Beantragung eines Server-Zertifikats unter Windows

Hier finden Sie die wichtigsten Links zur Beantragung von Zertifikaten:

Startseite der TU Clausthal CA der DFN-PKI	https://pki.pca.dfn.de/tu-clausthal-ca-g2/pub/	
Beantragung eines Nutzer-Zertifikats	Nutzerzertifikat beantragen	Infos zu Nutzer-Zertifikaten
Beantragung eines Server-Zertifikats	Serverzertifikat beantragen	Infos zu Server-Zertifikaten

Zertifikatanträge für Nutzer-Zertifikate sind **persönlich** bei einem/einer Mitarbeiter/in des Teilnehmerservice (= akkreditiere Personen) abzugeben. Dazu wird ein gültiger Lichtbildausweis (Personalausweis, Reisepass) benötigt.

Sie müssen dazu berechtigt sein Server-Zertifikate für eine bestimmte (Sub-)Domain der TU Clausthal beantragen zu dürfen. Sie müssen dafür ggf. erst noch eine Akkreditierung beantragen. Der Antrag dazu ist ggf. zusammen mit Ihrem ersten Zertifikatantrag persönlich beim Teilnehmerservice abzugeben.

Erstellen eines Certificate Signing Request für Server-Zertifikat

Um einen Zertifikatsantrag für Windows-Dienste anzufertigen müssen Sie das bei Windows mitgelieferte Tool *certreq.exe* nutzen, weil der Assistent zum Erstellen von Zertifikatsanträgen eine Formvorschrift unserer CA nicht erfüllen kann.

Für *Certreq* benötigen Sie folgende Konfigurationsdatei:

certreq.inf

```
[Version]

Signature="$Windows NT$

[NewRequest]
```

```
Subject = "CN=,O=Technische Universitaet
Clausthal,L=Clausthal,ST=Niedersachsen,C=DE"
; replace with the FQDN of the DC
KeySpec = 1
KeyLength = 2048
; Can be 1024, 2048, 4096, 8192, or 16384.
; Larger key sizes are more secure, but have
; a greater impact on performance.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
```

In dieser Konfigurationsdatei unter „Subject“ geben sie bitte den FQDN des Rechners (z.B. bsod.rz.tu-clausthal.de) im folgenden Format an:

```
Subject= "CN=bsod.rz.tu-clausthal.de,O=Technische Universitaet
Clausthal,L=Clausthal,ST=Niedersachsen,C=DE"
```

Der Rest der Datei bleibt unverändert für jeden Antrag.

Angenommen, Sie haben die Konfigurationsdatei unter dem Namen *request.inf* gespeichert, rufen Sie *Certreq* mit der Kommandozeile

```
certreq.exe -new request.inf request.req
```

auf und erhalten in der Datei *request.req* den Antrag, mit dem Sie bitte über die DFN-PKI-Webseite das Serverzertifikat beantragen. Das pdf-File reichen Sie unterschrieben an einen der akkreditierten Mitarbeiter weiter, damit der Antrag bearbeitet werden kann.

Nachdem das Zertifikat unterzeichnet wurde (Sie bekommen eine Mail mit dem unterzeichneten Zertifikat) müssen Sie dieses noch mit dem privaten Schlüssel zu einem Schlüsselpaar zusammenfügen. Angenommen Sie bekommen eine Datei *cert.cer*, dann müssen Sie dazu auf dem gleichen Rechner, auf dem Sie auch die Datei *request.req* generiert haben den folgenden Befehl eingeben:

```
certreq.exe -accept cert.cer
```

Danach können Sie ganz normal über das Zertifikat verfügen und es z.B. für eine IIS-Webseite verwenden. Falls Sie das Zertifikat sichern wollen oder es z.B. auf einen anderen Server übertragen

wollen, verwenden Sie das „Zertifikate-SnapIn“ der Management-Konsole (mmc) um es inklusive des Privatschlüssels zu exportieren bzw. zu importieren.