

Powershell Skripte signieren

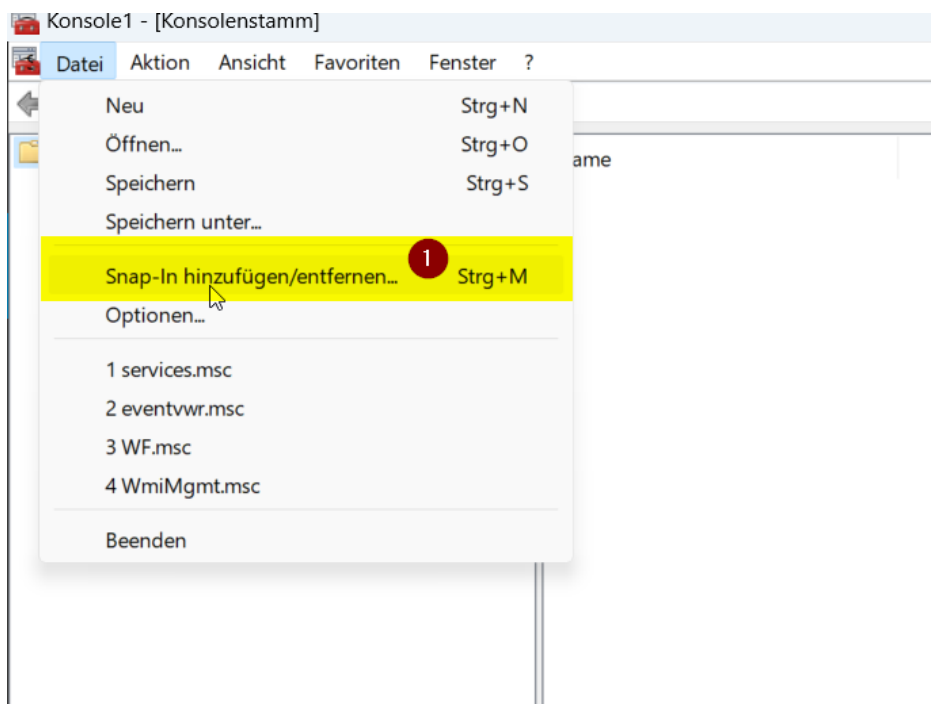
Inhalt

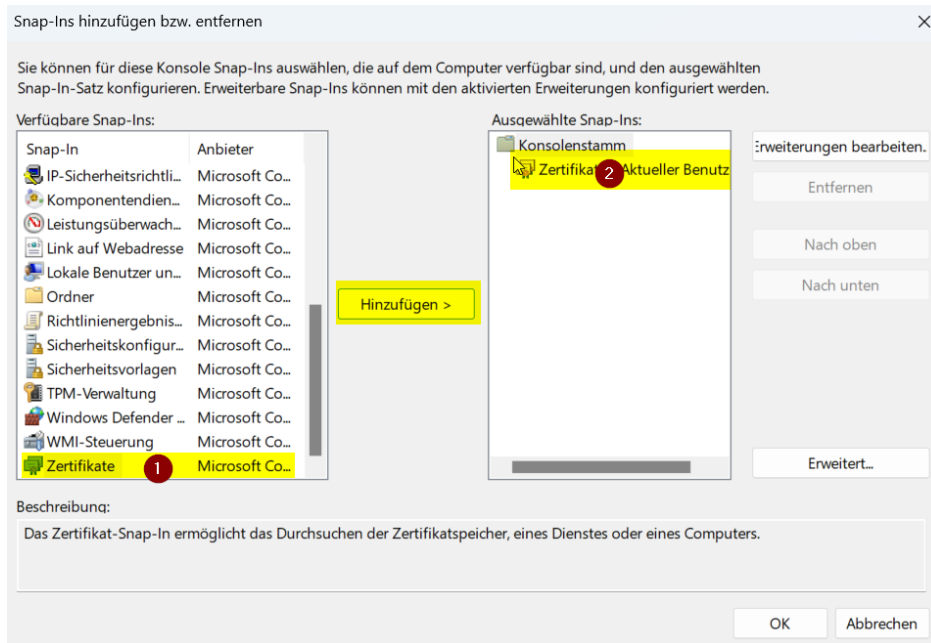
- [1.\) Codesigning Zertifikat abrufen](#)
- [2.\) Skript signieren](#)
- [3.\) Vertrauenswürdige Herausgeber hinzufügen](#)

1.) Codesigning Zertifikat abrufen

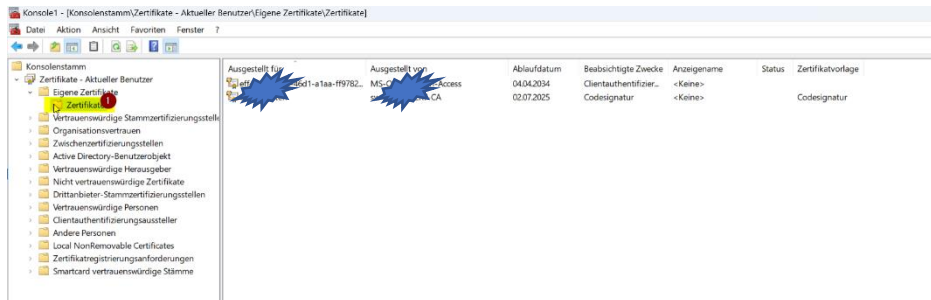
Im ActiveDirectory ist eine Zertifikatsvorlage, mit derer jeder Benutzer aus dem AD sich ein Codesigning Zertifikat abrufen kann. Mithilfe dieses Zertifikats werden z.B. Powershell Skripte signiert. Dies ist u.A. darum sinnvoll, um den Ersteller des Skripts kenntlich zu machen, aber auch um sicherzustellen,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

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

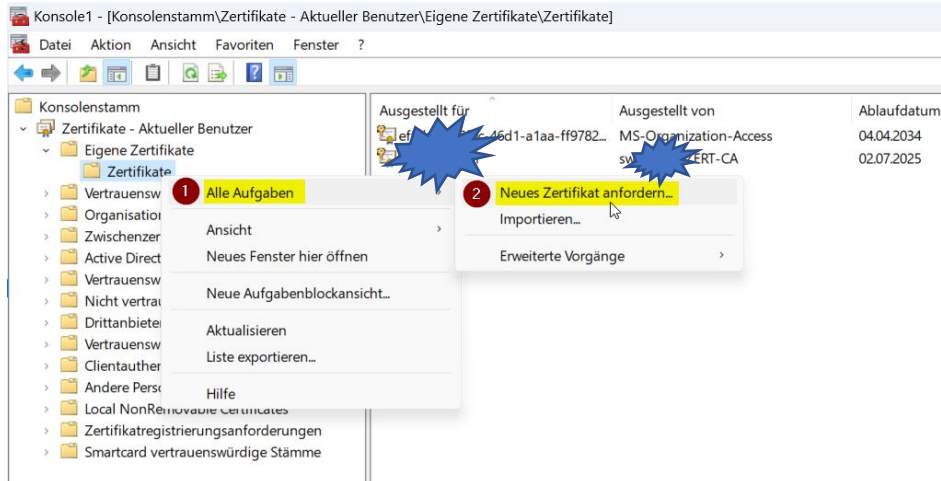




Anschließend wird noch mittels OK bestätigt. In der nachfolgenden Übersicht wählt man "Eigene Zertifikate → Zertifikate" (1)



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

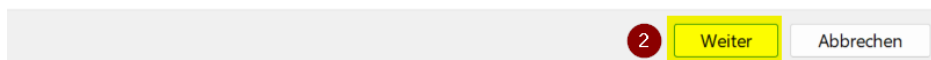
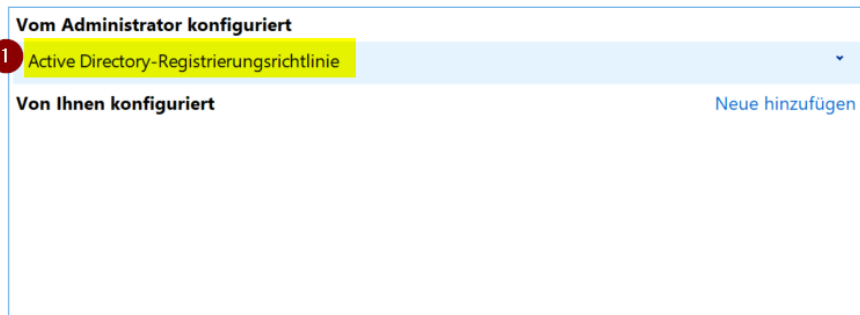


Man wählt die "Active Directory-Registrierungsrichtlinie"(1) und dann auf "Weiter"(2)



Zertifikatregistrierungsrichtlinie auswählen

Mithilfe der Zertifikatregistrierungsrichtlinie können Zertifikate basierend auf vordefinierten Zertifikatvorlagen registriert werden. Die Zertifikatregistrierungsrichtlinie ist möglicherweise bereits für Sie konfiguriert.



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

Zertifikate anfordern

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

☐ Benutzer

☒ Codesignatur

STATUS: Verfügbar

STATUS: Verfügbar

Details

Details

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

Schlüsselverwendung: Digitale Signatur

Anwendungsrichtlinien: Codesignatur

Gültigkeitszeitraum (Tage): 365

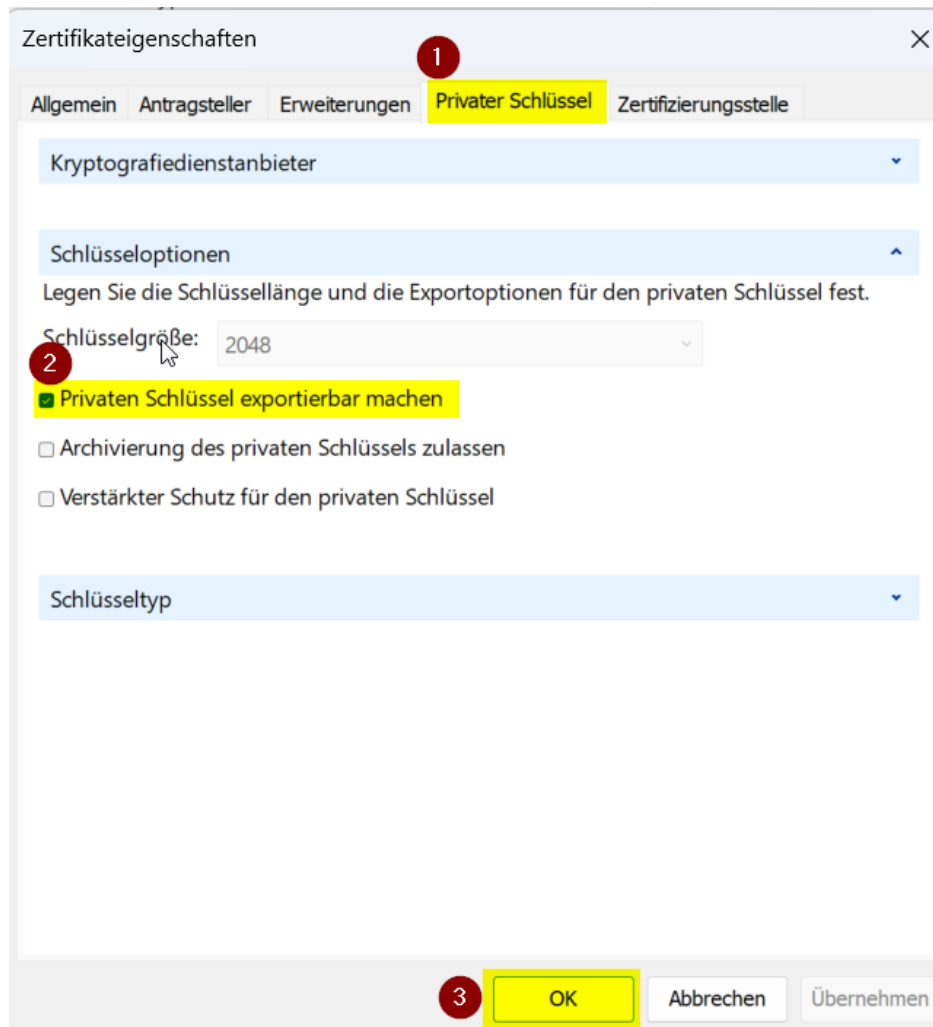
Eigenschaften

☐ Alle Vorlagen anzeigen

Registrieren

Abbrechen

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.

Zertifikatregistrierung

Zertifikate anfordern

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

☐ Benutzer **STATUS: Verfügbar** Details ▾

☒ Codesignatur **STATUS: Verfügbar** Details ▲

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

Konsole1 - [Konsole Stamm|Zertifikate - Aktueller Benutzer(Eigene Zertifikate|Zertifikate)]

Datei Aktion Ansicht Favoriten Fenster ?

	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigenname	Status	Zertifikatvorlage
Zertifikate	04.04.2034	MS-CA	04.04.2034	Clientauthentifizierung...	<Keine>		Codesignatur
Vertrauenswürdige Stammzertifizierungsstellen							
Organisationsvertrauen							
Zwischenzertifizierungsstellen							
Active Directory-Benutzerobjekt							
Vertrauenswürdige Herausgeber							
Nicht vertrauenswürdige Zertifikate							
Drittanbieter-Stammzertifizierungsstellen							
Vertrauenswürdige Personen							
Clientauthentifizierungsaussteller							
Andere Personen							
Local Nonremovable Certificates							
Zertifikatregistrierungsanforderungen							
Smartcard vertrauenswürdige Stämme							

2.) Skript signieren

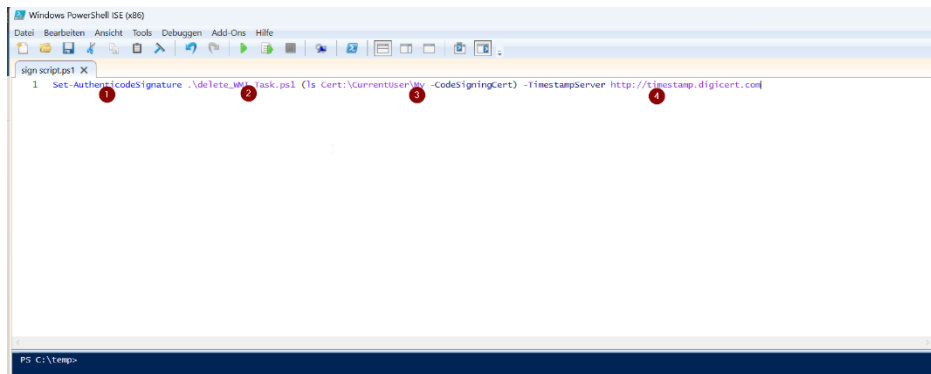
Das eigentliche Signieren ist mit nur einer Zeile erledigt. Der Befehl ist in 4 Bereiche gegliedert

(1) Das CMDlet

(2) das zu signierende Skript

(3) das zu verwendende Zertifikat

(4) der Timestampserver. Dieser ist nötig, damit die Skripte unbegrenzt gültig und dem Signierer auf unbestimmte Zeit vertraut wird.

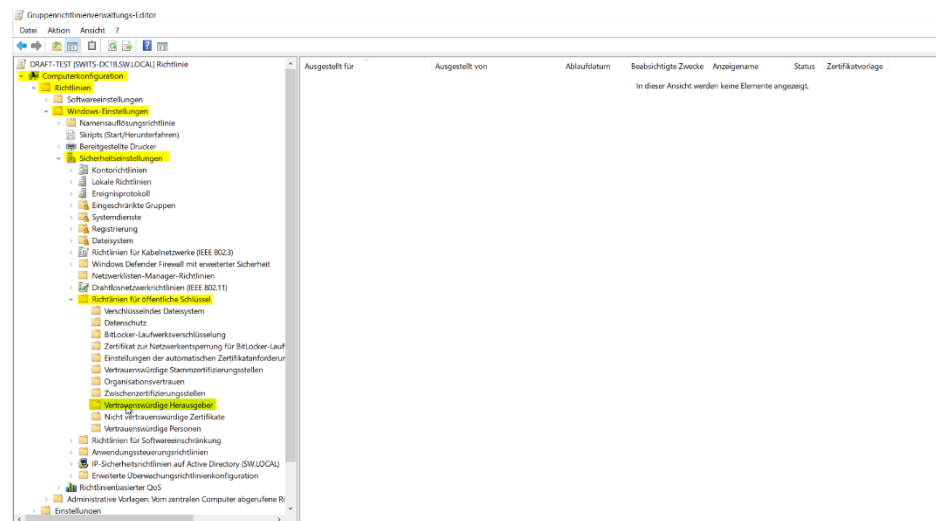


3.) Vertrauenswürdige Herausgeber hinzufügen

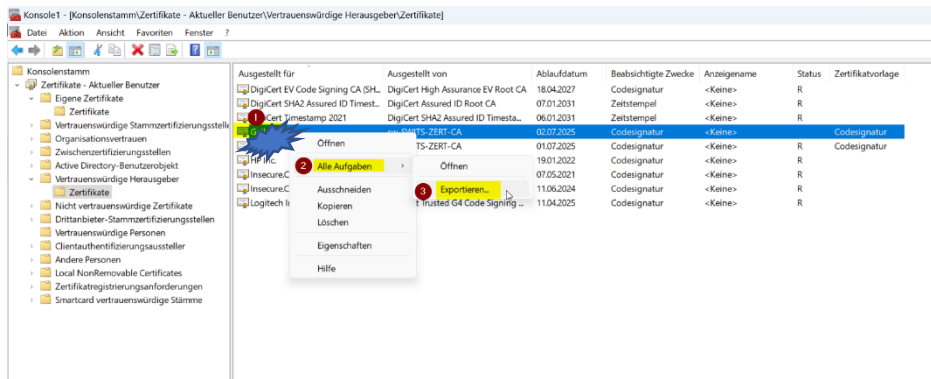
Führt man ein signiertes Skript erstmalig aus, so erhält man eine Warnung, dass der Signierer nicht vertrauenswürdig sei. Dies lässt sich manuell bestätigen. Dadurch wird der Signierer im

[illegible]

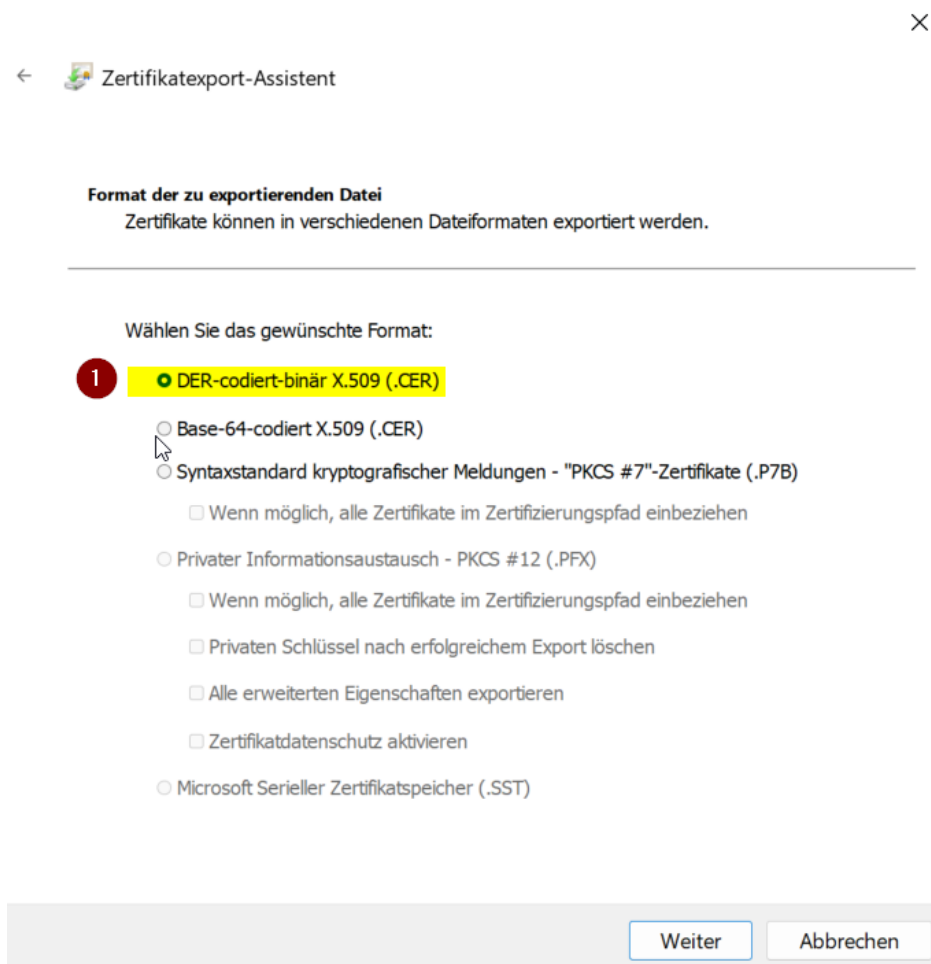
Innerhalb des GPO ist folgender Bereich zuständig



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



Die Voreinstellung(1) kann man so belassen



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

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.

Fertigstellen des Assistenten

Der Zertifikatexport-Assistent wurde erfolgreich abgeschlossen.

Sie haben folgende Einstellungen ausgewählt:

Dateiname	C:\temp\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.

