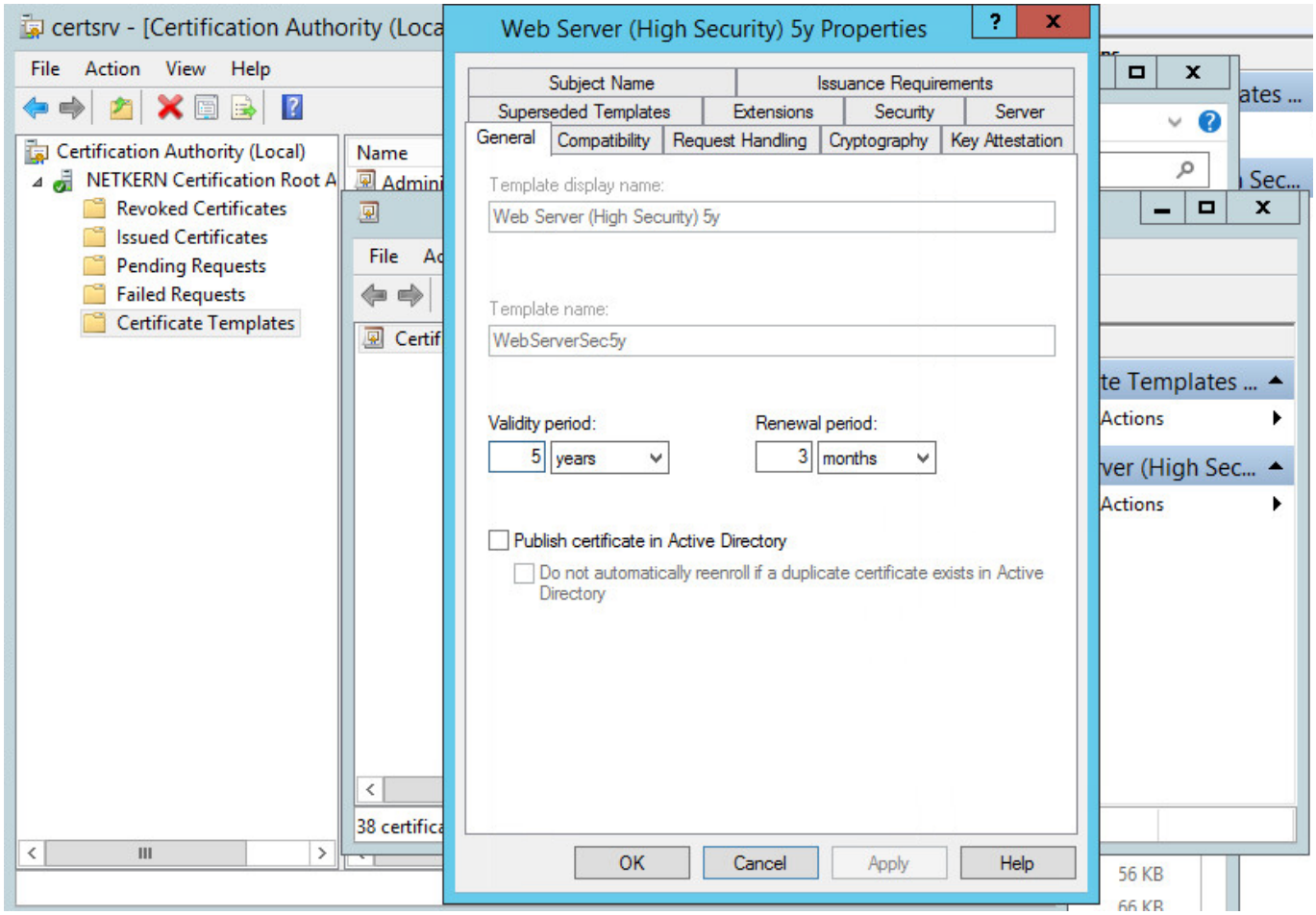
Windows CA: "The certificate validity period will be shorter..."

Author: Patrik Kernstock
Categories: Allgemein, Microsoft Windows, Tipps & Tricks
Date: 11. Juni 2016

Kurz notiert: Die **maximale Gültigkeitsdauer eines Zertifikates** ist **standardmäßig** seitens der Windows Zertifikatsstelle ("*Certification Authority*") **auf 2 Jahre beschränkt**. Wird eine Zertifikatsanforderung ("*Certificate Signing Request*") mit einer längeren Gültigkeitsdauer eingereicht, beschwert sich die Windows CA aufgrund der zu langen Dauer. Das Zertifikat wird zwar **dennoch erfolgreich ausgestellt**, jedoch **beschränkt** sich die **Gültigkeit** dieses Zertifikates dann auf die maximal zulässige Dauer.



Certificate Template mit 5 Jahren Gültigkeitsdauer

Ein Grund für eine längere Gültigkeitsdauer ist unter anderem, dass die Zertifikate weniger oft

auf den Zielsystemen gewechselt werden müssen. Spart natürlich ein wenig Arbeit ein. Jedoch sollte man vorab die Pro und Kontras diesbezüglich abwägen, **bevor** es zur **Umsetzung** geht - natürlich kommt es auch stark auf den geplanten Einsatzzweck an. Nicht vergessen: **Die Dauer des Zertifikates kann nicht die Dauer des Root-Zertifikates übersteigen**!

Die Antwort seitens der Certificate Authority von *certreq* fällt wie folgt aus:

```
C:\Users\Administrator>certreq
Active Directory Enrollment Policy
  {7E8A4907-B99D-4623-8602-308FC8E401A0}
  ldap:
RequestId: 33
RequestId: "33"
Certificate retrieved(Issued) Issued  The certificate validity period will be shorter than the WebServerSec5y Certificat
e Template specifies, because the template validity period is longer than the maximum certificate validity period allowe
d by the CA.  Consider renewing the CA certificate, reducing the template validity period, or increasing the registry va
lidity period.
```

Meldung aufgrund überschrittener Maximaldauer

> Certificate retrieved(Issued) Issued The certificate validity period will be shorter than the WebServerSec5y Certificate Template specifies, because the template validity period is longer than the maximum certificate validity period allowed by the CA. Consider renewing the CA certificate, reducing the template validity period, or increasing the registry validity period.

("WebServerSec5y" ist hierbei ein von mir selbst erstelltes CA-Template mit einer Gültigkeitsdauer von 5 Jahren)

Doch was wäre, wenn man dennoch länger gültige Zertifikate haben möchte?

Um nun Zertifikate mit einer längeren Dauer als 2 Jahren auszustellen, muss dazu der **Maximalwert** der Certification Authority in der Registry - genauer: den Wert "*ValidityPeriodUnits*" - **höher gesetzt werden**. Geht auch ganz fix - auch ohne manuelles Gesuche in der Registry.

Wert auslesen...

> certutil -getreg ca\ValidityPeriodUnits

```
C:\Users\Administrator>certutil -getreg ca\ValidityPeriodUnits
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\NETKE
RN Certification Root Authority X1\ValidityPeriodUnits:

  ValidityPeriodUnits REG_DWORD = 2
CertUtil: -getreg command completed successfully.
```

Aktuellen ValidityPeriodUnits-Wert auslesen

Wert auf 5 Jahre setzen...

certutil -setreg ca\ValidityPeriodUnits 5

```
C:\Users\Administrator>certutil -setreg ca\ValidityPeriodUnits 5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\NETKE
RN Certification Root Authority X1\ValidityPeriodUnits:

Old Value:
  ValidityPeriodUnits REG_DWORD = 2

New Value:
  ValidityPeriodUnits REG_DWORD = 5
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

ValidityPeriodUnits auf 5 setzen

Zur Kontrolle erneut prüfen...

certutil -getreg ca\ValidityPeriodUnits

```
C:\Users\Administrator>certutil -getreg ca\ValidityPeriodUnits
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\NETKE
RN Certification Root Authority X1\ValidityPeriodUnits:

  ValidityPeriodUnits REG_DWORD = 5
CertUtil: -getreg command completed successfully.
```

Aktuellen ValidityPeriodUnits-Wert prüfen

Abschließen nicht vergessen: Zur Übernahme der eben vorgenommen Änderungen **muss der Zertifikatsdienst neugestartet werden**! Die Einstellung wird zwar in der Registry geändert, jedoch zeigt diese Änderung erst nach dem Neustart Wirkung.