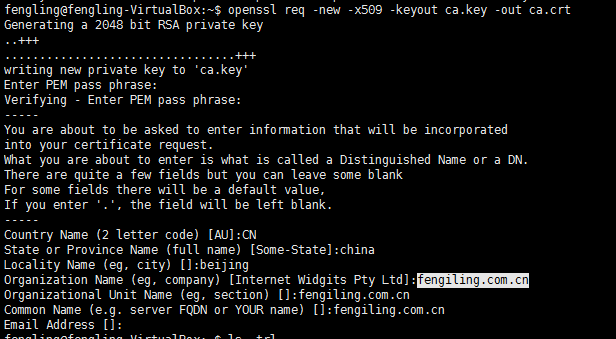
1. openssl req -new -x509 -keyout ca.key -out ca.crt -days 3650



Generating a 2048 bit RSA private key

...............................................+++

.................................................+++

writing new private key to 'ca.key'

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

-----

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) [AU]:CN

State or Province Name (full name) [Some-State]:china

Locality Name (eg, city) []:beijing

Organization Name (eg, company) [Internet Widgits Pty Ltd]:fengiling.com.cn

Organizational Unit Name (eg, section) []:fengiling.com.cn

Common Name (e.g. server FQDN or YOUR name) []:fengiling.com.cn

Email Address []:

2. openssl genrsa -des3 -out server.key 1024

Generating RSA private key, 1024 bit long modulus

........++++++

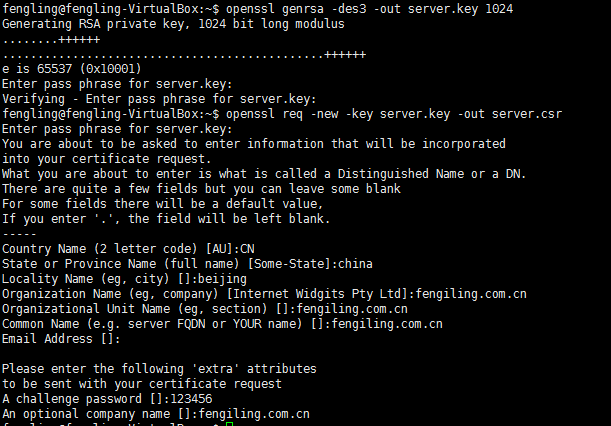
..............................................++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying - Enter pass phrase for server.key:

1. openssl req -new -key server.key -out server.csr



Generating RSA private key, 1024 bit long modulus

........++++++

..............................................++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying - Enter pass phrase for server.key:

fengling@fengling-VirtualBox:~$ openssl req -new -key server.key -out server.csr

Enter pass phrase for server.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) [AU]:CN

State or Province Name (full name) [Some-State]:china

Locality Name (eg, city) []:beijing

Organization Name (eg, company) [Internet Widgits Pty Ltd]:fengiling.com.cn

Organizational Unit Name (eg, section) []:fengiling.com.cn

Common Name (e.g. server FQDN or YOUR name) []:fengiling.com.cn

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:123456

An optional company name []:fengiling.com.cn

1. openssl genrsa -des3 -out client.key 1024

Generating RSA private key, 1024 bit long modulus

.........++++++

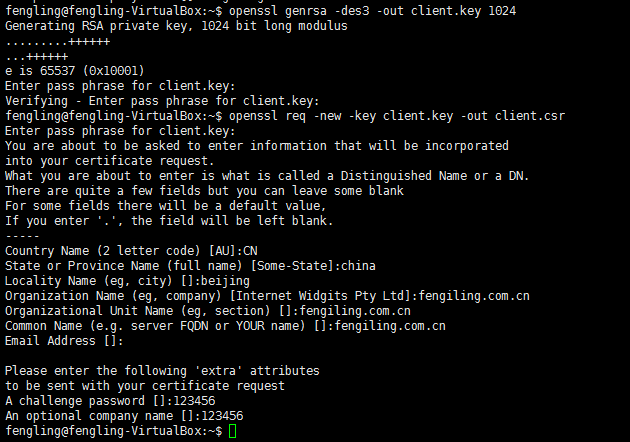
...++++++

e is 65537 (0x10001)

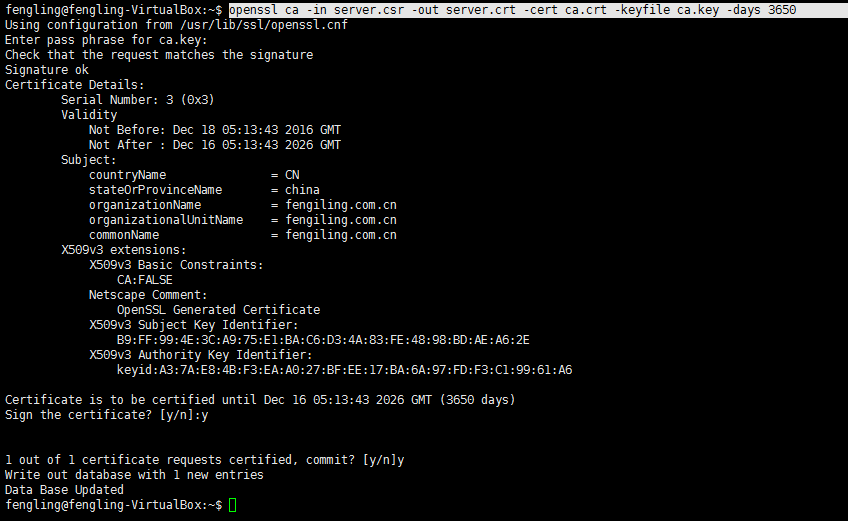
Enter pass phrase for client.key:

Verifying - Enter pass phrase for client.key:

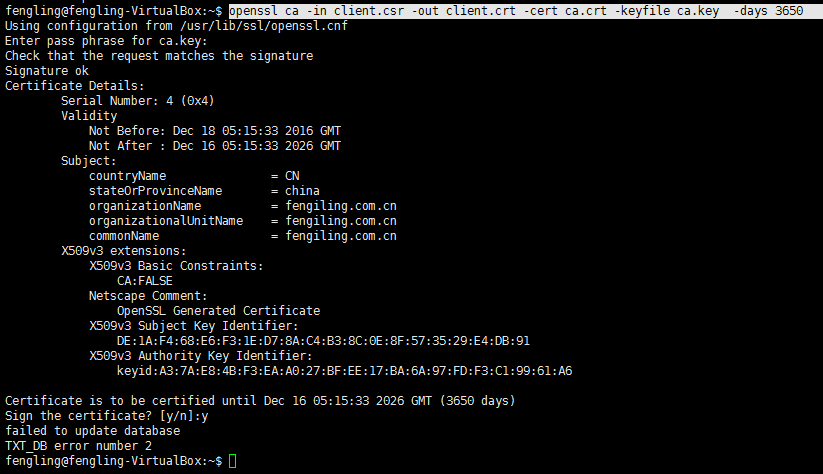
1. openssl req -new -key client.key -out client.csr



1. openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -days 3650



1. openssl ca -in client.csr -out client.crt -cert ca.crt -keyfile ca.key -days 3650



cat client.crt client.key> client.pem

cat server.crt server.key > server.pem

