eigen CA server opzetten

context

dit document beschrijft hoe je een eigen CA server opzet.

OpenSSL

- installeer openssl `apt install openssl`
- meld aan met gebruiker met beperkte rechten en voer uit: `mkdir /home/ca`
- open `vi /usr/lib/ssl/openssl.cnf` en pas de waarde **dir** aan:

```
dir             = /home/ca              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are
kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
...
```

- maak de nodige subdirectories aan:

```
for dir in certs crl newcerts serial crlnumber private; do mkdir
/home/ca/$dir; done
echo 1000 > /home/ca/serial
```

private key aanmaken

1. `cd /home/ca`
2. maak een private key paar aan voor de CA

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

3. geef een sterk wachtwoord op
4. dit maakt 1 (tekst)bestand aan: `server.CA.key` met vergelijkbare inhoud:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI2g3AahkapWYCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECBXvOoLtreyKBIIEyL01u/JxcHru
c7lEPudjbJCqu/hJXV17YX0znE7qZ990ZuVZanQ0hs/bfmPv3Qi2bGQ2odpWZCQ2
9cLXJDgziwKWo+P1L89lhShrLkOJN8lnVMMnQWxbtp1ryci+qKwZ4bgFpztzBZ98
JD3yGnSwo4xu6XfpIm0QR8ycprHTrzzUzvLO7jDAhvMYryN5dpfgBk4ntYyfufOG
KwVg4YKNGfLC9B19ol6DU5kgj2ION6r2HFTS0Pjd2VX5+TkeczHW8nfG/A+t601E
```

```
6N90dvkUTigAkhB4LXKteABkalzDWlsgPX37pbEnMwZli+uVCI6xkaTUR37iYjzR
gL2+hpg6C93snJPZ48ap19b1grqG5T1nw1QE2axXePW5IXAZ7HXI5zsgFk5/uyNl
...
OmpWkBcKd90qHc/uWa4eI+KvARNA5mlgG9vZHZehojWcpYFbRvID6TjcXn+VXuNm
BG2RNOX2StY8sUWt8dzJ/TjD50dBvrDwVeOnIBehAY+yTt5dr5JSWm6TBIIWJwZL
jKV1cI1Ssriz7OmkPDuOdJIVIjYf13C+d+MiID8GLlGH0KzMpvBBDFPQwA+oAfS5
sxehyfGJPl3Bk3AUFOXtPQ==
-----END ENCRYPTED PRIVATE KEY-----
```

Warning: bewaar deze sleutel veilig want hiermee zal je alle CA-acties uitvoeren!

(self-signed) certificate voor de CA aanmaken

Certificate Signing Request aanmaken

1. maak een CSR (certificate signing request) aan:

```
openssl req -verbose -new -key server.CA.key -out server.CA.csr -sha256
```

2. geef het wachtwoord van je private key op
3. geef voldoende relevante informatie op voor de DN (distinghuished name) van je server.
4. dit maakt 1 (tekst)bestand aan: `server.CA.csr` met vergelijkbare inhoud:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwgZkxCzAJBgNVBAYTAkJFMRgwFgYDVQQIDA9Pb3N0LVZsYWFu
ZGVyZW4xEjAQBgNVBAcMCU1lcmVsYmVrZTESMBAGA1UECgwJTG91J3MgTGFiMQww
CgYDVQQLDANERVYxETAPBgNVBAMMCExvdSdzIENBMScwJQYJKoZIhvcNAQkBFhhr
b2VuLnZleXNAcHJvdG9ubWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCQ5q5BSgwaeo/Y/q/CfOki7vhTnTzfkVetvwrysolC73kEmXuRwPnN
oJMRWKWNbXNM9u7tLQkUIJSndTl5UzW3S1ohbWwaYNtngColiAIQWgqIrYLhM0wk
CTgHektH72NkBTbbaDzLkbfkC/U/PXv53xPwoGZ1R0NWJD+PbnfLEdL641VNN0li
...
AQEAIvVJfZyiLgxfECHa2mvoMtyV8rj+aY2B6QL0/Xn/r/P+9Q8eYx76A56I+Gu4
hpSdnC75lEvQoFwK1IhktmDZxU3e6Y1eKO2sYs12hI1uL8rGywDNNObpy7BGiwT5
mpwqy3K+TpMq9DbItWugNlRDwIRj5YoRnvo4397wYWvMUPI+jQZBDxHZdokjNraN
AElE41j/JkJugykIviqNHUkJJ6awZLm2SqjUS2U7xE2inBKyC1VMlxuhDAcuzITK
Eafih+llrgOmgS9Z4Rkvo6ZJ7PPCk7l6AkE5kvAjKDFJpFZX3QL0Ic9xHu0N/Uda
PG9fpY3t/jujWmLz/5AvgSEyIg==
-----END CERTIFICATE REQUEST-----
```

achteraf kan je dit bestand inlezen ahv

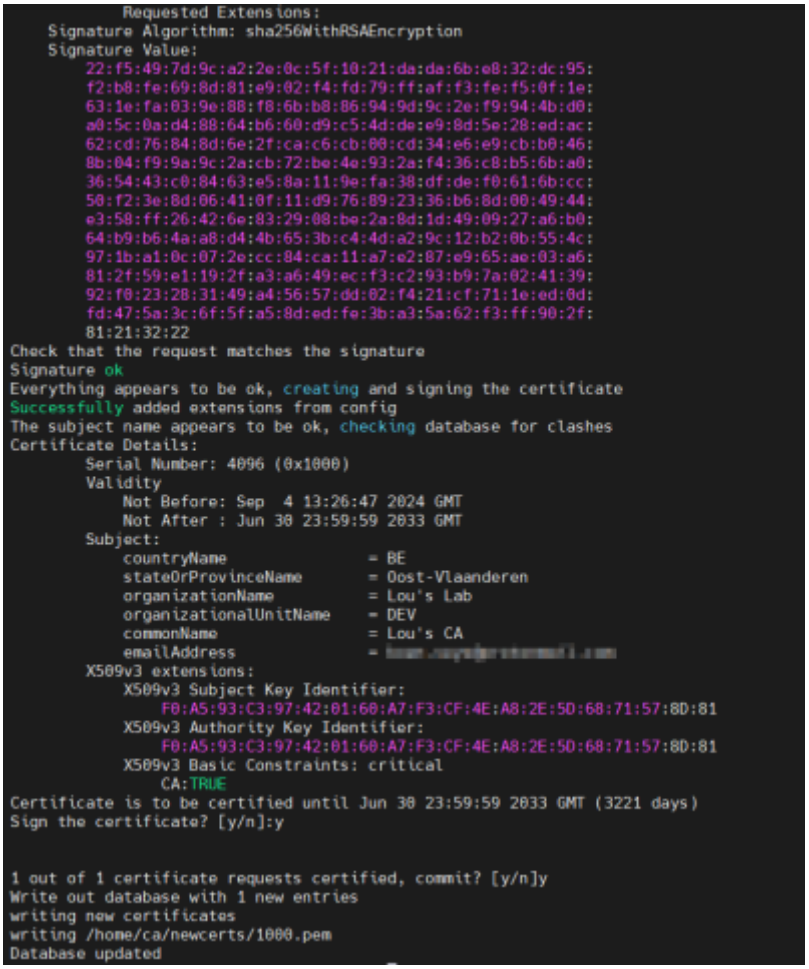
```
openssl req -text -in server.CA.csr -noout
```

tekenen van CA certificate

1. teken het certificate signing request:

```
openssl ca -extensions v3_ca -out server.CA-signed.crt -keyfile
server.CA.key -verbose -selfsign -md sha256 -enddate 330630235959Z -
infiles server.CA.csr
```

    1. enddate formaat: YYMMDDHHMMSSZ
2. geef wachtwoord van je private key in
3. bevestig de info (uit het csr)



4. volgend bestande bestanden worden aangemaakt:

```
    - /newcerts/1000.pem
    - /serial.old en /serial
    - /server.CA-signed.crt
```

Je kan het CA certificaat inlezen ahv

```
openssl x509 -noout -text -in server.CA-signed.crt
```

Note: Hiermee heb je een werkende CA die csr kan ondertekenen.
Bovenstaand werk kan ook wat eenvoudiger door easy-rsa

meer info

1. https://www.wikihow.com/Be-Your-Own-Certificate-Authority
2. Check SSL Certificate with OpenSSL in Linux

ssl