The certificates in this dir expire on Sept, 27th, 2118

Certificates generated using original instructions from this gist: https://gist.github.com/cecilemuller/9492b848eb8

Certificate authority (CA)

Generate RootCA.pem, RootCA.key, RootCA.crt:

```
openssl req -x509 -nodes -new -sha256 -days 36135 -newkey rsa:2048 -keyout RootCA.key -out R
openssl x509 -outform pem -in RootCA.pem -out RootCA.crt
```

Note that Example-Root-CA is an example, you can customize the name.

Domain name certificate

First, create a file domains.txt that lists all your local domains (here we only list localhost):

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = localhost
```

Generate localhost.key, localhost.csr, and localhost.crt:

```
openssl req -new -nodes -newkey rsa:2048 -keyout localhost.key -out localhost.csr -subj "/C=
openssl x509 -req -sha256 -days 36135 -in localhost.csr -CA RootCA.pem -CAkey RootCA.key -CA
```

Note that the country / state / city / name in the first command can be customized.

For testing purposes we need following files:

- `RootCA.crt`
- `RootCA.key`
- `RootCA.pem`
- `localhost.crt`
- `localhost.key`