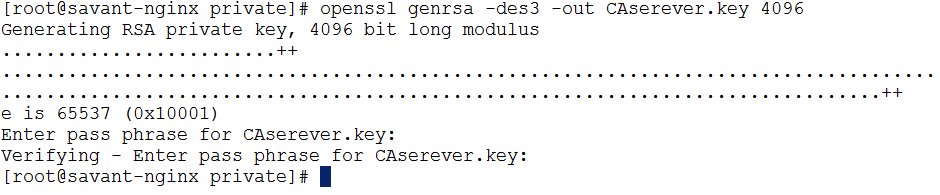
**Creating 2 Way Client Certificate (Self-Signed) for Nginx**

1. **Issue a self-signed server CA**

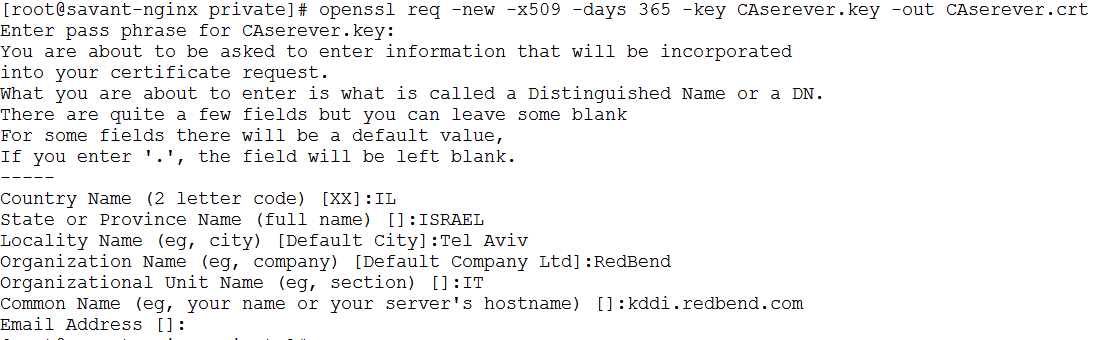
Enter the following Commands:

* **mkdir –p /etc/ssl/CA\_NAME/certs**
* **cd /etc/ssl/CA\_NAME/certs**
* **openssl genrsa -des3 -out CA\_NAME.key 4096** - (it will create a server CA.key file, you will be required to enter passphrase)



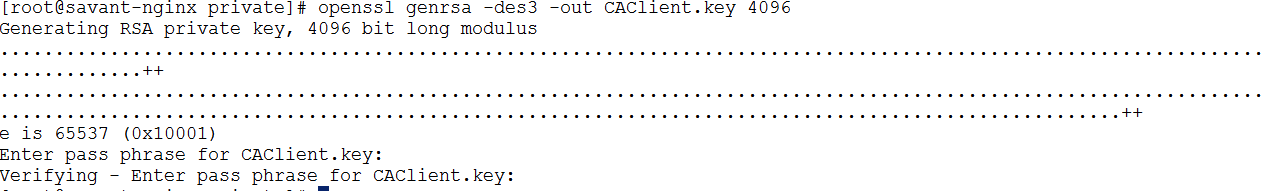
* **openssl req -new -x509 -days 730 -key CA\_NAME.key -out CA\_NAME.crt** - (it will create a server CA.crt file from the key file you’ve created earlier)

You will be asked to put the passphrase of the key file and some more details – under common name put the server public URL you can skip the Email address:

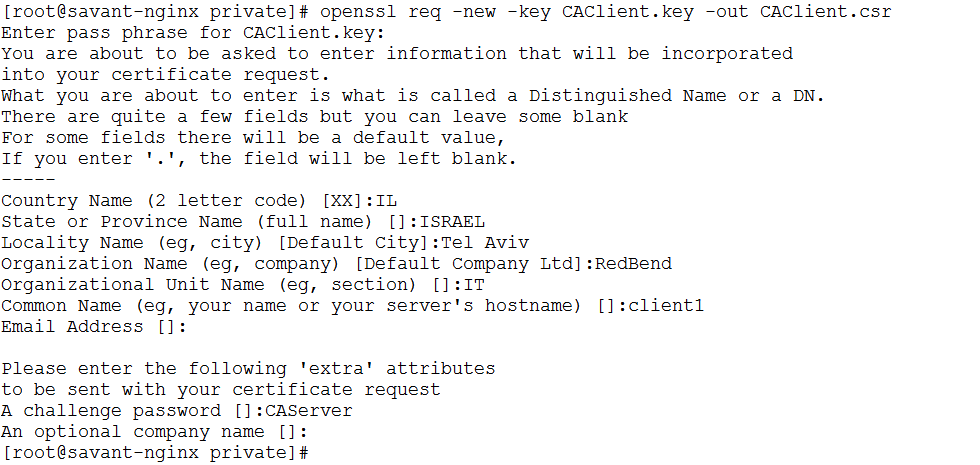


1. **Issue a client Certificate**

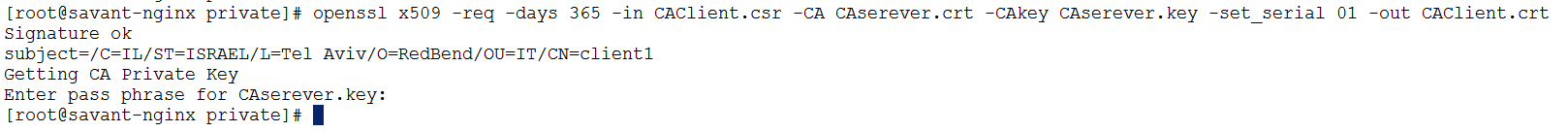
* **openssl genrsa -des3 -out Client.key 4096** - (it will create a Client.key file, you will be required to enter passphrase)



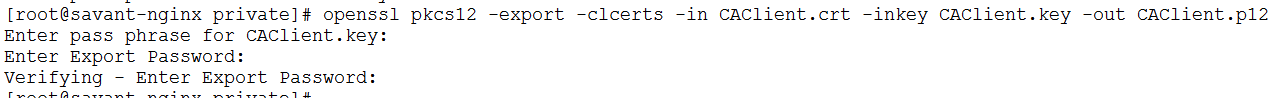
* **openssl req -new -key Client.key -out Client.csr** (it will create a CLient.csr file from the Client.key file you’ve created earlier)



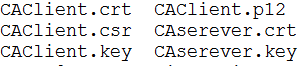
* **openssl x509 -req -days 730 -in Client.csr -CA CA\_NAME.crt -CAkey CA\_NAME.key -set\_serial 01 -out Client.crt** - (it will create a Handshake between the Server CA and The Client CA file)



* **openssl pkcs12 -export -clcerts -in Client.crt -inkey Client.key -out Client.p12** - (it will create a p12 file from the Client.key/crt files which is the file you should send to the client)



Now you should have the following files under /etc/ssl/CA\_NAME/certs:

****

1. **Nginx Configuration - edit /etc/nginx/conf.d/default.conf:**

**server {**

**listen 192.168.141.30:8080; ### Listenning Port for the Nginx**

**ssl on;**

**server\_name savant.redbend.com; ####Server public URL**

**# server\_name savant-nginx;**

**############# SSL Client Auth configuration ################**

**ssl\_client\_certificate /etc/ssl/savant/private/savantca.crt; ####Server CACert Location**

**ssl\_verify\_client on;**

**ssl\_session\_timeout 5m;**

**ssl\_protocols SSLv2 SSLv3 TLSv1;**

**ssl\_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv3:+EXP:HIGH:!aNULL:!MD5;**

**ssl\_prefer\_server\_ciphers on;**

**client\_max\_body\_size 1g;**

**################################################################**

**access\_log /var/log/nginx/log/sma.access.log main;**

**error\_log /var/log/nginx/log/sma.error.log;**

**root /usr/local/nginx/html;**

**location ~\* /(sma|resource|ex\_resources){ ####Server Access Specific URL**

**proxy\_pass <http://dm>; #### Upstream to the required port – in this using the existing dm port (8080)**

**proxy\_next\_upstream error timeout invalid\_header http\_500 http\_502 http\_503 http\_504;**

**proxy\_redirect off;**

**proxy\_buffering off;**

**proxy\_set\_header Host $host;**

**proxy\_set\_header X-Real-IP $remote\_addr;**

**proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;**

**proxy\_set\_header X-Forwarded-Proto https;**

**}**

**}**