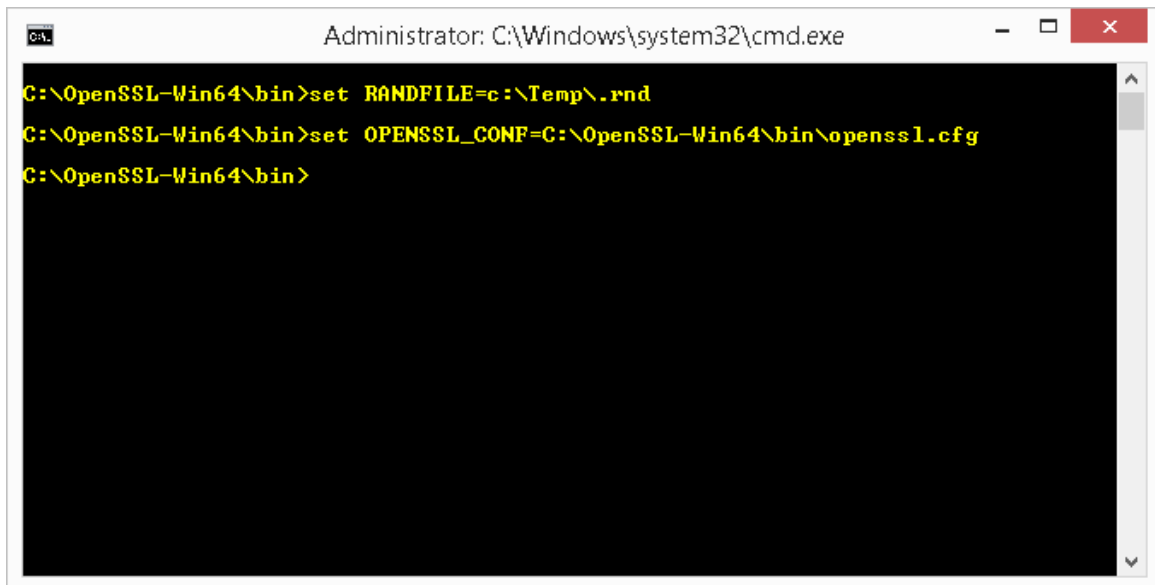


OpenSSL ROOT CA erstellen

Bevor wir starten setzen wir erst einmal 2 wichtige Umgebungsvariablen fest.

```
set RANDFILE=c:\Temp\.rnd
```

```
set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg
```

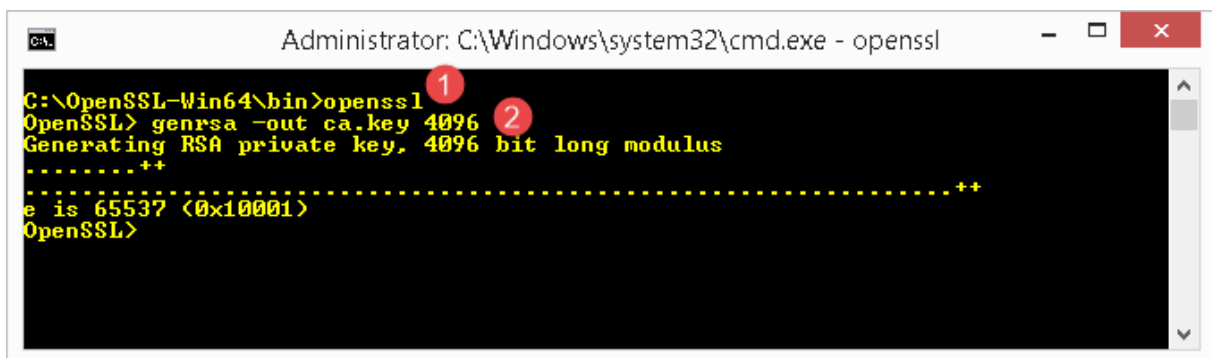


```
Administrator: C:\Windows\system32\cmd.exe

C:\OpenSSL-Win64\bin>set RANDFILE=c:\Temp\.rnd
C:\OpenSSL-Win64\bin>set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg
C:\OpenSSL-Win64\bin>
```

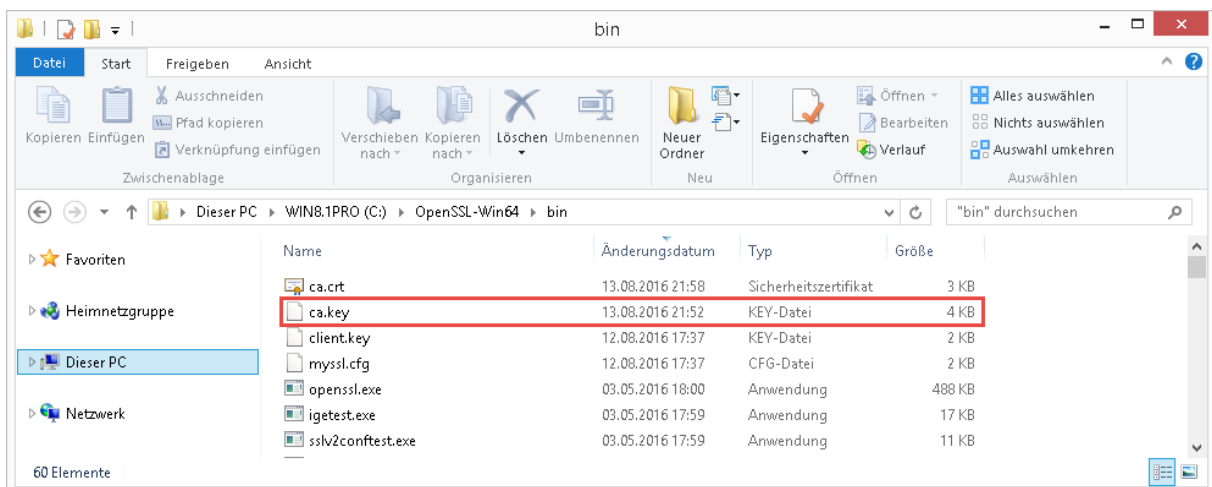
Als erstes erstellen wir einen 4096-Bit langen RSA Schlüssel für unsere root CA und speichern in als ca.key ab.

```
genrsa -out ca.key 4096
```



```
Administrator: C:\Windows\system32\cmd.exe - openssl

C:\OpenSSL-Win64\bin>openssl 1
OpenSSL> genrsa -out ca.key 4096 2
Generating RSA private key, 4096 bit long modulus
.....++
e is 65537 (0x10001)
OpenSSL>
```

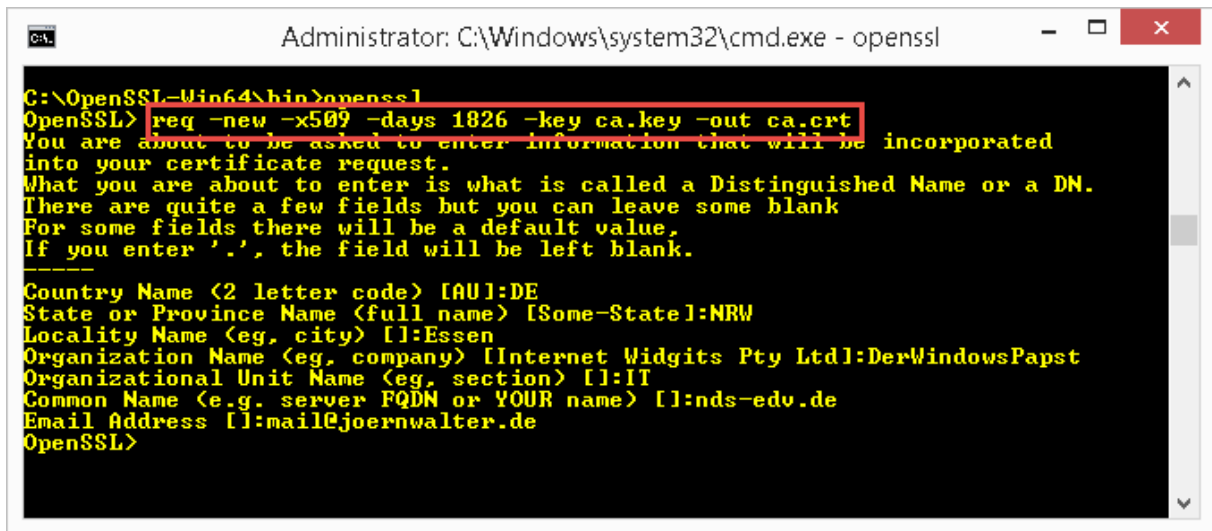


Name	Änderungsdatum	Typ	Größe
ca.crt	13.08.2016 21:58	Sicherheitszertifikat	3 KB
ca.key	13.08.2016 21:52	KEY-Datei	4 KB
client.key	12.08.2016 17:37	KEY-Datei	2 KB
myssl.cfg	12.08.2016 17:37	CFG-Datei	2 KB
openssl.exe	03.05.2016 18:00	Anwendung	488 KB
igetest.exe	03.05.2016 17:59	Anwendung	17 KB
ssl2conf.exe	03.05.2016 17:59	Anwendung	11 KB

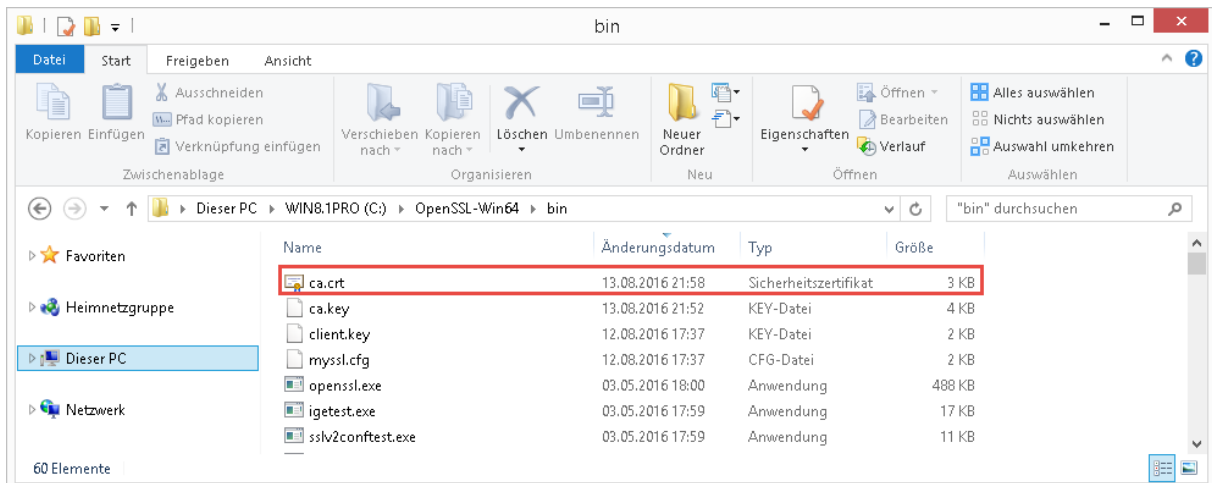
OpenSSL ROOT CA erstellen

Als nächstes erstellen wir unser selbstsigniertes root CA Zertifikat (5 Jahre). Das benötigen wir zur Identität unserer CA.

req -new -x509 -days 1826 -key ca.key -out ca.crt

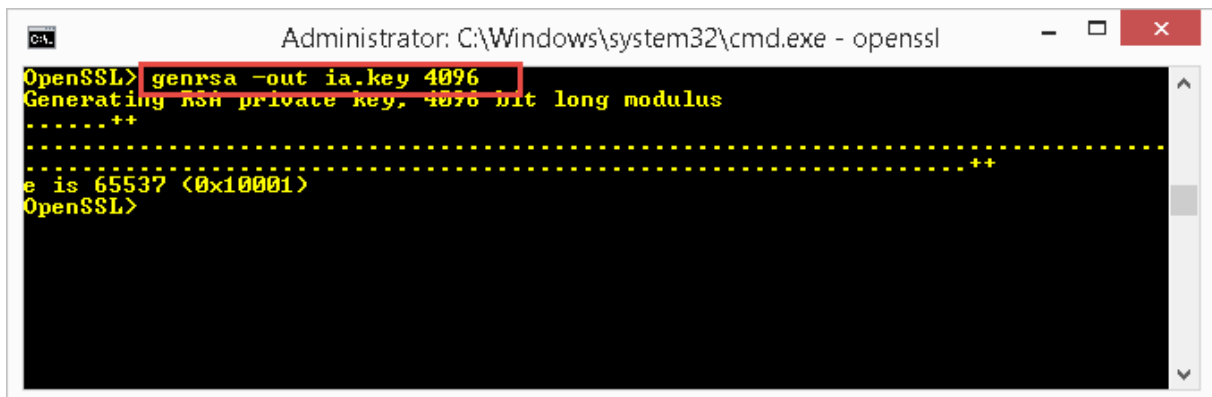


```
C:\OpenSSL-Win64\bin>openssl
OpenSSL> req -new -x509 -days 1826 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:NRW
Locality Name (eg, city) []:Essen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DerWindowsPapst
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:nds-edv.de
Email Address []:mail@joernwalter.de
OpenSSL>
```



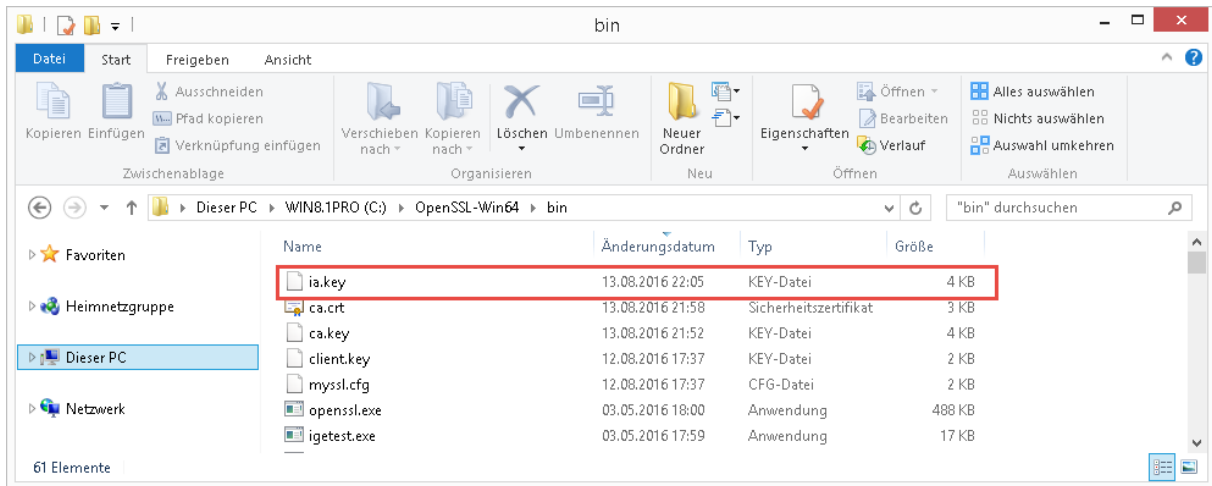
Jetzt erstellen wir unsere untergeordnete CA. Dafür benötigen wir wieder einen privaten Schlüssel.

genrsa -out ia.key 4096



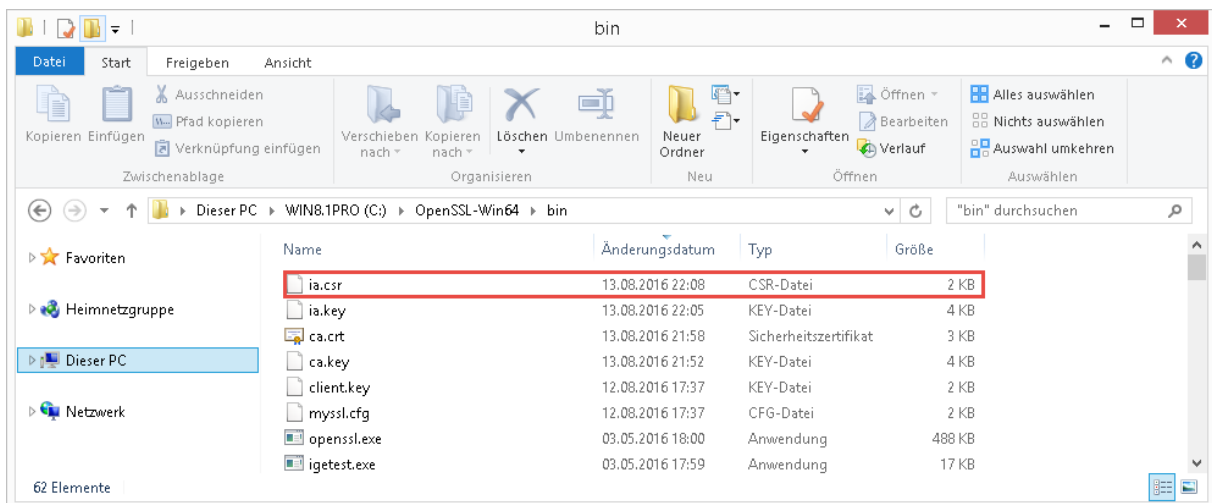
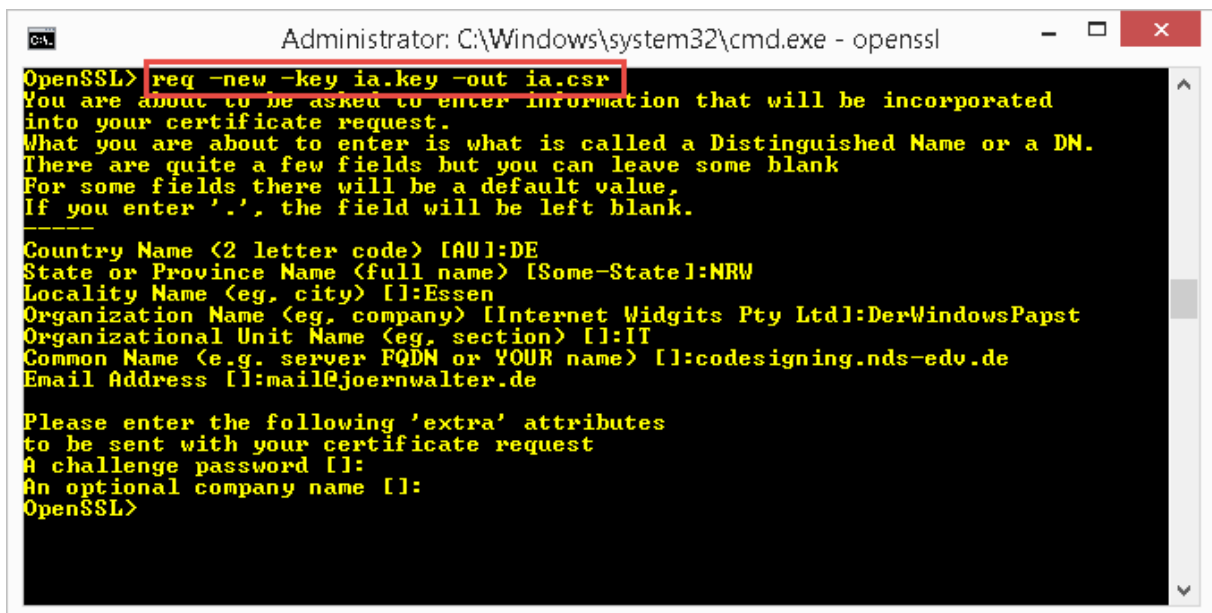
```
OpenSSL> genrsa -out ia.key 4096
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
OpenSSL>
```

OpenSSL ROOT CA erstellen



Nun erstellen wir einen Zertifikats-Request für unsere untergeordnete CA.

req -new -key ia.key -out ia.csr

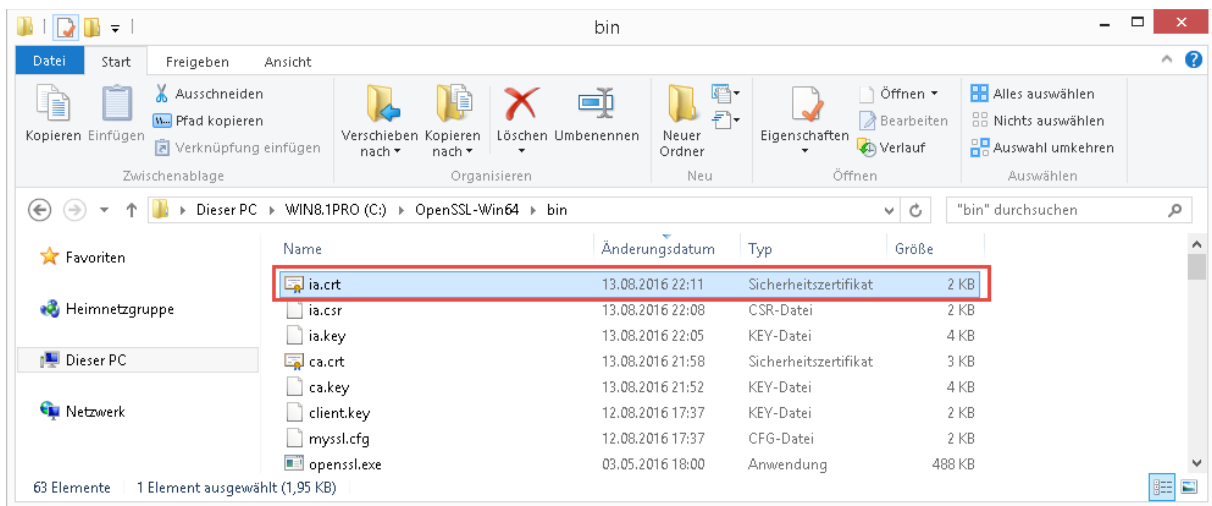


OpenSSL ROOT CA erstellen

Jetzt signiert die root CA den Zertifikats-Request der untergeordneten CA und vergeben eine Seriennummer.

x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt

```
Administrator: C:\Windows\system32\cmd.exe - openssl
OpenSSL> x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt
Signature ok
subject=/C=DE/ST=NRW/L=Essen/O=DerWindowsPapst/OU=IT/CN=codesigning.nds-edu.de/mailAddress=mail@joernwalter.de
Getting CA Private Key
OpenSSL>
```

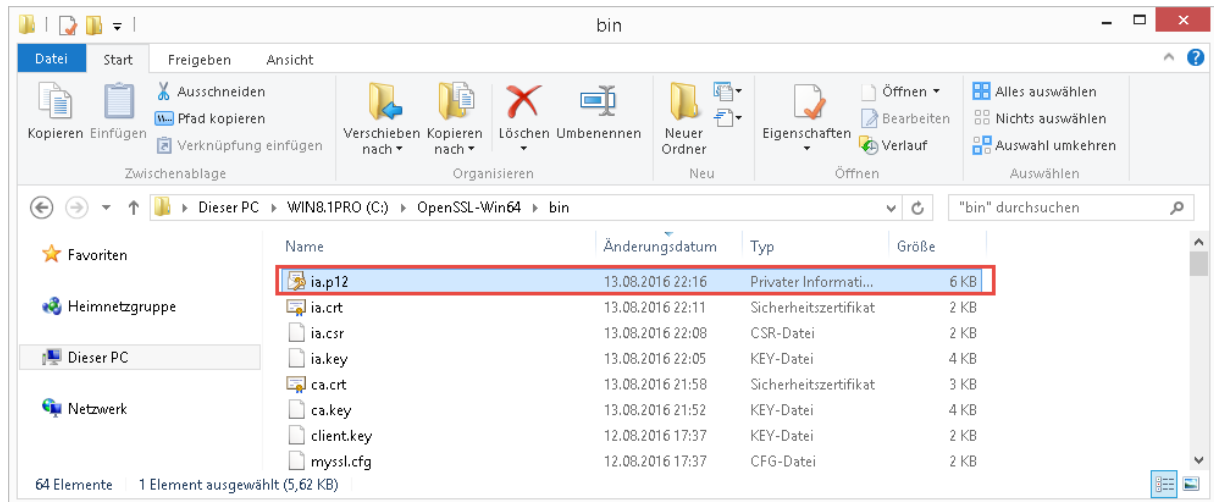


Wenn wir jetzt den Schlüssel der untergeordneten CA zum Signieren von Software nutzen möchten, benötigen wir ein PKCS12 File.

pkcs12 -export -out ia.p12 -inkey ia.key -in ia.crt -chain -CAfile ca.crt

```
Administrator: C:\Windows\system32\cmd.exe - openssl
OpenSSL> pkcs12 -export -out ia.p12 -inkey ia.key -in ia.crt -chain -CAfile ca.crt
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

OpenSSL ROOT CA erstellen



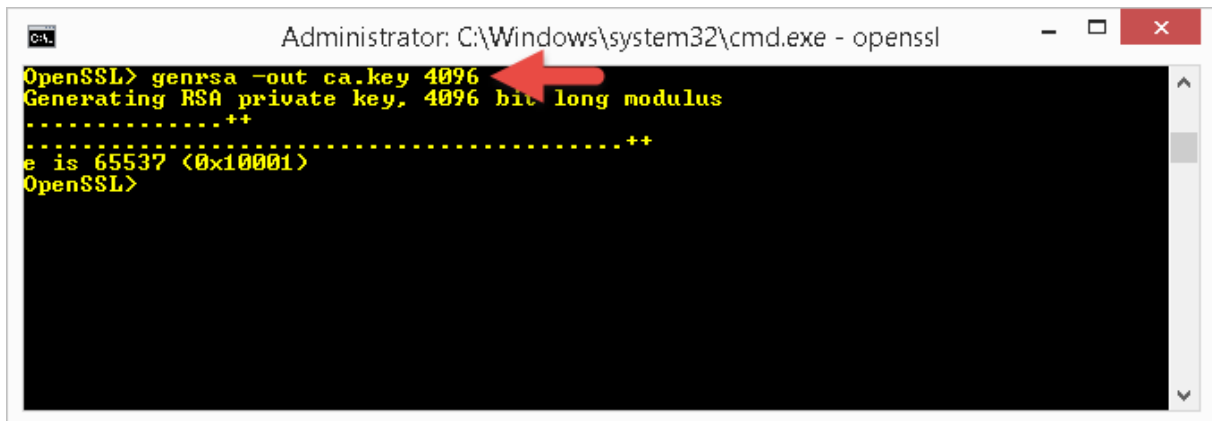
Zum Abschluss muss das ia.p12 Zertifikat in den lokalen Zertifikatsspeicher importiert werden.

OpenSSL ROOT CA erstellen

Erstellen eines Zertifikats für einen Webservice.

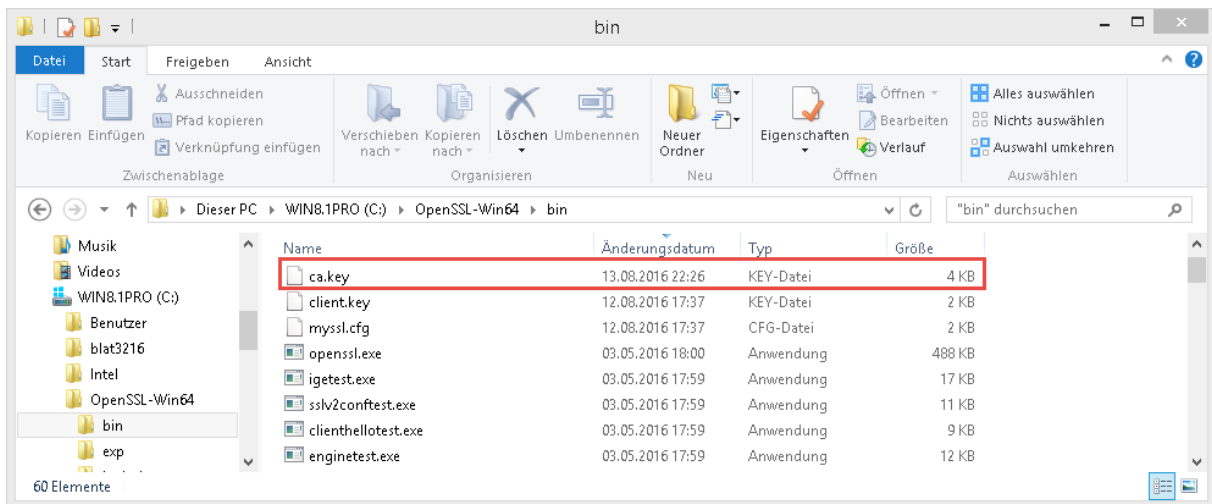
Zuerst erstellen wir wieder einen privaten Schlüssel.

openssl genrsa -out ca.key 4096



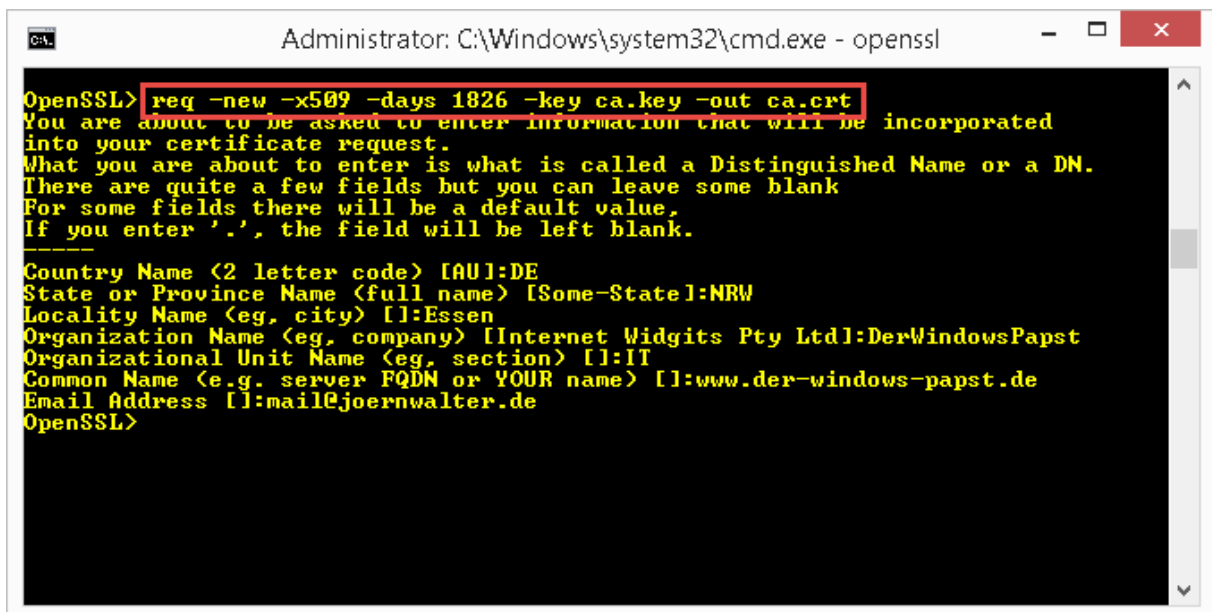
```
Administrator: C:\Windows\system32\cmd.exe - openssl

OpenSSL> genrsa -out ca.key 4096
Generating RSA private key, 4096 bit long modulus
.....++
e is 65537 (0x10001)
OpenSSL>
```



Erstellen unser selbstsigniertes root CA Zertifikat.

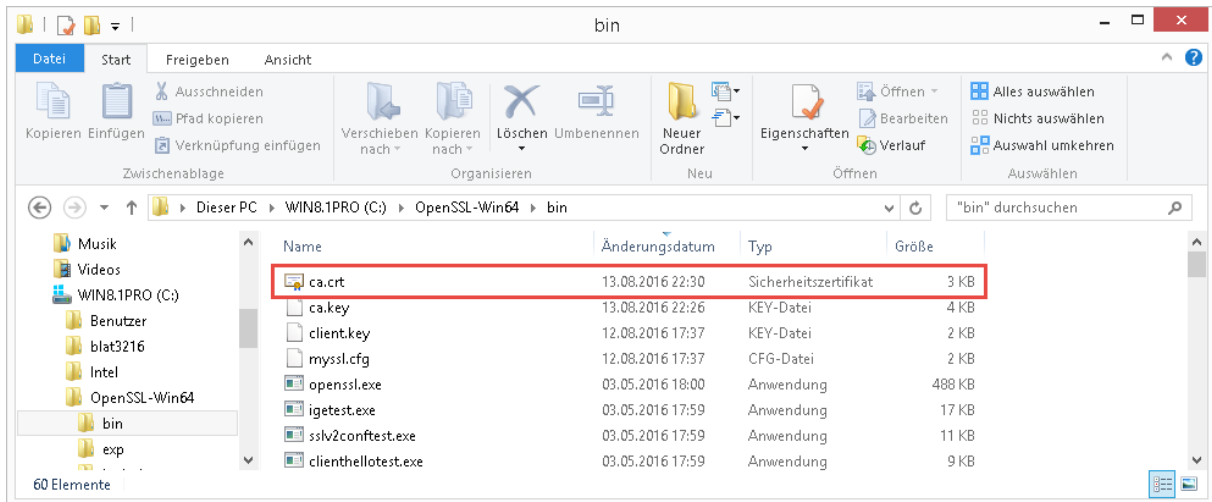
openssl req -new -x509 -days 1826 -key ca.key -out ca.crt



```
Administrator: C:\Windows\system32\cmd.exe - openssl

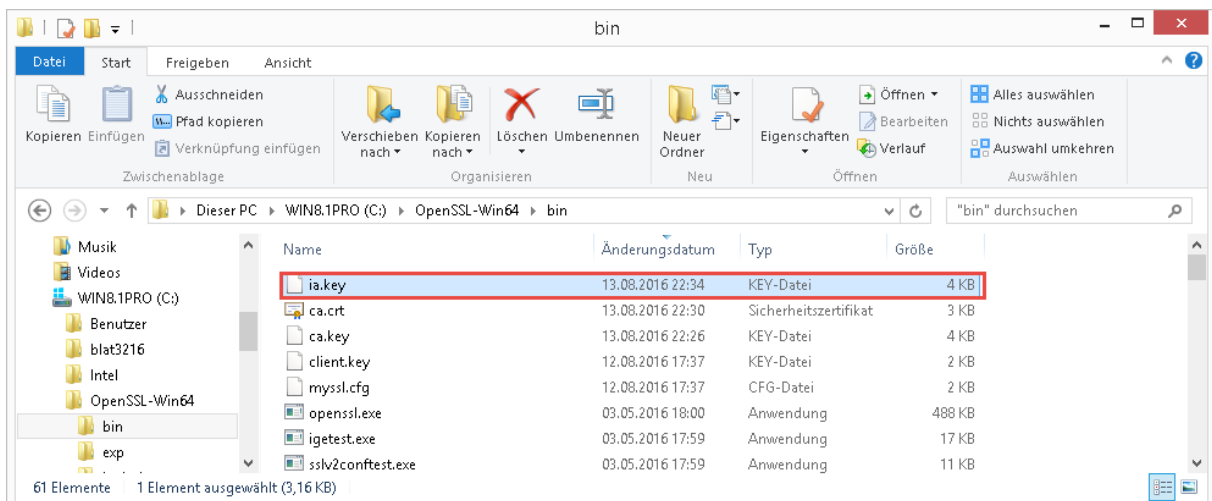
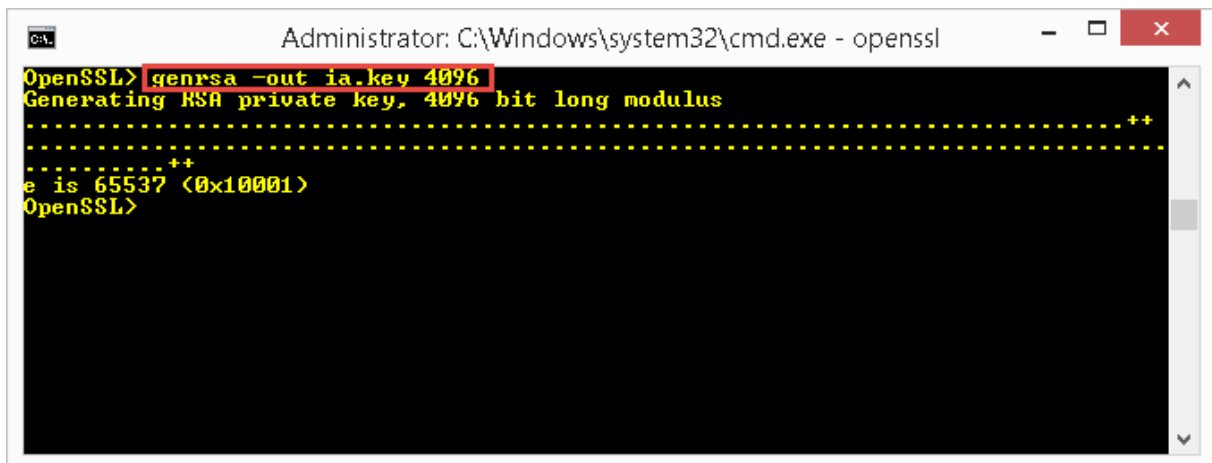
OpenSSL> req -new -x509 -days 1826 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:NRW
Locality Name (eg, city) []:Essen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DerWindowsPapst
Organizational Unit Name (eg, section) []:II
Common Name (e.g. server FQDN or YOUR name) []:www.der-windows-papst.de
Email Address []:mail@joernwalter.de
OpenSSL>
```

OpenSSL ROOT CA erstellen



Nun erstellen wir wieder den privaten Schlüssel für die untergeordnete CA.

openssl genrsa -out ia.key 4096



OpenSSL ROOT CA erstellen

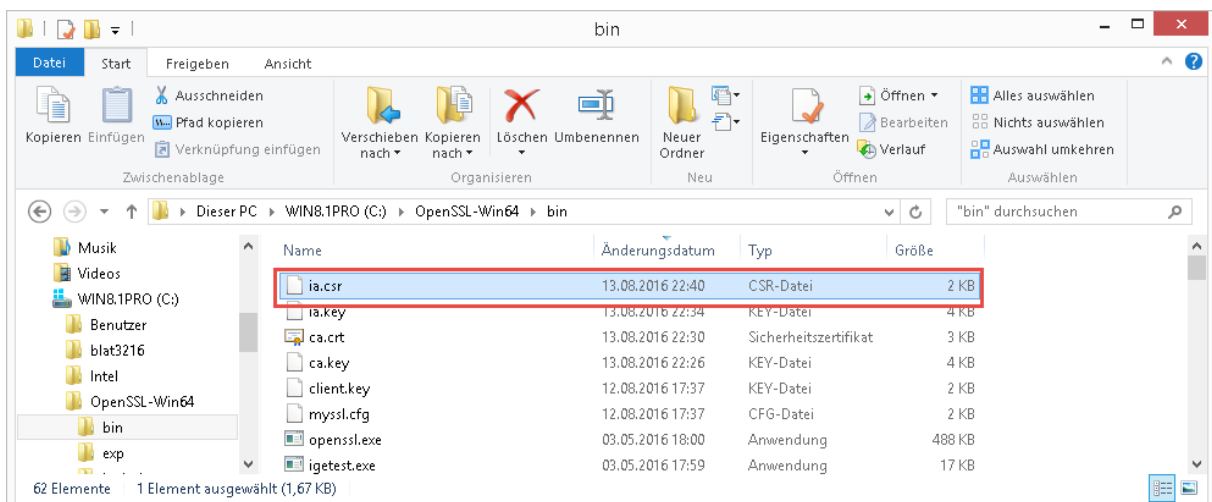
Dann fordern wir wieder ein Zertifikat für die untergeordnete CA an.

openssl req -new -key ia.key -out ia.csr

```
Administrator: C:\Windows\system32\cmd.exe - openssl

OpenSSL> req -new -key ia.key -out ia.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:NRW
Locality Name (eg, city) []:Essen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DerWindowsPapst
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:server01.nds-edv.de
Email Address []:mail@joernwalter.de

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL>
```



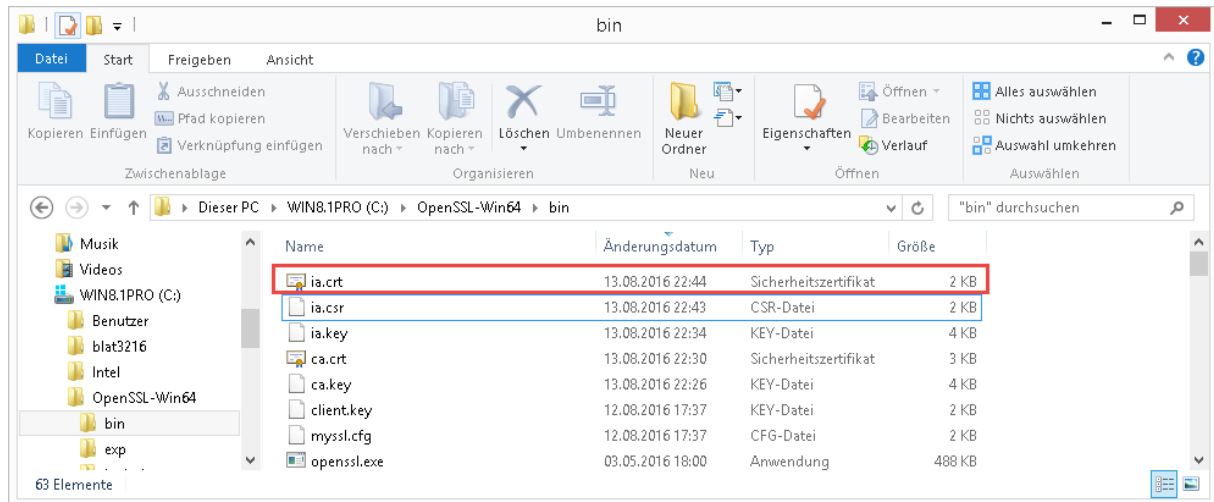
Jetzt stellen wir uns ein Server Zertifikat aus.

openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt

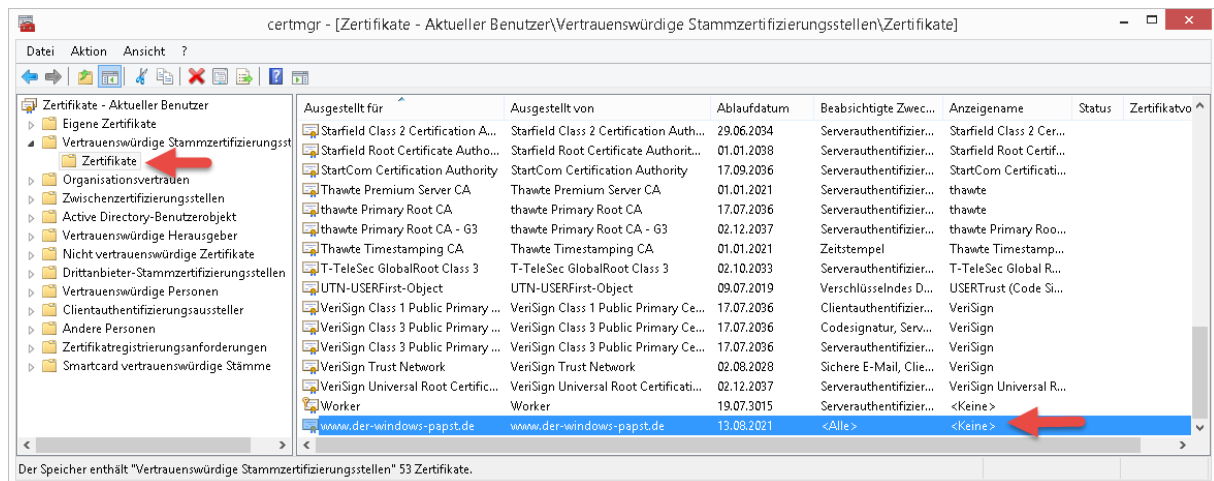
```
Administrator: C:\Windows\system32\cmd.exe - openssl

OpenSSL> x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01
-out ia.crt
Signature ok
subject=C=DE/ST=NRW/L=Essen/O=DerWindowsPapst/OU=IT/CN=server01.nds-edv.de/emailAddress=mail@joernwalter.de
Getting CA Private Key
OpenSSL>
```

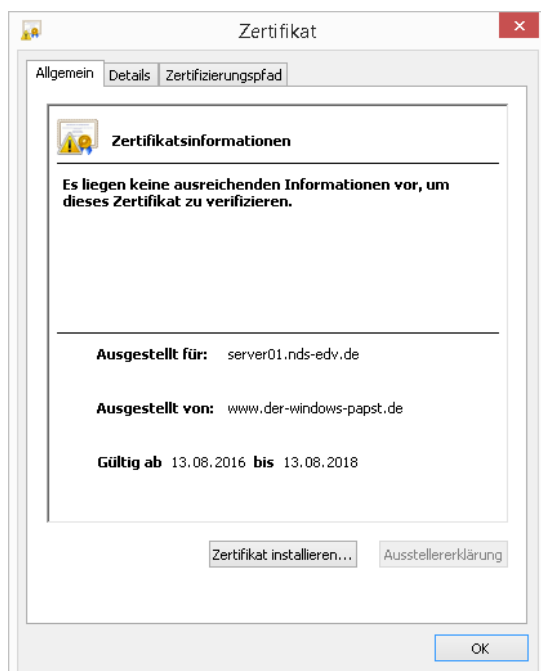

OpenSSL ROOT CA erstellen



Zum Abschluss importieren wir das ca.crt in den Vertrauenswürdigen Stammzertifizierungsstellenpeicher und das Serverzertifikat ist gültig.



Das Ergebnis:

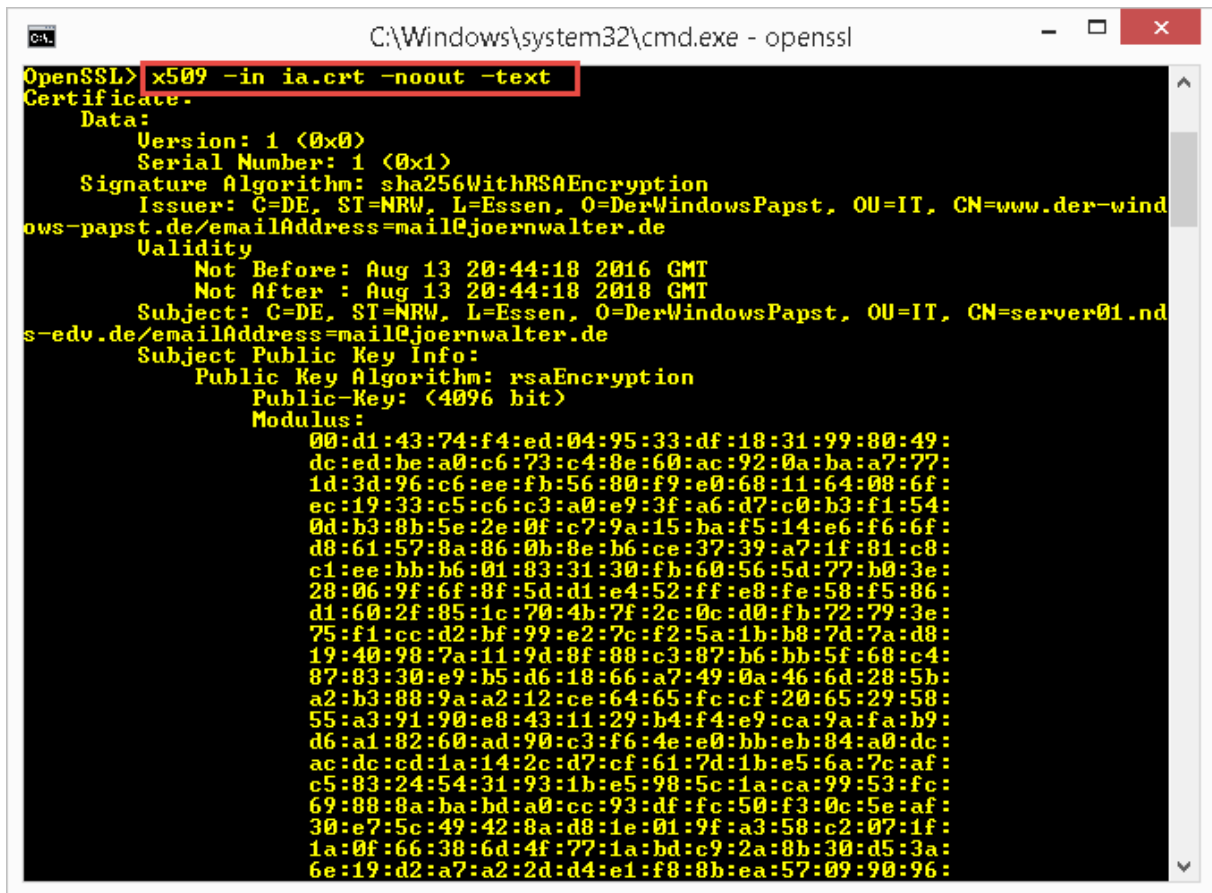


OpenSSL ROOT CA erstellen

Optional:

Mit diesem Befehl schauen wir uns die Details eines Zertifikats an.

openssl x509 -in ia.crt -noout -text



```
C:\Windows\system32\cmd.exe - openssl
OpenSSL> x509 -in ia.crt -noout -text
Certificate-
Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=DE, ST=NRW, L=Essen, O=DerWindowsPapst, OU=IT, CN=www.der-windows-papst.de/emailAddress=mail@joernwalter.de
  Validity
    Not Before: Aug 13 20:44:18 2016 GMT
    Not After : Aug 13 20:44:18 2018 GMT
  Subject: C=DE, ST=NRW, L=Essen, O=DerWindowsPapst, OU=IT, CN=server01.nds-edv.de/emailAddress=mail@joernwalter.de
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (4096 bit)
    Modulus:
      00:d1:43:74:f4:ed:04:95:33:df:18:31:99:80:49:
      dc:ed:be:a0:c6:73:c4:8e:60:ac:92:0a:ba:a7:77:
      1d:3d:96:c6:ee:fb:56:80:f9:e0:68:11:64:08:6f:
      ec:19:33:c5:c6:c3:a0:e9:3f:a6:d7:c0:b3:f1:54:
      0d:b3:8b:5e:2e:0f:c7:9a:15:ba:f5:14:e6:f6:6f:
      d8:61:57:8a:86:0b:8e:b6:ce:37:39:a7:1f:81:c8:
      c1:ee:bb:b6:01:83:31:30:fb:60:56:5d:77:b0:3e:
      28:06:9f:6f:8f:5d:d1:e4:52:ff:e8:fe:58:f5:86:
      d1:60:2f:85:1c:70:4b:7f:2c:0c:d0:fb:72:79:3e:
      75:f1:cc:d2:bf:99:e2:7c:f2:5a:1b:b8:7d:7a:d8:
      19:40:98:7a:11:9d:8f:88:c3:87:b6:bb:5f:68:c4:
      87:83:30:e9:b5:d6:18:66:a7:49:0a:46:6d:28:5b:
      a2:b3:88:9a:a2:12:ce:64:65:fc:cf:20:65:29:58:
      55:a3:91:90:e8:43:11:29:b4:f4:e9:ca:9a:fa:b9:
      d6:a1:82:60:ad:90:c3:f6:4e:e0:bb:eb:84:a0:dc:
      ac:dc:cd:1a:14:2c:d7:cf:61:7d:1b:e5:6a:7c:af:
      c5:83:24:54:31:93:1b:e5:98:5c:1a:ca:99:53:fc:
      69:88:8a:ba:bd:a0:cc:93:df:fc:50:f3:0c:5e:af:
      30:e7:5c:49:42:8a:d8:1e:01:9f:a3:58:c2:07:1f:
      1a:0f:66:38:6d:4f:77:1a:bd:c9:2a:8b:30:d5:3a:
      6e:19:d2:a7:a2:2d:d4:e1:f8:8b:ea:57:09:90:96:
```

Zertifikat in PKCS#12 (pfx) konvertieren:

openssl pkcs12 -nokeys -in ia.crt -export -out cert.pfx -name Server01

Ein Zertifikat entschlüsseln:

openssl rsa -in server-rsa-key.pem > server-key.pem