Install the Open-VPN on VPN client (Win7)

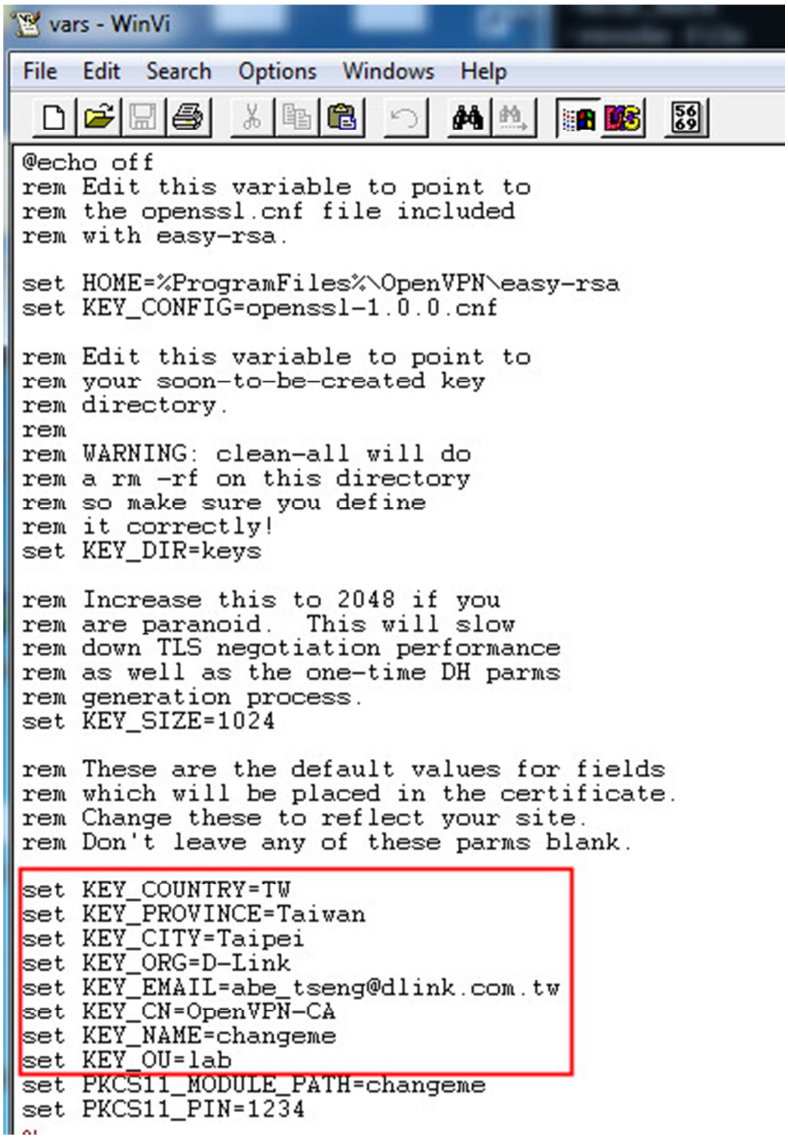
1. Install the Open-VPN software
   http://openvpn.net/index.php/open-source/downloads.html
   http://openvpn.net/index.php/open-source/documentation/howto.html

2. Open up a Command Prompt window and change directory to
   \ProgramFiles\OpenVPN\easy-rsa

Generate the master Certificate Authority (CA) certificate & key

3. Run the following batch file to copy configuration files into place
   c:\Program Files (x86)\OpenVPN\easy-rsa>**init-config.bat**

4. Now edit the **vars** file (called **vars.bat** on Windows) and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, and KEY_EMAIL parameters. Don't leave any of these parameters blank.



5. Next, initialize the PKI. On Windows:

>vars

>clean-all

>build-ca

The command (**build-ca**) will build the certificate authority (CA) certificate and key by invoking the interactive **openssl** command:

```
c:\Program Files (x86)\OpenVPN\easy-rsa>build-ca.bat
The system cannot find the path specified.
WARNING: can't open config file: c:\openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
........++++++
.............................++++++
unable to write 'random state'
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) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taipei]:
Organization Name (eg, company) [D-Link]:
Organizational Unit Name (eg, section) [lab]:
Common Name (eg, your name or your server's hostname) [OpenVPN-CA]:
Name [changeme]:abe
Email Address [abe_tseng@dlink.com.tw]:
```

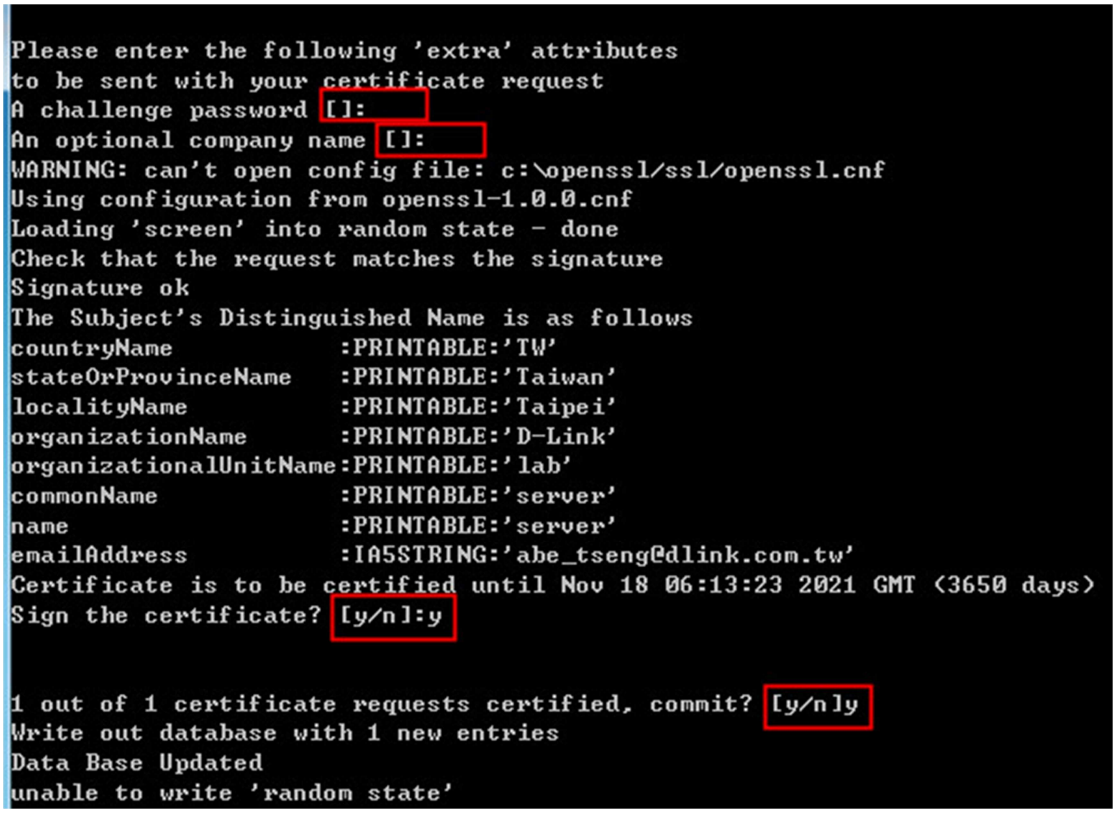
Generate certificate & key for server

Next, we will generate a certificate and private key for the server.

On Windows

>build-key-server server

```
c:\Program Files (x86)\OpenVPN\easy-rsa>build-key-server.bat server
The system cannot find the path specified.
WARNING: can't open config file: c:\openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..........++++++
....++++++
unable to write 'random state'
writing new private key to 'keys\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) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taipei]:
Organization Name (eg, company) [D-Link]:
Organizational Unit Name (eg, section) [lab]:
Common Name (eg, your name or your server's hostname) [OpenVPN-CA]:server
Name [changeme]:server
Email Address [abe_tseng@dlink.com.tw]:
```



The name of the server should be given in place of 'server'.

A challenge password: <leave blank>

An optional company name: <leave blank>

You will notice the two review questions at the end... simply press Y to those questions.

This will generate server.crt and server.key in the "keys" folder.

Generate certificates & keys for clients

Generating client certificates is very similar to the previous step.

>build-key client1

>build-key client2

Remember that for each client, make sure to type the appropriate **Common Name** when prompted, i.e. "client1", "client2", or "client3". Always use a unique common name for each client.

```
c:\Program Files (x86)\OpenVPN\easy-rsa>build-key client
The system cannot find the path specified.
WARNING: can't open config file: c:\openssl/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
..............................++++++
........++++++
unable to write 'random state'
writing new private key to 'keys\client.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) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taipei]:
Organization Name (eg, company) [D-Link]:
Organizational Unit Name (eg, section) [lab]:
Common Name (eg, your name or your server's hostname) [OpenVPN-CA]:client
Name [changeme]:client
Email Address [abe_tseng@dlink.com.tw]:
```

```
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: c:\openssl/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'TW'
stateOrProvinceName   :PRINTABLE:'Taiwan'
localityName          :PRINTABLE:'Taipei'
organizationName      :PRINTABLE:'D-Link'
organizationalUnitName:PRINTABLE:'lab'
commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'client'
emailAddress          :IA5STRING:'abe_tseng@dlink.com.tw'
Certificate is to be certified until Nov 18 06:18:51 2021 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
unable to write 'random state'
```

Generate Diffie Hellman key

The final step in creating your TLS keys is producing the Diffie Hellman, or DH, keys. Run the following command to produce them:

>build-dh

You will see a series of characters run across the screen. This process may take up to 30 seconds or more to complete. Upon completion you will be returned to the command prompt.

Key Files

Now we will find our newly-generated keys and certificates in the keys subdirectory. Here is an explanation of the relevant files:

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES

Generating Tls Authentication Key:

If you want to generate addition TLS Authentication key, You can use this command

>openvpn --genkey --secret ta.key

End of this document