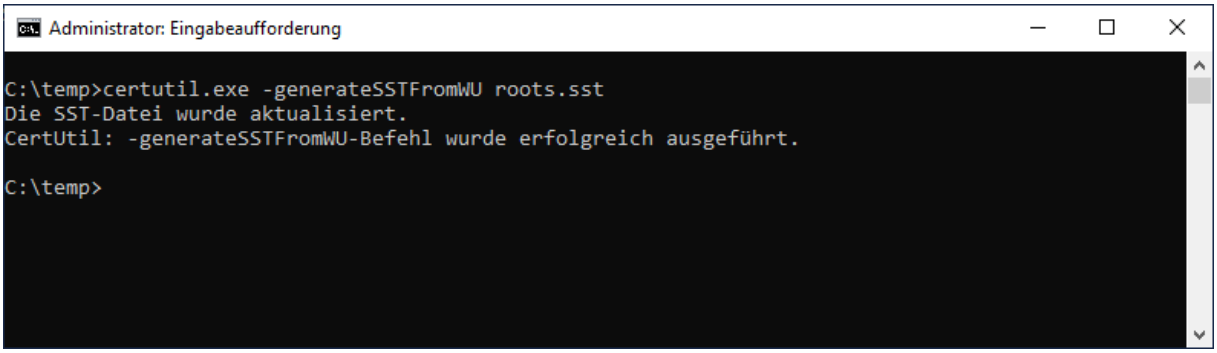
Root Zertifikate Offline aktualisieren

Normalerweise werden die Root-Zertifikate (Stammzertifikate), im Rahmen eines Automatismus wöchentlich aktualisiert.

Microsoft verwaltet im Rahmen des „Microsoft Trusted Root Certificate Program" eine Repository. Aus dieser Repository laden wir die Zertifikate herunter und verpacken diese in eine sst (Serialized Certificate Store File) Datei.

Mithilfe der Commandline und dem Befehl certutil erstellen wir nun diese Offline sst Datei.

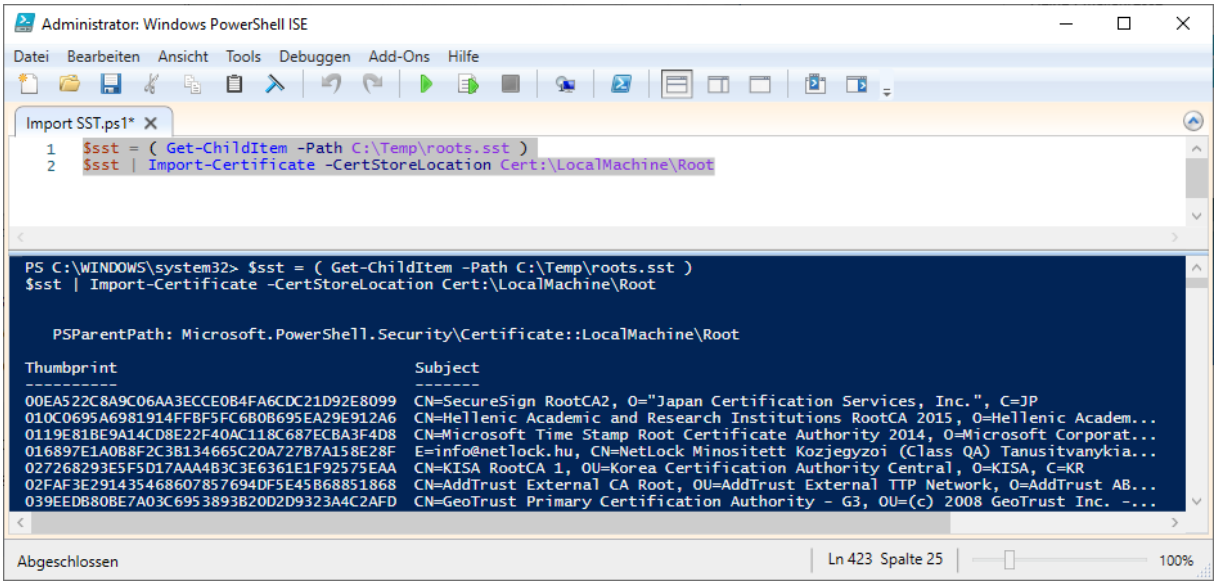
certutil.exe -generateSSTFromWU roots.sst



Importieren von Zertifikaten anhand einer vorhandenen sst Datei:

Die sst (Serialized Certificate Store File) Datei kann nun auf jeden beliebigen Computer ohne Internetzugang verteilt und importiert werden.

$sst = (Get-ChildItem -Path C:\Temp\roots.sst)
$sst | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root



Root Zertifikate Offline aktualisieren

Optional:

Get-Childitem cert:\LocalMachine\root | format-list
Get-ChildItem cert:\LocalMachine\root | Where {$_.NotAfter -lt (Get-Date).AddDays(90)}

Alternative mittels einer stl Datei. Diese wird alle 2 Monate von MS aktualisiert.

Download:

http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

Import per CMD:

certutil -addstore -f root authroot.stl

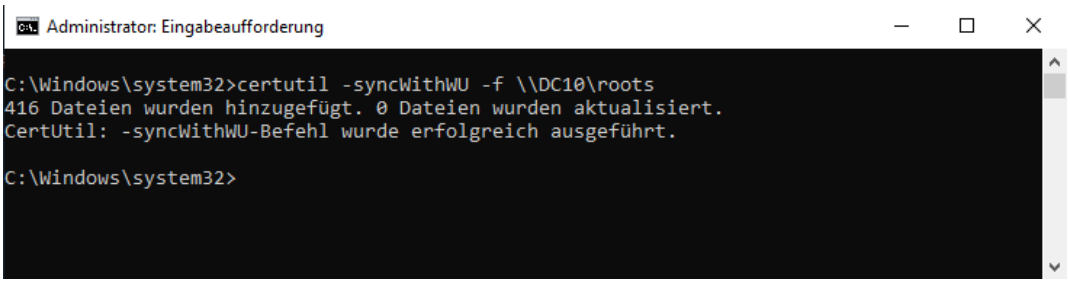
Import per Powershell:

$sst = (Get-ChildItem -Path C:\Temp\roots.sst)
$sst | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root

Alternative mittels einem Direktdownload der Zertifikatsdateien

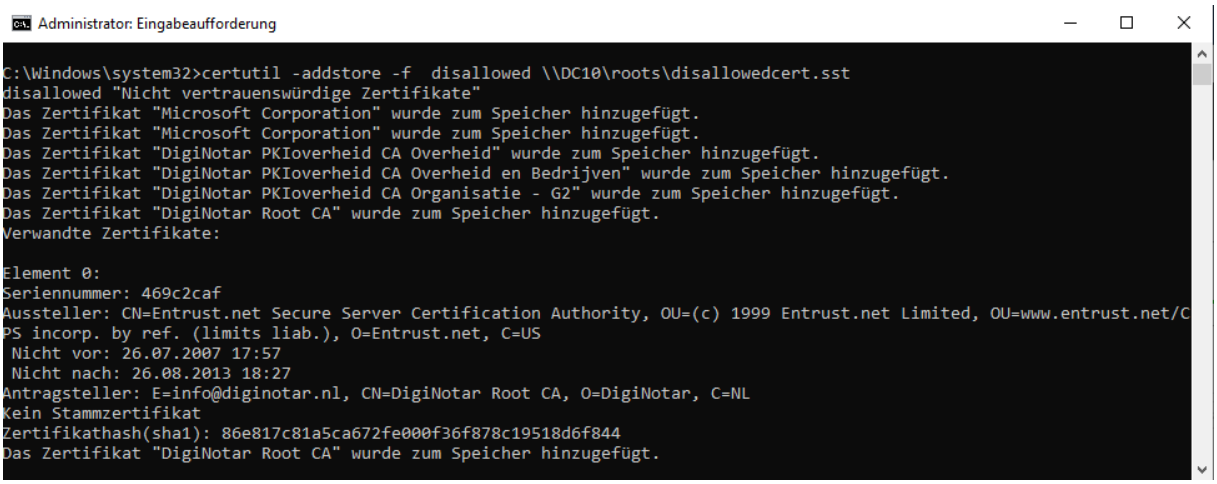
Download:

certutil -syncWithWU -f \\DC10\roots



Import per CMD:

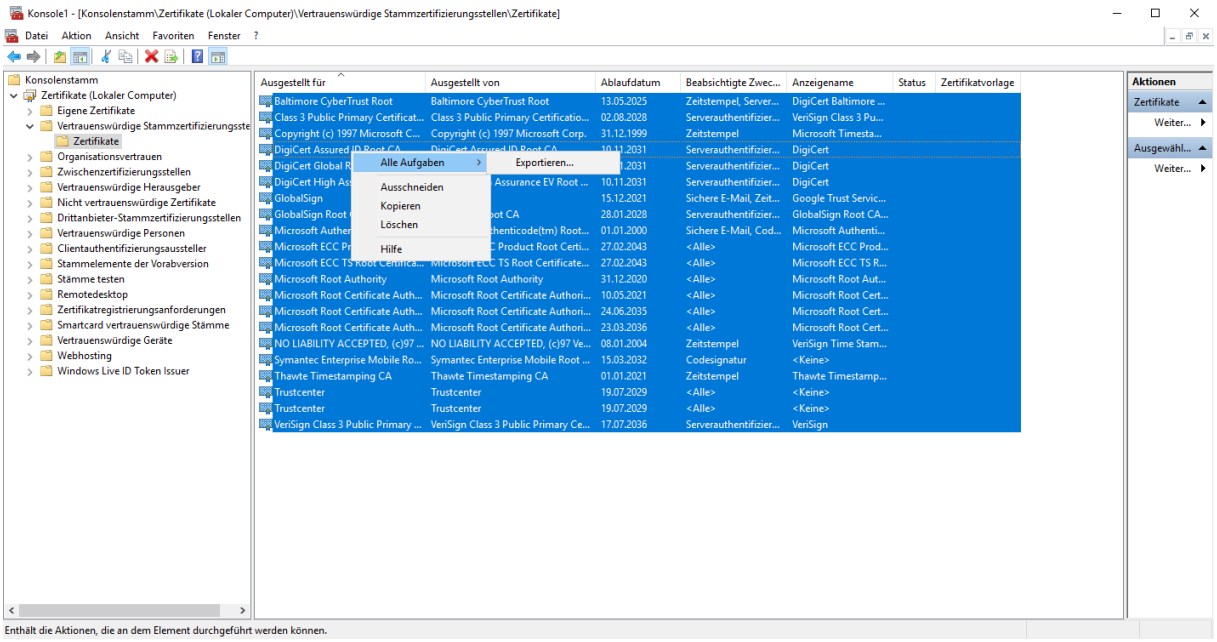
certutil -addstore -f disallowed \\DC10\roots\disallowedcert.sst

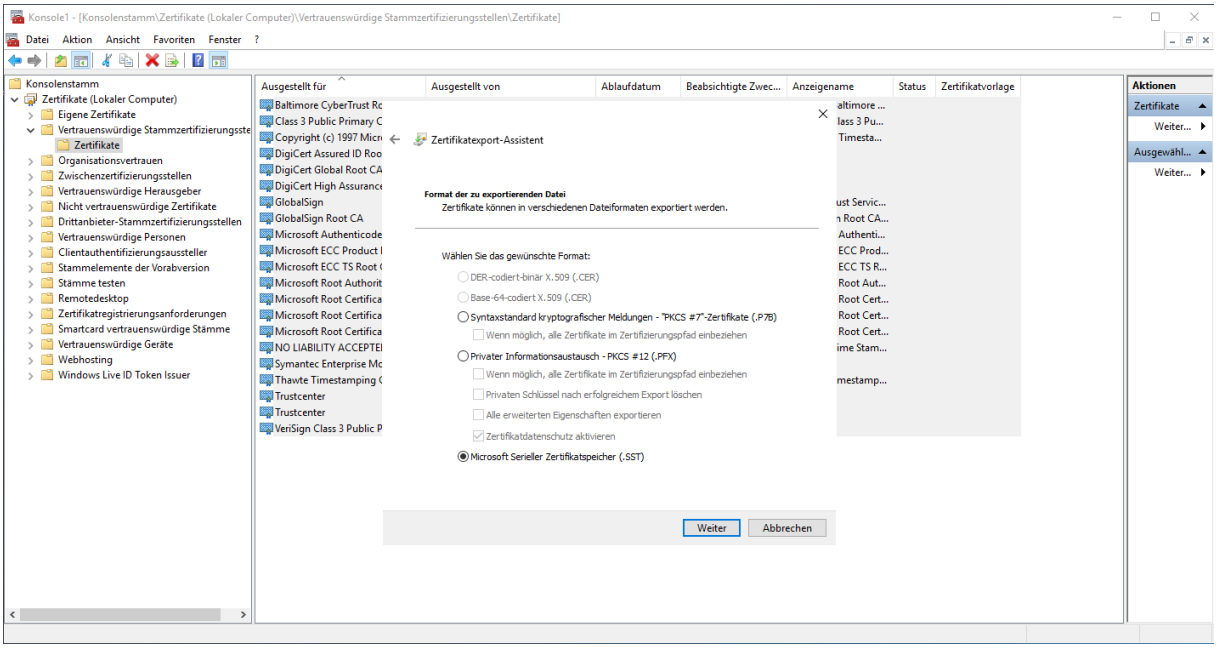


Root Zertifikate Offline aktualisieren

Synchronisierungsquelle per GPO an offline Computer verteilen:

Die im Speicher vorhandenen Zertifikate können zuvor gesichert werden, falls man sich unsicher ist.

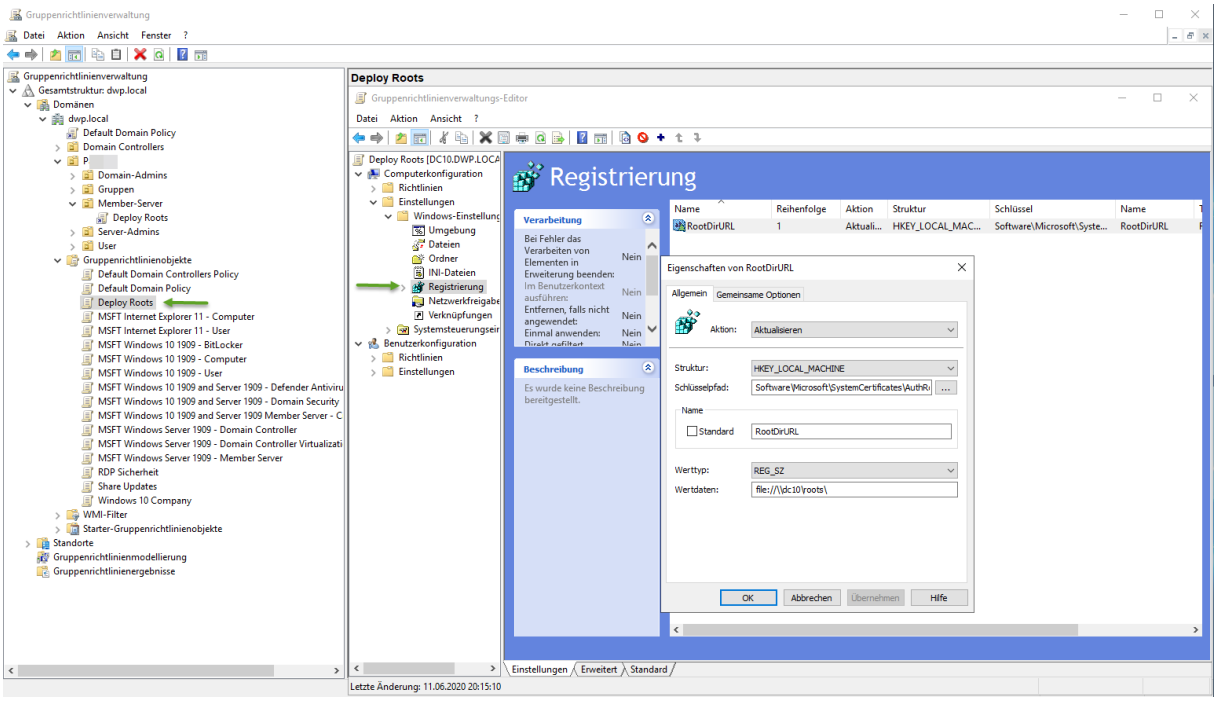


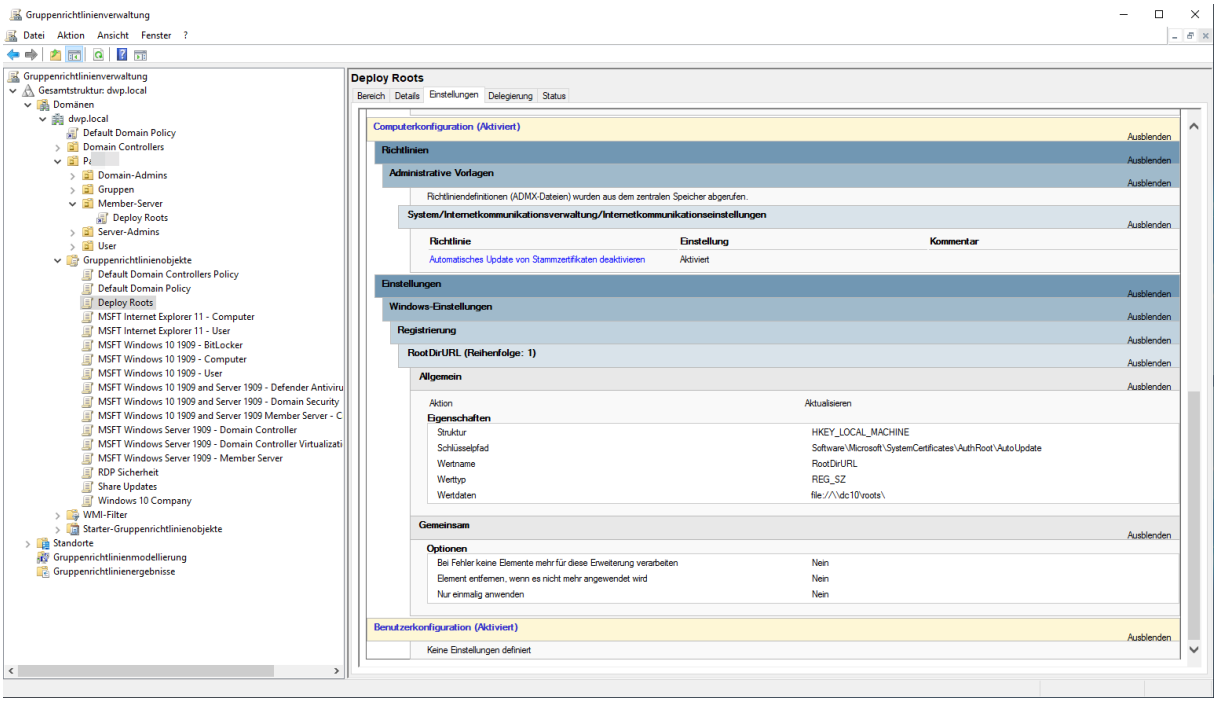


Root Zertifikate Offline aktualisieren

Erstellen ein neues Gruppenrichtlinienobjekt mit folgenden Einstellungen:

Aktion: Aktualisieren
Schlüsselpfad: HKLM
Schlüsselpfad: Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
Wertname: RootDirURL
WertTyp: REG_SZ
Wertdaten: file://\\DC10\roots\

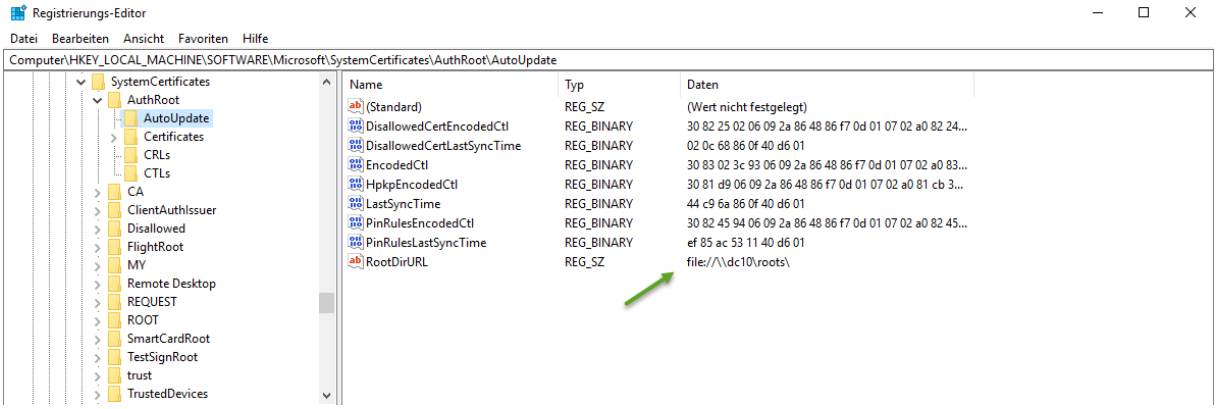


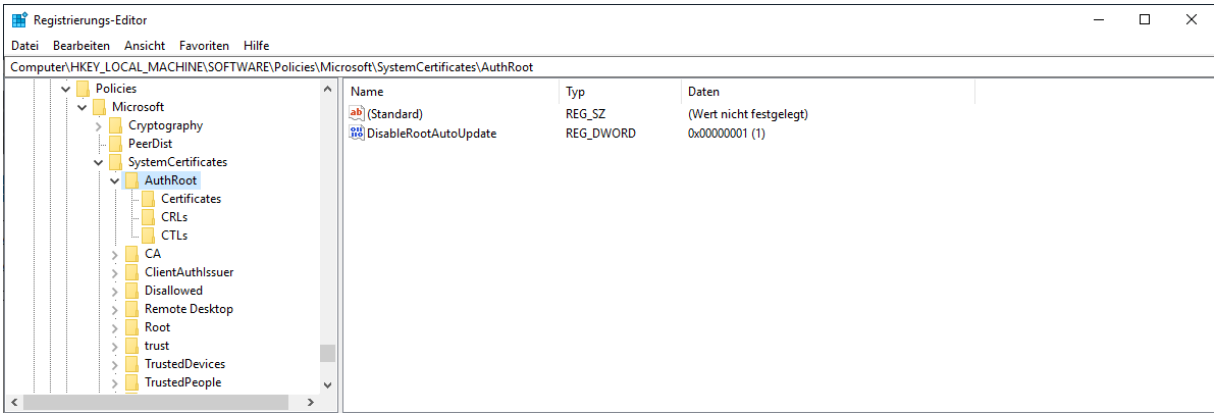


Erstellt von Jörn Walter **11.06.2020**

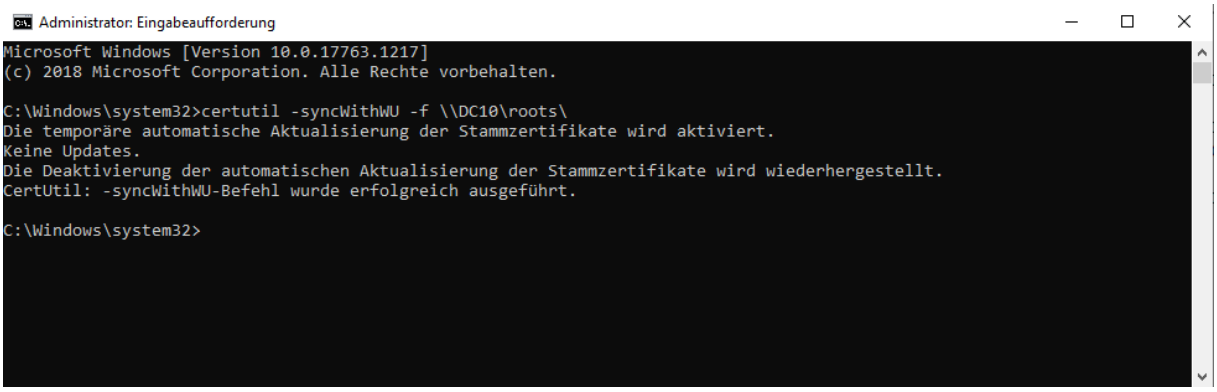
Root Zertifikate Offline aktualisieren

Nach dem die Richtlinie angewendet wurde, finden wir in der Registry den Remote-Pfad, um nach Root-Zertifikaten zu suchen sofern diese benötigt werden.





certutil -syncWithWU -f \\DC10\roots\



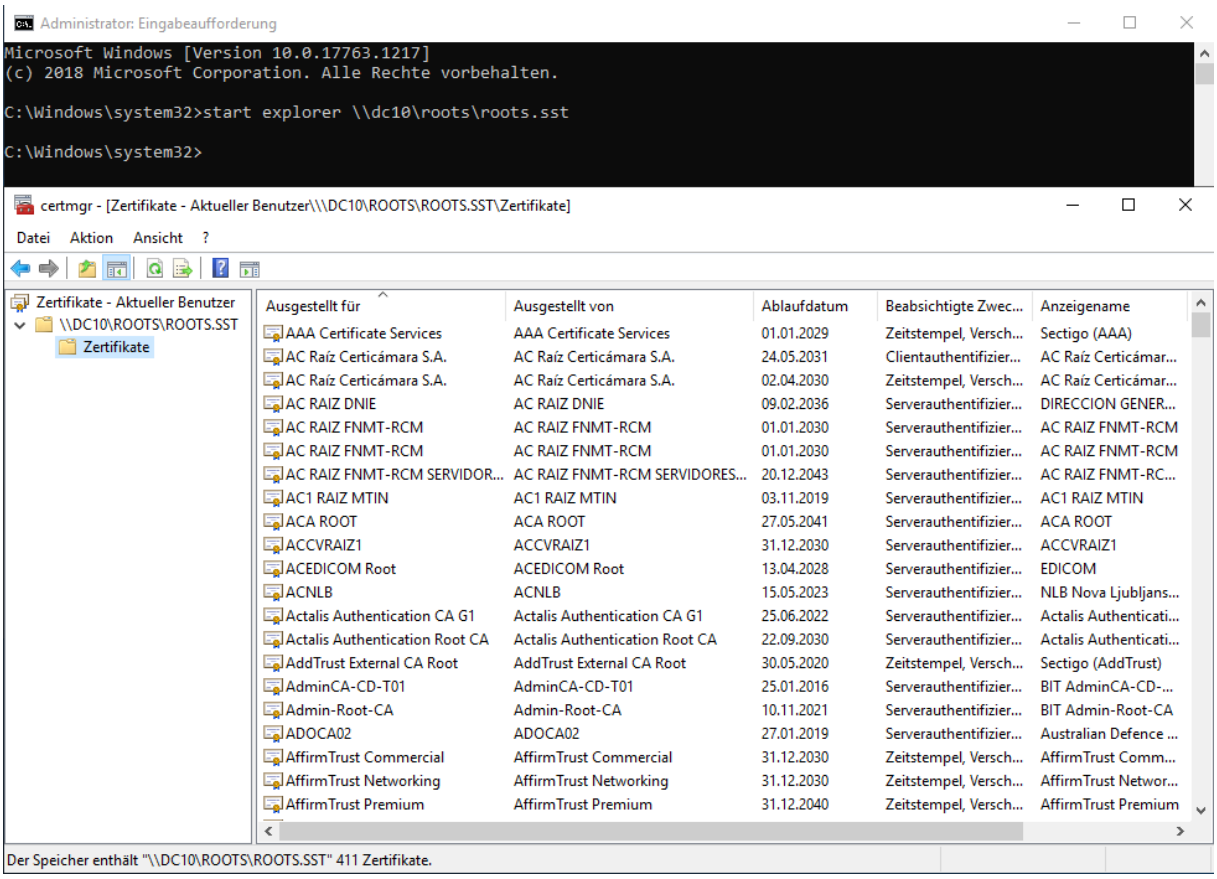
Registry keys	Value and Description
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate	A value of 1 disables the Windows AutoUpdate of the trusted CTL.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\EnableDisallowedCertAutoUpdate	A value of 1 enables the Windows AutoUpdate of the untrusted CTL.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\RootDirUrl	Configures the shared location (the HTTP or the FILE path).

Erstellt von Jörn Walter **11.06.2020**

Root Zertifikate Offline aktualisieren

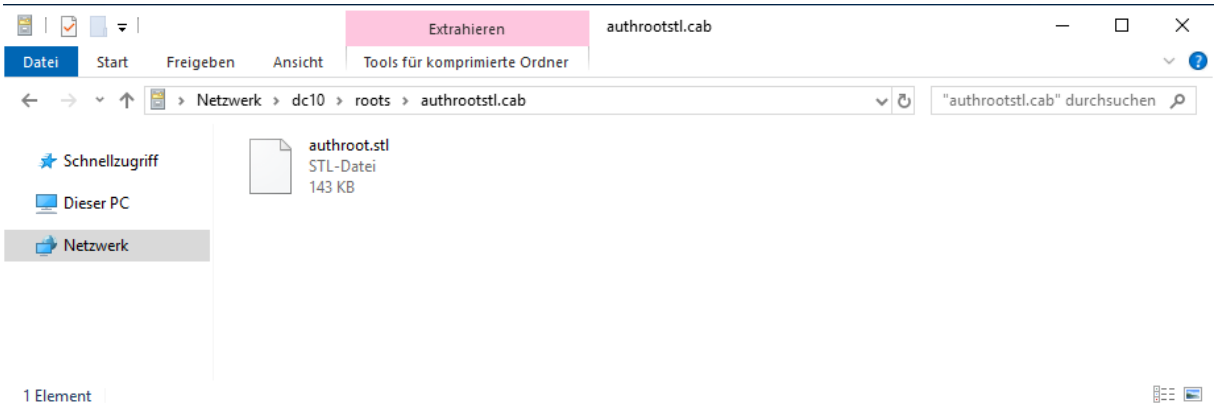
Einsicht in eine sst Datei:

start explorer \\dc10\roots\roots.sst



Welcher Container enthält welche Zertifikate?

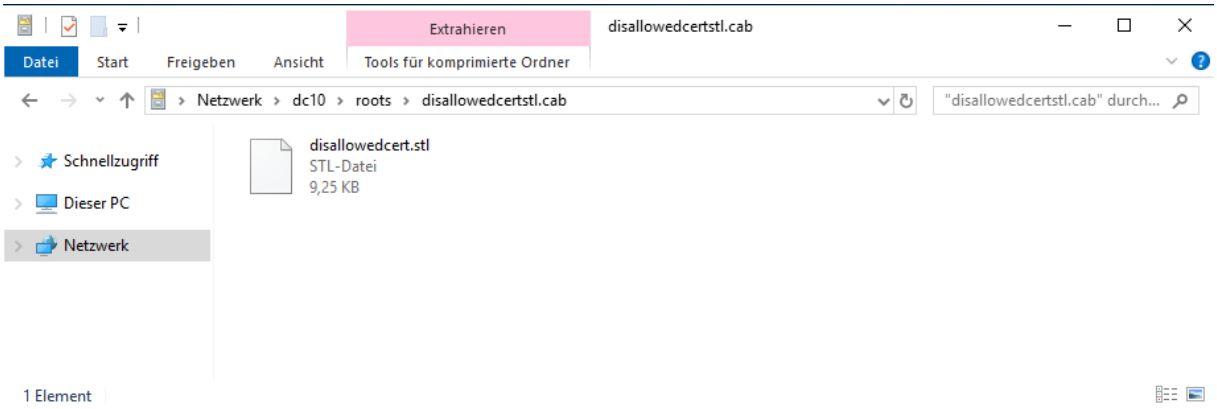
Die authrootstl.cab enthält Root-Zertifikate nur keine von Microsoft



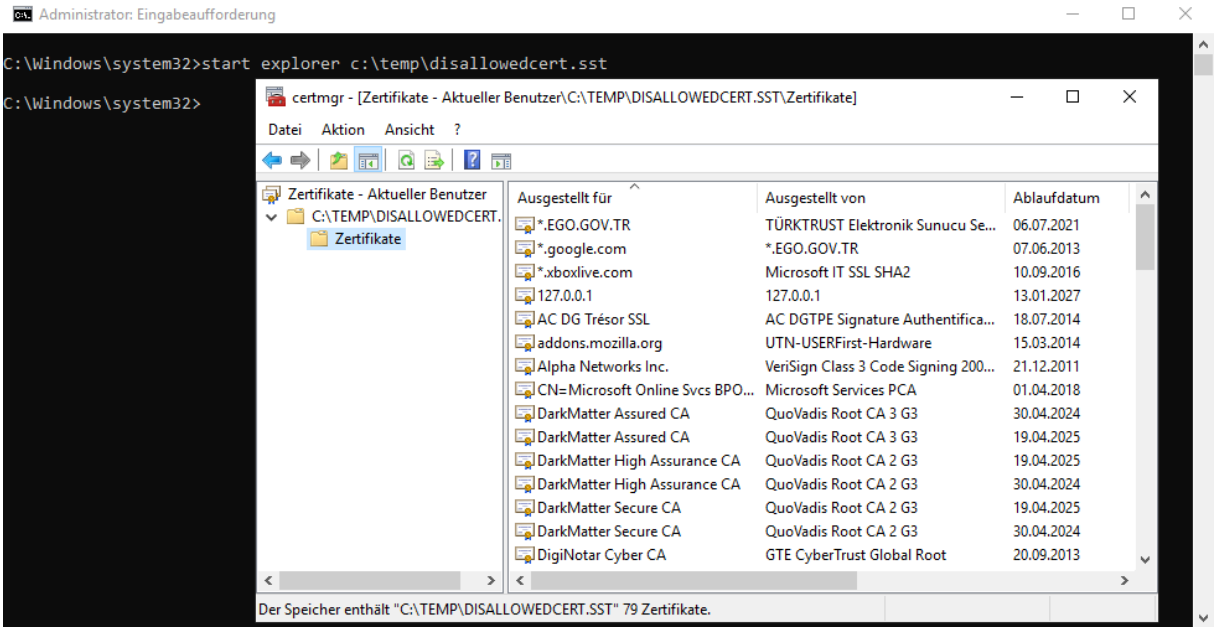
Erstellt von Jörn Walter **11.06.2020**

Root Zertifikate Offline aktualisieren

Die disallowedcertstl.cab enthält eine CTL mit nicht vertrauenswürdigen Zertifikaten



Die disallowedcert.sst enthält nicht vertrauenswürdige Zertifikate



Erstellt von Jörn Walter **11.06.2020**