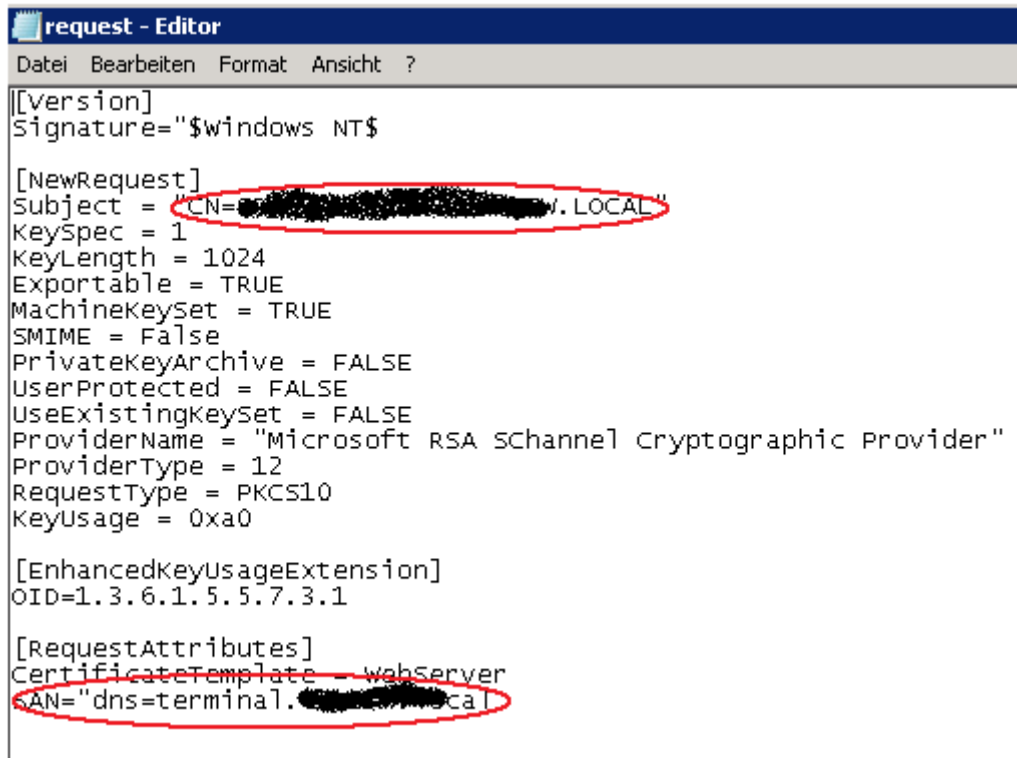


SAN (Subject Alternate Name) Request mit einer Request-Datei unter Windows Server 2008

Erstellen einer INF-Datei

Subject muss auf den Servernamen (FQDN) gesetzt werden

SAN muss auf den DNS Namen der Terminal Server NLB VIP gesetzt werden



```
request - Editor
Datei Bearbeiten Format Ansicht ?

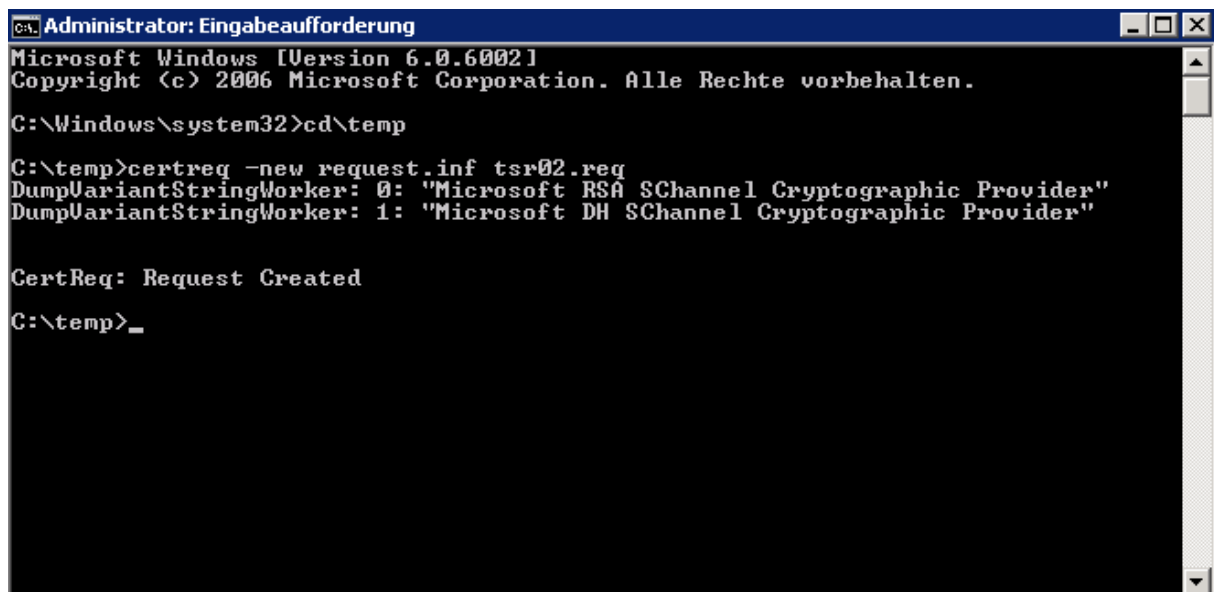
[[version]
Signature="$windows NT$"

[NewRequest]
Subject = "CN=XXXXXXXXXXXXX.W.LOCAL"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1

[RequestAttributes]
CertificateTemplate = wabserver
SAN="dns=terminal.XXXXXXXXXXXXXX.cal"
```

Aus der INF Datei eine CSR Request erstellen



```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>cd\temp

C:\temp>certreq -new request.inf tsr02.req
DumpVariantStringWorker: 0: "Microsoft RSA SChannel Cryptographic Provider"
DumpVariantStringWorker: 1: "Microsoft DH SChannel Cryptographic Provider"

CertReq: Request Created

C:\temp>_
```

Request erstellt

Anzeige des Request mit CERTUTIL -DUMP Angabe des CSR

```
Administrator: Eingabeaufforderung
C:\temp>certreq -new request.inf tsr02.req
DumpVariantStringWorker: 0: "Microsoft RSA SChannel Cryptographic Provider"
DumpVariantStringWorker: 1: "Microsoft DH SChannel Cryptographic Provider"

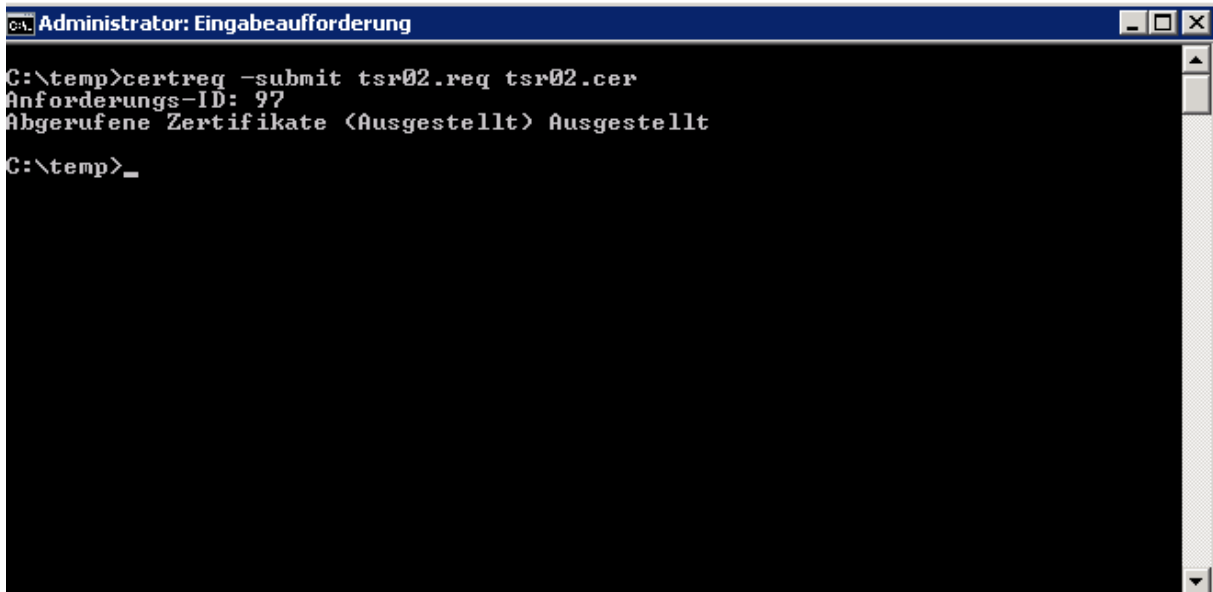
CertReq: Request Created

C:\temp>certutil -dump tsr02.req
PKCS10-Zertifikatanforderung:
Version: 1
Antragsteller:
  CN=SL. 220...
öffentlicher Schlüssel-Algorithmus:
  Algorithmus Objekt-ID: 1.2.840.113549.1.1.1 RSA (RSA_SIGN)
  Algorithmusparameter:
  05 00
Länge des öffentlichen Schlüssels: 1024 Bits
öffentlicher Schlüssel: Nicht verwendete Bits = 0
0000 30 81 89 02 81 81 00 c6 bb 8f 9c 43 ca 6b c5 56
0010 1a f8 f4 0c 21 73 71 9f db 90 df f4 d9 94 b4 af
0020 f0 23 70 e1 aa c4 be 49 e7 c5 a4 54 d6 f7 c0 c8
0030 42 6f cd 7e 51 26 06 05 d3 ca ab 1b 56 51 d9 58
0040 98 79 5d 99 63 fa 71 ec 78 81 92 ea 26 cb 9d d6
```

Den CSR gegen die CA senden

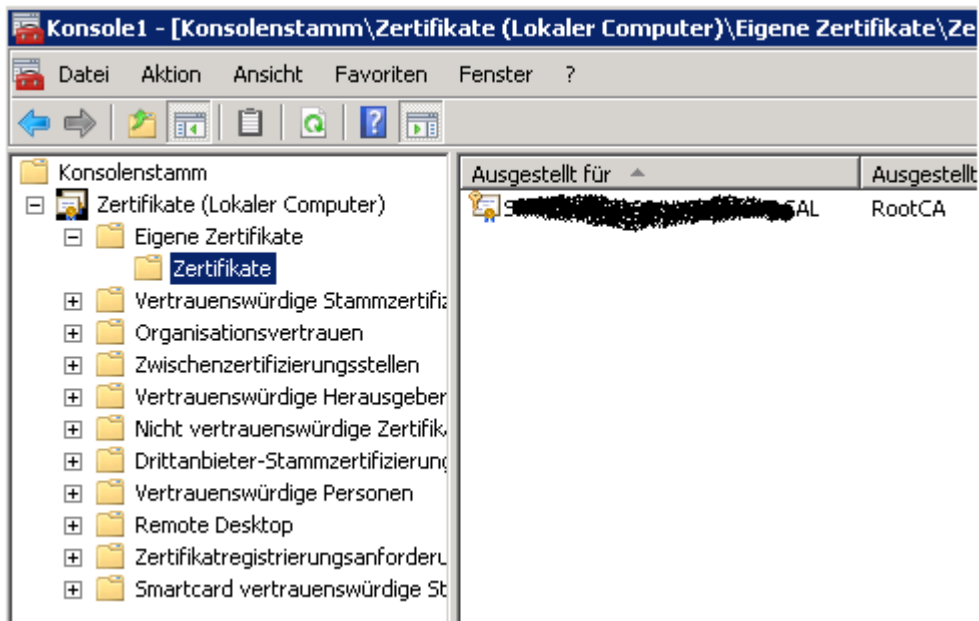
The image shows two overlapping windows from a Windows operating system. The top window is titled 'Zertifizierungsstelle auswählen' (Select Certification Authority) and contains a list with 'RootCA' selected under the 'Zertifizierungsstelle' column. The bottom window is a command prompt titled 'Administrator: Eingabeaufforderung - certreq -submit tsr02.req tsr02.cer' and shows the command 'C:\temp>certreq -submit tsr02.req tsr02.cer' being executed.

Erfolgreich ausgestellt (Kann man auch in der CA Verwaltung unter ausgestellt Zertifikate sehen)



```
Administrator: Eingabeaufforderung
C:\temp>certreq -submit tsr02.req tsr02.cer
Anforderungs-ID: 97
Abgerufene Zertifikate <Ausgestellt> Ausgestellt
C:\temp>_
```

Import des Zertifikats in den Zertifikatspeicher des lokalen Computers (Rechtsklick Zertifikate – Importieren – Angabe des Zertifikats)



Anzeige des SAN in den Zertifikateigenschaften

