NR500 Series
Industrial Cellular VPN Router

Application Note 016
OpenVPN Certificates Generated

Version:	V1.0.0
Date:	2018/09/14
Status:	Confidential

Directory

1. Introduction

1.1 Overview

This document contains information regarding how to generate the certificates for OpenVPN on Windows OS.

1.2 Corrections

Appreciate for corrections or rectifications to this application note, and if any request for new application notes please email to: support@navigateworx.com

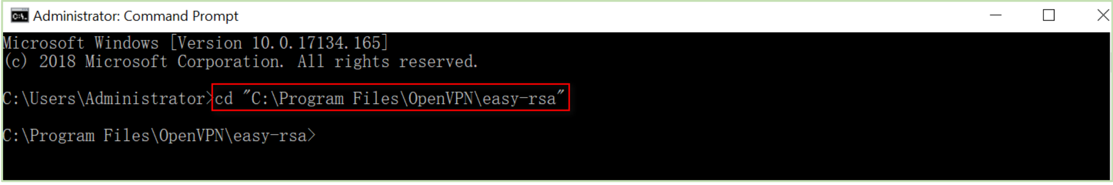
2. Certificates Generated

2.1 OpenVPN Software installed

1. Please download OpenVPN software and install onto Windows: http://openvpn.net/index.php

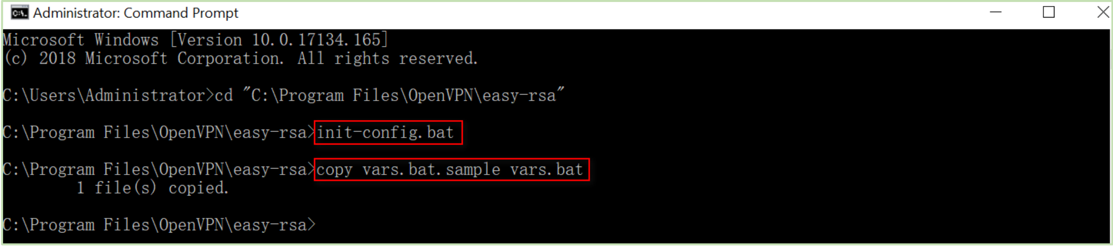
2. Certificates Generated

1. Open the command line with Administrator authority on Windows and **cd** to **C:\Program Files\OpenVPN\easy-rsa**



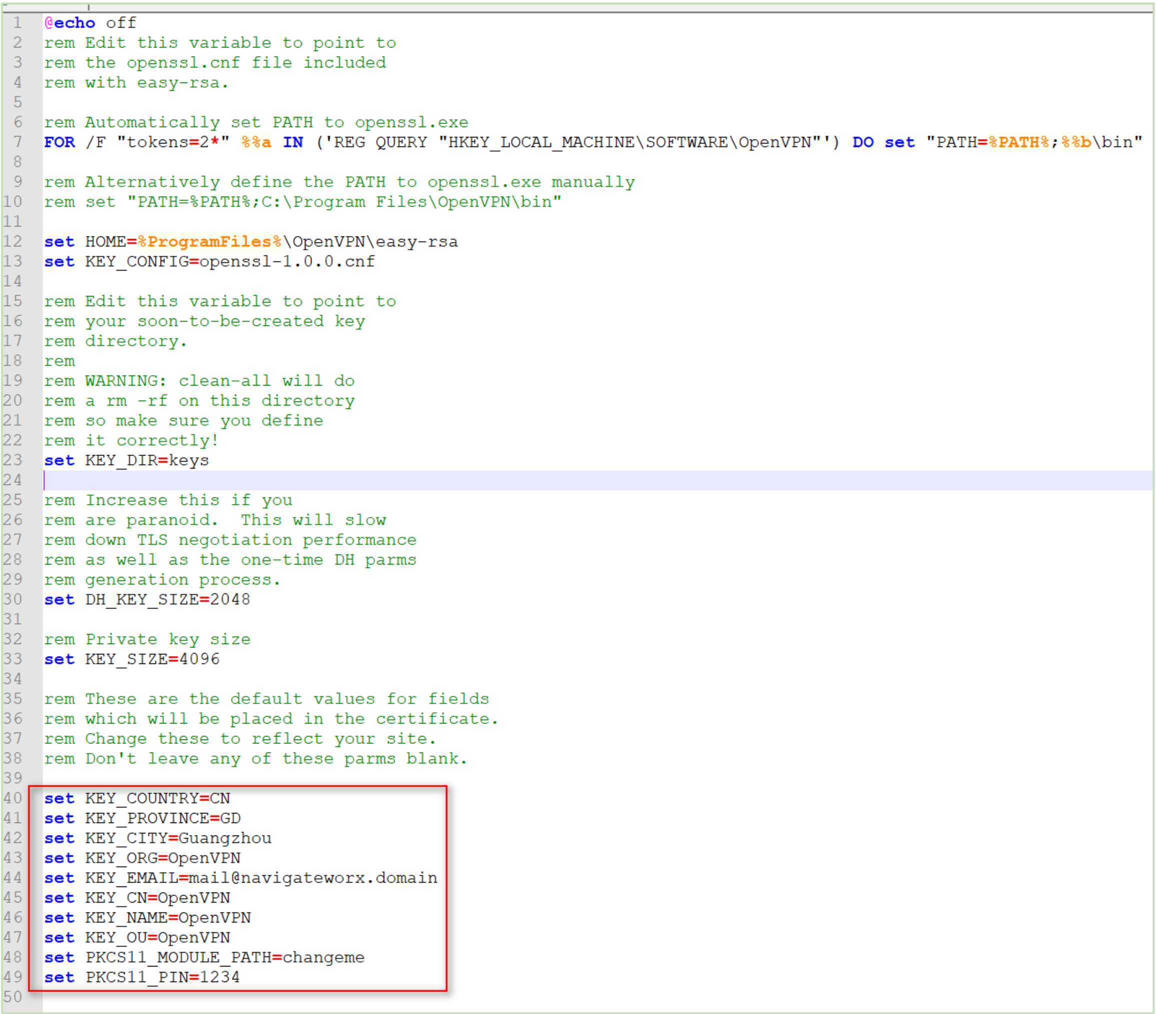
```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>
```

2. Run the **init-config.bat** to copy configuration files to **vars.bat** (this command would overwrite the previous vars.bat and openssl.cnf files).



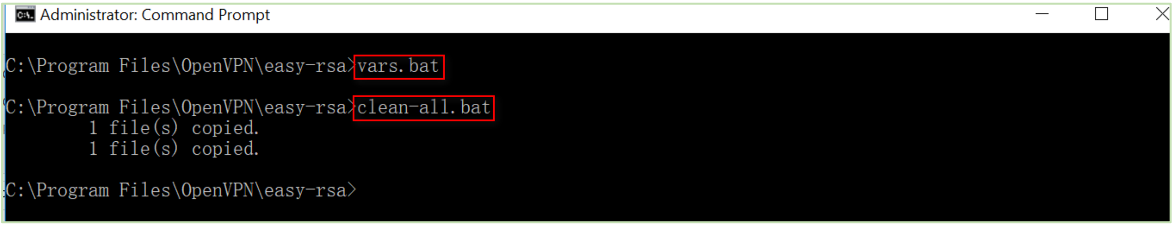
```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>init-config.bat

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

3. Edit the **vars.bat** and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL parameters and so on.
Note: The parameters enter without any space between them.



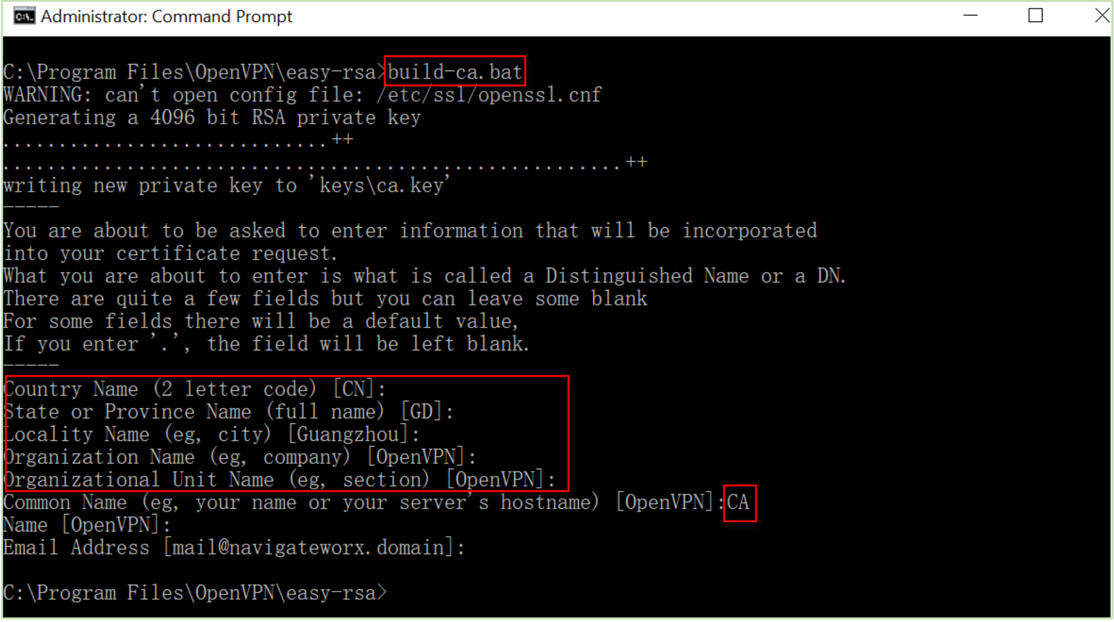
```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

rem Automatically set PATH to openssl.exe
FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"

rem Alternatively define the PATH to openssl.exe manually
rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set DH_KEY_SIZE=2048

rem Private key size
set KEY_SIZE=4096

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=Guangzhou
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@navigateworx.domain
set KEY_CN=OpenVPN
set KEY_NAME=OpenVPN
set KEY_OU=OpenVPN
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234

```

4. Run the following commands to initialize the environment.



```
C:\Program Files\OpenVPN\easy-rsa>vars.bat

C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

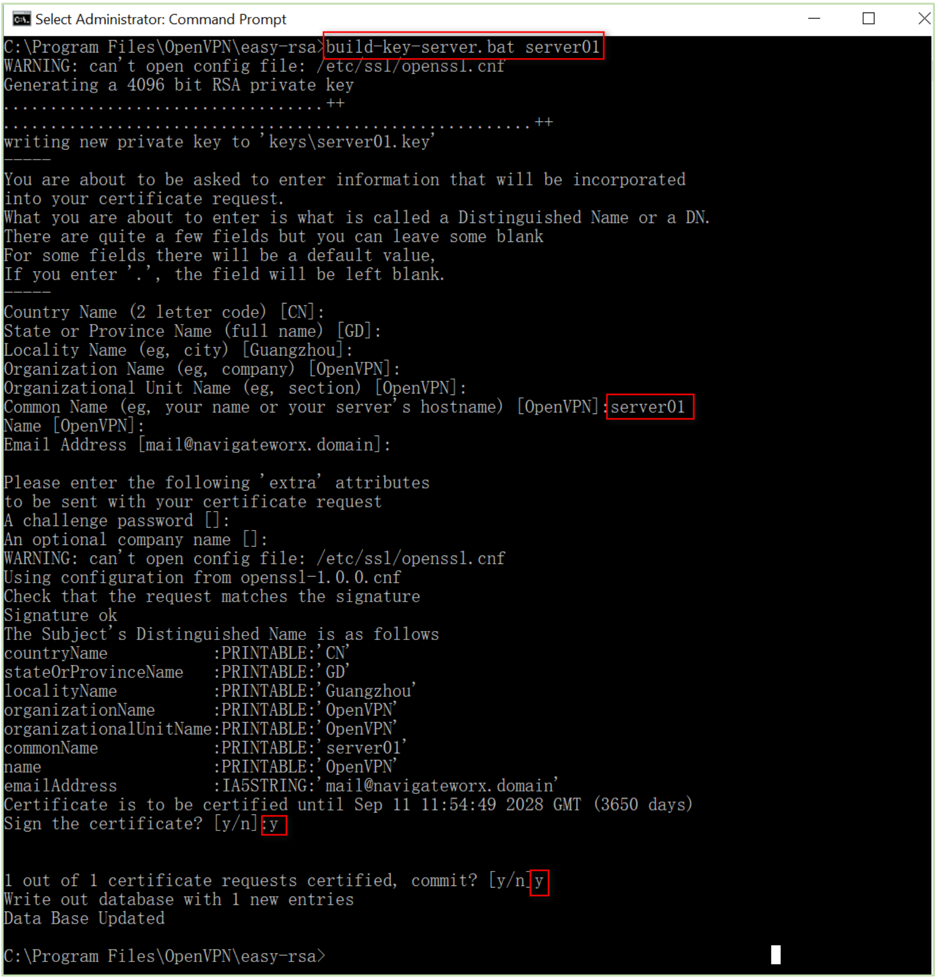
5. The command (**build-ca.bat**) will build the certificate authority(CA) certificate and the private key by invoking the interactive openssl command.



```
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.............................++
.......................................................++
writing new private key to 'keys\ca.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) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:CA
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

C:\Program Files\OpenVPN\easy-rsa>
```

Note: *In the above sequence, most of queried parameters were defaulted to the values set in the vars.bat file. The only parameter which must be explicitly entered is the Common Name.*

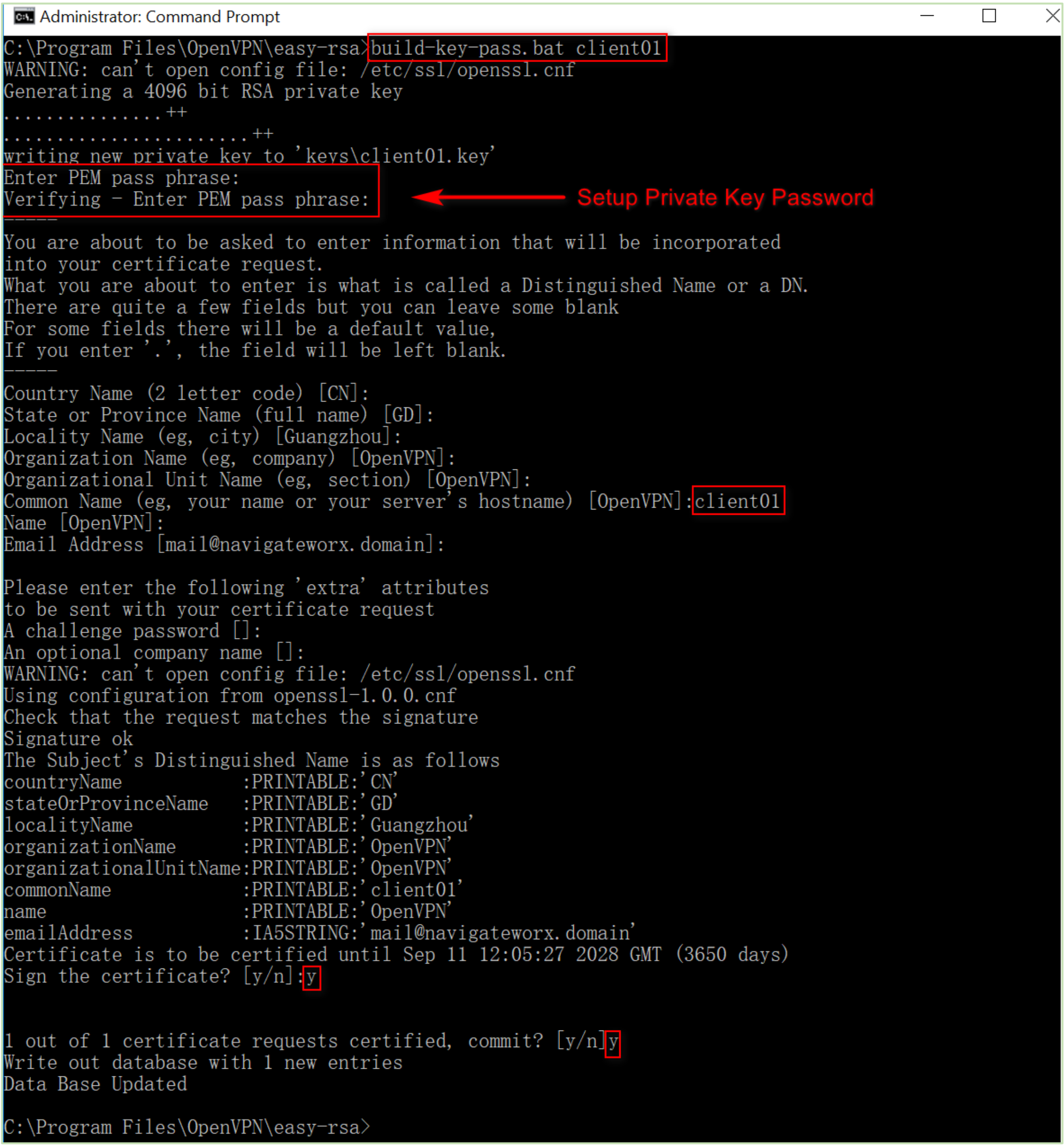
6. Generate a certificate and a private key for server by using **build-key-server.bat server01**. Enter **server01** when the Common Name is queried.



```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server01
WARNING: can’t open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
..................................++
........................................................++
writing new private key to ’keys\server01.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) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server’s hostname) [OpenVPN]:server01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following ’extra’ attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can’t open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject’s Distinguished Name is as follows
countryName           :PRINTABLE:’CN’
stateOrProvinceName   :PRINTABLE:’GD’
localityName          :PRINTABLE:’Guangzhou’
organizationName      :PRINTABLE:’OpenVPN’
organizationalUnitName:PRINTABLE:’OpenVPN’
commonName            :PRINTABLE:’server01’
name                  :PRINTABLE:’OpenVPN’
emailAddress          :IA5STRING:’mail@navigateworx.domain’
Certificate is to be certified until Sep 11 11:54:49 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

***Note**: __server01__ in “**build-key-server.bat server01**” is the file name of the certificate(the name of public key and private key).*

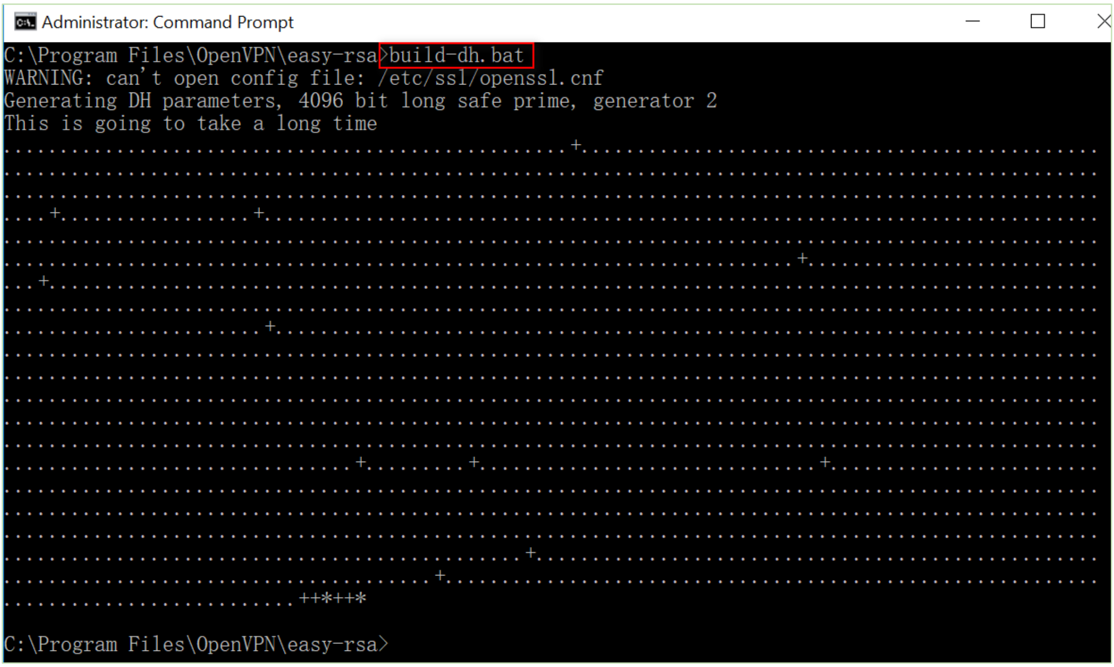
7. Generate a certificate and a private key for client by using **build-key-pass.bat client01.** Kindly note that **pass phrase** is generated as followings. It will be necessary to help the key authentication in OpenVPN client setting. Enter **client01** when the Common Name is queried.



```
C:\Program Files\OpenVPN\easy-rsa>build-key-pass.bat client01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
...............++
.......................++
writing new private key to 'keys\client01.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) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:client01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Guangzhou'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'client01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'mail@navigateworx.domain'
Certificate is to be certified until Sep 11 12:05:27 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Note: ***client01*** *in "**build-key-pass.bat client01**" is the file name of the certificate(the name of public key and private key). **Always use a unique common name for each client**.*

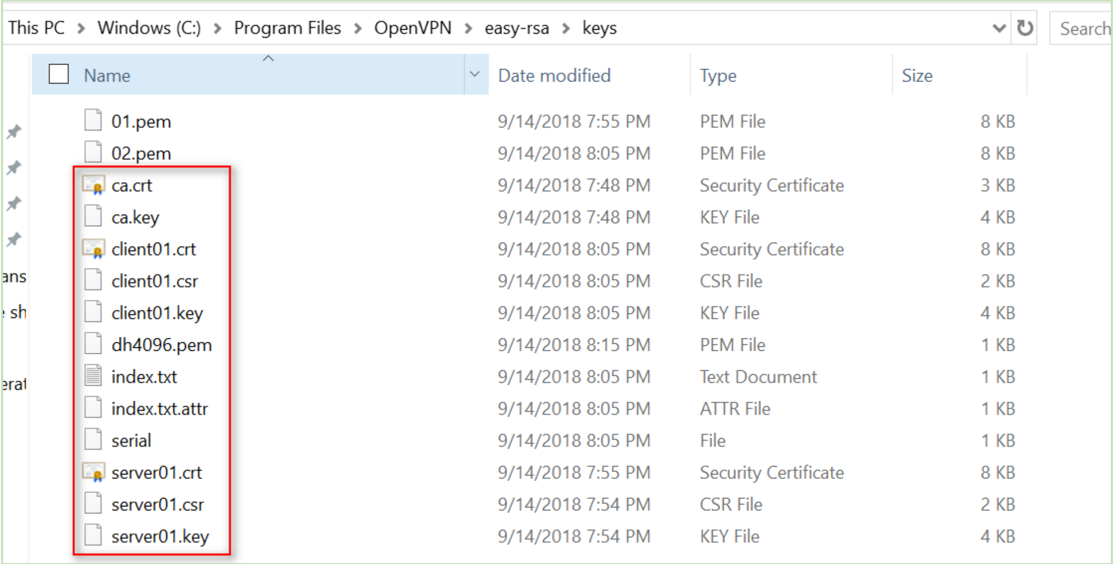
8. Generate Diffie Hellman parameters.



Administrator: Command Prompt

```
C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating DH parameters, 4096 bit long safe prime, generator 2
This is going to take a long time
..................................................+...............................
..................................................................................
....+.................+...........................................................
..................................................................................
......................................................................+...........
...+..............................................................................
......................+...........................................................
..................................................................................
..................................................................................
..................................................................................
..................................................................................
...............................+.........+..............................+.........
..................................................................................
..................................................................................
.................................................+................................
......................................+...........................................
..........................++++++*

C:\Program Files\OpenVPN\easy-rsa>
```

9. Certificates had been generated, go to the path to check it: **C:\Program Files\OpenVPN\easy-rsa\keys**



This PC › Windows (C:) › Program Files › OpenVPN › easy-rsa › keys

Name	Date modified	Type	Size
01.pem	9/14/2018 7:55 PM	PEM File	8 KB
02.pem	9/14/2018 8:05 PM	PEM File	8 KB
ca.crt	9/14/2018 7:48 PM	Security Certificate	3 KB
ca.key	9/14/2018 7:48 PM	KEY File	4 KB
client01.crt	9/14/2018 8:05 PM	Security Certificate	8 KB
client01.csr	9/14/2018 8:05 PM	CSR File	2 KB
client01.key	9/14/2018 8:05 PM	KEY File	4 KB
dh4096.pem	9/14/2018 8:15 PM	PEM File	1 KB
index.txt	9/14/2018 8:05 PM	Text Document	1 KB
index.txt.attr	9/14/2018 8:05 PM	ATTR File	1 KB
serial	9/14/2018 8:05 PM	File	1 KB
server01.crt	9/14/2018 7:55 PM	Security Certificate	8 KB
server01.csr	9/14/2018 7:54 PM	CSR File	2 KB
server01.key	9/14/2018 7:54 PM	KEY File	4 KB