Zertifikat mit AD erzeugen

Wenn du eine **klassische AD-Zertifizierungsstelle** hast und **nur mit Windows-Bordmitteln** ein Zertifikat anfordern willst, geht das sehr stabil mit **certreq + certutil + openssl**. Damit bekommst du auch die drei Dateien (`.crt`, `.key`, `.chain.pem`), die Nginx Proxy Manager erwartet.

□□ Schritt-für-Schritt mit Windows Bordmitteln

1. Request-Datei erstellen

Erstelle eine INF-Datei, z. B. `request.inf`:

```
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=app.contoso.com"
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[Extensions]
```

```
2.5.29.17 = "{text}"
_continue_ = "dns=app.contoso.com&"
_continue_ = "dns=www.app.contoso.com"

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; Server Authentication
```

2. CSR erzeugen

```
certreq -new request.inf request.csr
```

3. Zertifikat bei der AD-CA beantragen

Falls dein Client Mitglied der Domäne ist und du Berechtigungen hast:

```
certreq -submit -config "CA-SERVER\CA-NAME" request.csr cert.cer
```

- `CA-SERVER\CA-NAME` ist deine AD-CA (findest du in der CA-Konsole).
- Ergebnis: `cert.cer` (dein Serverzertifikat).
- Private Keys liegen im Windows-Keystore.

4. In PFX exportieren

Zuerst Zertifikat in den Store importieren:

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

Dann per `certutil` mit privatem Schlüssel exportieren:

```
certutil -exportPFX -p SuperGeheimesPasswort My "CN=app.contoso.com" app.pfx
```

Jetzt hast du alles in `app.pfx`.

5. Aufsplitten in 3 Dateien

Windows kann kein `.pem` direkt erzeugen → hier kommt **OpenSSL** ins Spiel (kannst du von slproweb.com installieren).

```
# privater Schlüssel extrahieren
openssl pkcs12 -in app.pfx -nocerts -out privkey.pem -nodes -password pass:SuperGeheimesPasswort

# Zertifikat extrahieren
openssl pkcs12 -in app.pfx -clcerts -nokeys -out cert.pem -password pass:SuperGeheimesPasswort

# Kette (Root + Intermediate) extrahieren
openssl pkcs12 -in app.pfx -cacerts -nokeys -out chain.pem -password pass:SuperGeheimesPasswort
```

Damit hast du:

- `privkey.pem` → der private Schlüssel
- `cert.pem` → dein Serverzertifikat
- `chain.pem` → die Zwischen-/Root-Zertifikate

Diese drei Dateien kannst du dann im **Nginx Proxy Manager** unter „Custom SSL Certificate“ hochladen.

Zusammenfassung

- Mit **`certreq`** → CSR erzeugen und Zertifikat von AD CS holen
- Mit **`certutil`** → in PFX exportieren
- Mit **`openssl`** → in die drei Dateien (`privkey.pem`, `cert.pem`, `chain.pem`) zerlegen

Das ist der „saubere“ Microsoft-Weg, kein Gefrickel.

 Soll ich dir ein komplettes **PowerShell-Skript** bauen, das all diese Schritte (CSR → AD-CA → PFX → PEMs) automatisch abwickelt? Dann müsstest du nur einmal CN/Domains eintragen und hättest am Ende direkt die 3 Dateien im gewünschten Ordner.

Revision #1
Created 17 August 2025 12:49:40 by Stefan Mechler
Updated 17 August 2025 12:50:27 by Stefan Mechler