Creating Validated SSL Certificates

this is just a bunch of steps i can't seem to remember each time i need a new certificate.. so i write it down in here :)

I used to use startssl.com as they are free. but eventually i got annoyed by having to renew my certificates every year and messing around with the client certificate needed to acecss their customer portal, so i changed over to gogetssl.com which sell ridiculously cheap (as in $4 per year) certificats which last 3 years and all you need to access the portal is an email address and password :)

with most providers of simple domain verification certificates, you usually need to prove ownership of a domain by receiving an email at webmaster@domain or some other @domain email address THEY propose.

SSL Certificate

to create an ssl certificate you need to first create a Certificate Signing Request on your server (it's running ubuntu in my case)

1. create a key

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

   this creates a key without a password which you most likely want to use if you need it for a webserver or such. it also means, that if your key is stolen anybody can run another service with the same key, so it is less secure..

2. create the CSR

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

now go to the startssl.com webpage and enter the certificates wizard. chose web server ssl / tls certificate and continue

on the next screen choose skip

now on your server get the csr file contents

```
cat server.csr
```

copy and paste this into the textarea on the startssl page and follow the wizard

when you receive the pem encoded certificate copy and paste it back to your server. in the terminal window wher you have your server shell enter

```
cat > server.crt
```

then paste the certificate and hit return and then ctrl+D

For StartSSL, download the Certificate Chain File to your server. Other providers sometimes include a pem file or a bundle file in their downloads with the certificate itself and some others (like comodo) provide a set of crt files which need to be combined into a package for apache. for comodo you get three files and they need to be cat-ed togeterher into one bundle.crt:

```
cat COMODORSADomainValidationSecureServerCA.crt COMODORSAAddTrustCA.crt
AddTrustExternalCARoot.crt >> bundle.crt
```

last but not least you need to make sure your apache ssl config is pointing to those files. make sure you have these lines in your virtual host configuration to enable and configure ssl for your site. of course you need to make sure the paths match your setup :)

```
        SSLEngine on
        SSLProtocol all -SSLv2
        SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM
        SSLCertificateFile    /etc/ssl/certs/server.crt
        SSLCertificateKeyFile /etc/ssl/certs/server.key
```

if you have a pem file add this line as well:

```
SSLCertificateChainFile /etc/ssl/certs/sub.class1.server.ca.pem
```

if you had to compile your package like shown above, you can use this line

```
SSLCACertificateFile "/ssl/bundle.crt"
```

now **reload apache**

sec_error_ocsp_unknown_cert

shortly after updating (orp probalby also creating) a certificate with startssl firefox might not allow you to access the site, returning an error sec_error_ocsp_unknown_cert. this is because apparently startssl's ocsp server needs to reload its cached entries first in order for the new certificates to be usable through firefox. so just allow it some time to catch up and it should all work.