Exercise 7.6: Create a Certificate Signing Request

Use the same settings in the last exercise to generate a CSR.

Solution 7.6

1. Create a new private key

   - On **CentOS**:

     ```
     # /usr/bin/openssl genrsa -aes128 2048 > /etc/pki/tls/private/ipvhost.example.com.key
     ```

   - On **OpenSUSE**:

     ```
     # /usr/bin/openssl genrsa -aes128 2048 > /etc/apache2/ssl.key/server.key
     ```

   - On **Ubuntu**:

     ```
     # /usr/bin/openssl genrsa -aes128 2048 > /etc/ssl/private/server.key
     ```

2. Create a new CSR.

   - On **CentOS**:

     ```
     # /usr/bin/openssl req -utf8 -new -key \
                       -key /etc/pki/tls/private/ipvhost.example.com.key \
                       -out /etc/pki/tls/certs/ipvhost.example.com.csr
     ```

   - On **OpenSUSE**:

     ```
     # /usr/bin/openssl req -utf8 -new \
                        -key /etc/apache2/ssl.key/server.key \
                        -out /etc/apache2/ssl.csr/server.csr
     ```

   - On **Ubuntu**:

     ```
     # /usr/bin/openssl req -utf8 -new \
                        -key /etc/ssl/private/server.key \
                        -out /etc/ssl/server.csr
     ```

   You'll be asked for a challenge password. Make sure you remember it.

3. You must then send off this CSR to be signed by a Certificate Authority.