  
SYk+rNmcmWx4IMK3lf9d5mtCnMXF8JbrDLRIQvqdh60fiF/SPcdvDXZicVigvAY  
8LFeZ1gr5kvxhpzkN/Jfuz6BTka0s0/mh2vqaGCLY36hvf9mv00c2Xw1JanakWan  
TWILrylsvkp269+tNd1bvFFeFsa0Huh25b7TijXQhA4CJKsFzAy/8SugAcWPKhxt  
LJg9Cw9eRmPsKA4SPGXTuV4zWCI70mj7j2wRNEHDl2m1clLN2rg==  
-----END CERTIFICATE REQUEST-----  
[admin@wserver ~]$
```

6. Em seguida, volte ao site da CA, efetue login, vá até a página que contém o certificado SSL que você comprou e ative-o. Em seguida, em uma janela como a abaixo, cole seu CSR no campo de entrada correto. Neste exemplo, criamos um CSR para um certificado de vários domínios adquirido do Namecheap .

7. Em seguida, siga o restante das instruções para iniciar a ativação do seu certificado SSL. Para mais informações sobre o comando OpenSSL, veja sua página man:

```
$ man openssl
```

- É tudo por agora! Lembre-se sempre de que o primeiro passo para obter seu próprio certificado SSL de uma CA é gerar um CSR.