Instructions: Generation of CSR for Nginx

1. Login to your server via your terminal client (ssh). At the prompt, type the following command:

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

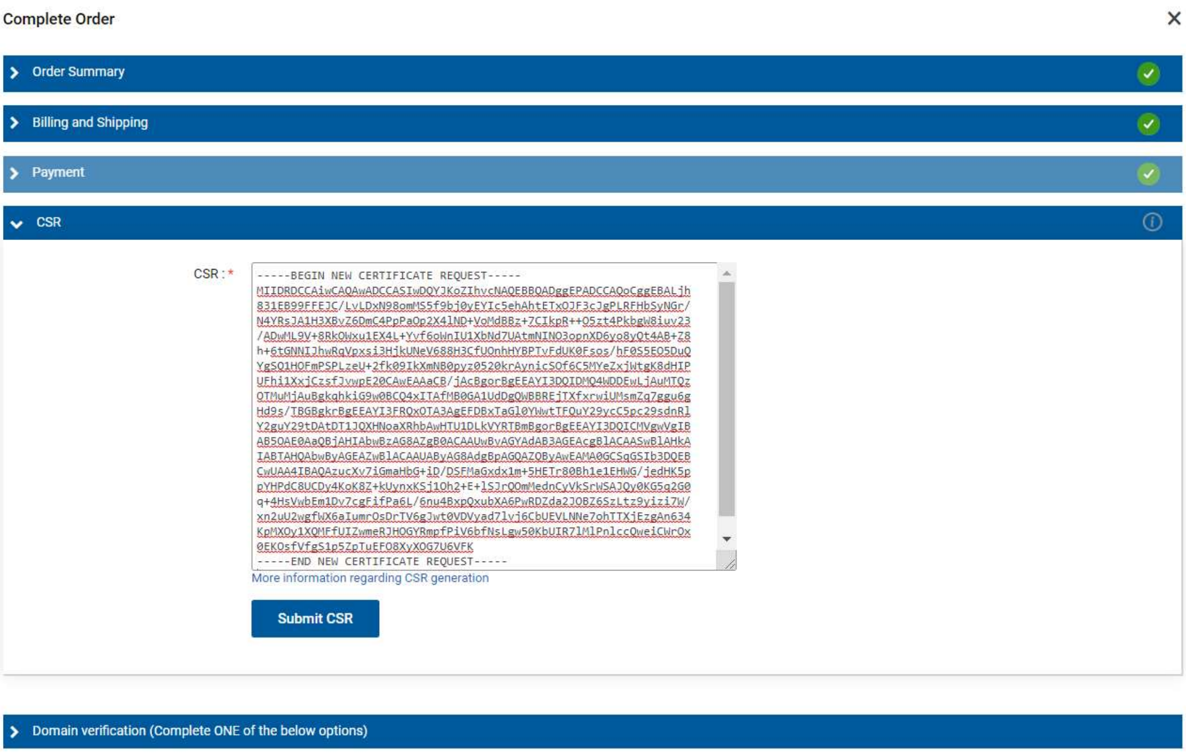
   At the prompts to enter the full subject distinguished name:

   - Country Name (C) :
   - State or Province (S) :
   - Locality or City (L) :
   - Organization Unit (O) :
   - Common Name (CN) :
   - Optional Fields :

   - Press Enter at the prompt for any other information (e.g. Email Address, Challenge Password, Optional Company Name etc)

   Your CSR file will then be created.

   Proceed to Complete Order in the TrustFactory portal and paste the CSR in relevant section when required



CSR :*

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDRDCCAiwCAQAwADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALjh
831EB99FFEJC/LvLDxN98omMS5f9bj0yEYIc5ehAhtETxOJF3cJgPLRFHbSyNGr/
N4YRsJA1H3XBvZ6DmC4PpPaOp2X4lND+VoMdBBz+7CIkpR++O5zt4PkbgW8iuv23
/ADwML9V+8RkOWxu1EX4L+Yvf6oWnIU1XbNd7UAtmNINO3opnXD6yo8yQt4AB+Z8
h+6tGNNIJhwRqVpxsi3HjkUNeV688H3CfUOnhHYBPTvFdUK0Fsos/hF0S5EO5DuQ
YgSO1HOFmPSPLzeU+2fk09IkXmNB0pyz0520krAynicSOf6C5MYeZxjWtgK8dHIP
UFhi1XxjCzsfJvwpE20CAwEAAaCB/jAcBgorBgEEAYI3DQIDMQ4WDDEwLjAuMTQz
OTMuMjAuBgkqhkiG9w0BCQ4xITAfMB0GA1UdDgQWBBREjTXfxrwiUMsmZq7ggu6g
Hd9s/TBGBgkrBgEEAYI3FRQxOTA3AgEFDBxTaGl0YWwtTFQuY29ycC5pc29sdnRl
Y2guY29tDAtDT1JQXHNoaXRhbAwHTU1DLkVYRTBmBgorBgEEAYI3DQICMVgwVgIB
AB5OAE0AaQBjAHIAbwBzAG8AZgB0ACAAUwBvAGYAdAB3AGEAcgBlACAASwBlAHkA
IABTAHQAbwByAGEAZwBlACAAUAByAG8AdgBpAGQAZQByAwEAMA0GCSqGSIb3DQEB
CwUAA4IBAQAzucXv7iGmaHbG+iD/DSFMaGxdx1m+5HETr80Bh1e1EHWG/jedHK5p
pYHPdC8UCDy4KoK8Z+kUynxKSj1Oh2+E+1SJrQOmMednCyVkSrWSAJQy0KG5q2G0
q+4HsVwbEm1Dv7cgFifPa6L/6nu4BxpQxubXA6PwRDZda2JOBZ6SzLtz9yizi7W/
xn2uU2wgfWX6aIumrOsDrTV6gJwt0VDVyad7lvj6CbUEVLNNe7ohTTXjEzgAn634
KpMXOy1XQMFfUIZwmeRJHOGYRmpfPiV6bfNsLgw50KbUIR7lMlPnlccQweiCWrOx
0EKOsfVfgS1p5ZpTuEFO8XyXOG7U6VFK
-----END NEW CERTIFICATE REQUEST-----
```

More information regarding CSR generation

Installing & Configuring Your SSL Certificate

Step 1 : Primary and intermediate certificates

You should've received a your_domain_name.pem file from TrustFactory in an email when your certificate was issued. This .pem file contains both your primary certificate and the intermediate certificate. If you have that .pem file, you can skip to step 4.

If you need to concatenate your primary certificate and your intermediate certificate in to a single file, see step 2.

Step 2: Copy the certificate files to your server

Log in to your TF account and download the intermediate (TF.crt) and your primary certificate (*your_domain_name.crt*) files.

Copy these files, along with the .key file you generated when creating the CSR, to the directory on the server where you'll keep your certificate and key files.

Note: Make them readable by root only to increase security.

Step 3: Concatenate the primary and intermediate certificates

You need to concatenate your primary certificate file (your_domain_name.crt) and the intermediate certificate file (TrustFactory.crt) into a single .pem file.

To concatenate the files, run the following command:

```
cat your_domain_name.crt TF.crt >> bundle.crt
```

Step 4: Edit the Nginx virtual hosts file

Open your Nginx virtual host file for the website you're securing.

Make a copy of the existing non-secure server module and paste it below the original.

Note: If you need your site to be accessible through both secure (https) and non-secure (http) connections, you will need a server module for each type of connection.

Next, add the lines in **bold** below:

```
server {

listen   443;

ssl    on;
ssl_certificate    /etc/ssl/your_domain_name.pem; (or bundle.crt)
ssl_certificate_key    /etc/ssl/your_domain_name.key;

server_name your.domain.com;
access_log /var/log/nginx/nginx.vhost.access.log;
error_log /var/log/nginx/nginx.vhost.error.log;
location / {
root   /home/www/public_html/your.domain.com/public/;
index  index.html;
}

}
```

Adjust the file names to match your certificate files:

ssl_certificate should be your primary certificate combined with the intermediate certificate that you made in the previous step (e.g., *your_domain_name.crt*).

ssl_certificate_key should be the .key file generated when you created the CSR.

1. Restart Nginx.

   Run the following command to restart Nginx:

   ```
   sudo /etc/init.d/nginx restart
   ```