Troubleshooting Preparation of OpenVPN® Certificates

One of the principal features of routers is their support of virtual private networks (VPNs). This document discusses resolution of problems when preparing OpenVPN certificates.[1]

If the procedures for preparing OpenVPN certificates go smoothly, you do not need to review this document. However, if some problems occur, see the following:

- Section 7.1, *Resolving Problems with Certificates*, on page 1
- Section 7.2, *More Information*, on page 3

7.1 Resolving Problems with Certificates

Determine where the problem with certificates has occurred:

- If a mistake in generation of a client certificate or a server certificate has occurred, but the certificate authority has not been affected, that is a minor problem. Merely revoke each affected certificate and generate a replacement certificate. See Section 7.1.1, *Regeneration and Replacement of Certificates when the Certificate Authority has Not been Affected*.
- However, if a problem has occurred earlier—during the certificate authority procedure (for example, a mistaken parameter was entered) or immediately after performing the certificate authority procedure—then see Section 7.1.2, *Redevelopment of Certificate Authority and Replacement of Certificates*.

[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*

For information on trademarks, safety, limitations
of liability, and similar topics, see
http://www.encorenetworks.com/disclaimer/.

7.1.1 Regeneration and Replacement of Certificates when the Certificate Authority has Not been Affected

If a mistake in generation of a client certificate or a server certificate has occurred, but the certificate authority has not been affected, that is a minor problem. Merely revoke each affected certificate and generate a replacement certificate. Do the following, in the order shown, for each certificate that must be replaced:

Close All Procedures

- If any procedure (for example, certificate generation) is open, close that procedure.

Remove Affected Certificates

- Remove each affected certificate from its router assignment. See step 11 on page 14 through page 15 of the document *Configuring EN™ Routers for OpenVPN®*.

  Note: Settings for Diffie–Hellman parameters (**dh**) and indication of certificate authority (**ca**) do not need to be removed unless the certificate authority has been affected. In that case, see Section 7.1.2, *Redevelopment of Certificate Authority and Replacement of Certificates*.

Revoke Affected Certificates

- Revoke the certificate(s) in question. See the document *Revoking OpenVPN® Certificates*.

Replace Affected Certificates

- After each affected certificate has been revoked, see the document *Generating Certificates for OpenVPN® Connections* to generate one or more replacement certificates.
- Assign the new (replacement) certificates to the routers from which the revoked certificates were removed. See step 11 on page 14 through page 15 of the document *Configuring EN™ Routers for OpenVPN®*.

7.1.2 Redevelopment of Certificate Authority and Replacement of Certificates

If a problem has occurred during the certificate authority procedure or immediately after performing the certificate authority procedure (for example, if a mistaken value had been entered for a parameter in the certificate authority), then all of the following must be performed (even if any or all of it has been performed earlier), in the order shown:

Close All Procedures

- If any procedure (for example, certificate generation) is open, close that procedure.

Remove All Certificates

- If certificates for clients or servers had already been assigned to routers, remove those certificates from their assigned routers.
- Because the certificate authority is going to be regenerated, also remove the certificate authority (**ca**) reference from each router's OpenVPN cryptography settings. See Figure 5-25 on page 15 of the document *Configuring EN™ Routers for OpenVPN®*.
- Because the Diffie–Hellman (dh) parameters are going to be regenerated, also remove the **dh** parameter set from each server's OpenVPN cryptography settings. See Figure 5-26 on page 15 of the document *Configuring EN™ Routers for OpenVPN®*.

Revoke All Certificates

- If certificates for clients or servers had already been generated (even if no certificate had been assigned to a router), those certificates must be revoked. See the document *Revoking OpenVPN® Certificates*.

Redevelop the Certificate Authority

- Perform step 3 on page 2 of the document *Installing Software for the OpenVPN® Certificate Authority*, to reset all parameter values in the OpenVPN® software to their initial default values (their values when downloaded to the management computer).
- Perform all procedures in the document *Developing the OpenVPN® Certificate Authority*.

Replace All Certificates

- Generate new (replacement) certificates for OpenVPN connections. See the document *Generating Certificates for OpenVPN® Connections*.
- Download the new certificates to the routers acting as servers and to the routers acting as clients in the OpenVPN connection. See step 11 on page 14 through page 15 of the document *Configuring EN™ Routers for OpenVPN®*.

7.2 More Information

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