Developing the OpenVPN® Certificate Authority

One of the principal features of routers is their support of virtual private networks (VPNs). This document discusses development of an OpenVPN® certificate authority and 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 first of two documents that develop an OpenVPN PKI. The second document is *Generating Certificates for OpenVPN® Connections*.

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 *Installing Software for the OpenVPN® Certificate Authority* must be completed before the procedures in this current document can be performed.

The steps for development of certificate authority must be performed in the following order:

- Change parameter values to match your system environment—for example, to indicate your organization's name and location.
- Develop the certificate authority.

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*

Version A.4, March 2019

See the following:

3.1 Setting Parameter Values for the OpenVPN® Certificate Authority

Perform the steps in the following procedure to set values for your OpenVPN® certificate authority.

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 **init-config** and press the **Enter** key.

❖ The init-config.bat file runs, copying the vars.bat.sample file to the vars.bat file (Figure 3-1).

Figure 3-1. init-config Batch File Process/Execution

```
C:\Program Files\OpenVPN\easy-rsa>init-config

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
     1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

3 Open a text editor (for example, Windows Notepad) and edit the vars.bat file. (That is, type **notepad vars.bat**, as shown in Figure 3-2, and press the **Enter** key.)

Figure 3-2. Opening Notepad to Edit the vars.bat File

```
C:\Program Files\OpenVPN\easy-rsa>notepad vars.bat
```

❖ Windows Notepad opens, displaying code for the vars.bat file.

4 In the vars.bat file, type codes for your country, state or province, city or other location, company or organization, and so forth. (Figure 3-3).

Figure 3-3. Editing the vars Batch File

```
Country Name (2 letter code) [US]:US
State or Province Name (full name) [CA}: VA
Locality Name (eg, city) [SanFrancisco]:Chantilly
Organization Name (eg, company) [OpenVPN]: EncoreNetworksInc
```

5 Save the vars.bat file, and close the file.

6 Then, in the \easy-rsa subdirectory, type **vars** and press the **Enter** key.

❖ The organization's default parameter values are established in the certificate authorization **build** files.

7 Still in the \easy-rsa subdirectory, type **clean-all** and press the **Enter** key.

❖ The clean-all batch file runs, removing any existing certificates in the **keys** subdirectory (Figure 3-4).

Figure 3-4. Cleaning the Directory

```
C:\Program Files\OpenVPN\easy-rsa>clean-all
C:\Program Files\OpenVPN\easy-rsa>
```

3.2 Developing the OpenVPN® Certificate Authority

Note: The procedure in Section 3.1, *Setting Parameter Values for the OpenVPN® Certificate Authority*, on page 2, must be completed before the steps in this section can be performed.

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-ca** and press the **Enter** key.

❖ The batch file builds a certificate authority on your computer (Figure 3-5).

Note: You will need to enter information for your site and organization. If you wish to leave a field blank, type **.** (a period) and press the **Enter** key. Some fields cannot be left blank.

Figure 3-5. Building a Certificate Authority

```
C:\Program Files\OpenVPN\easy-rsa>build-ca
Generating a RSA private kay
.....................................................++++
............++++
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) [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]:
Name [changeme]:
Email Address[login-name@domain.org]:

C:\Program Files\OpenVPN\easy-rsa>
```

3 Then type **build-dh** and press the **Enter** key.

❖ The batch file generates Diffie–Hellman parameters for key exchange (Figure 3-6).

Figure 3-6. Generating Diffie–Hellman Parameters

```
C:\Program Files\OpenVPN\easy-rsa>build-dh
Generating DH parameters, 2018 bit long safe prime, generator 2
This is going to take a long time
,,,,,,,+....+.................................................
...................+
.............................................................
.....................++*++*+++*

C:\Program Files\OpenVPN\easy-rsa>
```

4 Proceed to the document *Generating Certificates for OpenVPN® Connections*.

3.3 More Information

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