eBOOK

How to generate the CSR for SSL Certificate

bluegrid.io

The only thing that you absolutely have to know, is the location of the library.

Albert Einstein

Famous Librarian

Introduction

In this ebook, we are covering how to generate the CSR for SSL Certificate:

openssl req -new -newkey rsa:2048 -nodes -keyout domain.com.key -out domain.com.csr

Specification:

OS Version: CentOs 8.2 x64
OpenSSL Version: OpenSSL 1.1.1c FIPS 28 May 2019
NOTE: Below commands are cross-platform compatible/no specific OS is required.

CSR

CSR or Certificate Signing Request is a file we need to generate and provide to the **CA (Certificate Authority).**
Authority to get what we know as SSL Certificate and CA bundle.

CA bundle is the chain of Certificates used to verify the Certificate against several CA's.

Now, let's see how to generate CSR for an SSL Certificate.

CSR

To begin with let's first clear up the potential naming confusion.

SSL Certificate is the wrong name for what we are talking about here.

SSL (Secure Sockets Layer) was decommissioned in 2018 due to a number of security flaws.
Since then the only legitimate HTTPS protocol is the TLS (Transport Layer Security) version 1.1 and 1.2.

Step by step

To understand the steps needed for a Certificate to be valid we need to go from the beginning of the process.

First, we need to have the SSL Key generated.
This key will then be used to generate the CSR. CSR is sent to the CA Authority (SSL Certificate place market - where you go to buy your SSL Certificate).

Step by step follows:

1

Login to your server for which you are generating above mentioned files:

ssh user@domain.com

2

Execute the following command to generate the SSL key and then immediately use this key for generating the CSR file.
We are using the OpenSSL package:

[root@bluegrid-edu ~]# openssl req -new -newkey rsa:2048 -nodes -keyout domain.com.key -out domain.com.csr

Note: Replace domain.com with your actual domain for which you are generating the CSR.

3

You are going to be prompted for some details as the command executes.

Below are the fields and example of how to enter them:

Note: If there is no value entered it means we skipped it in making this example. t's optional fields.

Country Name (2 letter code) [XX]:RS
State or Province Name (full name) []:Serbia
Locality Name (eg, city) [Default City]:Belgrade
Organization Name (eg, company) [Default Company Ltd]:Blue Grid DOO
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:domain.com
Email Address []:office@domain.com

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password []:
An optional company name []:

4

After this, you will be able to see the .csr and the .key files generated by executing the following command:

[root@bluegrid-edu ~]# ls -l domain.com.*

And thee output would be something like:
-rw-r--r--. 1 root root 1041 Jul 31 13:09 **domain.com.csr** -rw-------. 1 root root 1704 Jul 31 13:07 **domain.com.key**

What to do with these files now? Excellent questions!

The next step is to send the content of the CSR file to your CA Authority (SSL marketplace like namecheap.com, godaddy.com...).

When you get the Certificate files (certificate and ca-bundle) you can install the certificate files and key on your Web server.

That is about it!

Enjoy!

FOLLOW @BLUEGRID ON SOCIAL NETWORKS

OTHER TECH ARTICLES YOU CAN FIND HERE