

OpenVPN Keys Generation

Install Easy-RSA

Install easy-rsa package on your Debian system with the following command:

```
# apt install easy-rsa
```

Create a directory where whole key structure will be stored:

```
# make-cadir /tmp/certs  
# cd /tmp/certs
```

Edit the vars file to configure Certificate Authority (CA) variables:

```
#nano ./vars  
-----  
Uncomment:  
  
set_var EASYRSA_KEY_SIZE          2048  
set_var EASYRSA_REQ_COUNTRY      "NL"  
set_var EASYRSA_REQ_PROVINCE     "Zuid-Holland"  
set_var EASYRSA_REQ_CITY         "Rijnsburg"  
set_var EASYRSA_REQ_ORG          "Oscar.de.Groot"  
set_var EASYRSA_REQ_EMAIL        "oscar@oscardegroot.nl"  
set_var EASYRSA_REQ_OU           "MySites"
```

Generate the required certificates and keys:

```
$ ./easysrsa init-pki
```

Create own CA certificate

```
$ ./easysrsa build-ca
```

Create Server Certificate, Key, and Encryption Files

Throughout this tutorial, the OpenVPN server's common name will simply be "server". Be sure to include the nopass option as well. Failing to do so will password-protect the request file, which could lead to permissions issues later on.

```
$ ./easysrsa gen-req server nopass
```

This will create a private key for the server and a certificate request file called `server.req`. Then sign the request by running `easysrsa` with the `sign-req` option, followed by the request type and the common name. The request type can either be `client` or `server`, so for the OpenVPN server's certificate request, be sure to use the `server` request type.

```
$ ./easysrsa sign-req server server
```

In the output, you'll be asked to verify that the request comes from a trusted source. Type `yes` and press `ENTER` to confirm this.

From there, create a strong Diffie-Hellman key to use during key exchange by typing:

```
$ ./easysrsa gen-dh
```

This may take a few minutes to complete. Once it does, generate an HMAC signature to strengthen the server's TLS integrity verification capabilities:

```
$ openvpn --genkey --secret pki/ta.key
```

When the command finishes, copy the two new files to your `/etc/openvpn/` directory:

```
sudo cp ~/easy-rsa/ta.key /etc/openvpn/  
sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/
```

With that, all the certificate and key files needed by your server have been generated. You're ready to create the corresponding certificates and keys that your client machine will use to access your OpenVPN server.

From:

<https://wiki.oscardegroot.nl/> - **HomeWiki**

Permanent link:

<https://wiki.oscardegroot.nl/doku.php?id=networking:openvpn&rev=1723484716>

Last update: **2024/08/12 17:45**

