Own SSL CA Authority for Local HTTPS

Become your own Certificate Authority

When you generate a self-signed certificate the browser doesn't trust it. It hasn't been signed by a CA. The way to get around this is to generate our own root certificate and private key. We then add the root certificate to all the devices we own just once, and then all the self-signed certificates we generate will be inherently trusted.

Step 1: Create private key for local CA Certificate

To generate the private key to become a local CA execute:

```
openssl genrsa -des3 -out Home-CA.key 2048
```

OpenSSL will ask for a passphrase, which we recommend not skipping and keeping safe. The passphrase will prevent anyone who gets your private key from generating a root certificate of their own. The output should look like this:

```
$ openssl genrsa -des3 -out Home-CA.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.............................+++++
.......................+++++
e is 65537 (0x010001)
Enter pass phrase for Home-CA.key:
Verifying - Enter pass phrase for Home-CA.key:
```

The following key file is generated:

```
$ ls -al
total 4
drwxr-xr-x  2 oscar oscar   60 Apr  1 21:55 .
drwxrwxrwt 16 root  root   380 Apr  1 21:49 ..
-rw-------  1 oscar oscar 1743 Apr  1 21:52 Home-CA.key
```

Step 2: Generate a root certificate

Next, we generate a root certificate:

```
openssl req -x509 -new -nodes -key Home-CA.key -sha256 -days 15000 -out
Home-CA.pem
```

You will be prompted for the passphrase of the private key you just chose and a bunch of questions. The answers to those questions aren't that important. They show up when looking at the certificate,

which you will almost never do. I suggest making the Common Name something that you'll recognize as your root certificate in a list of other certificates. That's really the only thing that matters.

```
Enter pass phrase for Home-CA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:NL
State or Province Name (full name) [Some-State]:Zuid-Holland
Locality Name (eg, city) []:Rijnsburg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:oscardegroot.nl
Organizational Unit Name (eg, section) []:oscardegroot.nl
Common Name (e.g. server FQDN or YOUR name) []:Oscar de Groot
Email Address []:oscar@oscardegroot.nl
```

When you should see the following two files: Home-CA.key (your private key) and Home-CA.pem (your root certificate), you're now a CA.