Obtaining an SSL cert - Signing up with a free authority

Since I don't have any domains to purchase an SSL certificate for. I am only providing a step by step on how to create a free certificate with StartSSL.

Signing up with StartSSL

- Goto https://www.startssl.com and click the control panel link near the top right
- Click the sign up link, assuming you don't already have an account
- Fill in all the required fields
- Check your e-mail to obtain the verification code they sent
- Complete the registration by entering in the code and clicking continue
- Generate a High Grade key, this is only to login, not your certificate
- Click the install button and it will install the login certificate in your browser

What you just created is a client side certificate and it is verify yourself to StartSSL, it is an alternative to a more traditional username/password combination and has nothing to do with your SSL certificates.

Provide to StartSSL that you own your domain

Now that you can sign in, you need to begin creating your certificate but first you need to verify you own the domain. Head over to the control panel and follow the steps below:

- Click the Validations Wizard tab
- Choose Domain Name Validation from the dropdown list
- Enter in your domain name
- Select postmaster@productionexample.com from the list and hit continue
- Check your e-mail to obtain the verification code they sent
- Complete the validation process by entering in the code and clicking continue

Create your certificate

With verification out of the way, you can go ahead and generate the certificate. Head over to the control panel and follow the steps below:

- Click the Certificates Wizard tab
- Choose Web Server SSL/TLS Certificate from the dropdown list
- Click skip when it comes time to generate the private key
    - *We want to generate our own key so StartSSL does not know it*
- **Move into the deploy/production/certs folder**
- In a terminal, run the following 2 commands:
    - `openssl genrsa 2048 > productionexample.key`
    - `openssl req -new -key productionexample.key -out csr.pem`
- Enter in the Common Name that you used earlier in the validation process
- Open csr.pem in your favorite editor and copy it to your clipboard

- Paste the contents of your clipboard into the textarea on StartSSL
- Click continue to submit your certificate request file
- Select the domain name you validated earlier
- Enter in www as a subdomain that you want this to also work on
- Confirm everything by clicking continue
- You may or may not need to wait an hour for StartSSL to verify it
- Copy the contents of that textarea to a file named productionexample-raw.crt
- This is your certificate, do not lose it!

Create a proper certificate chain

In order to get A+ SSL certificate status you need to create a certificate chain. It will be a combination of your certificate and StartSSL's intermediary certificate.

Download StartSSL's intermediary certificate:

```
wget
https://www.startssl.com/certs/class1/sha2/pem/sub.class1.server.sha2
.ca.pem
```

Concatenate your certificate with theirs:

```
cat productionexample-raw.crt sub.class1.server.sha2.ca.pem >
productionexample.crt
```