Details about security used in OpenVPN and how keys are generated and shared

OpenVPN uses a Public Key Infrastructure (PKI). It uses

1. A public certificate and private key for the server and each client and
2. A master certificate Authority (CA) certificate and key which is used to sign each of the server and client certificates.

The client must authenticate the server certificate and the server must authenticate the client certificate before connection is established.

The various features it has are:

1. The server only needs its own certificate. It doesn't need any client's keys ass this will be validated by the CA.
2. It will accept clients whose certificates are signed by the master CA authority. And as the server can perform this signature verification without needing access to CA private key. It is possible for the CA key to reside on a different machine than the server.
3. If a Private Key is compromised it can be disabled by adding its certificate to a CRL (Certificate revocation list).

Steps to generate master certificate authority (CA) certificate and key:

On windows

1. Open Command prompt to **\Program Files\OpenVPN\easy-rsa** Run the following batch command.
   init-config
2. Now edit the **vars** file and set the KEY_COUNTRY, KEY_PROVINC, KEY_CITY, KEY_ORG, KEY_EMAIL parameters.
3. Run the following commands one by one
   vars
   clean-all - removes all existing certificates in the system
   build-ca - builds the CA by invoking the interactive openssl command.

   All the query parameters are set to default while this executes just set the common name to the server name.
4. Execute **build-key-server server** - Generate certificate and key for the server
5. As in the previous step 3, sign the certificate "y". Commit the changes "y".
6. Generate certificate and key for clients using build-key client1 command.
7. Also, as for the server give the common name to be client1, client2 and so on.
8. Generate the Diffie Hellman parameters
   build-dh
9. The keys will be present in the easy-rsa folder.
10. Copy all the files in respective machines as per the following table

Filename	Needed By	Purpose	Secret
ca.crt	Server + Clients	Root CA Certificate	No
ca.key	Key singing machine only	Root CA key	YES
dh{n}.pem	Server only	Diffie Hellman Parameters	NO
server.crt	Server only	Server ceritifcate	NO
server.key	Server only	Server key	YES
client.crt	client only	Client certificate	NO
client.key	Client only	Client Key	YES