Auto-Enrollment RDP Zertifikate mit IP

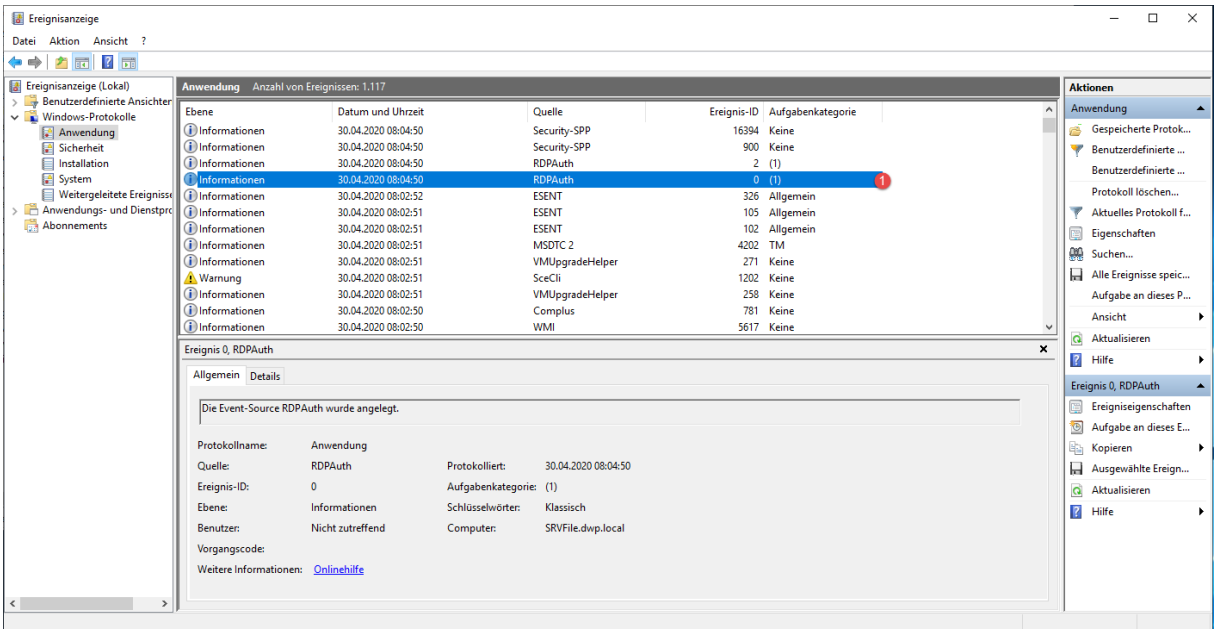
Das Ziel ist es, jedes Windows System mit einem Remote Desktop Zertifikat auszustatten. Bei der Nutzung des automatischen Enrollments, wird leider kein Subject Alternative Name eingetragen, wie z.B. die IP-Adresse.

Somit habe ich für mich eine gangbare Lösung gefunden, dieses Problem zu lösen. Es geht mich Sicherheit auch anders und vielleicht auch schicker, aber irgendjemand muss ja bekanntlich den Anfang machen.

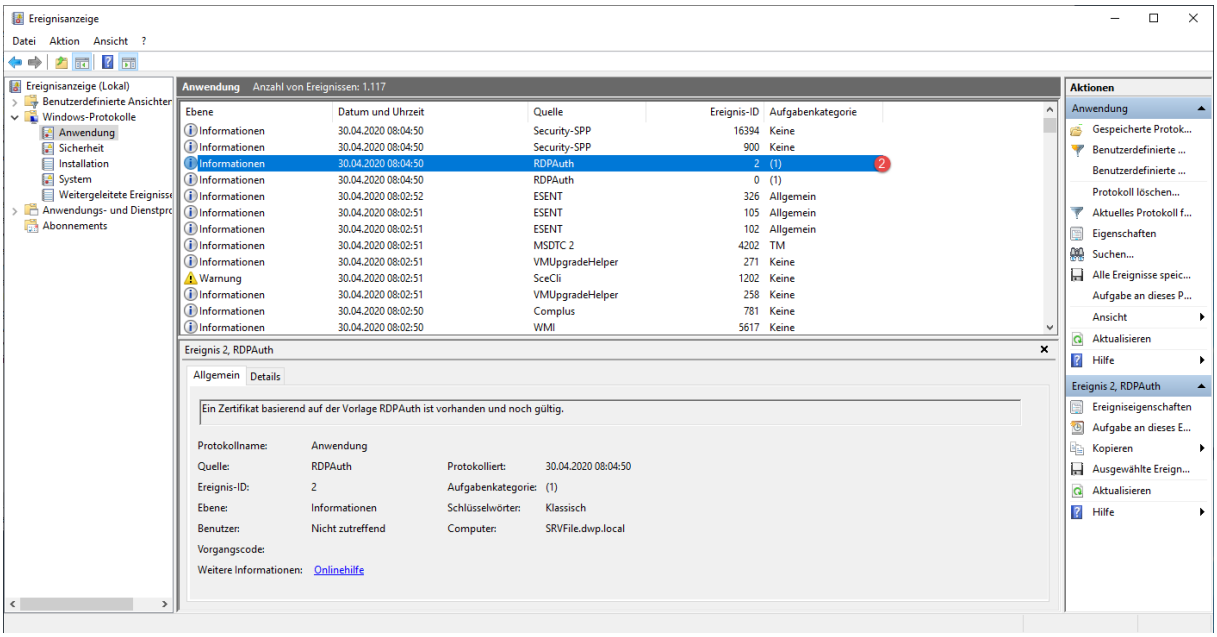
Bei der Umsetzung hatte ich einen großartigen Tippgeber. Vielen Dank an Martin F.

Umsetzung:

Damit das Skript wichtige Aktivitäten ins Logbuch schreiben kann, erstellen wir zuerst eine neue Event-Source namens RDPAuth.

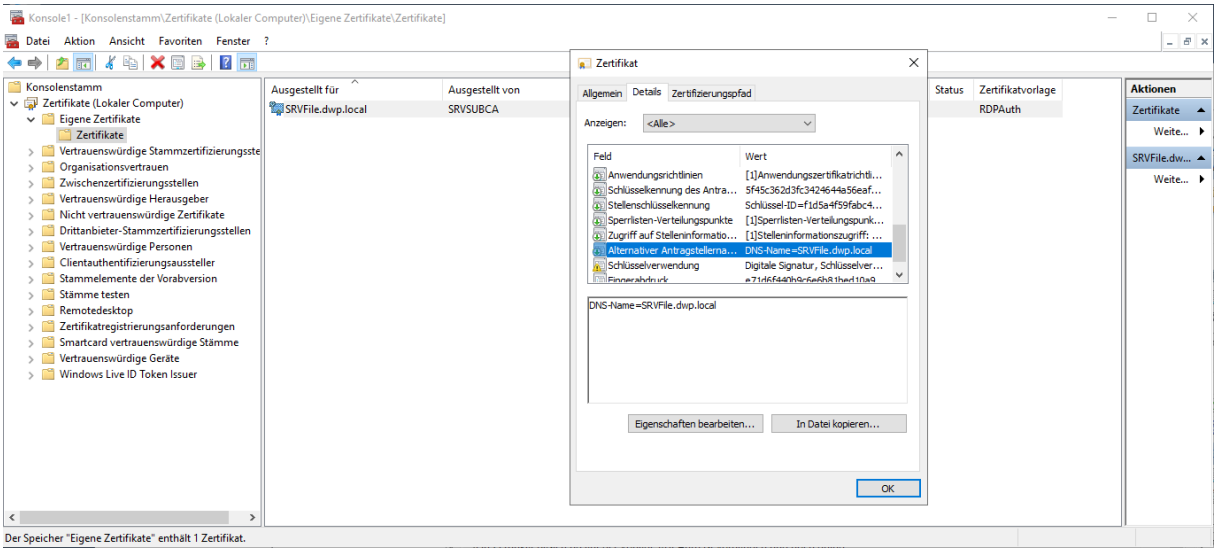


Als erstes prüft das Skript, ob sich ein Zertifikat auf dem System befindet und noch gültig ist.

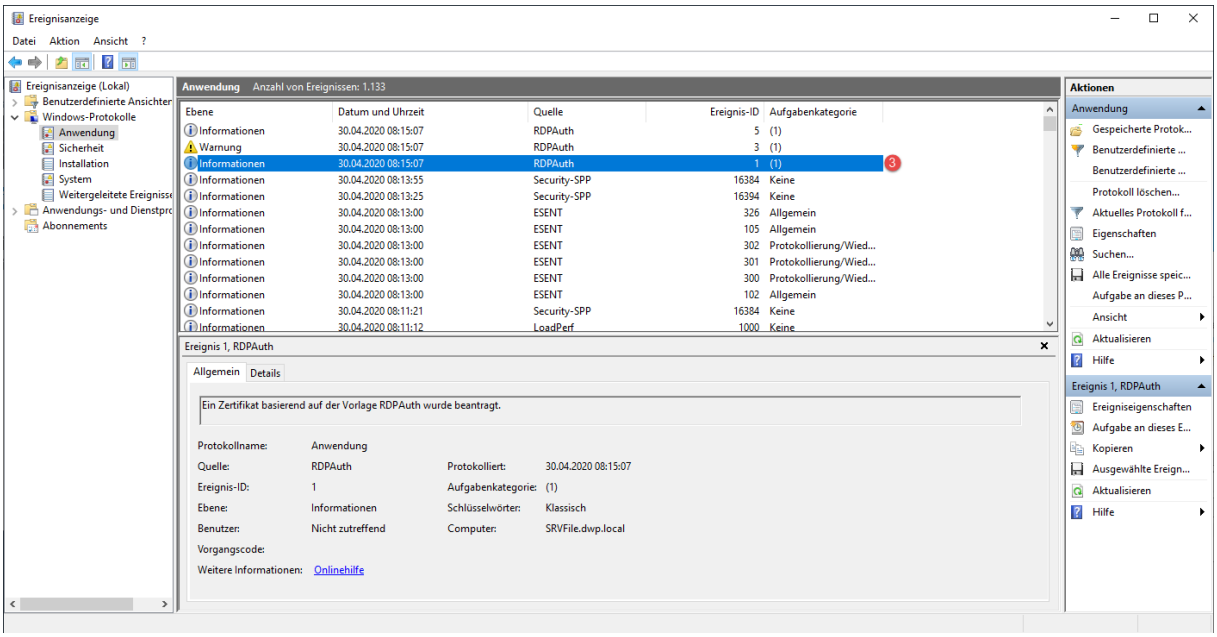


Auto-Enrollment RDP Zertifikate mit IP

Das aktuelle Zertifikat stammt aus dem automatischen Enrollment.
Es ist keine IP-Adresse hinterlegt. ;-(

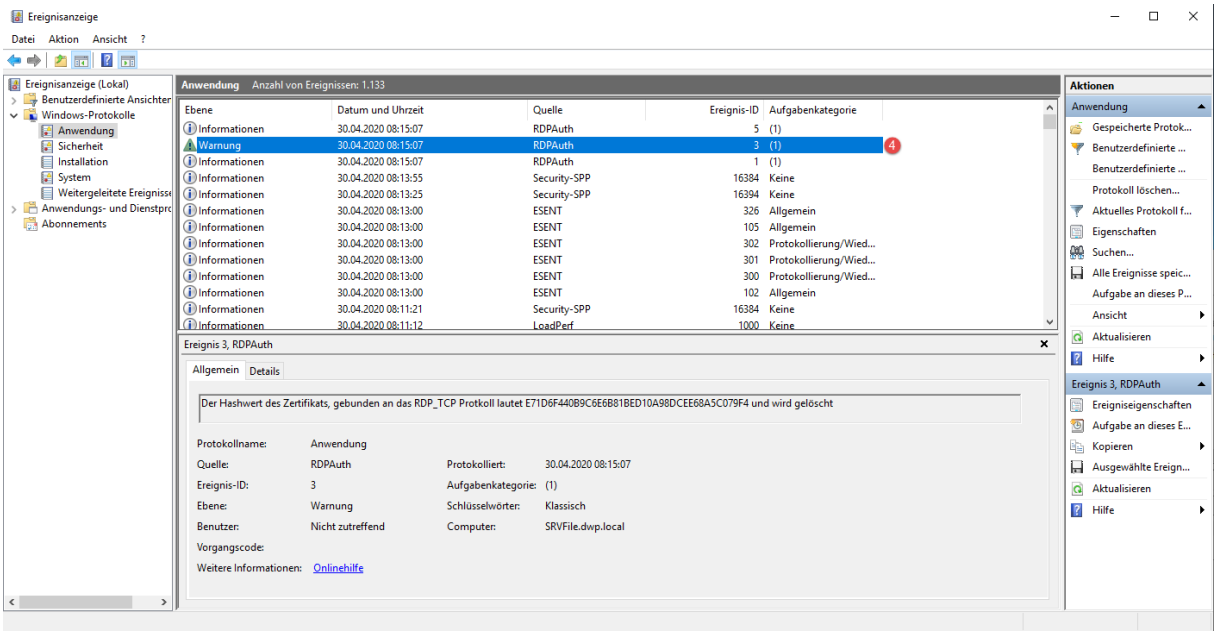


Ist das aktuelle im System vorhandene Zertifikat nur noch 3 Tage gültig oder nicht vorhanden, startet der Prozess zur Beantragung eines „neuen" Zertifikats.

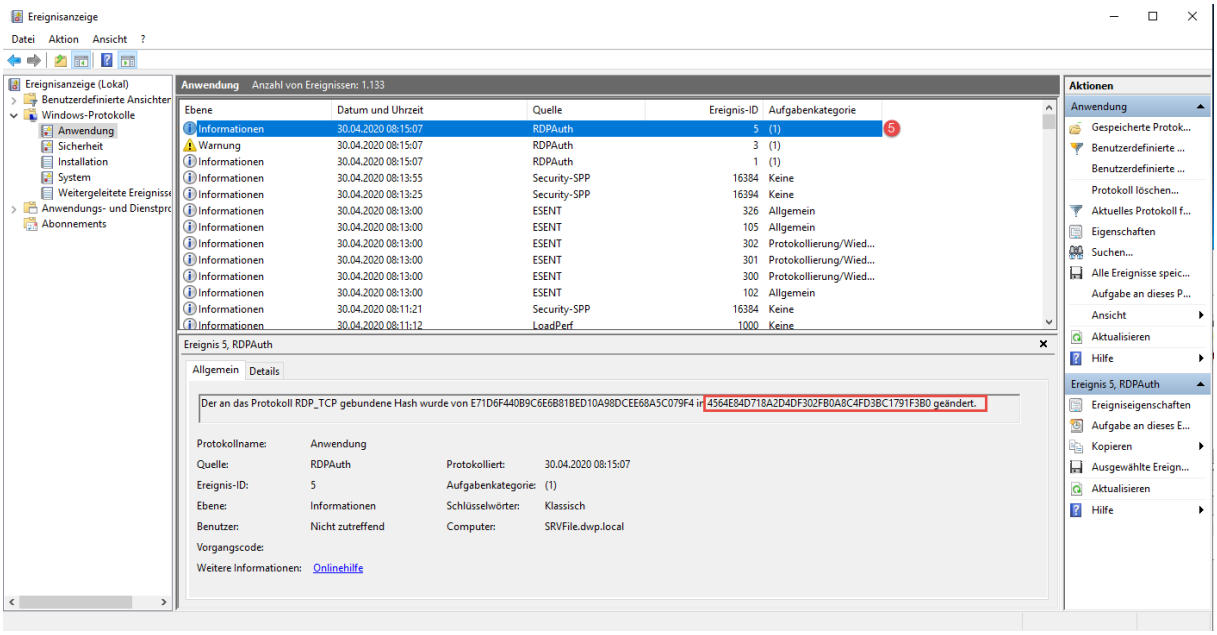


Auto-Enrollment RDP Zertifikate mit IP

Sobald das neue Zertifikat auf dem System vorhanden ist, wird anhand des Thumbprints verglichen, welches Zertifikat aktuell an das RDP_TCP Protokoll gebunden ist. Neu oder alt. Ist es das alte so wird es aus dem Computerspeicher gelöscht

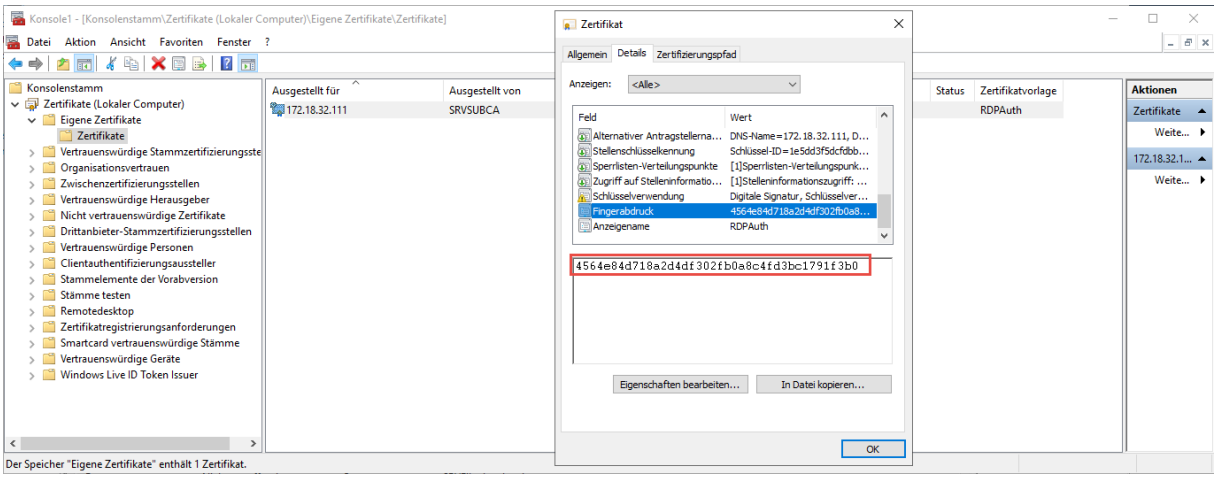


Danach wird das neue Zertifikat (F3B0) an das RDP_TCP Protkoll gebunden.

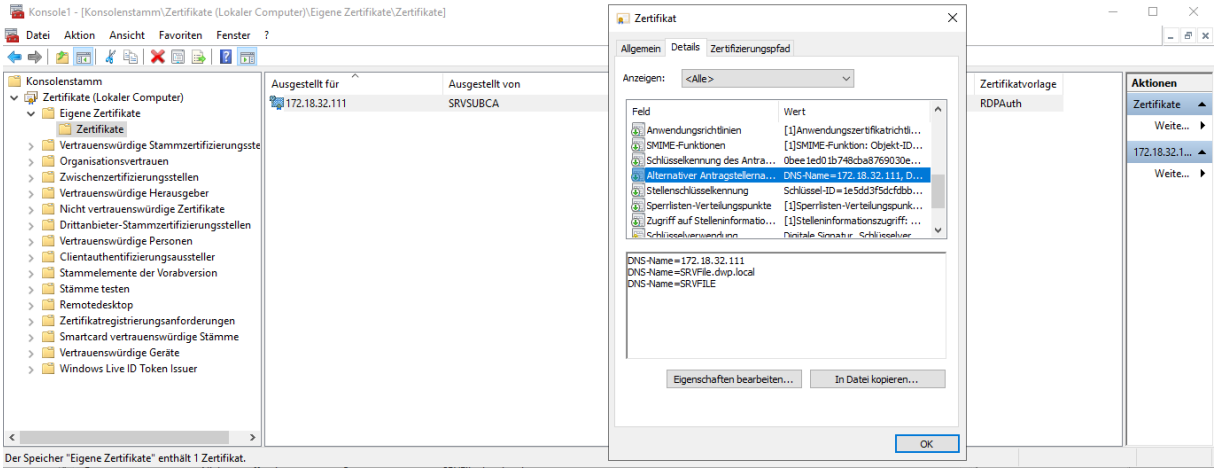


Auto-Enrollment RDP Zertifikate mit IP

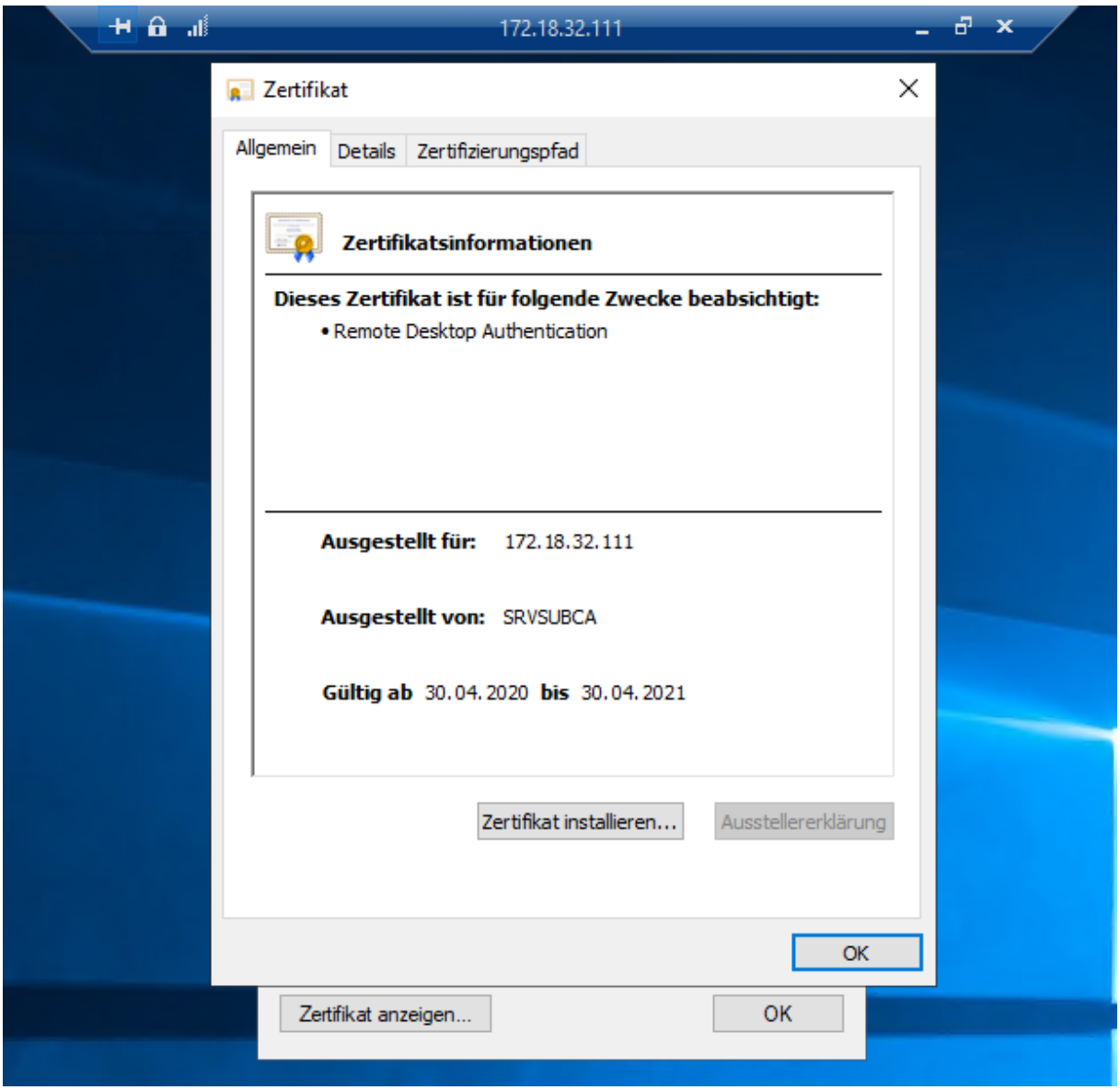
Werfen wir einen Blick auf das neue Zertifkat. Es endet mit F3B0.



Im SAN sehen wir nun die 3 Attribute IP, FQDN, DN.



Somit hat die Zertifikatswarnung ihr Ende gefunden. 😉



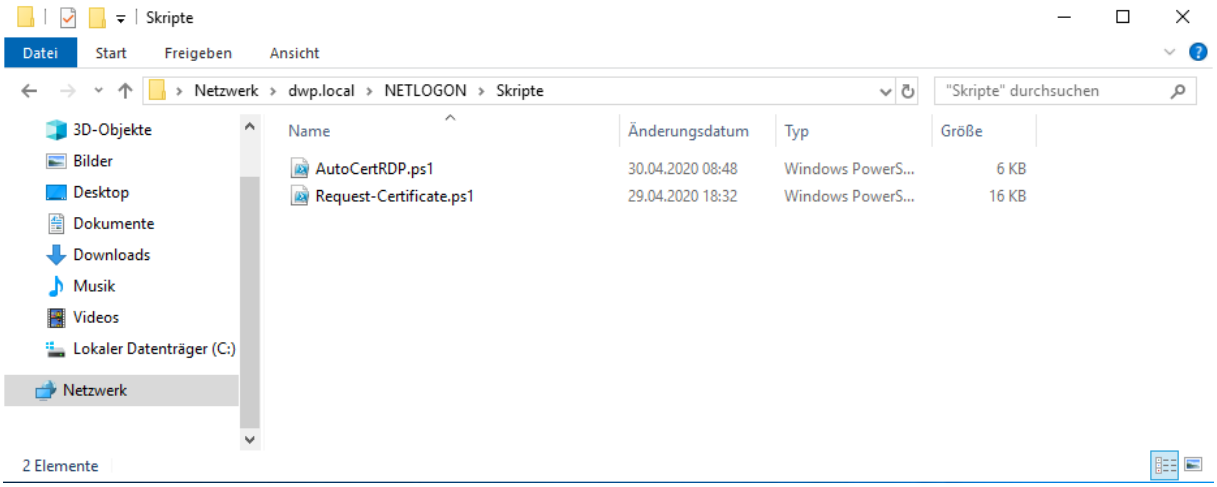
Im Skript habe ich alles an Schritten beschrieben, so dass meine Gedankengänge nachvollziehbar sind.

Wenn jemand Vorschläge zur Verbesserung hat, immer gern!

Auto-Enrollment RDP Zertifikate mit IP

Vorbereitung:

Der gesamte Prozess besteht aus 2 Skripten, die zusammen in einem Verzeichnis liegen sollten.

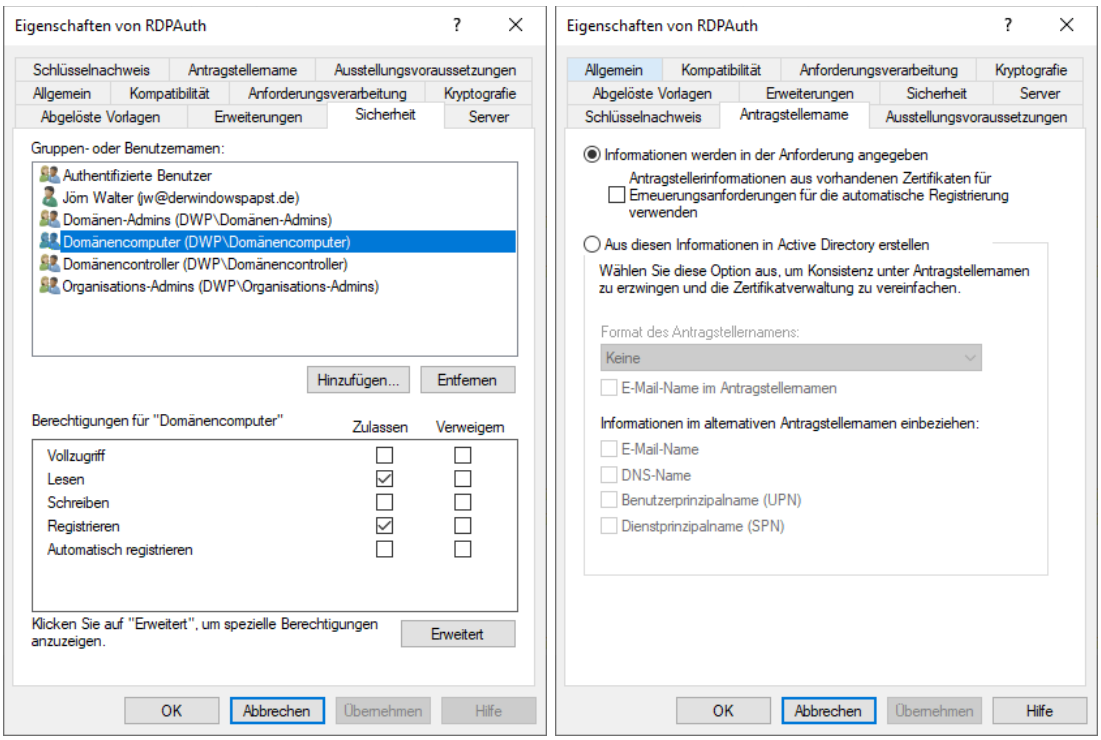


Quelle des 2. Skripts:

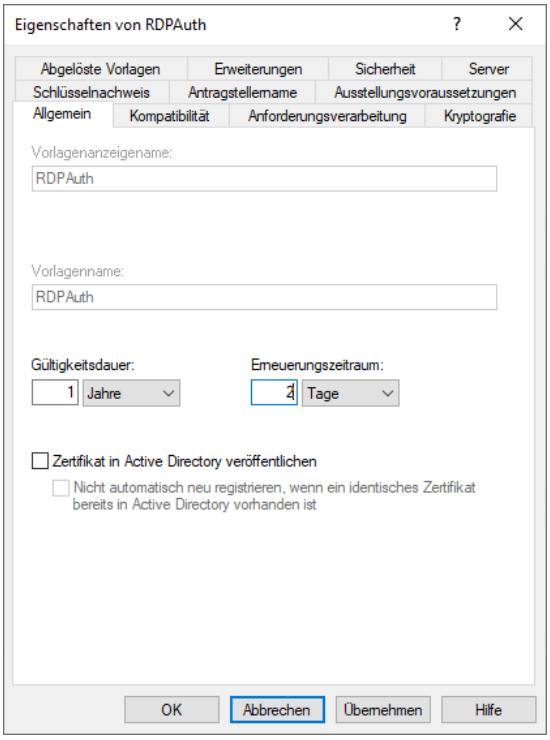
https://github.com/J0F3/PowerShell/blob/master/Request-Certificate.ps1

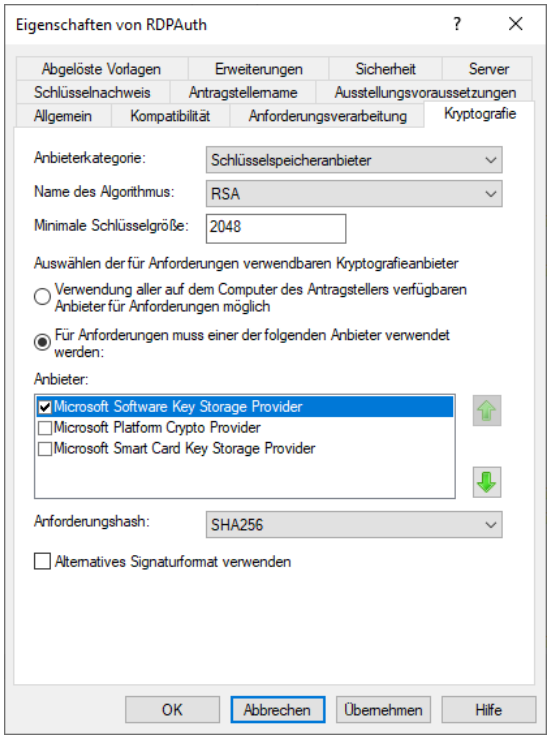
Schritt 1:

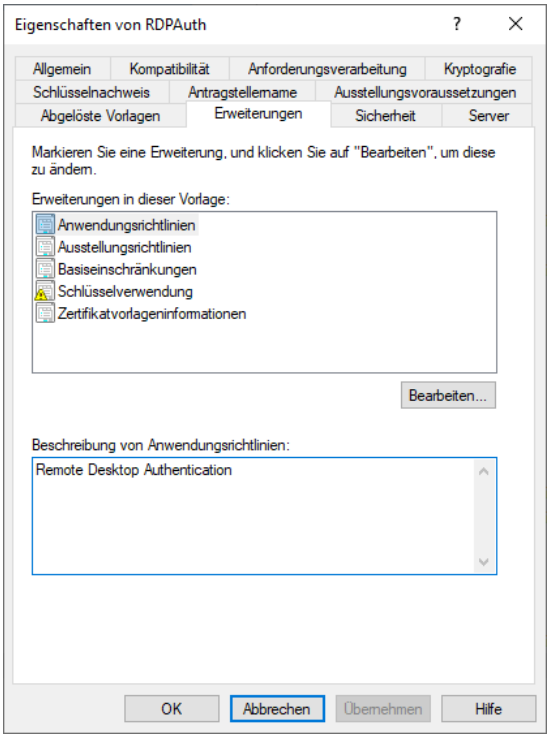
Erstellen einer Zertifikatvorlage mit entsprechenden Berechtigungen für Domänencomputer und Domänencontroller.



Auto-Enrollment RDP Zertifikate mit IP





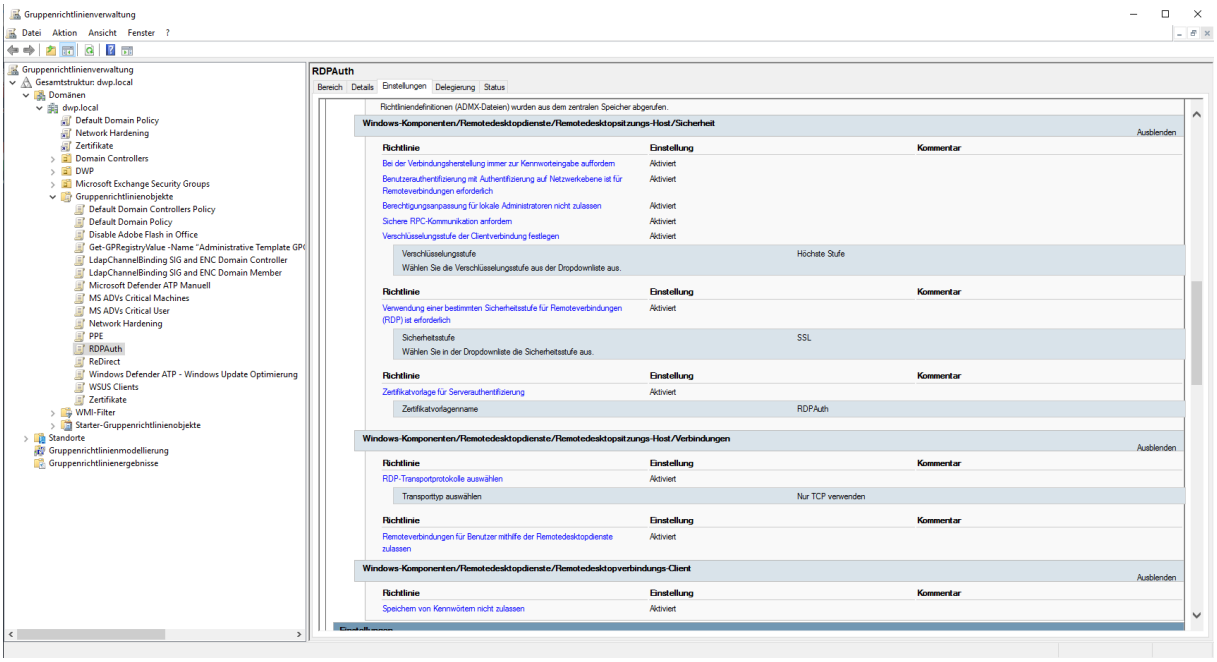


Erstellt von Jörn Walter **30.04.2020**

Auto-Enrollment RDP Zertifikate mit IP

Schritt 2:

Erstellen einer Gruppenrichtlinie zur Erstellung einer geplanten (täglichen) Aufgabe auf jedem Windows-System.



-NoProfile -ExecutionPolicy bypass -File \\dwp.local\NETLOGON\Skripte\AutoCertRDP.ps1

Den Task hatte ich zum Testen auf alle „5 Minuten" gestellt.