



Step 1: Generate a Private Key

- * Log in to your server using the root password and open the Terminal application.
- * At the prompt, type the following commands and press return after each one:

```
cd
openssl md5 * > rand.dat
openssl genrsa -rand rand.dat -des 1024 > key.pem
```

- * At the next prompt, type a passphrase, then press return. The passphrase you create unlocks the server's certificate key. You will use this passphrase when you enable SSL on your Web server.
- * If it doesn't already exist on your server, create a directory at the following location:

```
/etc/httpd/ssl.key
```

- * Make a copy of the key.pem file that you just created and rename it server.key. Then copy server.key to the ssl.key directory.

Step 2: Create your Certificate Signing Request

- * At the prompt, type the following command and press return:

```
openssl req -new -key key.pem -out csr.pem
```

- * When prompted, enter the following information:

- o Country: Enter the two-letter country code for your country.
- o State: Enter the name of the State or Province in which your organization operates. Do not abbreviate.
- o Locality: Enter the name of your city, town, or other locality.
- o Organization Name: Enter the name of your organization.
- o Organizational Unit: Enter the name of your division, department, or other operational unit of your organization.
- o Common Name: Enter the domain name that you want to use your SSL certificate with.
- o E-mail address: Enter your e-mail address.

The file csr.pem is generated from the information you provided.

When asked to "Copy & Paste" your CSR into the CSR field during the order process, open the csr.pem file with a text editor and copy and paste the content into the CSR field on the order form.

For additional MAC OSX information please visit the Apple site:
<http://www.apple.com/support/macossxserver/index.html>

For Mac OS X client specific information please visit:
<http://developer.apple.com/internet/serverside/modssl.html>