

Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen

Mit OpenSSL erstellen wir zuerst einen Private-Key (KEY), basierend auf dem Private-Key ein Certificate Signing Request (CSR). Als nächstes signieren wir den CSR mit dem Hash des Private-Keys, das Resultat daraus ist ein (Public) Zertifikat (CRT). Zum Abschluss bringen wir die 2 Zertifikate (Privat- und Public-Key) zusammen und kreieren ein p12 Zertifikat.

Der Befehl 2 ist optional und der Befehl 4 (in der CMD nicht ausgeführt) würde uns den Inhalt des CSR anzeigen.

```
Neues Textdokument.txt - Editor
Datei Bearbeiten Format Ansicht ?

# Privaten Schlüssel erstellen
openssl genrsa -des3 -out PrivaterSchluessel.Key 2048

# Passwort entfernen - Optional auf eigene Gefahr
openssl rsa -in PrivaterSchluessel.Key -out PrivaterSchluesselohnePasswort.key

# Signing Request für den privaten Schlüssel erstellen
openssl req -new -key PrivaterSchluesselohnePasswort.key -out MeinRequest.csr -config openssl.cnf

# Prüfen ob die Erweiterungen enthalten sind
openssl req -text -noout -in MeinRequest.csr

# Erstellen des selbstsignierten Zertifikats
openssl x509 -req -days 3650 -in MeinRequest.csr -signkey PrivaterSchluesselohnePasswort.key -out MeinZertifikat.crt -extensions v3_req -extfile openssl.cnf

# Konvertierung in ein P12 Zertifikat
openssl pkcs12 -export -in MeinZertifikat.crt -inkey PrivaterSchluesselohnePasswort.key -out meintest.p12
```

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

C:\OpenSSL-Win64\bin>openssl genrsa -des3 -out PrivaterSchluessel.Key 2048 1
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 (0x010001)
Enter pass phrase for PrivaterSchluessel.Key:
Verifying - Enter pass phrase for PrivaterSchluessel.Key:

C:\OpenSSL-Win64\bin>openssl rsa -in PrivaterSchluessel.Key -out PrivaterSchluesselohnePasswort.key 2
Enter pass phrase for PrivaterSchluessel.Key:
writing RSA key

C:\OpenSSL-Win64\bin>openssl req -new -key PrivaterSchluesselohnePasswort.key -out MeinRequest.csr -config openssl.cnf 3
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.
-----
1. Country Name <(2 letter code)> [DE]:
2. State or Province Name <(full name)> [NRW]:
3. Locality Name <(eg, city)> [Essen]:
4. Organization Name <(eg, company)> [DerWindowsPapst]:
5. Organizational Unit Name <(eg, section)> [IT]:
6. Common Name <(eg, CA name)> [www.der-windows-papst.de]:
7. Email Address <(eg, name@FQDN)> [info@der-windows-papst.de]:

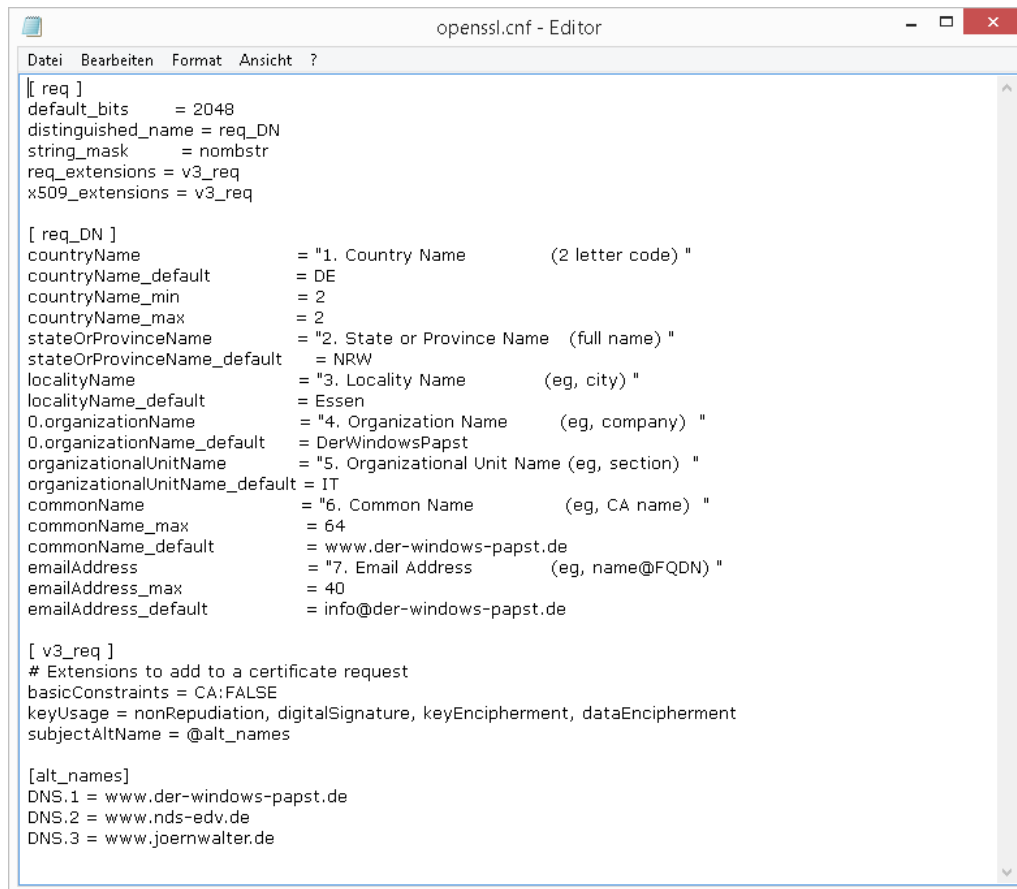
C:\OpenSSL-Win64\bin>openssl x509 -req -days 3650 -in MeinRequest.csr -signkey PrivaterSchluesselohnePasswort.key -out MeinZertifikat.crt -extensions v3_req -extfile openssl.cnf 5
Signature ok
subject=C = DE, ST = NRW, L = Essen, O = DerWindowsPapst, OU = IT, CN = www.der-windows-papst.de, emailAddress = info@der-windows-papst.de
Getting Private key

C:\OpenSSL-Win64\bin>openssl pkcs12 -export -in MeinZertifikat.crt -inkey PrivaterSchluesselohnePasswort.key -out meintest.p12 6
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win64\bin>
```

Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen

Den CSR erstellen wir aus der Vorlage openssl.cnf. Der Parameter commonName_default ist der Name des Servers oder Clients für den wir ein Zertifikat erstellen wollen.



```
[ req ]
default_bits = 2048
distinguished_name = req_DN
string_mask = nombstr
req_extensions = v3_req
x509_extensions = v3_req

[ req_DN ]
countryName = "1. Country Name (2 letter code) "
countryName_default = DE
countryName_min = 2
countryName_max = 2
stateOrProvinceName = "2. State or Province Name (full name) "
stateOrProvinceName_default = NRW
localityName = "3. Locality Name (eg, city) "
localityName_default = Essen
0.organizationName = "4. Organization Name (eg, company) "
0.organizationName_default = DerWindowsPapst
organizationalUnitName = "5. Organizational Unit Name (eg, section) "
organizationalUnitName_default = IT
commonName = "6. Common Name (eg, CA name) "
commonName_max = 64
commonName_default = www.der-windows-papst.de
emailAddress = "7. Email Address (eg, name@FQDN) "
emailAddress_max = 40
emailAddress_default = info@der-windows-papst.de

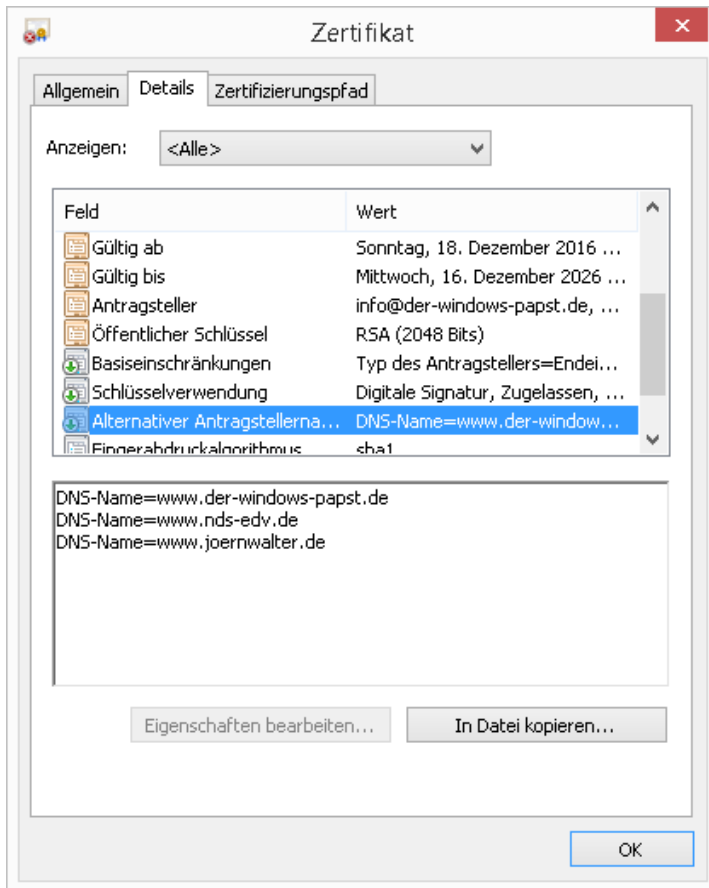
[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = www.der-windows-papst.de
DNS.2 = www.nds-edv.de
DNS.3 = www.joernwalter.de
```

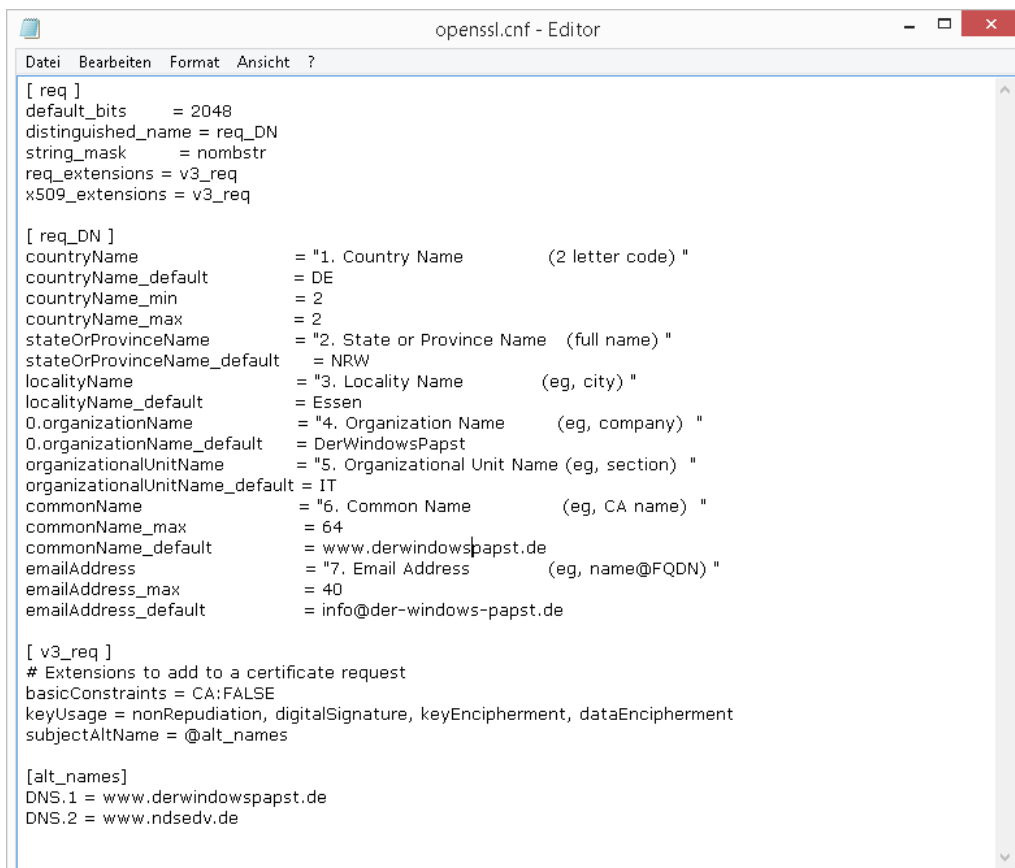
In diesem Fall www.der-windows-papst.de mit den alternativen DNS Namen

- www.der-windows-papst.de
- www.nds-edv.de
- www.joernwalter.de

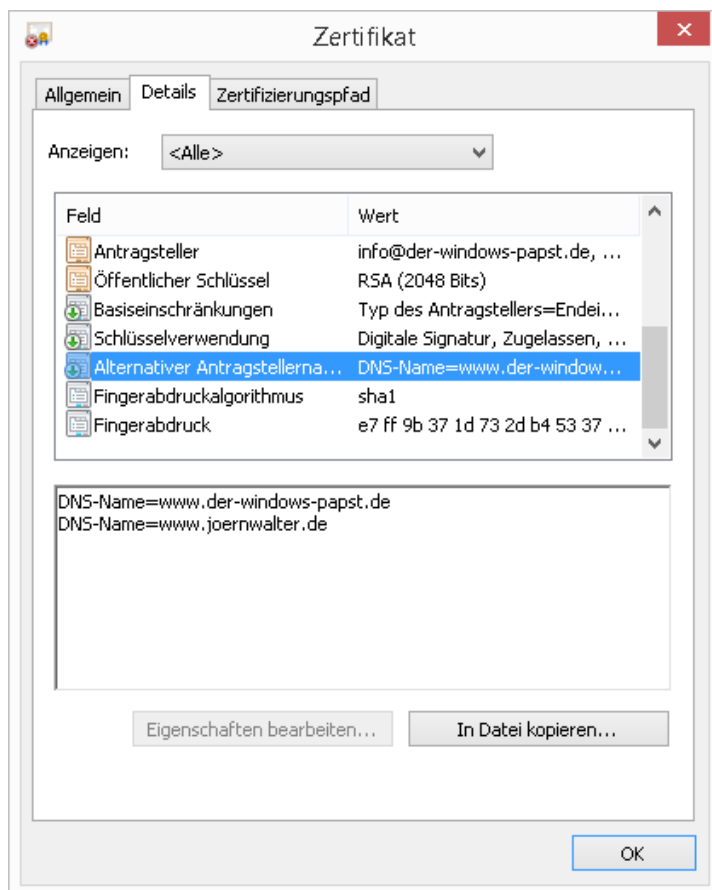
Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen



Vorlage verändert und die Bindestriche in den alternativen DNS Namen entfernt. Ein weiteren Request erstellt und wieder mit dem Hash des Private-Keys signiert.



Weitere Zertifikate auf Basis eines privaten Schlüssels erstellen



Beide Zertifikate nebeneinander gelegt und finden den gleichen öffentlichen Schlüssel des Private-Keys wieder.

