

# Powershell Skripte signieren

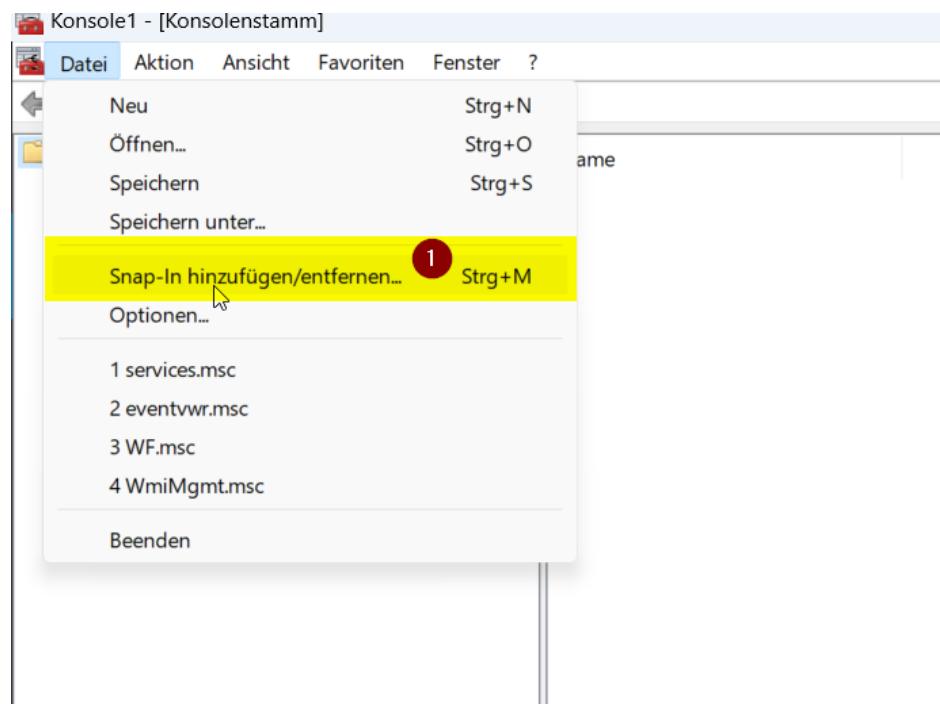
## Inhalt

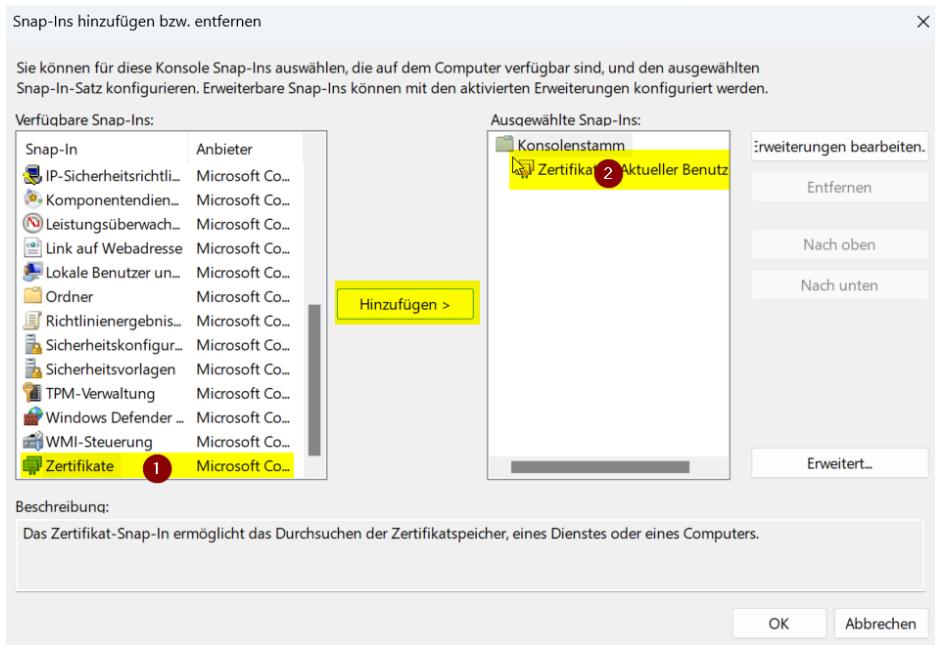
- [\*\*1.\) Codesigning Zertifikat abrufen\*\*](#)
- [\*\*2.\) Skript signieren\*\*](#)
- [\*\*3.\) Vertrauenswürdige Herausgeber hinzufügen\*\*](#)

## **1.) Codesigning Zertifikat abrufen**

Im ActiveDirectory ist eine Zertifikatsvorlage, mit derer jeder Benutzer aus dem AD sich ein Codesigning Zertifikat abrufen kann. Mithilfe dieses Zertifikats werden z.B. Powershell Skripte signiert. Dies ist u.A. darum sinnvoll, um den Ersteller des Skripts kenntlich zu machen, aber auch um sicherzustellen, dass das Skript nicht manipuliert wurde.

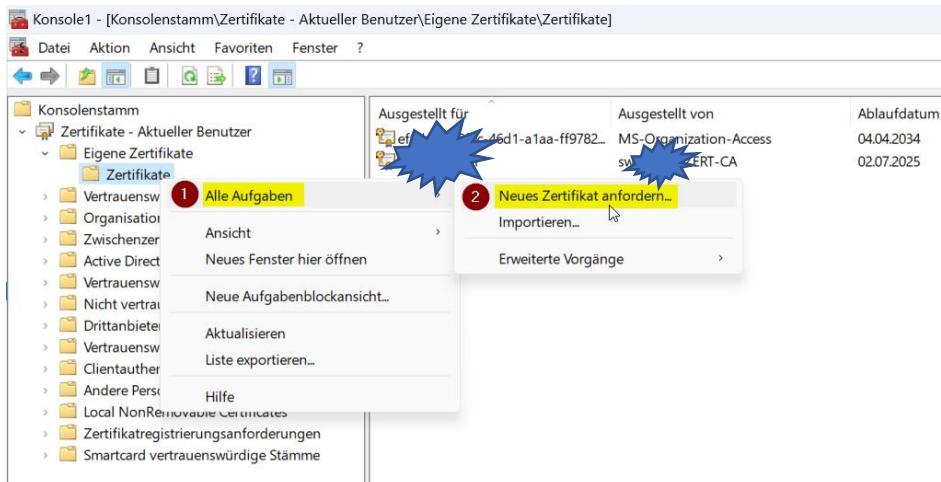
Zum Abrufen des eigenen Zertifikats öffnen wir die MMC und fügen das Snap-IN (1) Zertifikate(2) hinzu



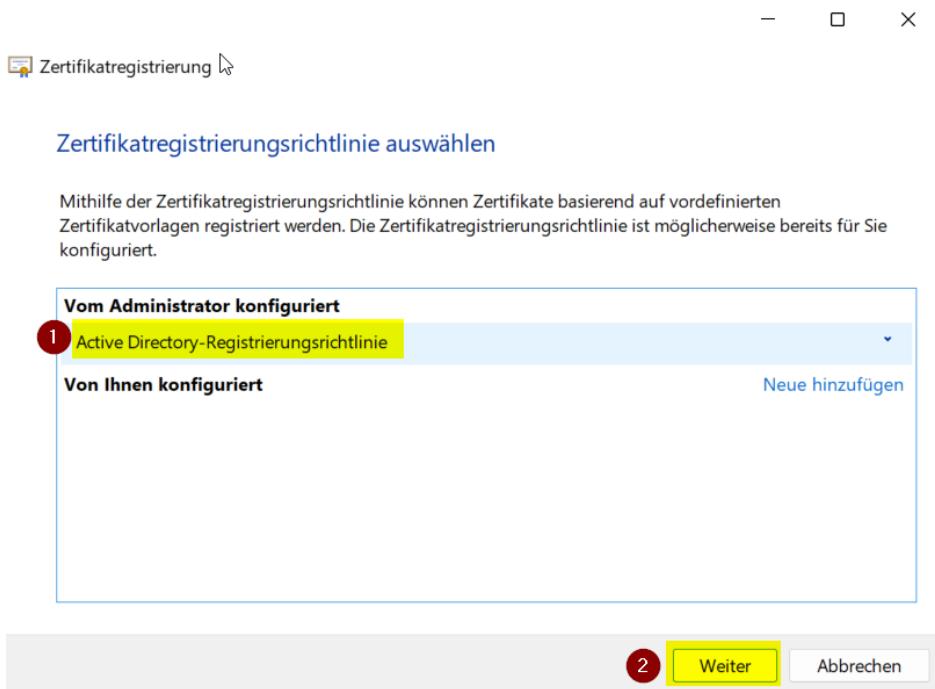


Anschließend wird noch mittels OK bestätigt. In der nachfolgenden Übersicht wählt man "Eigene Zertifikate → Zertifikate" (1)

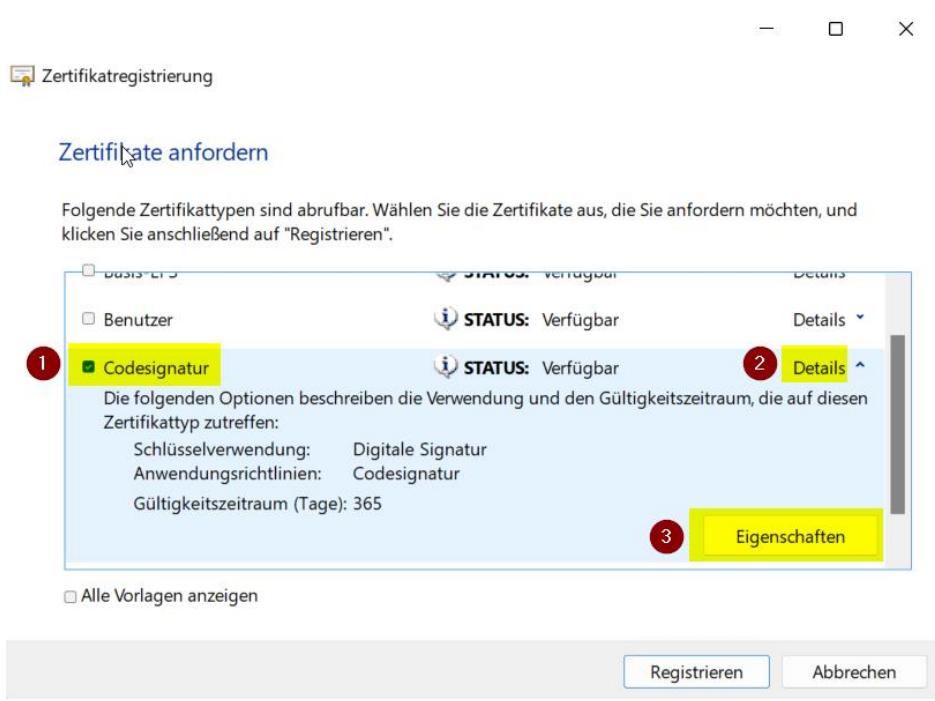
Danach mit der rechten Maustaste auf "Zertifikate → Alle Zertifikate(1) → Neues Zertifikat anfordern(2)"



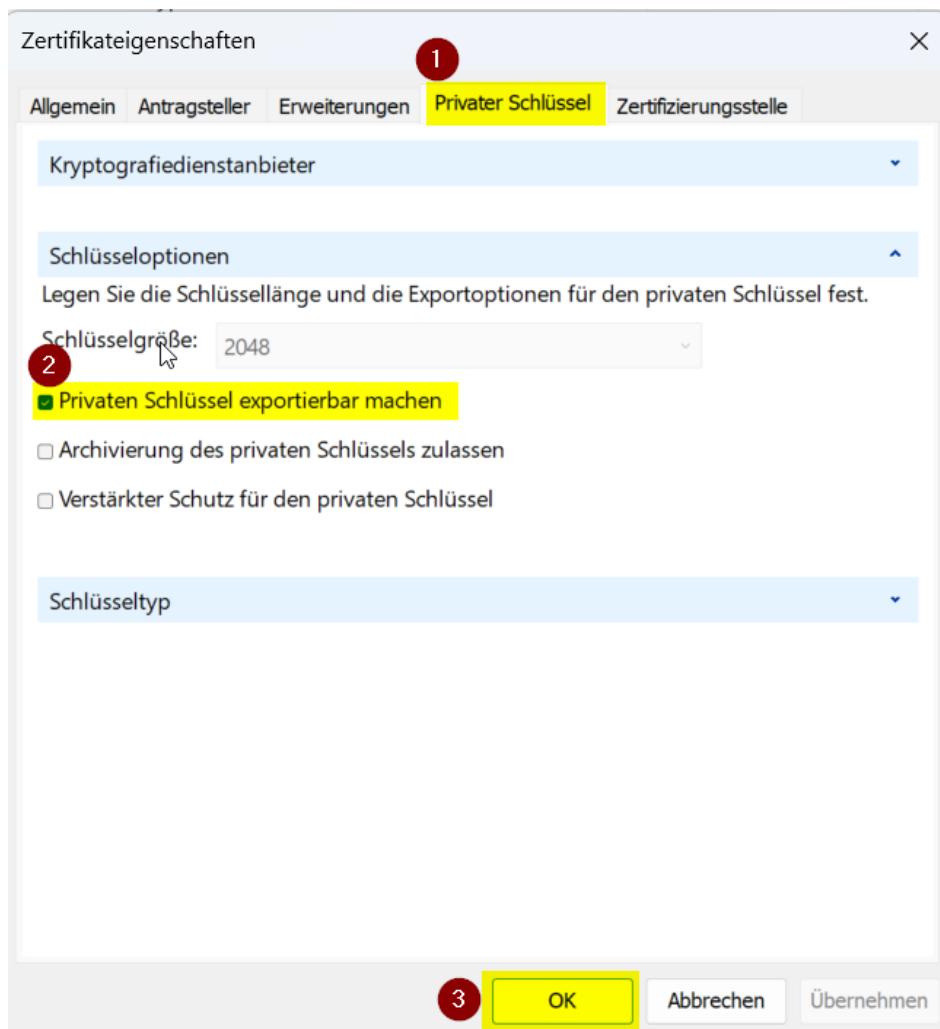
Man wählt die "Active Directory-Registrierungsrichtlinie"(1) und dann auf "Weiter"(2)



Im folgende Screen wählen wir die Vorlage "Codesignatur"(1) aus, klicken auf "Details"(2) und dann auf "Eigenschaften"(3)



Jetzt markiert man noch den privaten Schlüssel(1) als exportierbar(2) und klickt auf OK(3)



Die Zertifikatsanforderung wird mit Klick auf "Registrieren"(1) komplettiert.



Folgende Zertifikattypen sind abrufbar. Wählen Sie die Zertifikate aus, die Sie anfordern möchten, und klicken Sie anschließend auf "Registrieren".

2

Benutzer

Codesignatur

Die folgenden Optionen beschreiben die Verwendung und den Gültigkeitszeitraum, die auf diesen Zertifikattyp zutreffen:

Schlüsselverwendung: Digitale Signatur  
Anwendungsrichtlinien: Codesignatur  
Gültigkeitszeitraum (Tage): 365

Eigenschaften

Alle Vorlagen anzeigen

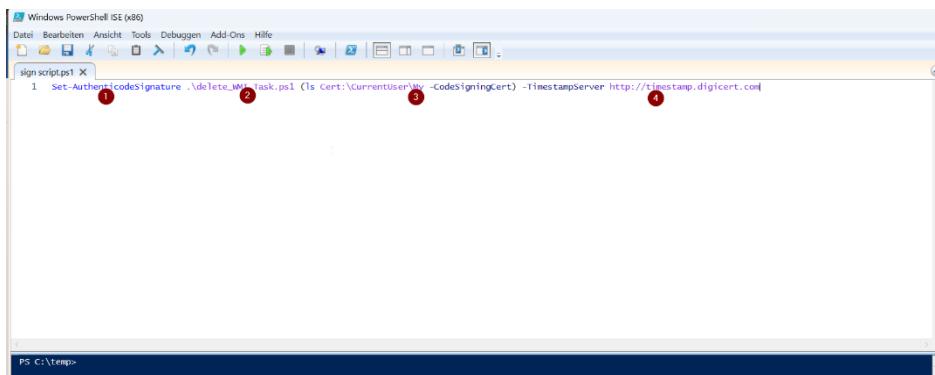
1 Registrieren Abbrechen

Nun steht das Zertifikat im Speicher(1) zur Verfügung und kann verwendet werden

## 2.) Skript signieren

Das eigentliche Signieren ist mit nur einer Zeile erledigt. Der Befehl ist in 4 Bereiche gegliedert

- (1) Das CMDlet
- (2) das zu signierende Skript
- (3) das zu verwendende Zertifikat
- (4) der Timstampserver. Dieser ist nötig, damit die Skripte unbegrenzt gültig und dem Signierer auf unbestimmte Zeit vertraut wird.



```
Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-ons Hilfe
sign script.ps1 X
1 Set-AuthenticodeSignature .\delete_WinTask.ps1 (ls Cert:\CurrentUser\My -CodeSigningCert) -TimestampServer http://timestamp.digicert.com
2
3
4
```

The screenshot shows a Windows PowerShell ISE window with a script named "sign script.ps1". The command in the editor is:

```
Set-AuthenticodeSignature .\delete_WinTask.ps1 (ls Cert:\CurrentUser\My -CodeSigningCert) -TimestampServer http://timestamp.digicert.com
```

Four red circles with numbers 1 through 4 are overlaid on the command line to indicate specific parameters:

- 1 points to the cmdlet name "Set-AuthenticodeSignature".
- 2 points to the first parameter ".\delete\_WinTask.ps1".
- 3 points to the second parameter "(ls Cert:\CurrentUser\My -CodeSigningCert)".
- 4 points to the third parameter "-TimestampServer http://timestamp.digicert.com".

## 3.) Vertrauenswürdige Herausgeber hinzufügen

Führt man ein signiertes Skript erstmalig aus, so erhält man eine Warnung, dass der Signierer nicht vertrauenswürdig sei. Dies lässt sich manuell bestätigen. Dadurch wird der Signierer im

Zertifikatsspeicher unter "Vertrauenswürdige Herausgeber"(1) u. (2) abgelegt und bei einem weiteren Mal wird ihm automatisch vertraut.

The screenshot shows the Windows Management Console (Konsolenstamm) with the path 'Zertifikate - Aktueller Benutzer > Vertrauenswürdige Herausgeber'. A yellow box highlights the 'Vertrauenswürdige Herausgeber' folder. A blue starburst effect highlights the 'Zertifikate' icon within it. The right pane displays a table of certificates:

Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigename	Status	Zertifikatvorlage
DigiCert EV Code Signing CA (SHA2)	DigiCert High Assurance EV Root CA	18.04.2027	Codesignatur	<Keine>	R	
DigiCert SHA2 Assured ID Timestamp...	DigiCert Assured ID Root CA	07.01.2031	Zeitstempel	<Keine>	R	
DigiCert Trusted 2021	DigiCert Assured ID Timestamp...	06.01.2031	Zeitstempel	<Keine>	R	
GeForce GTX 1080 Ti	DigiCert SHA2 Assured ID Root CA	02.07.2025	Codesignatur	<Keine>	R	Codesignatur
HP Inc.	DigiCert EV Code Signing CA (SHA2)	19.01.2022	Codesignatur	<Keine>	R	
InsecureCom LLC	DigiCert EV Code Signing CA (SHA2)	07.05.2021	Codesignatur	<Keine>	R	
InsecureCom LLC	DigiCert EV Code Signing CA (SHA2)	11.06.2024	Codesignatur	<Keine>	R	
Logitech Inc	DigiCert Trusted G4 Code Signing -	11.04.2025	Codesignatur	<Keine>	R	

Einfacher ist es jedoch, den "Vertrauenswürdigen Herausgeber" via GPO zu verteilen. So steht er allen im Scope befindlichen Objekten zur Verfügung und muss nicht manuell bestätigt werden.

Innerhalb des GPO ist folgender Bereich zuständig

The screenshot shows the 'Gruppenrichtlinienverwaltung-Editor' (Group Policy Management Editor) with the path 'DRAFT-TEST SWTS-DCH18 SW (LOCAL) Richtlinie > Computerkonfiguration > Richtlinien > Sicherheitsrichtlinien > Sicherheitszertifizierungstechnologien > Zertifikatshierarchien > Vertrauenswürdige Herausgeber'. A yellow box highlights the 'Vertrauenswürdige Herausgeber' icon. A blue starburst effect highlights the 'Zertifikatshierarchien' icon.

Dort lässt sich das eigene Zertifikat hinterlegen, welches man vorher am eigenen PC exportiert hat. Der Exportvorgang wird wie folgt durchgeführt:

Man wählt im Zertifikatsspeicher das eigene Codesigning Zertifikat aus(1) und klickt mit rechts auf "Alle Aufgaben"(2) und wählt "Exportieren"(3).

KonsolenstammZertifikate - Aktueller Benutzer\Vertrauenswürdige Herausgeber\Zertifikate

Datei Aktion Ansicht Favoriten Fenster ?

Ausgestellt für Ausgestellt von Ablaufdatum Beabsichtigte Zwecke Anzeigename Status Zertifikatvorlage

DigiCert EV Code Signing CA (S)	DigiCert High Assurance EV Root CA	18.04.2027	Codesignatur <Keine>	R	
DigiCert SHA2 Assured ID Timest...	DigiCert Assured ID Root CA	07.01.2031	Zeitstempel <Keine>	R	
DigiCert Timestamp 2021	DigiCert SHA2 Assured ID Timesta...	06.01.2031	Zeitstempel <Keine>	R	
<b>TS-ZERT-CA</b>			Codesignatur <Keine>	<b>Codesignatur</b>	
Offnen	TS-ZERT-CA	01.07.2025	Codesignatur <Keine>	R	Codesignatur
Alle Aufgaben...					
Ausschneiden					
Kopieren					
Löschen					
Eigenschaften					
Hilfe					

Die Voreinstellung(1) kann man so belassen

Zertifikatexport-Assistent

**Format der zu exportierenden Datei**

Zertifikate können in verschiedenen Dateiformaten exportiert werden.

---

Wählen Sie das gewünschte Format:

**1**  **DER-codiert-binär X.509 (.CER)**

- Base-64-codiert X.509 (.CER)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
  - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Privater Informationsaustausch - PKCS #12 (.PFX)
  - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
  - Privaten Schlüssel nach erfolgreichem Export löschen
  - Alle erweiterten Eigenschaften exportieren
  - Zertifikatdatenschutz aktivieren
- Microsoft Serieller Zertifikatspeicher (.SST)

Weiter Abbrechen

Es kann ein beliebiger Speicherort und Dateiname(1) gewählt werden

X

← Zertifikatexport-Assistent

**Zu exportierende Datei**

Geben Sie den Namen der zu exportierenden Datei an.

1

Dateiname:

C:\temp\Code Signing Herausgeber.cer

Durchsuchen...



Weiter

Abbrechen

Am Ende nur noch auf "Fertig stellen"(1) klicken.

X

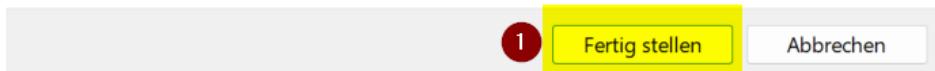
← Zertifikatexport-Assistent

## Fertigstellen des Assistenten

Der Zertifikatexport-Assistent wurde erfolgreich abgeschlossen.

Sie haben folgende Einstellungen ausgewählt:

Dateiname	C:\temp\7z - Code Signing Her
Exportschlüssel	Nein
Alle Zertifikate im Zertifizierungspfad einbeziehen	Nein
Dateiformat	DER-codiertes binäres X.509 (*.CE



Das exportierte Zertifikat lässt sich dann in das GPO laden.

