

1. Vorbereitung

- Download und Installation von OpenSSL
(<http://slproweb.com/products/Win32OpenSSL.html>)
- Download und Entpacken des CSR-Generators
(<http://www2.futureware.at/~philipp/CSRGenerator.zip>)

⚠ Den CSR-Generator entpackt Ihr am besten mit in das „bin“ Verzeichnis von OpenSSL.

2. Zertifikatsanforderung erstellen

- CSR-Generator starten
- CN's für das Zertifikat eingeben

Server CRGenerator - Win32

Main Hostname (CN):

Alternative Names (SAN):

Generated Certificate Request (CSR):

Now you can login at <https://www.cacert.org/> and paste the CSR under Server Certificates -> New

Paste ready certificate here:

Password for File:

3. Request generieren

Per „Generate ..“ den Certificate-Request generieren

Server CRGenerator - Win32

Main Hostname (CN):

Alternative Names (SAN):

Generated Certificate Request (CSR):

```
-----BEGIN CERTIFICATE REQUEST-----
MIICITCCAboCAQAwITEGMB0GA1UEAxMWd3d3d3LmF2e2NlYXNta3JlZWJlci52TCC
ASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM+ZNOYf9YmDUm3HU78Xyp
2HAMVH2C23Q6c4zNfDVSj2odGQsLALAhX2pZLUVmWR7w5Qwkt4Cn8eJhdetyO
MXXgV78x00TvoQj9MHY3Gb+PI7OM+U2X3boHrskQCW4C0ca0qaX858Vwglfij
ychw8ghKcQaUqOLLjoi5IqAaxDgppN+ipBHGVS0sdD53Rm675GDvagGRa8MxHxhg
PpAvR4tM5qkDa+u8Qm/rHbwNFMIS/ImF3MS1S/QC2DpQwC6V7k6YkpYVDzK1wC4E
EB+2R72cGv6ygY15dzUSdCXLV8E49dCP28Iw+2Pu2EzopCs2tjA0/KMZM39EC
AwEAAa3BvMG0GCSqGSIb3DQEJDPgMFP4wXAYDVR0RBFOwU4ISd3d3LmtydWV2Xkt
```

Now you can login at <https://www.cacert.org/> and paste the CSR under Server Certificates -> New

Paste ready certificate here:

Password for File:

4. Request verarbeiten

Per Copy & Paste wird die Anforderung in das Webformular von CAcert übertragen.

Da sich das Handling einer Multidomainanforderung nicht von einem normalen Zertifikats-Request unterscheidet, führe ich das hier nicht weiteren aus.

5. Zertifikat verarbeiten

Das von CAcert erzeugte Serverzertifikat wird wiederum per Copy & Paste in das Feld des CSR-Generators eingefügt. Nach vergeben eines Passwortes wird das Zertifikat mit „Save to File“ gespeichert.

Server CRGenerator - Win32

Main Hostname (CN):

Alternative Names (SAN):

Generated Certificate Request (CSR):

```

2XIu2GWCdmtjdWVn2XI2GU0b3JnMA0GCSqGSIb3DQEBAQUAA4IBAQAcwd4STUg
uvouMGr72gtTUUMZYfge6YaBna/WOPFD1bQNLFXuCrY+1qudP11KEBmXrWskHvD1
Tx+pX8LO2Ij9yEIyF5V73cENigjQmCldeendy3wA0qj4dfbAYJ9VcBMyxWm2/6MI
aBJ2VHHHWa2wPQLvEny80KH0lrVXz2vPyUkrmiW6yMylgrnc0VMsmt+*W/+6IPj
usj4zOgTrLLvQTlb60uPD7W8cp8loEfrGBmg?txA5rSHIEEQL85VFqxXUbjntz/
IlcyeHSEck/wFvLYCyd4r0DyjctCxfb/+HKB/O995ygRSEdY9Ge6aL0wmz2X
04uM7HEMre8W
-----END CERTIFICATE REQUEST-----

```

Now you can login at <https://www.cacert.org/> and paste the CSR under Server Certificates -> New

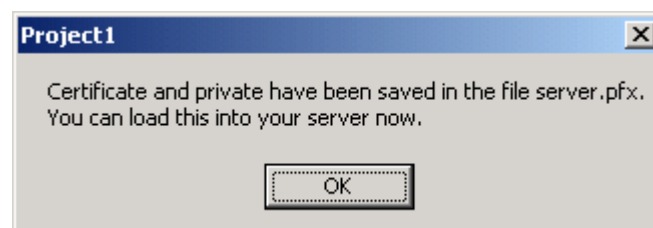
Paste ready certificate here:

```

pl7TaV
2swllVcSjM9eCSzmVJcFPE+mgqZHhHV2++IVgBi5B/bx9kK42wP9vxPnNv
kvRVV/
8U908uSbn068E.w==
-----END CERTIFICATE-----

```

Password for File:



6. Ergebnis

Es sollten sich nun folgende Dateien im Anwendungsverzeichnis befinden:

csr.pem

privatekey.pem

servercert.pem

server.pfx (dieses kann ignoriert werden, es hat keinen Inhalt)

7. Konvertierung für den IIS

Da der Microsoft-IIS das Zertifikat nicht direkt nutzen kann, muss es mit Hilfe von OpenSSL konvertiert werden. Dafür öffnen wir nun eine Kommandozeile. Wechselt in das „bin“-Verzeichnis von OpenSSL und setzt folgenden Befehl (ohne Zeilenumbruch) ab:

```
openssl.exe pkcs12 -export -in servercert.pem -inkey privatekey.pem  
-out servercert.p12 -name "ZertifikatsIdentifizier"
```

⚠ Als ZertifikatsIdentifizier sollte für die Zuordnung der CN, für den das Zertifikat gedacht ist, gewählt werden !

Im folgenden Dialog ist noch ein Passwort für den Zertifikatscontainer zu vergeben. Dieses muss zur Bestätigung wiederholt werden.

```
Loading „screen‘ into random state – done  
Enter Export Password : *****  
Verifying – Enter Export Password: *****
```

Als Ergebnis findet sich nun die Datei „servercert.p12“ im Verzeichnis, die das Zertifikat für den IIS enthält.

8. Einbinden im IIS

Dieses muss jetzt noch über die Zertifikatsverwaltung des IIS (nicht certmgr.msc) importiert und dann der Serverinstanz zugewiesen werden.