利用OpenSSL创建自签名的SSL证书备忘

转自http://wangye.org/blog/archives/732/

之前申请的StartSSL免费一年的证书到期了，考虑到我对SSL一般仅用于博客登录和后台管理上面，所以不打算续申请，自己创建一个就足够了。

本来想使用Windows下的makecert实用工具创建的，结果折腾了很久导入到Linux服务器上，服务器没有正确识别，遂放弃，转而使用OpenSSL，收集了网上的一些材料，通过下面的方法创建成功：

1. SSH登录到服务器，使用下述命令创建根证书的私匙：

```
openssl genrsa -out ca.key 2048
```

网上很多是使用了1024，我这里强度加强到了2048。

2. 利用私钥创建根证书：

```
openssl req -new -x509 -days 36500 -key ca.key -out ca.crt -subj \
"/C=CN/ST=Jiangsu/L=Yangzhou/O=Your Company Name/OU=Your Root CA"
```

这里/C表示国家(Country)，只能是国家字母缩写，如CN、US等；/ST表示州或者省(State/Provice)；/L表示城市或者地区(Locality)；/O表示组织名(Organization Name)；/OU其他显示内容，一般会显示在颁发者这栏。

到这里根证书就已经创建完毕了（注：根证书也是SSL证书，nginx也是可以正常使用的），下面介绍建立网站SSL证书的步骤：

3. 创建SSL证书私匙，这里加密强度仍然选择2048：

```
openssl genrsa -out server.key 2048
```

4. 利用刚才的私匙建立SSL证书：

```
openssl req -new -key server.key -out server.csr -subj \
"/C=CN/ST=Jiangsu/L=Yangzhou/O=Your Company Name/OU=wangye.org/CN=wangye.org"
```

这里需要注意的是，/O字段内容必须与刚才的CA根证书相同；/CN字段为公用名称(Common Name)，必须为网站的域名(不带www)；/OU字段最好也与为网站域名，当然选择其他名字也没关系。

5. 做些准备工作：

```
mkdir demoCA
cd demoCA
mkdir newcerts
touch index.txt
```

```
echo '01' > serial
cd ..
```

注意 `cd ..` ，利用 `ls` 命令检查一下是不是有个demoCA的目录。

6. 用CA根证书签署SSL自建证书：

```
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key
```

接下来有一段提示，找到 `Sign the certificate? [y/n]` 这句，打入y并回车，然后出现 `out of 1 certificate requests certified, commit? [y/n]` ，同样y回车。

好了，现在目录下有两个服务器需要的SSL证书及相关文件了，分别是server.crt和server.key，接下来就可以利用它们配置你的服务器软件了。

需要注意的是由于是自签名证书，所以客户端需要安装根证书，将刚才第2步创建的根证书ca.crt下载到客户端，然后双击导入，否则会提示不受信任的证书发布商问题。

通常情况下私人或者内部用的话，自建证书已经绰绰有余了，但是如果你的产品面向的是大众，那就花点银子去买正规的SSL证书吧，可不能学某售票系统强制要求安装自建的根证书哦。