Template:Generating certificates and keys

Step 3: generating certificates and keys

- Now we can start generating the certificates and keys. Begin with the **certificate authority** (**CA**) - the root certificate file that will be used to sign other certificates and keys:

  ```
  ./easyrsa build-ca nopass
  ```

- Next, build the **server** certificate and key:

  ```
  ./easyrsa build-server-full server nopass
  ```

- Next, build certificates and keys for the **clients**:

  ```
  ./easyrsa build-client-full Client1 nopass
  ```

  Note: replace *Client1* with this client's Common Name (CN). Omit "nopass" and you will be prompted to choose the client's password.

- Lastly, generate **Diffie Hellman parameters**:

  ```
  ./easyrsa gen-dh
  ```

The generated and signed files should appear in the following directories (by default):

File(s)		Location
CA certificate	→	*C:\Program Files\OpenVPN\easy-rsa\pki*
Diffie-Hellman parameters	→	*C:\Program Files\OpenVPN\easy-rsa\pki*
Client and Server keys	→	*C:\Program Files\OpenVPN\easy-rsa\pki\private*
Client and Server certificates	→	*C:\Program Files\OpenVPN\easy-rsa\pki\issued*