Renewing a Comodo SSL Certificate in Ubuntu and Apache2

Purchase the renewal of your existing SSL certificate with you domain registrar, such as namecheap. Make sure to renew for two years instead of only one year. It will save you time and effort in the future.

Use Putty to login remotely to your ubuntu web server using SSH. Login with your non-root username and corresponding password. Switch to the root user by again supplying the user password. Navigate away from your user directories and go to /etc/ssl by using the command cd /etc/ssl/. Use the "ls" command to list the contents of the /etc/ssl directory. Notice that you are within the same directory that has the expiring certificate file "<your_domain>.crt" and the private key "<server>.key."

You may use OpenSSL to generate a new CSR (code signing request or certificate signing request) based upon the old certificate and the existing private key. Many instructions will suggest that you generate a new private key and a new CSR from that new key. It seems so unnecessary. In fact, within the /etc/ssl directory, you may find the original or previous CSR file that was used to generate the original SSL certificate. The file name might be "<yourDomain_com>.csr." Use FTP to download a copy of the CSR file to your windows based PC. Using Notepad++ editor (recommended), you can Open that previously generated CSR file, copy its entire contents to your windows clipboard (including the "Beginning" and "Ending" lines at the top and bottom of the file contents), and paste the clipboard contents (as text) into the CSR Activation screen at your Domain Registrar. In other words, after you have purchased the 2 year renewal of the SSL certificate, you can go back to your domains page and click "Activate" on the action dropdown box next to the renewed SSL certificate product that is associated with your particular domain, and you will be asked to paste the CSR the entire text "CODE" into the Text Box. Paste the code from **= = = Beginning = = = through = = = End = = =** , and then click the button to submit the CSR (request). Choose your validation method (email, web, Dns, whatever). I use email for validation of my authority to control the domain - just setup an email account for admin@yourdomain.com. "Admin" is usually one of the choices of email account names for email validation.

After you validate your authority, then your domain registrar or certificate authority (CA) will send you a new CRT file (such as – YourDomain_com.crt) and a new CA chain or bundle file (such as – YourDomain_com.ca-bundle).

Using Filezilla FTP - Site Manager - SSH login with your standard username and password, just upload the new domain.csr and domain.ca-bundle file. Sometimes the ca-bundle file has not changed.

FTP upload those 2 files to the sub-folder in this path: /home/yourusername/Downloads/newcrt/

Login again as the standard user, using Putty SSH, and switch to root user in the terminal window. Switch to /etc/ssl/ directory and rename the old crt and ca-bundle files. Use the Move command to rename files, such as

```
mv yourdomain_com.crt yourdomain_com.crt-expired
mv yourdomain_com.ca-bundle yourdomain_com.ca-bundle-expired
```

Copy the two newly generated SSL files from your /home/yourusername/Downloads/newcrt/ directory to the /etc/ssl/ directory. Make sure you use a capital "D" in Downloads. Example:

```
cp /home/yourusername/Downloads/newcrt/yourdomain_com.crt /etc/ssl/
cp /home/yourusername/Downloads/newcrt/yourdomain_com.ca-bundle /etc/ssl/
```

While switched to root user, the purpose for using root to copy these two files is (1) so that copying is permitted to a web/root user directory like /etc/ssl/, and, most importantly (2) that these files' Owner/Group access permissions are changed to root:root without the necessity of running chmod commands, and these root:root owner/group permissions are required for apache2 and/or the linux system to properly access these files. You can confirm the ownership and chmod permissions using your filezilla FTP client. Just login to the server with ftp ssh, navigate to the /etc/ssl/ directory, and check the permission properties of rw-r–r–, and r–r–r–, and r–r–r–, and that the user-owner:group-owner should be root:root.

A reminder here, that your yourdomain.conf and yourdomain-ssl.conf files should already have been configured the last time you setup SSL, and, unless you changed the filenames of the CSR and CA-Bundle, then your yourdomain-ssl.conf files for your website should already contain the paths and exact filenames to access these 2 file names (CSR and CA-bundle) as well as the path to the server.key (or private.key) file either located in the path /etc/ssl/ or the path /etc/ssl/private/.

All you need to do now from the Putty terminal prompt is restart the apache2 service.

```
service apache2 restart
```

If you are not switched to root user, then try this restart command.

```
sudo service apache2 restart
```