Root CA Signing

Overview

A Certificate Authority (CA) is responsible for signing valid certificates. This ensures that the certificates came from a trusted authority and verifies their authenticity.

Generate a new Root CA

Follow these instructions to generate a new Root CA and learn how to sign certificates with it:

https://gist.github.com/fntlnz/cf14feb5a46b2eda428e000157447309

NOTE: If you don't have a real domain to use, you can set an entry in `/etc/hosts` as a temporary workaround for testing purposes.

Trust Your Root CA

Finally, you need to add this new Root CA to the list of trusted certificate authorities. This ensures that certificates signed by your Root CA are not flagged by the browser or e-mail servers on the machines which they have been added.

The location of the list of trusted Root CAs depends on your OS or distro;

CentOS / Ubuntu: https://gist.github.com/kekru/deabd57f0605ed95d5c8246d18483687

Other distros may take some research to find the right directory / file to place them.

Testing Locally with NGINX

Install NGINX and use the following configuration to use your new certs:

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        listen 443 ssl http2 default_server;
        listen [::]:443 ssl http2 default_server;
        ssl_certificate /etc/ssl/certs/mydomain.com.crt;
        ssl_certificate_key /etc/ssl/private/mydomain.com.key;
        # New root location
        location / {
                root /usr/share/nginx/html/;
                # return 404;
        }
        # You may need this to prevent return 404 recursion.
        location = /404.html {
                internal;
        }
}
```

Once NGINX is running, you can test that your certificates are valid using `curl` :

```
curl https://mydomain.com -vvvvv
```

NOTE: You should not need to use `--insecure` , as your Root CA is trusted and your certificate is signed by the Root CA. If an error is thrown here then something is wrong.

The `-vvvvv` raises the verbosity level in the output of curl, and should show the certificate chain

Testing with NGINX in Docker

To run an NGINX Docker container that mounts in your new root ca as well as the certs you've signed with it:

```
sudo docker run --name nginx -itd -p 80:80 -p 443:443 \
     -v $(pwd)/nginx.conf:/etc/nginx/conf.d/default.conf \
     -v $(pwd)/mydomain.com.crt:/etc/ssl/certs/mydomain.com.crt \
     -v /etc/pki/ca-trust/source/anchors/mynewrootca.crt:/usr/local/share/ca-certificates/mynewrootca.crt \
     -v $(pwd)/mydomain.com.key:/etc/ssl/private/mydomain.com.key \
     nginx
```

Depending on your distro, you may need to run a command to regenerate the trusted list:

```
sudo docker exec -it nginx sh -c 'chmod 644 /usr/local/share/ca-certificates/mynewrootca.crt && update-ca-
certificates'
```