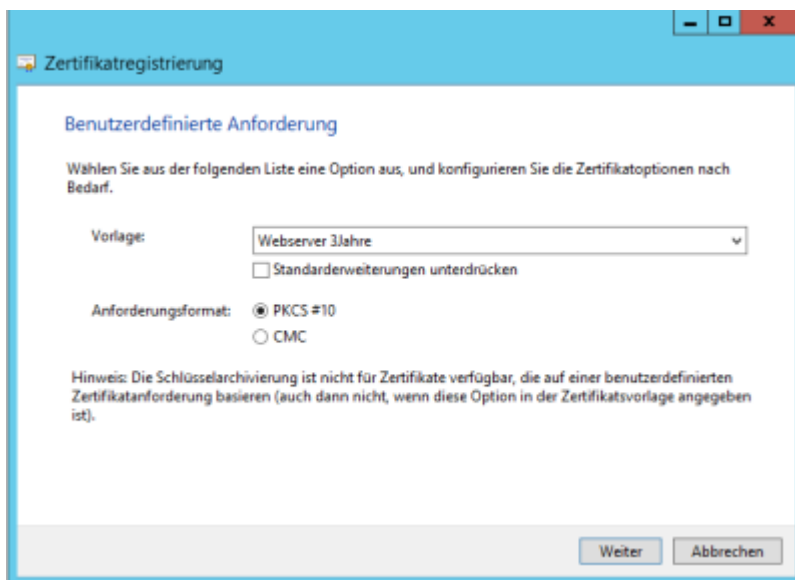
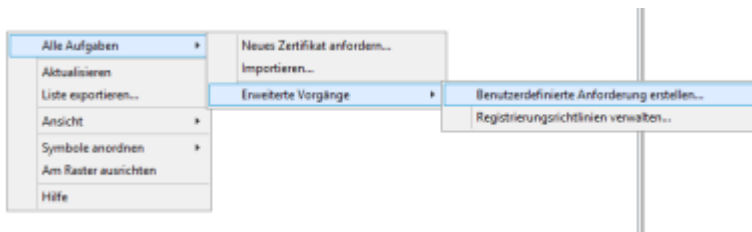


Active Directory Webserver Zertifikat

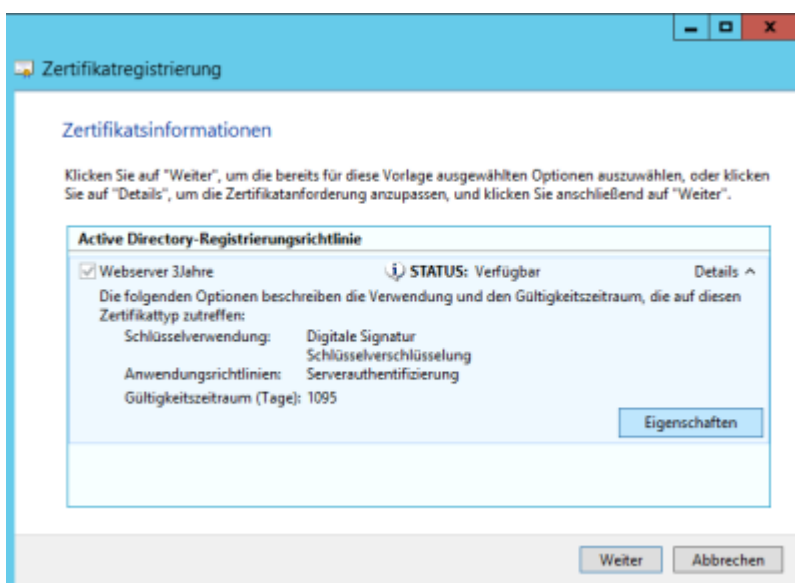
Zertifikat erstellen

Zunächst über Ausführen die „mmc“ öffnen, und das Zertifikate Snap-In für das Computerkonto hinzufügen.

Unter den eigenen Zertifikaten einen Rechtsklick machen und eine „Benutzerdefinierte Anforderung erstellen, als Vorlage wird Webserver 3Jahre verwendet.



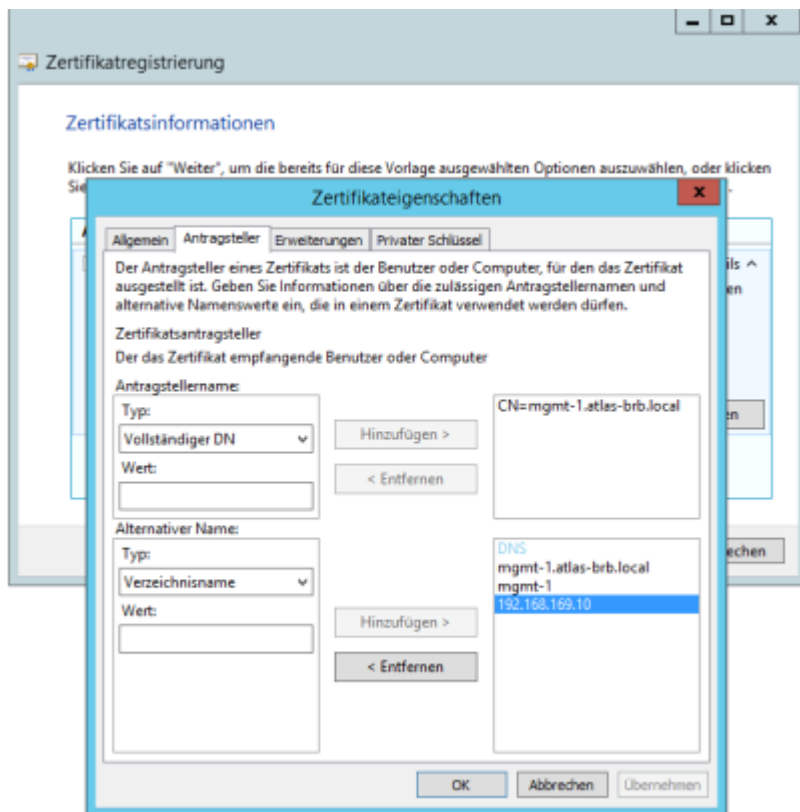
In dieser Ansicht auf den kleinen Pfeil bei „Details“ klicken und auf den Button Eigenschaften.



In diesem Fenster wird der Allgemeine Name (Common Name) = FQDN des Servers eingetragen,

zusätzlich werden in den Alternativen Namen der FQDN, der Shortname, sowie die IP-Adresse eingetragen.

Beim Speichern der Zertifikatanforderung, wird das Zertifikat als Base64 kodierte Datei gespeichert.



Zertifikat in der CA signieren

Die Base64 kodierte Zertifikatsanforderung wird nun als Text kopiert (z.B. mittels Notepad++), auf dem Zertifikatsdienste Server nun die **certsrv** URL öffnen, und eine erweiterte Zertifikatanforderung erstellen.

Ist das signieren des Zertifikats abgeschlossen, muss nun die Zertifikatskette (.p7b Datei) heruntergeladen

und auf dem Zielsystem in den Eigenen Zertifikaten des Computerkontos importiert werden.



Zertifikat im IIS einspielen

Um das Zertifikat im IIS einzuspielen, wird der IIS Manager gestartet und die entsprechende Site ausgewählt.

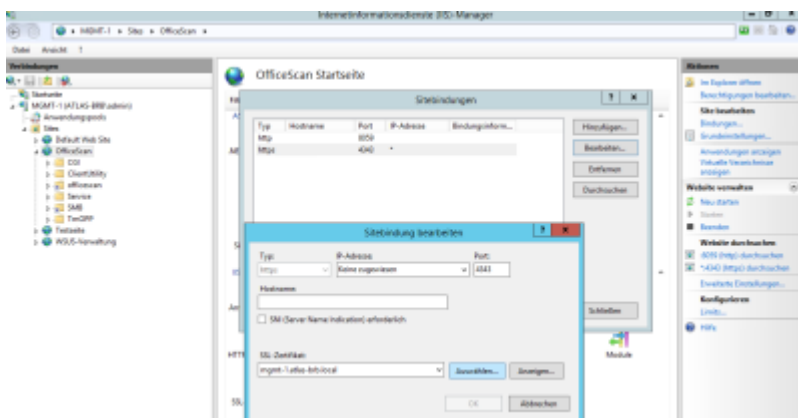
Im Menü-Baum rechts öffnet man die Bindungen.

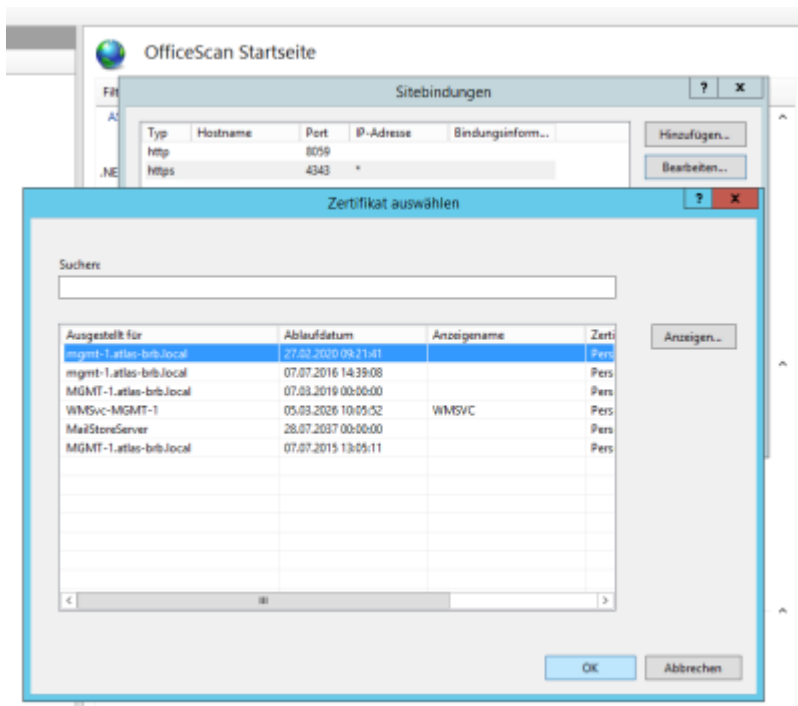
Nun wählt man die entsprechende **https** Bindung aus und klickt auf **Bearbeiten**.

Unter **SSL-Zertifikat** noch ein Klick auf **Auswählen** und im sich öffnenden Fenster das entsprechende Zertifikat auswählen.

Alle Fenster mit OK schließen und im rechten Menü der ausgewählten Site auf **Neustarten** klicken.

Fertig!





From: <http://dokuwiki.atlas-brb.net/> - Wissensdatenbank

Permanent link: http://dokuwiki.atlas-brb.net/doku.php?id=windows_server:zertifikatdienste:webserver&rev=1519728367

Last update: 2018/02/27 11:46

