# eigen SSL certficaat aanmaken

1/5

## context

2025/07/07 05:53

dit document beschrijft hoe je een eigen SSL certificaat aanmaakt op Windows.

# **OpenSSL**

- installeer openssl choco install openssl
- verkenner: C:\Program Files\OpenSSL-Win64\tests\start

## private key aanmaken voor je server

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

openssl genrsa -des3 -out server.key 2048

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

```
----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDB0BgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI2g3AahkapWYCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECBXv0oLtreyKBIIEyL01u/JxcHru
c7lEPudjbJCqu/hJXV17YX0znE7qZ990ZuVZanQ0hs/bfmPv3Qi2bGQ2odpWZCQ2
9cLXJDgziwKWo+P1L89lhShrLk0JN8lnVMMnQWxbtp1ryci+qKwZ4bgFpztzBZ98
JD3yGnSwo4xu6XfpIm0QR8ycprHTrzzUzvL07jDAhvMYryN5dpfgBk4ntYyfuf0G
KwVg4YKNGfLC9B19ol6DU5kgj2I0N6r2HFTS0Pjd2VX5+TkeczHW8nfG/A+t601E
6N90dvkUTigAkhB4LXKteABkalzDWlsgPX37pbEnMwZli+uVCI6xkaTUR37iYjzR
gL2+hpg6C93snJPZ48ap19b1grqG5T1nw1QE2axXePW5IXAZ7HXI5zsgFk5/uyNl
...
OmpWkBcKd90qHc/uWa4eI+KvARNA5mlgG9vZHZehojWcpYFbRvID6TjcXn+VXuNm
BG2RN0X2StY8sUWt8dzJ/TjD50dBvrDwVe0nIBehAY+yTt5dr5JSWm6TBIIWJwZL
jKV1cI1Ssriz70mkPDu0dJIVIjYf13C+d+MiID8GLlGH0KzMpvBBDFPQwA+oAfS5
sxehyfGJPl3Bk3AUF0XtPQ==
```

----END ENCRYPTED PRIVATE KEY----

Warning: bewaar deze sleutel veilig want hiermee wordt later de SSL communiatie mee opgezet!

achteraf kan je dit bestand inlezen ahv

×

openssl rsa -text -in server.key -noout

## certificate signing request voor de server aanmaken

#### Certificate Signing Request aanmaken

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

openssl req -verbose -new -key server.key -out server.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 ZGVyZW4xEjAQBgNVBAcMCU11cmVsYmVrZTESMBAGA1UECgwJTG91J3MgTGFiMQww CgYDVQQLDANERVYxETAPBgNVBAMMCExvdSdzIENBMScwJQYJKoZIhvcNAQkBFhhr b2VuLnZleXNAcHJvdG9ubWFpbC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw ggEKAoIBAQCQ5q5BSgwaeo/Y/q/Cf0ki7vhTnTzfkVetvwrysolC73kEmXuRwPnN oJMRWKWNbXNM9u7tLQkUIJSndTl5UzW3S1ohbWwaYNtngColiAIQWgqIrYLhM0wk CTgHektH72NkBTbbaDzLkbfkC/U/PXv53xPwoGZ1R0NWJD+PbnfLEdL641VNN0li ... AQEAIvVJfZyiLgxfECHa2mvoMtyV8rj+aY2B6QL0/Xn/r/P+9Q8eYx76A56I+Gu4

AQEAIVVJT29ILgXTECHa2mVOMT9V8T]+aY2B6QL0/Xh/T/P+9Q8EYX76A56I+Gu4 hpSdnC75lEvQoFwK1IhktmDZxU3e6Y1eK02sYs12hI1uL8rGywDNN0bpy7BGiwT5 mpwqy3K+TpMq9DbItWugNlRDwIRj5YoRnvo4397wYWvMUPI+jQZBDxHZdokjNraN AElE41j/JkJugykIviqNHUkJJ6awZLm2SqjUS2U7xE2inBKyC1VMlxuhDAcuzITK Eafih+llrg0mgS9Z4Rkvo6ZJ7PPCk7l6AkE5kvAjKDFJpFZX3QL0Ic9xHu0N/Uda PG9fpY3t/jujWmLz/5AvgSEyIg==

-----END CERTIFICATE REQUEST-----

achteraf kan je dit bestand inlezen ahv

openssl req -text -in server.csr -noout

lease the test of the second lease the	
openssi Peq (text (in uv kve/1500.csr noout	
Detricate Request:	
Vector 1 (Ave)	
Subject C.B. ST-Dert-Vlanderen L-Baralbera O-Support OV	
Subject, Cate, Struct-Alamberen, Cateleases, Catelease,	
Dublic Fuel Alance the realizement in	
Buble-Fau (2049 b(t))	
Machines:	
- 00:50:77:67:66:5f:fa:66:8a:c7:bc:e2:a0:a6:00:	
26 14 15 28 20 45 28 26 85 47 66 52 11 54 35	
2#:cb:26:e1:26:14:75:f5:92:a8:b1:78:43:ec:32:	
da:59:a1:b2:da:e7:b2:8a:73:a8:a7:e7:e6:58:49:	
50:05:c2:Be:ae:30:a1:dd:e1:09:5e:49:92:29:BE:	
3213d14218610f19f1331a616b1581fd1e616c1481891	
16:d3:c2:0d:cc:e2:f8:9a:4f:0d:19:5f:75:08:95:	
0e:62:99:87:44:1f:0a:e6:68:99:fd:db:19:55:43:	
b6:dc:de:26:bf:48:80:12:ac:dc:5e:ed:41:9b:8a:	
b9:9e:65:86:4f:93:3d:10:a7:ca:e4:c1:35:0f:fe:	
81:aa:51:f0:f7:a8:2f:70:ba:1c:a0:16:0c:fd:	
7c:c2:42:f7:84:26:0b:a1:9c:ef:2c:6c:5b:2e:3e:	
39:98:95:8f:63:98:bd:51:2f:fc:cd:9c:a1:fa:7d:	
2a:ba:11:95:b6:61:44:24:b9:68:15:87:9d:28:ca:	
2d:3f:20:3f:82:b3:8e:5c:51:c3:e3:8a:17:28:9b:	
61:8a:ac:e1:76:96:f9:aa:bc:d4:a4:ac:55:4f:11:	
15:ec:12:9f:ef:ea:a0:56:8c:d5:5e:34:93:09:ee:	
e51c1	
Exponent: 05537 (8x10001)	
Attributes:	
(none)	
Requested Extensions:	
Signature Algorithm: shazsbuithAsencryption	
Signature value:	
45(5)(5)(5)(5)(5)(5)(1)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)	
at: 00.001.00.001.001.001.001.001.001.001.0	
64 (56 (54 (26 (46 (51 (26 (11 (15 (47 (15 (15 (15 (15 (15 (15 (15 (15 (15 (15	
84 a 0 a 1 35 (85 ) First 3 a 1 da 34 a 27 ) First 6 a 1 da 1 da 7 da 1 da 1 da 1 da 1 da 1	
25 1r - 79 - 84 - 9d - 9b - 11 - 85 - ad - 8a - 67 - 18 - 55 - 8b - 28 - c4 - 91 - fc -	
57:3h:e3:69:64:48:18:e6:ec:52:19:3f:c0:d1:68:7e:17:d4:	
4d:f4.b2:1e:Ba:ba:9e:bc:8f:29:71:19:bd:40:e9:48:cd:f5:	
80:a4:8e:05:db:87:7d:3c:e0:1a:5c:91:2e:87:c2:b8:6e:ac:	
82:14:4d:53:d5:be:51:8b:f3:a7:c8:bd:89:80:de:e3:b9:fc:	
b8:8e:35:85:3a:fd:5b:a9:9e:68:46:06:3f:7d:d4:2b:22:69:	
1a:a3:00:90:7a:7e:8d:8d:83:20:2d:a6:0d:00:25:54:8b:	
f1:e3:79:a8:9e:c7:8d:eb:b6:24:d2:2b:6b:b8:cd:3b:94:3e:	
bb:6f:01:9b	

#### 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)

Last update: 2024/11/16 18:14 ssl:eigen\_ca\_certificaaat\_aanmaken https://louslab.be/doku.php?id=ssl:eigen\_ca\_certificaaat\_aanmaken



- 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

From: https://louslab.be/ - **Lou's lab** 

Permanent link: https://louslab.be/doku.php?id=ssl:eigen\_ca\_certificaaat\_aanmaken



Last update: 2024/11/16 18:14