

Generating a Certificate Authority

A step-by-step guide based off a reference of how to create a certificate authority.

- [Creating a Certificate Authority](#)

Creating a Certificate Authority

This guide is based upon a [deliciousbrains.com article](https://deliciousbrains.com/openssl-ca/).

Creating a CA

1. Generate a private key.

```
openssl genrsa -des3 -out myCA.key 2048
```

2. Generate a root certificate with the private key.

```
openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out myCA.pem
```

That's literally it. If you want to 'be' a certificate authority, you will have to add this certificate to your certificate store as a trusted certificate. You can do this using `mmc`. Use the Certificate Snap-in, under the 'Computer Account' > 'Local Computer'. Then double click 'Certificates (local computer)' and add a certificate to the 'Trusted Root Certificate Authorities'.

Generating and Signing Certificates

1. Create a private key for the new certificate.

```
openssl genrsa -out subdomain.test.key 2048
```

2. Generate a CSR.

```
openssl req -new -key subdomain.test.key -out subdomain.test.csr
```

3. We can create an extension configuration file if we wish to supply a SAN.

```
authorityKeyIdentifier=keyid,issuer  
basicConstraints=CA:FALSE  
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment  
subjectAltName = @alt_names
```

```
[alt_names]
DNS.1 = hellfish.test
```

4. Create the certificate.

```
openssl x509 -req -in subdomain.test.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out
subdomain.test.crt -days 825 -sha256 -extfile subdomain.test.ext
```

Script

The author of the article provided the following [script](#):

```
#!/bin/sh

if [ "$#" -ne 1 ]
then
    echo "Usage: Must supply a domain"
    exit 1
fi

DOMAIN=$1

cd ~/certs

openssl genrsa -out $DOMAIN.key 2048
openssl req -new -key $DOMAIN.key -out $DOMAIN.csr

cat > $DOMAIN.ext << EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = $DOMAIN
EOF

openssl x509 -req -in $DOMAIN.csr -CA ../myCA.pem -CAkey ../myCA.key -CAcreateserial \
-out $DOMAIN.crt -days 825 -sha256 -extfile $DOMAIN.ext
```