



## 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.

The screenshot shows the Windows Event Viewer window. The left pane shows the 'Anwendung' (Application) log. The main pane displays a list of events. The event 'Ereignis 0, RDPAuth' is selected, and its details are shown in the right pane. The details indicate that the event source 'RDPAuth' was successfully created.

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	30.04.2020 08:04:50	Security-SPP	16394	Keine
Informationen	30.04.2020 08:04:50	Security-SPP	900	Keine
Informationen	30.04.2020 08:04:50	RDPAuth	2 (1)	Keine
Informationen	30.04.2020 08:04:50	RDPAuth	0 (1)	Keine
Informationen	30.04.2020 08:02:52	ESENT	326	Allgemein
Informationen	30.04.2020 08:02:51	ESENT	105	Allgemein
Informationen	30.04.2020 08:02:51	ESENT	102	Allgemein
Informationen	30.04.2020 08:02:51	MSDTC 2	4202	TM
Informationen	30.04.2020 08:02:51	VMUpgradeHelper	271	Keine
Warnung	30.04.2020 08:02:51	SecCli	1202	Keine
Informationen	30.04.2020 08:02:51	VMUpgradeHelper	258	Keine
Informationen	30.04.2020 08:02:50	Complus	781	Keine
Informationen	30.04.2020 08:02:50	WMI	5617	Keine

**Ereignis 0, RDPAuth**

Allgemein Details

Die Event-Source RDPAuth wurde angelegt.

Protokollname: Anwendung  
Quelle: RDPAuth  
Ereignis-ID: 0  
Ebene: Informationen  
Benutzer: Nicht zutreffend  
Vorgangscode:  
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 30.04.2020 08:04:50  
Aufgabenkategorie: (1)  
Schlüsselwörter: Klassisch  
Computer: SRVFile.dwp.local

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

The screenshot shows the Windows Event Viewer window. The left pane shows the 'Anwendung' (Application) log. The main pane displays a list of events. The event 'Ereignis 2, RDPAuth' is selected, and its details are shown in the right pane. The details indicate that a valid certificate based on the RDPAuth template is present on the system.

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	30.04.2020 08:04:50	Security-SPP	16394	Keine
Informationen	30.04.2020 08:04:50	Security-SPP	900	Keine
Informationen	30.04.2020 08:04:50	RDPAuth	2 (1)	Keine
Informationen	30.04.2020 08:04:50	RDPAuth	0 (1)	Keine
Informationen	30.04.2020 08:02:52	ESENT	326	Allgemein
Informationen	30.04.2020 08:02:51	ESENT	105	Allgemein
Informationen	30.04.2020 08:02:51	ESENT	102	Allgemein
Informationen	30.04.2020 08:02:51	MSDTC 2	4202	TM
Informationen	30.04.2020 08:02:51	VMUpgradeHelper	271	Keine
Warnung	30.04.2020 08:02:51	SecCli	1202	Keine
Informationen	30.04.2020 08:02:51	VMUpgradeHelper	258	Keine
Informationen	30.04.2020 08:02:50	Complus	781	Keine
Informationen	30.04.2020 08:02:50	WMI	5617	Keine

**Ereignis 2, RDPAuth**

Allgemein Details

Ein Zertifikat basierend auf der Vorlage RDPAuth ist vorhanden und noch gültig.

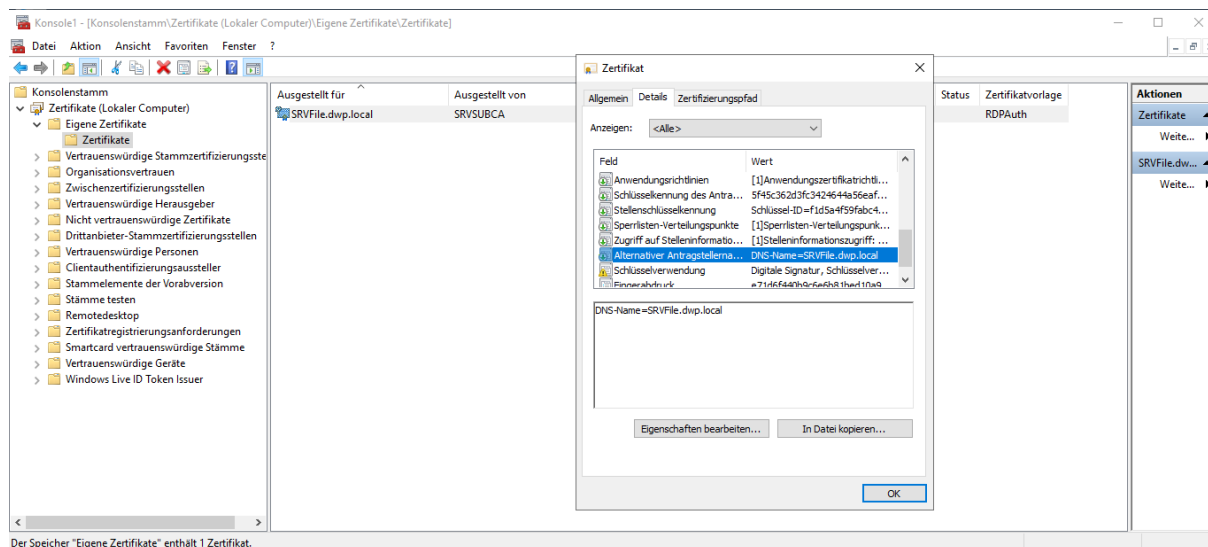
Protokollname: Anwendung  
Quelle: RDPAuth  
Ereignis-ID: 2  
Ebene: Informationen  
Benutzer: Nicht zutreffend  
Vorgangscode:  
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 30.04.2020 08:04:50  
Aufgabenkategorie: (1)  
Schlüsselwörter: Klassisch  
Computer: SRVFile.dwp.local

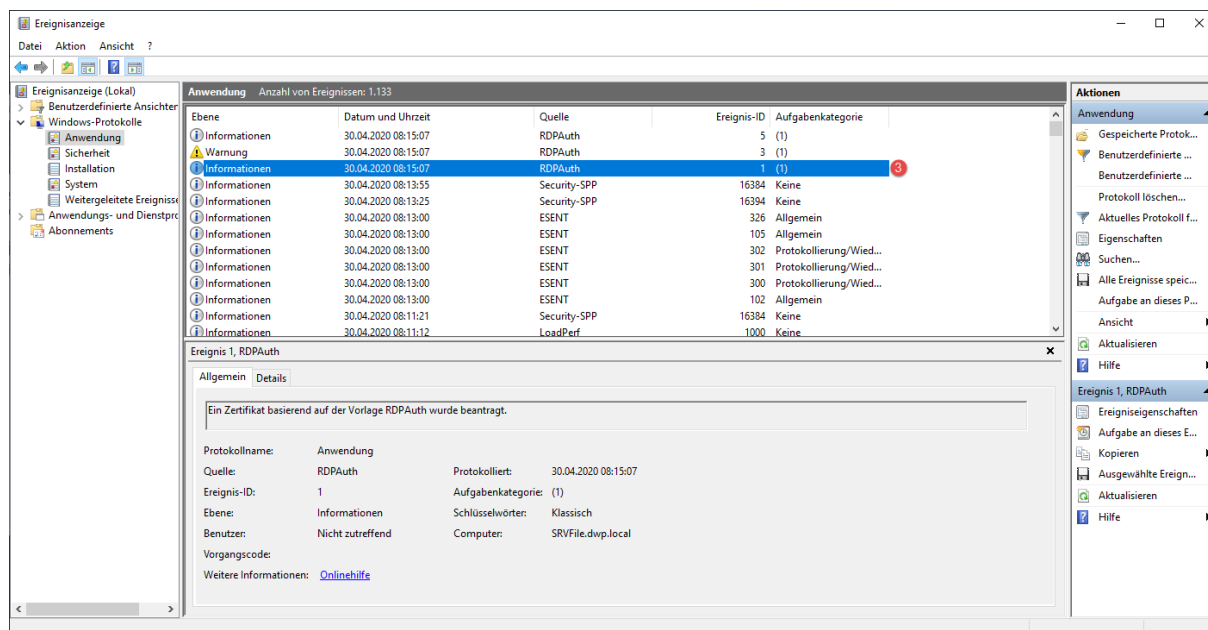


## Auto-Enrollment RDP Zertifikate mit IP

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

Event Viewer (Ereignisanzeige) - Windows-Protokolle > Sicherheit > System > Weitergeleitete Ereignisse > Anwendungs- und Dienstprotokolle > Abonnement

Event 3, RDPAuth

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	30.04.2020 08:15:07	RDPAuth	5 (1)	
Warnung	30.04.2020 08:15:07	RDPAuth	3 (1)	
Informationen	30.04.2020 08:15:07	RDPAuth	1 (1)	
Informationen	30.04.2020 08:13:55	Security-SPP	16384	Keine
Informationen	30.04.2020 08:13:25	Security-SPP	16394	Keine
Informationen	30.04.2020 08:13:00	ESENT	326	Allgemein
Informationen	30.04.2020 08:13:00	ESENT	105	Allgemein
Informationen	30.04.2020 08:13:00	ESENT	302	Protokollierung/Wied...
Informationen	30.04.2020 08:13:00	ESENT	301	Protokollierung/Wied...
Informationen	30.04.2020 08:13:00	ESENT	300	Protokollierung/Wied...
Informationen	30.04.2020 08:13:00	ESENT	102	Allgemein
Informationen	30.04.2020 08:11:21	Security-SPP	16384	Keine
Informationen	30.04.2020 08:11:12	LoadPerf	1000	Keine

Der Hashwert des Zertifikats, gebunden an das RDP\_TCP Protokoll lautet E71D6F440B9C6E6B81BED10A98DCEE6A5C079F4 und wird gelöscht

Protokollname: Anwendung  
Quelle: RDPAuth  
Ereignis-ID: 3  
Ebene: Warnung  
Benutzer: Nicht zutreffend  
Vorgangscode:  
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 30.04.2020 08:15:07  
Aufgabenkategorie: (1)  
Schlüsselwörter: Klassisch  
Computer: SRVFile.dwp.local

Danach wird das neue Zertifikat (F3B0) an das RDP\_TCP Protokoll gebunden.

Event Viewer (Ereignisanzeige) - Windows-Protokolle > Sicherheit > System > Weitergeleitete Ereignisse > Anwendungs- und Dienstprotokolle > Abonnement

Event 5, RDPAuth

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	30.04.2020 08:15:07	RDPAuth	5 (1)	
Warnung	30.04.2020 08:15:07	RDPAuth	3 (1)	
Informationen	30.04.2020 08:15:07	RDPAuth	1 (1)	
Informationen	30.04.2020 08:13:55	Security-SPP	16384	Keine
Informationen	30.04.2020 08:13:25	Security-SPP	16394	Keine
Informationen	30.04.2020 08:13:00	ESENT	326	Allgemein
Informationen	30.04.2020 08:13:00	ESENT	105	Allgemein
Informationen	30.04.2020 08:13:00	ESENT	302	Protokollierung/Wied...
Informationen	30.04.2020 08:13:00	ESENT	301	Protokollierung/Wied...
Informationen	30.04.2020 08:13:00	ESENT	300	Protokollierung/Wied...
Informationen	30.04.2020 08:13:00	ESENT	102	Allgemein
Informationen	30.04.2020 08:11:21	Security-SPP	16384	Keine
Informationen	30.04.2020 08:11:12	LoadPerf	1000	Keine

Der an das Protokoll RDP\_TCP gebundene Hash wurde von E71D6F440B9C6E6B81BED10A98DCEE6A5C079F4 in 4564E84D718A2D4DF302F80A8C4FD3BC1791F3B0 geändert.

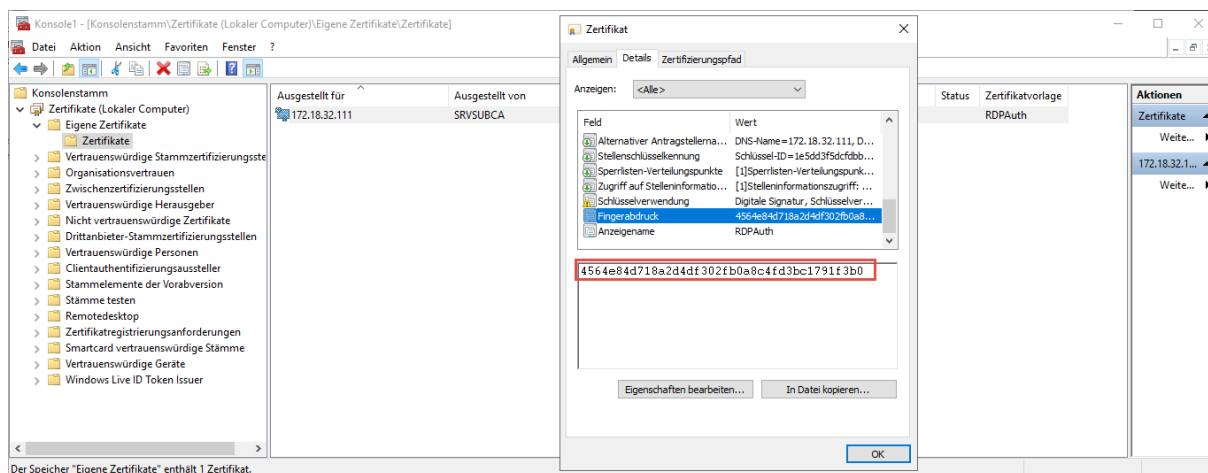
Protokollname: Anwendung  
Quelle: RDPAuth  
Ereignis-ID: 5  
Ebene: Informationen  
Benutzer: Nicht zutreffend  
Vorgangscode:  
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 30.04.2020 08:15:07  
Aufgabenkategorie: (1)  
Schlüsselwörter: Klassisch  
Computer: SRVFile.dwp.local

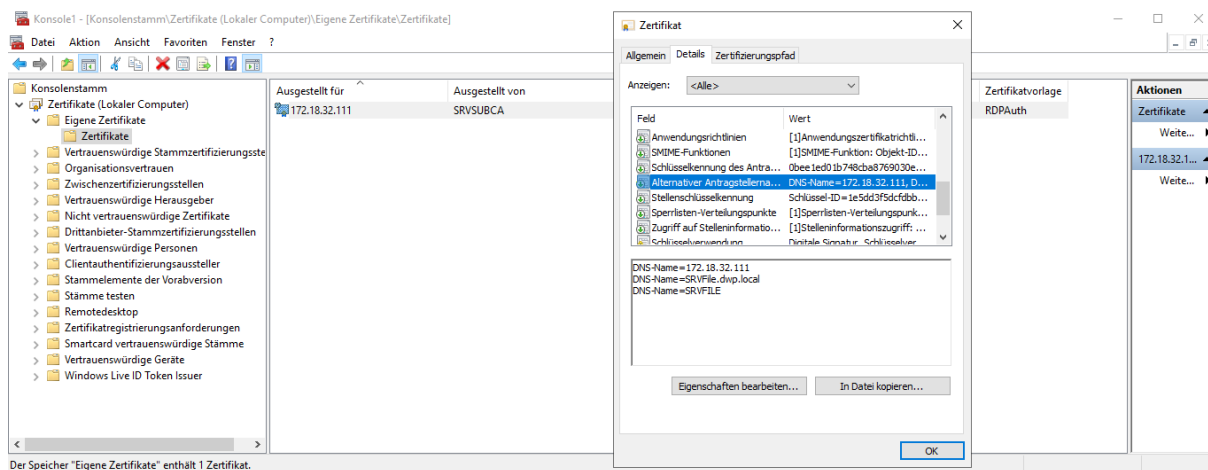


## Auto-Enrollment RDP Zertifikate mit IP

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



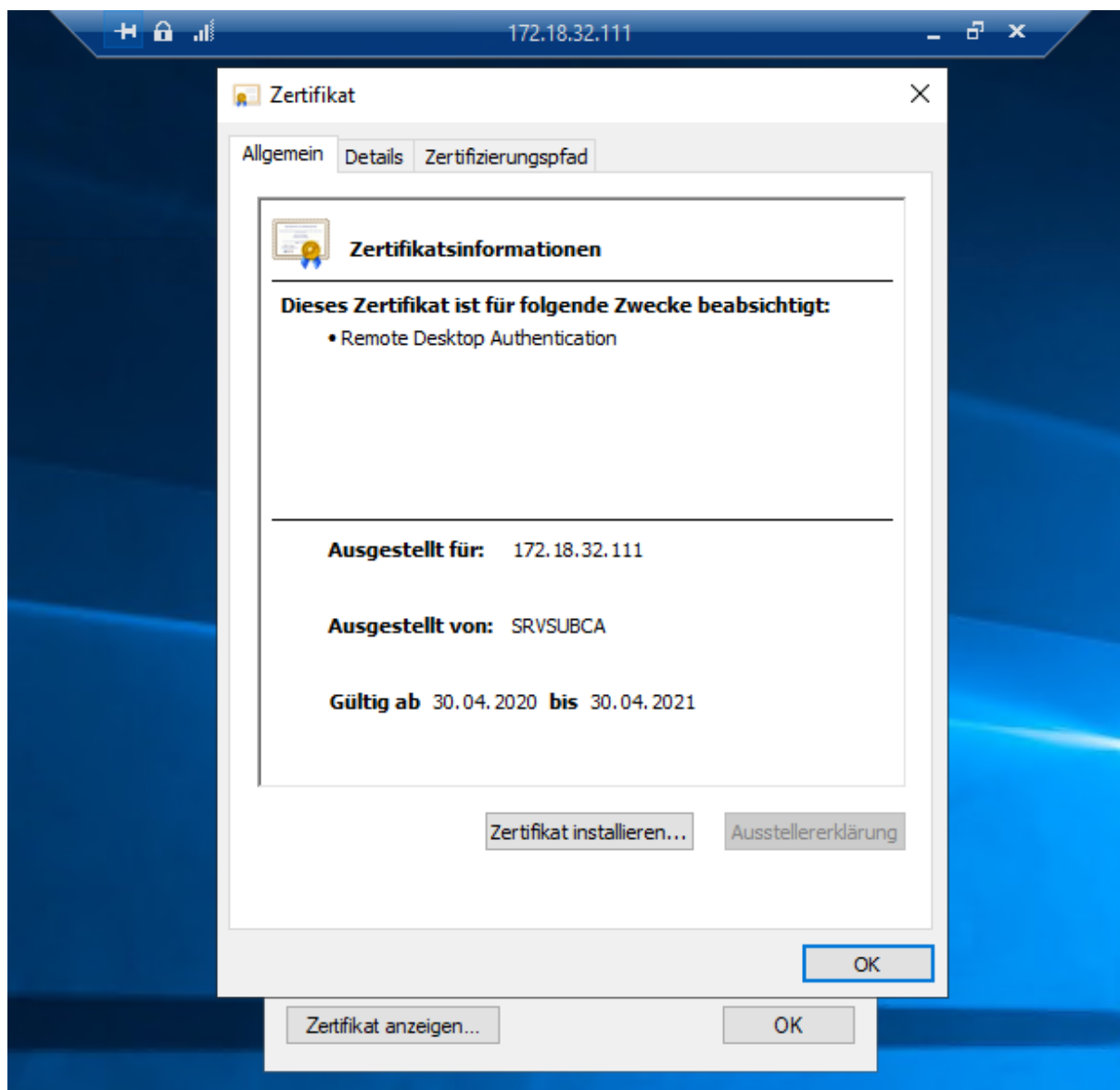
Im SAN sehen wir nun die 3 Attribute IP, FQDN, DN.





## Auto-Enrollment RDP Zertifikate mit IP

Somit hat die Zertifikatswarnung ihr Ende gefunden. 😊



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

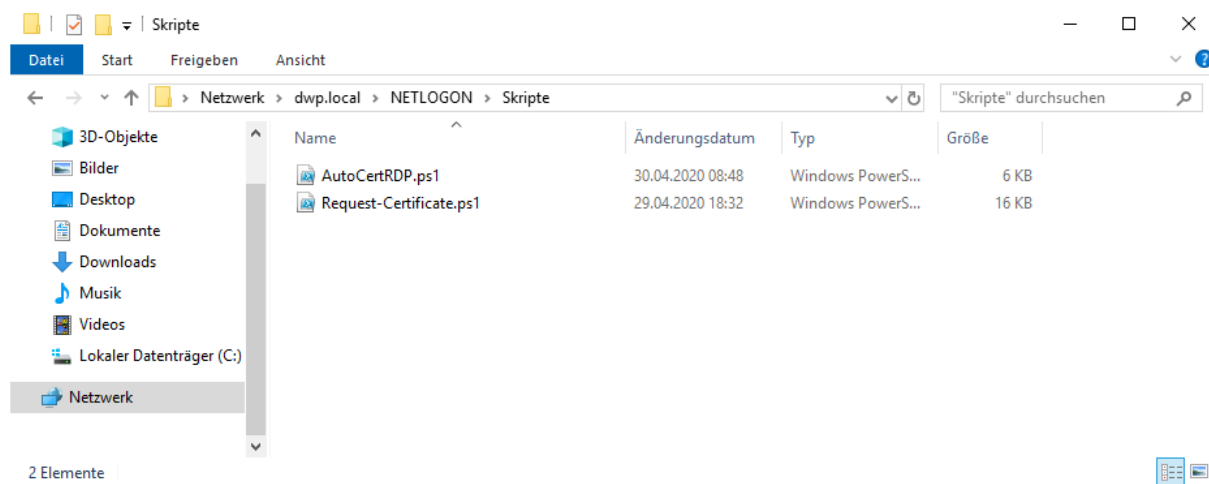
Wenn jemand Vorschläge zur Verbesserung hat, immer gern!



## Auto-Enrollment RDP Zertifikate mit IP

### Vorbereitung:

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

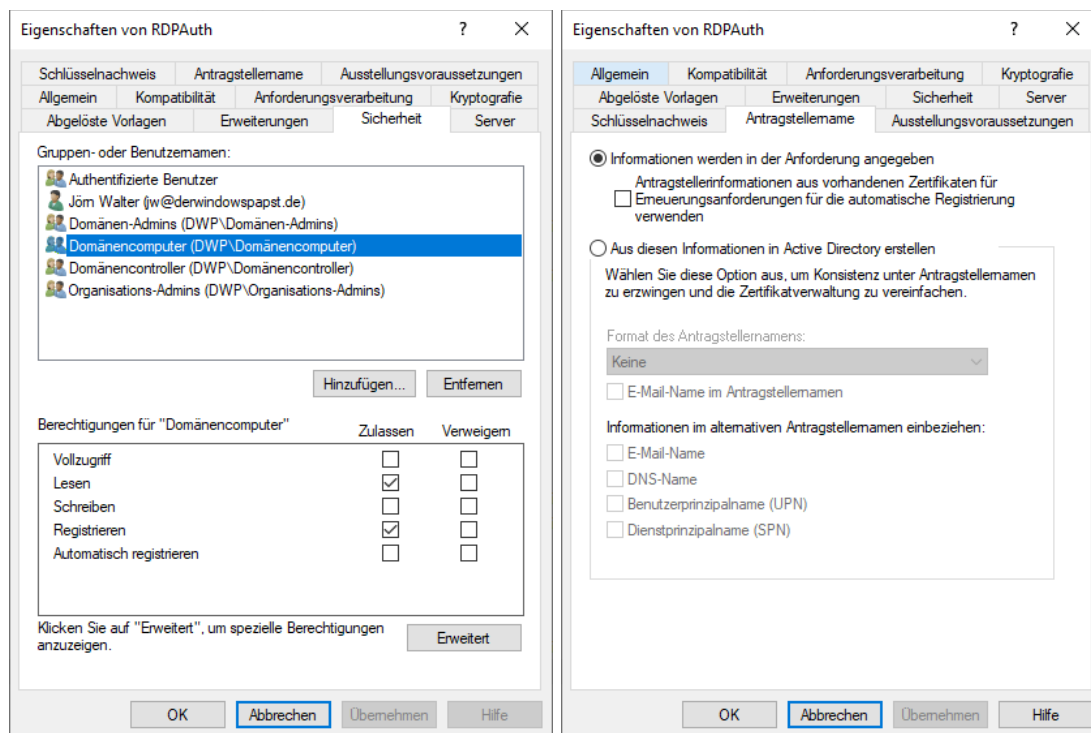


### Quelle des 2. Skripts:

<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

Eigenschaften von RDPAAuth

Abgelöste Vorlagen Erweiterungen Sicherheit Server

Schlüsselnachweis Antragstellername Ausstellungsvoraussetzungen

Allgemein Kompatibilität Anforderungsverarbeitung Kryptografie

Vorlagenanzeigename:  
RDPAAuth

Vorlagenname:  
RDPAAuth

Gültigkeitsdauer: 1 Jahre Erneuerungszeitraum: 2 Tage

☐ Zertifikat in Active Directory veröffentlichen  
☐ Nicht automatisch neu registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist

OK Abbrechen Übernehmen Hilfe

Eigenschaften von RDPAAuth

Abgelöste Vorlagen Erweiterungen Sicherheit Server

Schlüsselnachweis Antragstellername Ausstellungsvoraussetzungen

Allgemein Kompatibilität Anforderungsverarbeitung Kryptografie

Anbieterkategorie: Schlüsselspeicheranbieter

Name des Algorithmus: RSA

Minimale Schlüsselgröße: 2048

Auswählen der für Anforderungen verwendbaren Kryptografieanbieter

☐ Verwendung aller auf dem Computer des Antragstellers verfügbaren Anbieter für Anforderungen möglich

☒ Für Anforderungen muss einer der folgenden Anbieter verwendet werden:

Anbieter:

- ☒ Microsoft Software Key Storage Provider
- ☐ Microsoft Platform Crypto Provider
- ☐ Microsoft Smart Card Key Storage Provider

Anforderungshash: SHA256

☐ Alternatives Signaturformat verwenden

OK Abbrechen Übernehmen Hilfe

Eigenschaften von RDPAAuth

Allgemein Kompatibilität Anforderungsverarbeitung Kryptografie

Schlüsselnachweis Antragstellername Ausstellungsvoraussetzungen

Abgelöste Vorlagen Erweiterungen Sicherheit Server

Markieren Sie eine Erweiterung, und klicken Sie auf "Bearbeiten", um diese zu ändern.

Erweiterungen in dieser Vorlage:

- Anwendungsrichtlinien
- Ausstellungsrichtlinien
- Basiseinschränkungen
- Schlüsselverwendung
- Zertifikatvorlageninformationen

Bearbeiten...

Beschreibung von Anwendungsrichtlinien:  
Remote Desktop Authentication

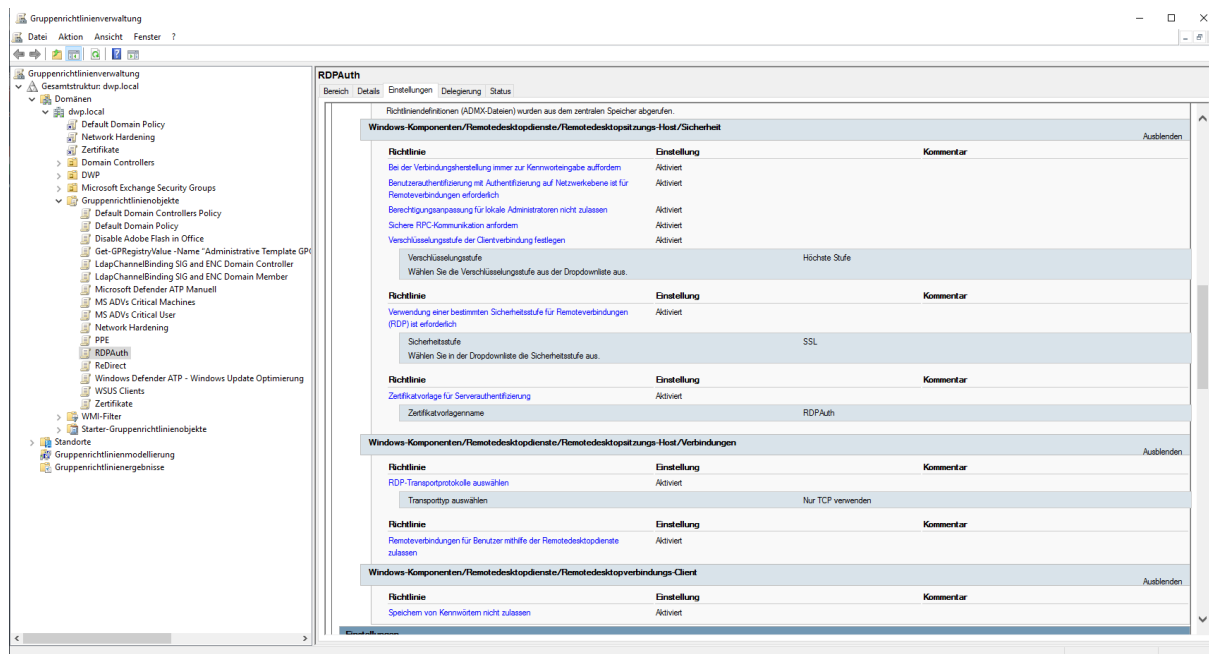
OK Abbrechen Übernehmen Hilfe



# Auto-Enrollment RDP Zertifikate mit IP

## Schritt 2:

Erstellen einer Gruppenrichtlinie zur Erstellung einer geplanten (täglich) 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.

