Generating Certificates for OpenVPN® Connections

One of the principal features of routers is their support of virtual private networks (VPNs). This document discusses generation of certificates for OpenVPN® connection security.[1]

VPNs use public key infrastructure (PKI). A PKI is established when:

- The certificate authority (CA) has been developed, and
- Unique certificates (signed by the CA) have been issued to one or more servers and to each client.

The current document is the second of two documents that develop an OpenVPN PKI. The first document is *Developing the OpenVPN® Certificate Authority*.

Caution: It is recommended that separate machines be used for generating certificates and for hosting a VPN endpoint port, as an extra layer of security. Generate certificates on a management console, not on an EN™ router. Then use the EN™ router's management system to load the certificates onto the router.

Note: The procedures in the document *Developing the OpenVPN® Certificate Authority* must be completed before the procedures in the current document can be performed.

The client in the OpenVPN® connection needs three certificates for the VPN connection; the server in the OpenVPN® connection needs four certificates.[2] The

---

1. OpenVPN® uses transport layer security (TLS, successor to secure socket layers, SSL). For information about VPNs that use IP security (IPsec), see one of the following documents:
   - *Configuring IPsec VPNs in the EN-1000™*
   - *Configuring IPsec VPNs in the EN-2000™*
   - *The EN-4000™ in IPsec Virtual Private Networks*
2. To identify certificates needed for the client and for the server, see step 11 on page 14 through page 15 of the document *Configuring EN™ Routers for OpenVPN®*.

Version A.4, March 2019

current document has steps to generate those certificates. The steps for generation of certificates may be performed in either order:

- Generate one or more server certificates.
- Generate a certificate for each client.

After the certificates have been generated for your OpenVPN® connections, the certificates can be downloaded to the appropriate EN™ routers.

Caution: It is recommended that separate machines be used for generating certificates and for hosting a VPN endpoint port, as an extra layer of security. Generate certificates on a management console, not on an EN™ router. Then use the EN™ router's management system to load the certificates onto the router.

See the following sections:

- Section 4.1, *Generation of OpenVPN® Server Certificates*, on page 2
- Section 4.2, *Generation of OpenVPN® Client Certificates*, on page 4

  Note: The procedure to load certificates from the console to each appropriate router is discussed in the document *Configuring EN™ Routers for OpenVPN®*. (In that document, see step 11 on page 14 through page 15.)
- Section 4.3, *More Information*, on page 6

4.1 Generation of OpenVPN® Server Certificates

1 In the management computer's directory system, navigate to the directory for certificate authorization and generation. (In the Windows directory, that is the \easy-rsa subdirectory.)

Note: For details, see Section 2.1, *Navigating to the OpenVPN Directories*, on page 2 of the document *Navigating to OpenVPN Directories*.

2 In the \easy-rsa subdirectory, type **build-key-server *server1name*** and press the **Enter** key.

❖ The certificate authority develops a certificate and key for the stated entity (*server1name*, Figure 4-1).

Note: You will need to answer **y** when asked to sign the certificate and when asked to commit to the certificate.

Figure 4-1. Generating a Server Key

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server1
Generating a RSA private kay
.....................................................
.........................
.....................................................
.................,++++
.............................++++
writing new private key to "keys\server1.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.
For some fields there will be a default value.
If you enter ".", the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name {full name) [ST]: VA
Locality Name (eg, city) [CityName]: Chantilly
Organization Name (eg, company) [OrganizationNameInc]: companyname
Organizational Unit Name (eg, section) [changeme]: organizationname
Common Name (eg, your name or your server's hostname) [changeme]: server1
Name [changeme]:
Email Address[user@domainname.org]:

Please enter the following 'extra'atributes to be sent with your
certificate request
A challenge password []:
An optional company name []:
Using configurtaion from openss1-1.0.0.cnf
Can't open keys/index.txt.attr for reading. No such file or directory
9072:error:82001882:system library:fopen:No such file or directory:
  crypto/bio/bss_file.r:74:fopen('keys/index.txt.attr','r')
9072:error:28060888:BIO routines:BIO_newfile:no such file:crypto/bio/
       bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'US'
stateOrProvinceName       :PRINTABLE:'VA'
localityName              :PRINTABLE:'Chantilly'
organizationName          :PRINTABLE:'companyname'
commonName                :PRINTABLE:'server1'
name                      :PRINTABLE:'organizationname'
emailAddress              :IASSTRING:'user@domainname.org'
Certificate is to be certified until Apr  9 21:07:14 2029 GMT (3658 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
```

3 (Optional) If there is more than one server that might connect at the remote end of the OpenVPN® connection, type **build-key-server *server2name*** and press the **Enter** key.

Note: An OpenVPN® connection has only one client and one server. However, a client might connect to different servers at different times.

❖ The certificate authority develops a certificate and key for the stated entity.

4 (Optional) Repeat Step 3 for each additional server in the OpenVPN® set-up.

4.2 Generation of OpenVPN® Client Certificates

1 In the management computer's directory system, navigate to the directory for certificate authorization and generation. (In the Windows directory, that is the \easy-rsa subdirectory.)

Note: For details, see Section 2.1, *Navigating to the OpenVPN Directories*, on page 2 of the document *Navigating to OpenVPN Directories*.

2 In the \easy-rsa subdirectory, type **build-key *client1name*** and press the **Enter** key.

Note: If you wish to protect the client key with a password, instead use the command **build-key-pass *client1name*** and press the **Enter** key.

❖ The certificate authority develops a certificate and key for the stated entity (*client1name*, Figure 4-2).

Note: You will need to answer **y** when asked to sign the certificate and when asked to commit to the certificate.

Figure 4-2. Generating a Client Key

```
C:\Program Files\OpenVPN\easy-rsa>build-key-client client1
Generating a RSA private kay
.....................................................
.....................................................
.............................................,++++
..............................++++
writing new private key to "keys\client1.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.
For some fields there will be a default value.
If you enter ".", the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name {full name) [ST]:
Locality Name (eg, city) [CityName]:
Organization Name (eg, company) [OrganizationNameInc]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
  client1.part-a
Name [changeme]:
Email Address[loginname@domain.org]:

Please enter the following 'extra'atributes to be sent with your
  certificate request
A challenge password []:
An optional company name []:
Using configurtaion from openss1-1.0.0.cnf
Can't open keys/index.txt.attr for reading. No such file or directory
9072:error:82001882:system library:fopen:No such file or directory:
  crypto/bio/bss_file.r:74:fopen('keys/index.txt.attr','r')
9072:error:28060888:BIO routines:BIO_newfile:no such file:
  crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName               :PRINTABLE:'US'
stateOrProvinceName       :PRINTABLE:'VA'
localityName              :PRINTABLE:'Chantilly'
organizationName               :PRINTABLE:'changeme'
commonName                     :PRINTABLE:'client1'
name                      :PRINTABLE:'organizationname'
emailAddress              :IASSTRING:'user@domainname.org'
Certificate is to be certified until Apr  9 21:07:14 2029 GMT (3658 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>
```

3 (Optional) If there is more than one client that might connect at the remote end of the OpenVPN® connection, type **build-key *client2name*** and press the **Enter** key.

Note: If you wish to protect the client key with a password, instead use the command **build-key-pass *client2name*** and press the **Enter** key.

Note: An OpenVPN® connection has only one client and one server. However, individual clients might connect to a server at different times.

❖ The certificate authority develops a certificate and key for the stated entity.

4 (Optional) Repeat Step 3 for each additional client in the OpenVPN® set-up.

5 (Optional) Type **build-key-pkcs12 *machineclient1name*** and press the **Enter** key.

❖ The certificate authority develops a certificate and key for the stated entity (*machineclient1name*).

Note: You will need to answer **y** when asked to sign the certificate and when asked to commit to the certificate.

6 (Optional) If there is more than one machine client that might connect at the remote end of the OpenVPN® connection, type **build-key-pkcs12 *machineclient2name*** and press the **Enter** key.

Note: An OpenVPN® connection has only one client and one server. However, individual clients might connect to a server at different times.

❖ The certificate authority develops a certificate and key for the stated entity.

7 (Optional) Repeat Step 6 for each additional machine client in the OpenVPN® set-up.

8 Close the command window.

4.3 More Information

For a list of documents for OpenVPN® connections over EN routers, see the *Reference Manual for OpenVPN® on EN™ Routers*.