HowTo own SSL Certificate on DSR-Series (neue WebGUI)

[Voraussetzungen]

1. DSR-150N A2-Rev mit Firmwareversion 2.11B301 und höher
2. DSR-250N mit Firmwareversion 2.11B301 und höher
3. DSR-500N mit Firmwareversion 2.11B301 und höher
4. DSR-1000N mit Firmwareversion 2.11B301 und höher
5. DSR-1000AC mit Firmwareversion 3.08B301 und höher

[Szenario]

Es soll ein eigenes SSL Zertifikat für den HTTPS-Zugriff auf dem Gerät installiert werden.

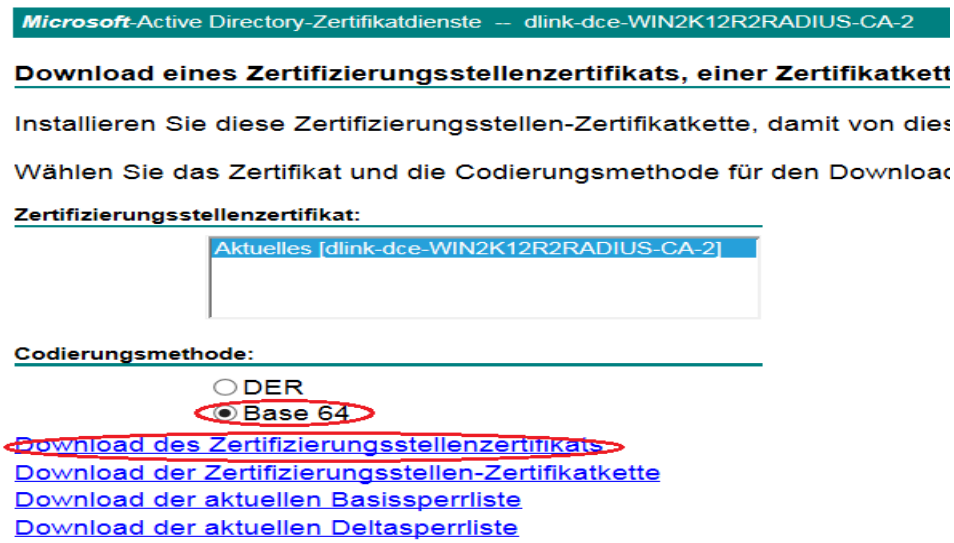
[Voraussetzungen]

Stellen Sie bitte sicher, dass sich Server und Client in der korrekten, gleichen Zeitzone befinden.

Bitte kontaktieren Sie den in Ihrer Organisation für die Zertifikatsaustellung verantwortlichen Mitarbeiter.
Alternativ suchen Sie sich bitte einen für Sie passenden Zertifikatsaussteller (z.B. verisign.com) oder erstellen Ihre eigene CA-Struktur.
Das Stammzertifikat muss BASE64 Codiert sein.

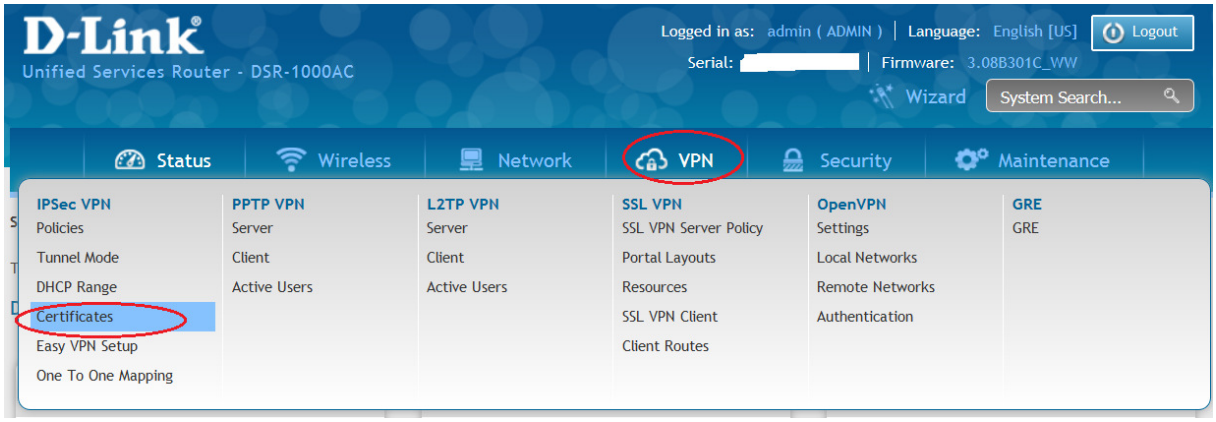
In diesem Beispiel wird ein lokaler Zertifizierungsserver (Windows Server 2012R2) benutzt.

⇨ Download CA-Stammzertifikat vom Zertifizierungsserver (http://<IPServer>/certsrv)

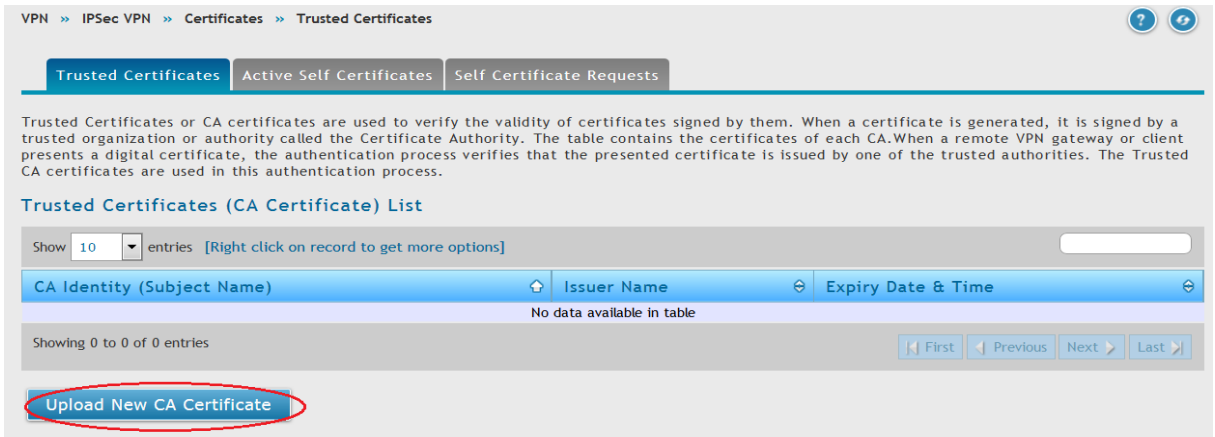


[Installation des CA-Stammzertifikates]

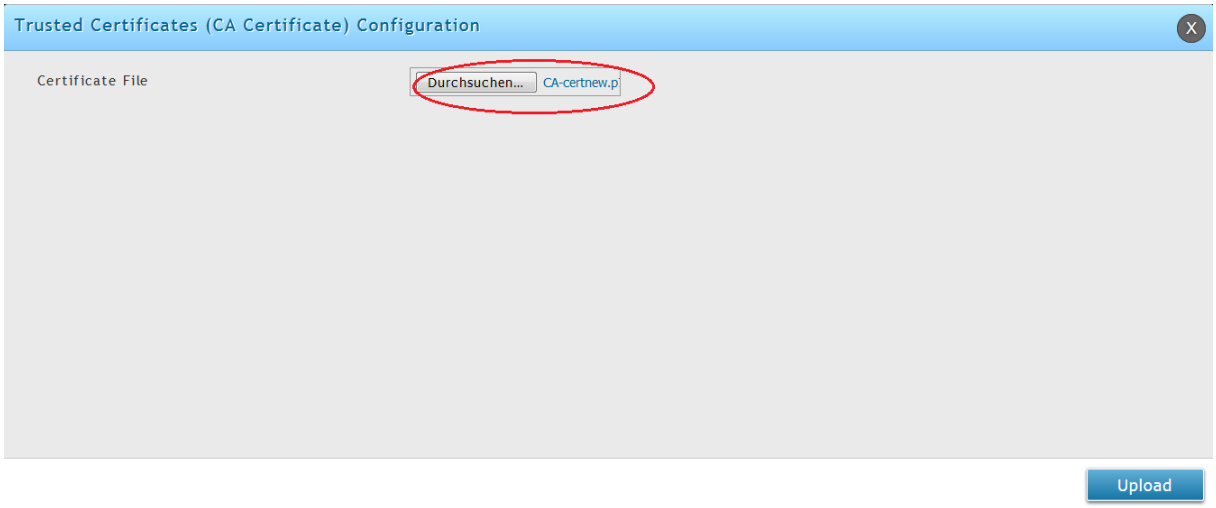
1. greifen Sie auf Ihren DSR-1000AC zu
   a. gehen Sie auf „VPN > Certificates“



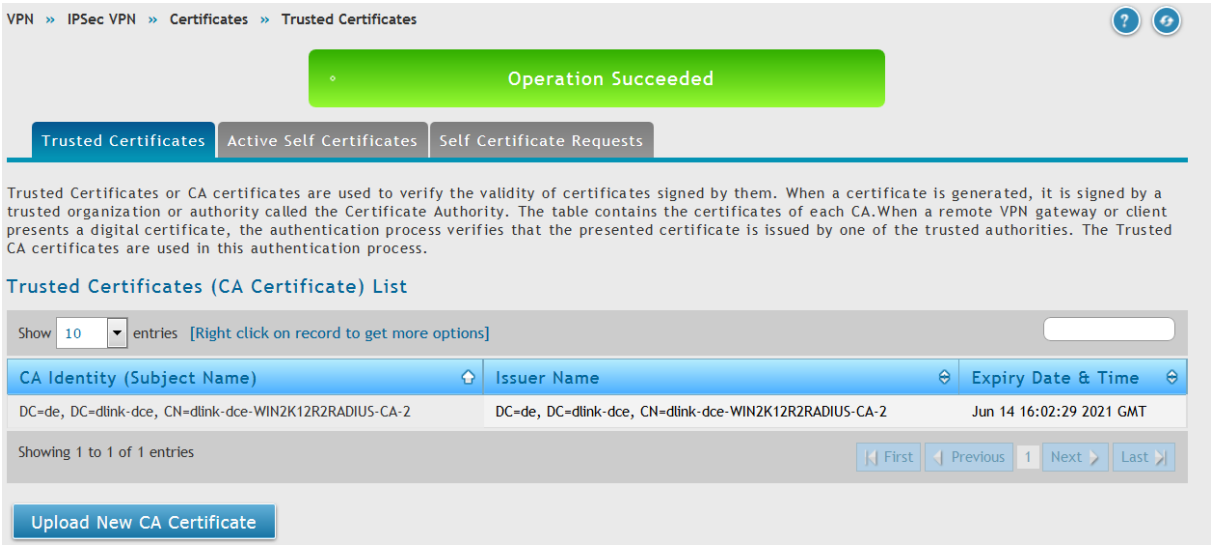
   b. wählen Sie “Upload New CA Certifikat” um ein neues Stammzertifikat auf den DSR-1000AC hochzuladen



   c. wählen Sie Ihr gültiges Stammzertifikat (CA Certifikat) aus und laden Sie dieses auf den DSR-1000AC

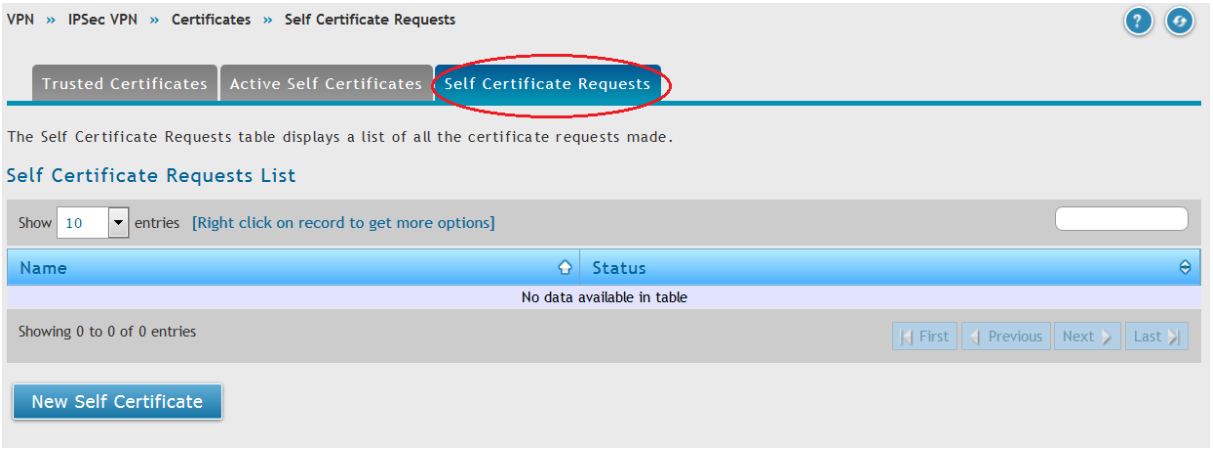


d. nachdem das Stammzertifikat (CA) erfolgreich hochgeladen wurde sehen Sie CA-Identität

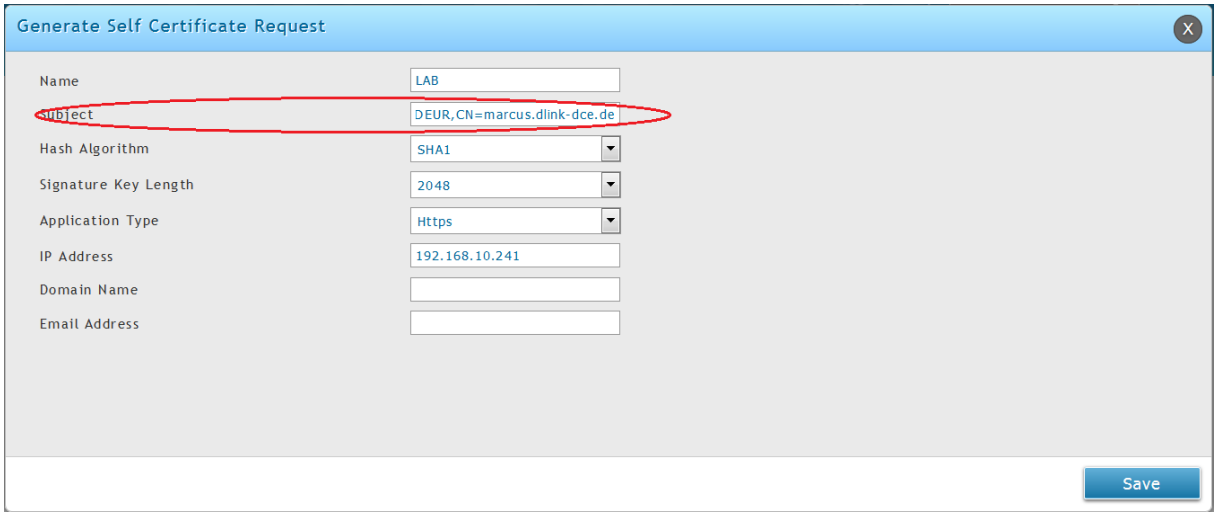


[Erstellen eines CSR (Certificate Self Request)]

1. greifen Sie auf Ihren DSR-1000AC zu
   a. gehen Sie auf „VPN > Certificates > Self Certificate Requests“
   b. wählen Sie “New Self Certificate” zur Erstellung eines neuen CSR aus



c. tragen Sie die notwendigen Daten für Ihr CSR ein
   i. Name = Name Ihres CSR
   ii. Subjekt = Ihre Daten für das Zertifikat
   iii. Hash Algorithmus = SHA1
   iv. Signature Key Length = 2048
   v. Application Tye = HTTPS für SSL oder IPSEC für Tunnel
   vi. IP Adresse = optional
   vii. Domain Name = optional
   viii. eMail Address = optional

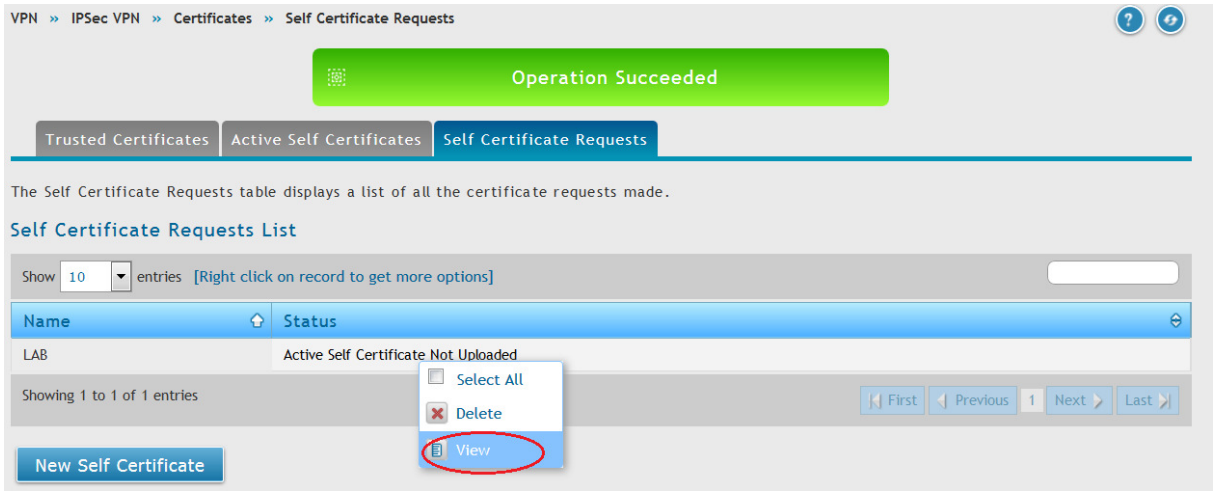


In diesem Beispiel wurden folgende Daten verwendet:

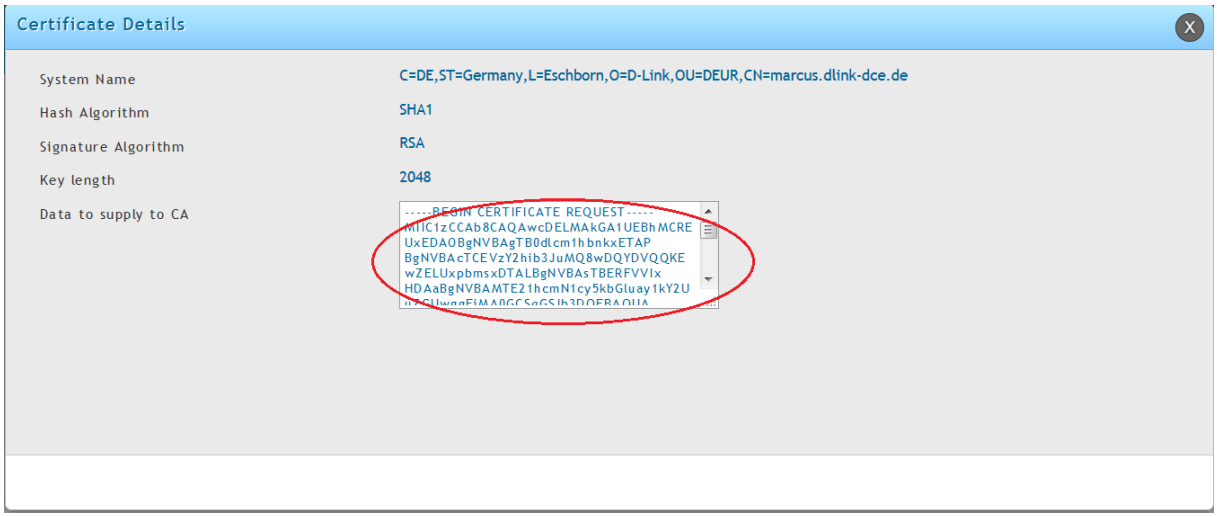
„
C=DE,ST=Germany,L=Eschborn,O=D-Link,OU=DEUR,CN=marcus.dlink-dce.de
“

C = Land, ST = Land/Bundesland, L = Ort, O = Organisation, OU = Abteilung, CN = Common Name

d. nachdem Sie den CSR Erstellt haben,können Sie es sich anschauen
e. klicken Sie mit der rechten Maustaste auf den CSR und wählen „View“ aus

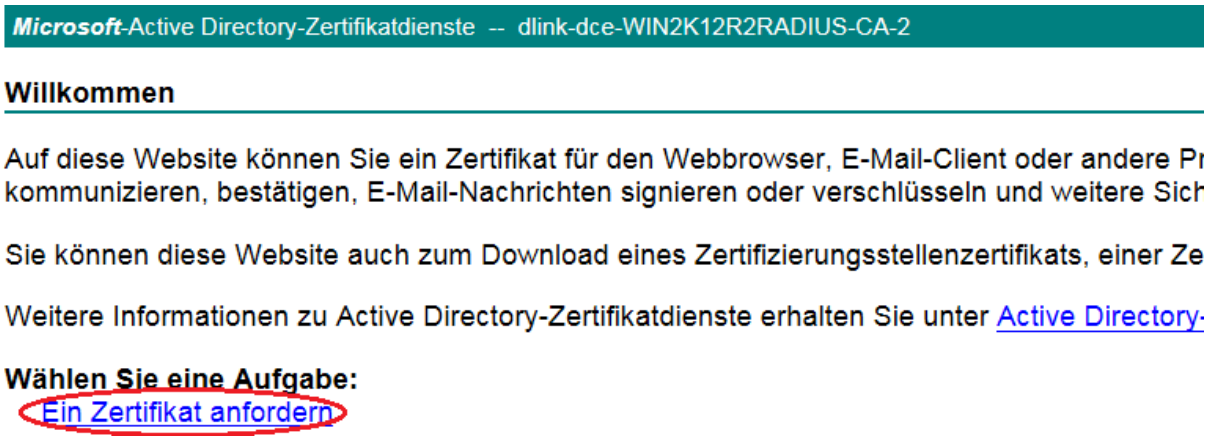


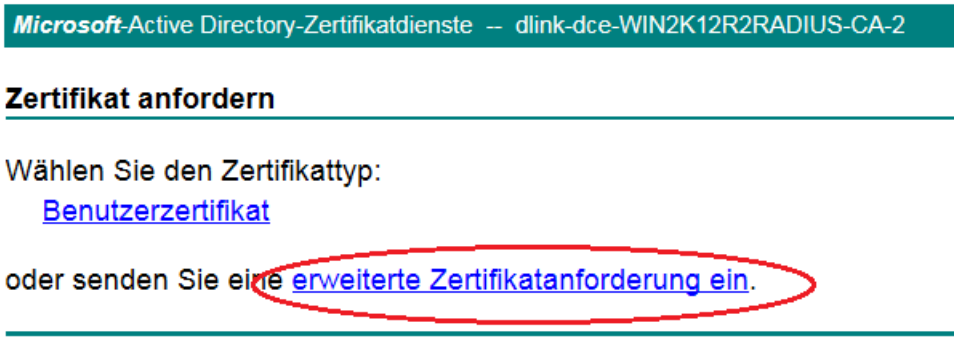
f. kopieren Sie den Inhalt des Feldes „Data to supply to CA“
g. schließen Sie das Fenster anschließend mir klick auf „x“

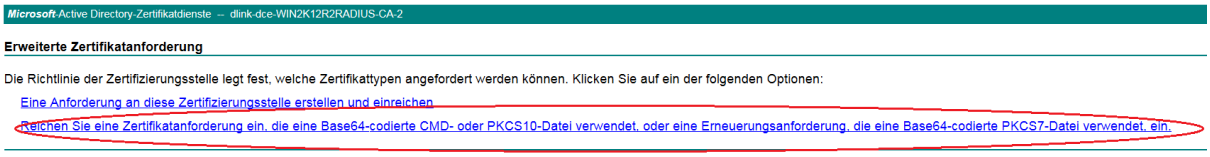


[Erstellen eines Zertifikates aus dem CSR]

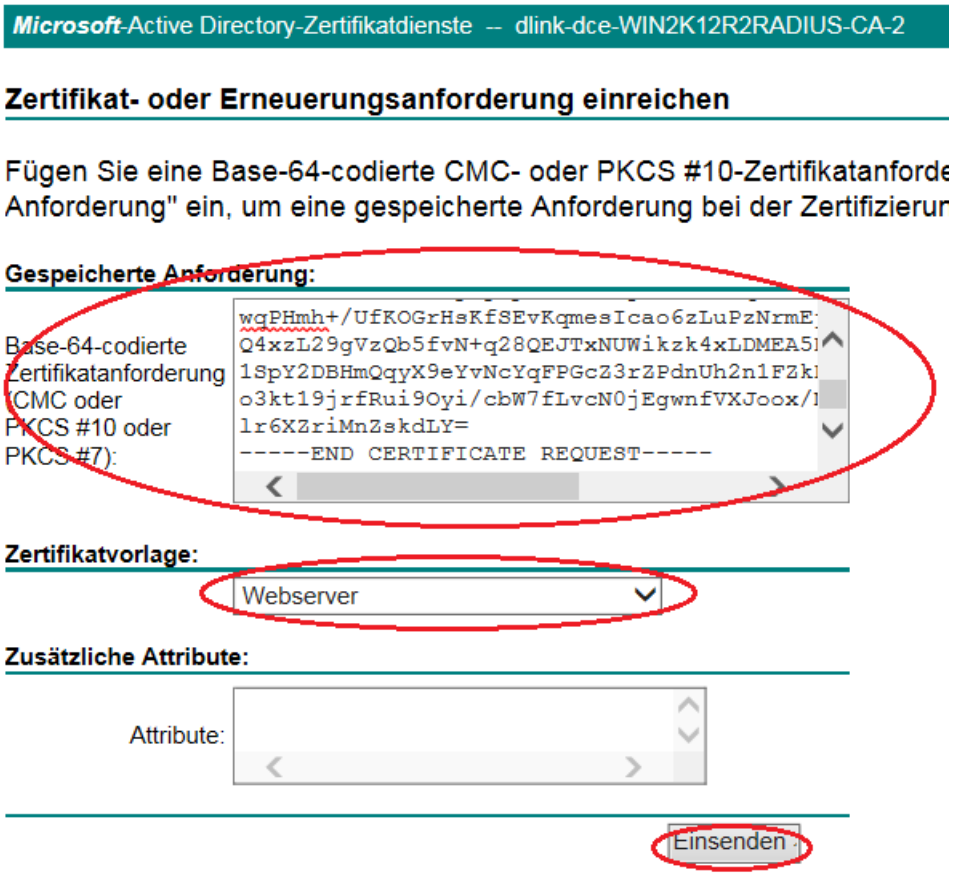
1. greifen Sie nun erneut auf Ihren Zertifikasserver zu um aus dem CSR ein Zertifikat zu erstellen.





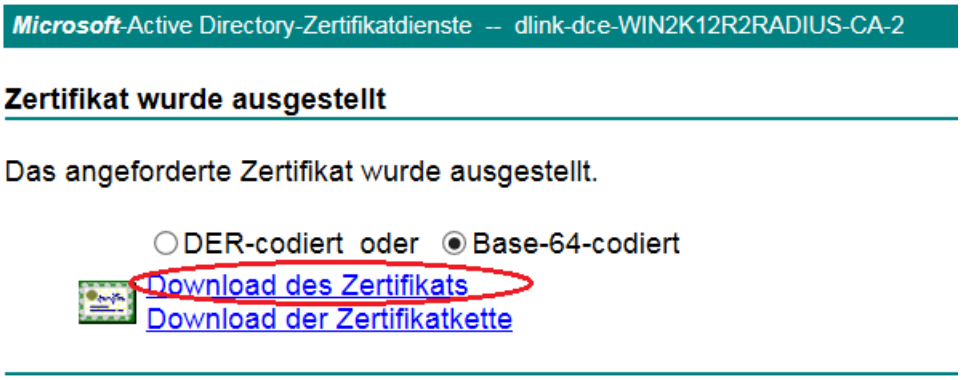


   a. kopieren Sie die Daten des CSR in das Feld (achten Sie darauf, dass keine Leerzeichen am Ende des Requests mit eingetragen sind)
   b. Wählen die gglfs.die entstprechende Zertifikatsvorlage (IPSEC oder Webserver, ..) aus
   c. Drücken Sie einsenden um ein Zertifikat zu erhalten



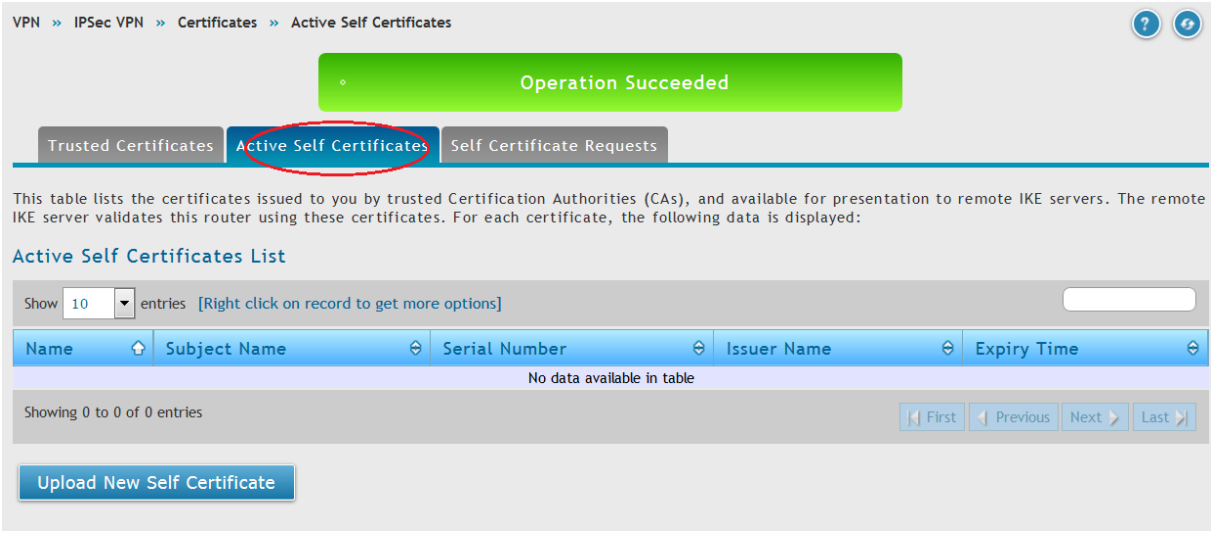
Je nach Vorgabe muss dieses Zertifikat noch durch den Zertifikatsverantwortlichen freigegeben werden.

d. Laden Sie das soeben erstellte Zertifikat herunter

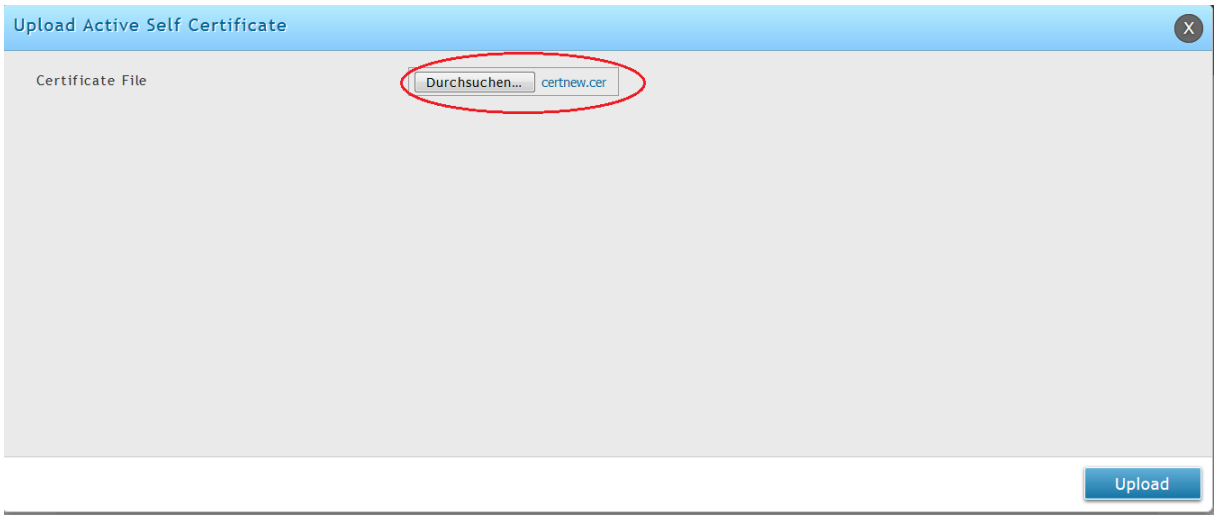


[Hochladen des Zertifikates auf den DSR-1000AC]

1. greifen Sie auf Ihren DSR-1000AC zu
   a. gehen Sie auf „VPN > Certificates > Active Self Certificares“
   b. wählen Sie „Upload New Self Certificate“ um das soeben erstellte Zertifikat auf den DSR-1000AC zu laden

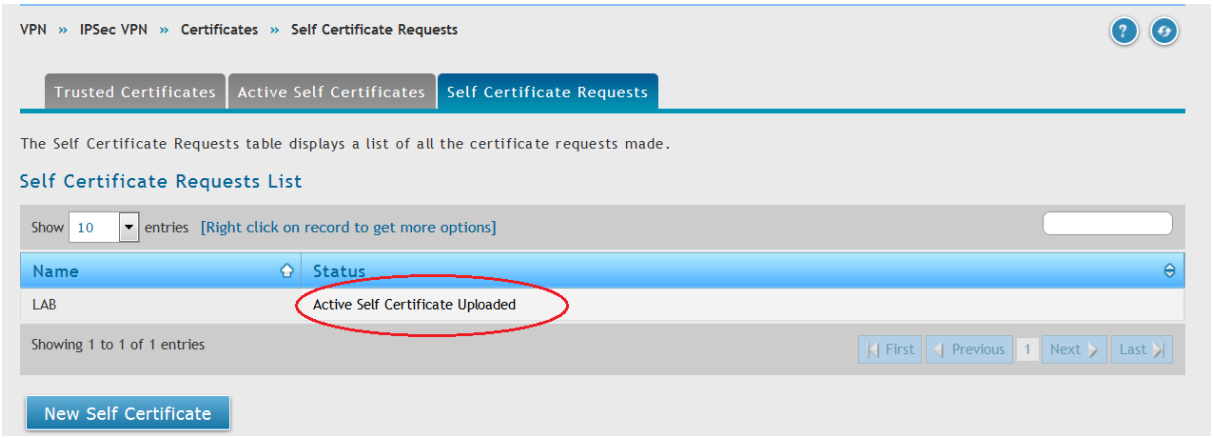


   e. wählen Sie das soeben erstellte Zertifikat aus und laden es mittels „Upload“ auf den DSR-1000AC



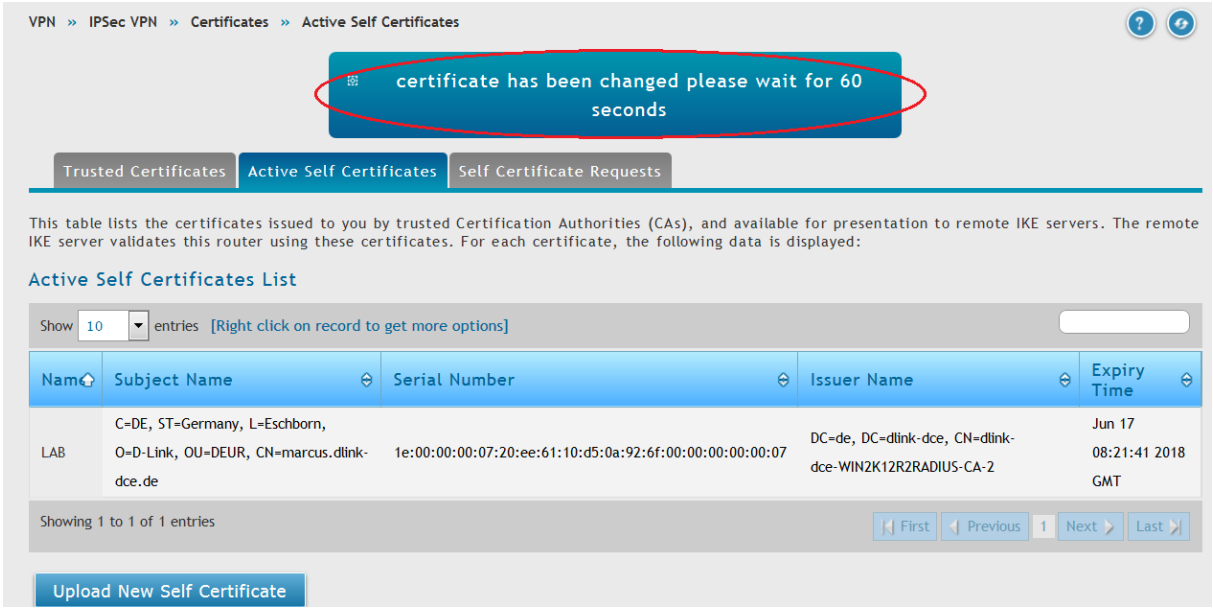
2. nach dem Upload sehen Sie die Daten Ihres gerade installierten Zertifikates

3. unter dem Menüpunkt Self Certificate Requests sehen Sie, dass Ihr Zertifikat aus dem CSR heraufgeladen wurde

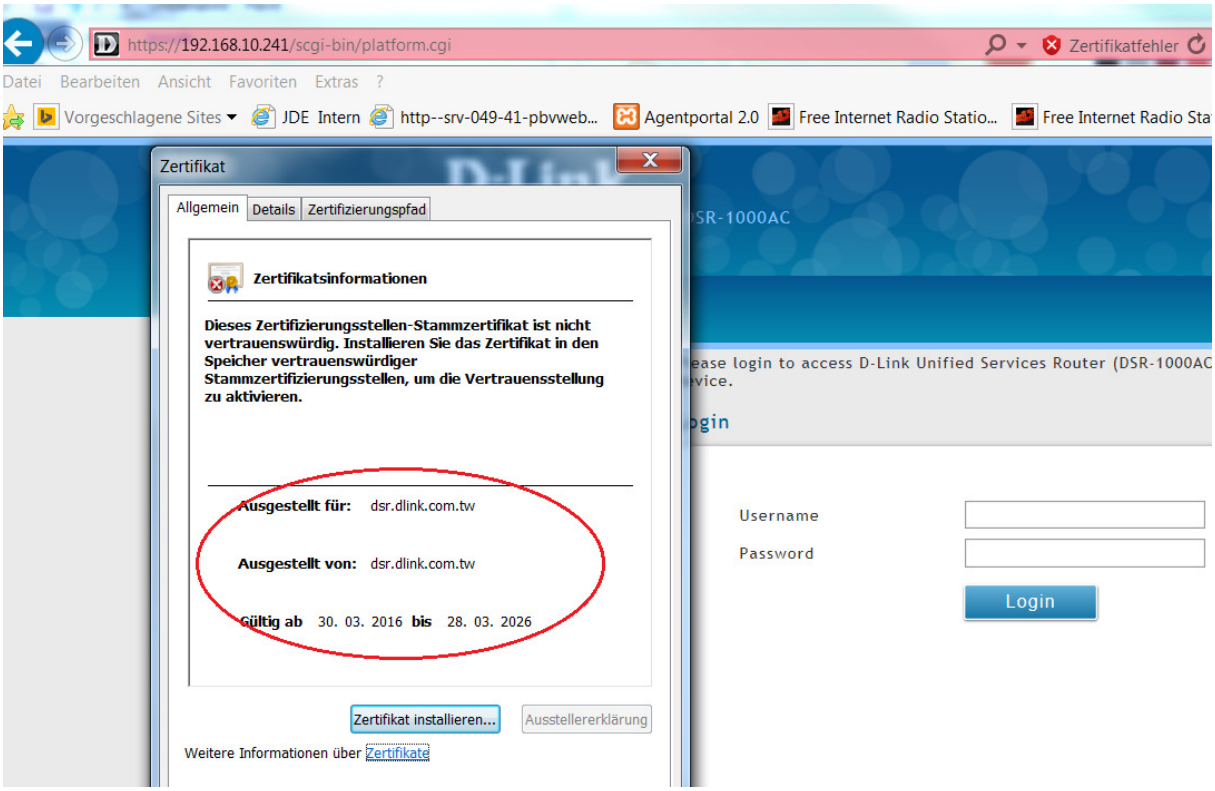


[Aktivieren des Zertifikates auf den DSR-1000AC]

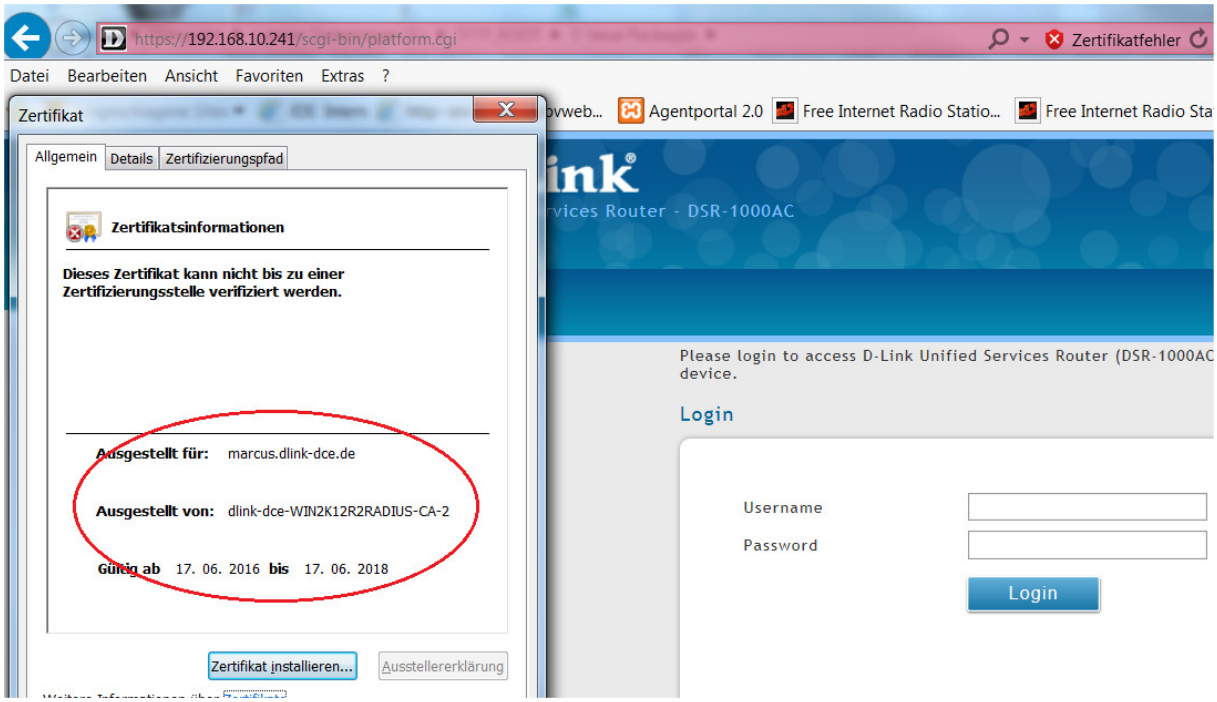
1. greifen Sie auf Ihren DSR-1000AC zu
   a. gehen Sie auf „VPN > Certificates > Active Self Certificares“
   b. klicken Sie mit der rechten Mausaste auf das Zertifikat und setzen dies als “Default”, damit es aktiv ist



Zertifikat vor der Aktivierung:



Zertifikat nach der Aktivierung:



Anschließend müssen sie das Zertifikat und ggfls. das CA-Stammzertifikat bei Ihren Clients installieren.