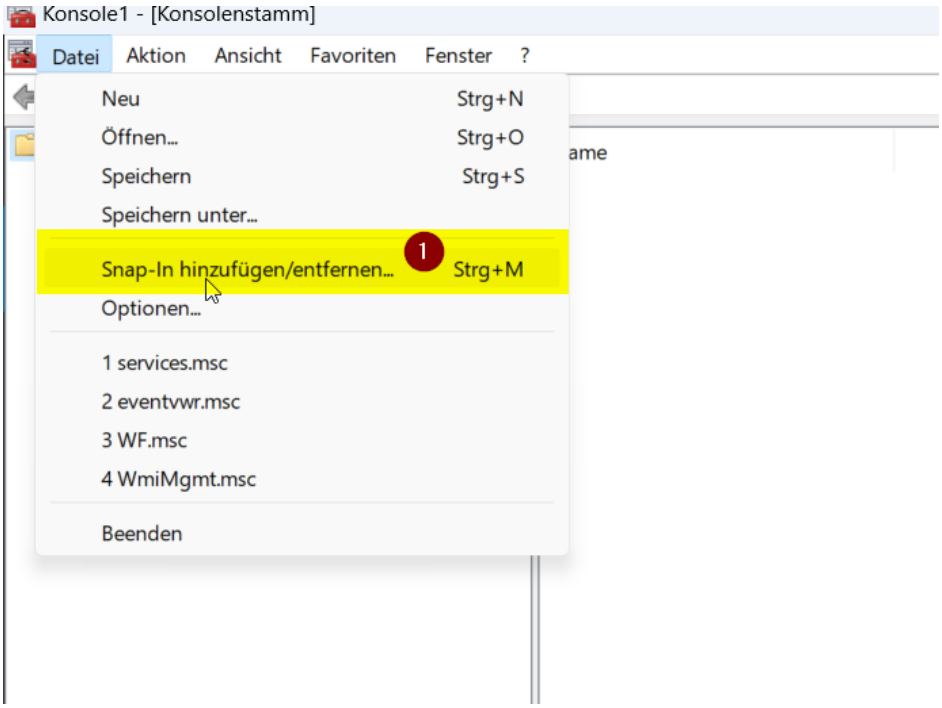
Powershell Skripte signieren

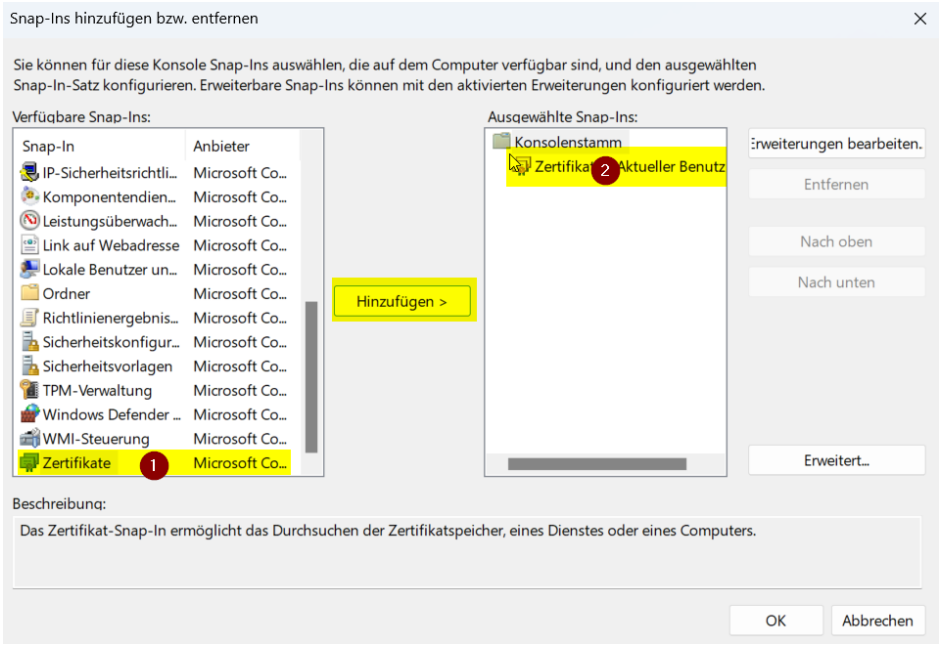
Inhalt

1.) Codesigning Zertifikat abrufen

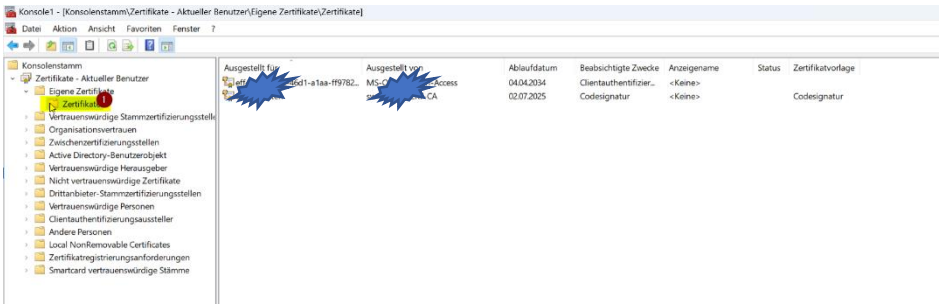
Im ActiveDirectory ist eine Zertifikatsvorlage, mit derer jeder Benutzer aus dem AD sich ein Codesigning Zertifikat abrufen kann. Mithilfe dieses Zertifikats werden z.B. Powershell Skripte signiert. Dies ist u.A. darum sinnvoll, um den Ersteller des Skripts kenntlich zu machen, aber auch um sicherzustellen,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

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

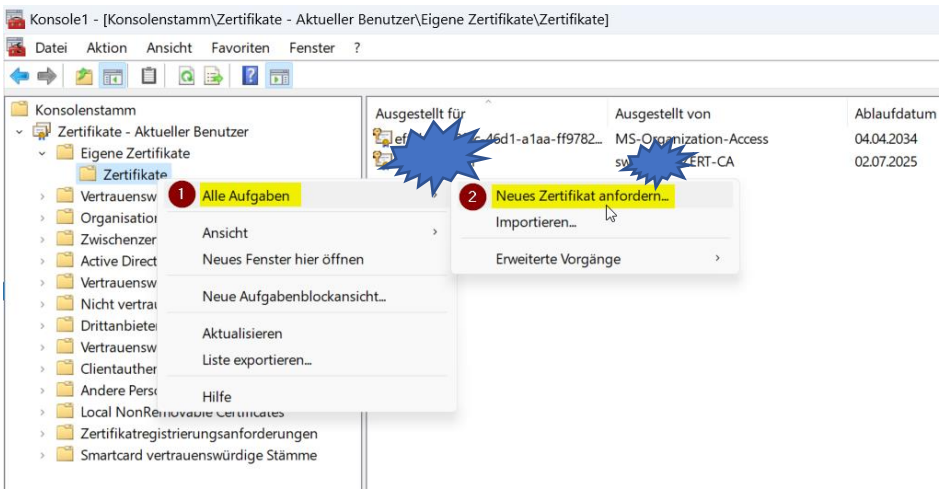




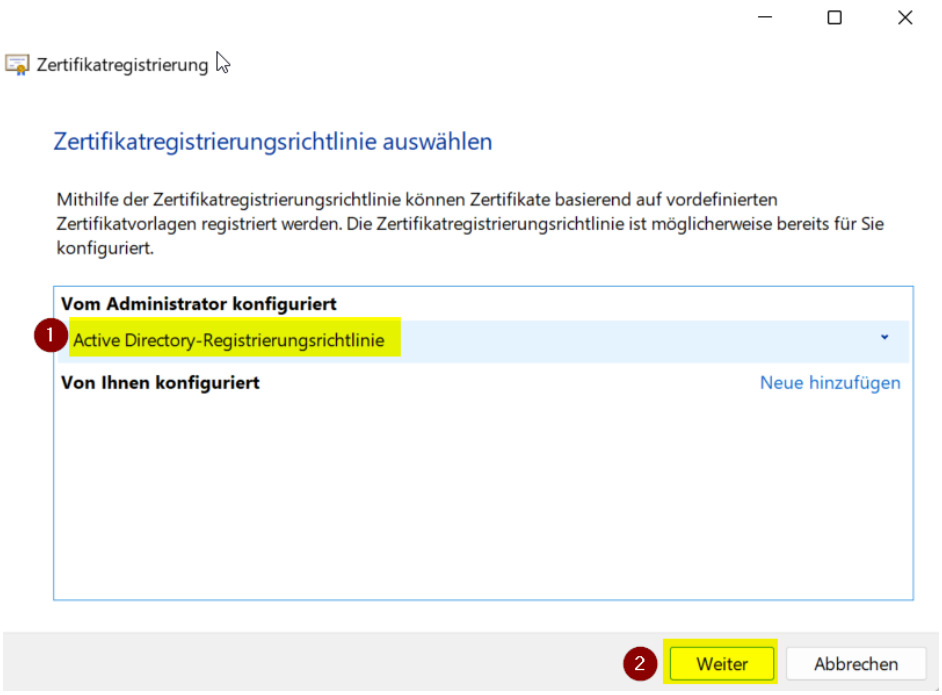
Anschließend wird noch mittels OK bestätigt. In der nachfolgenden Übersicht wählt man "Eigene Zertifikate → Zertifikate" (1)



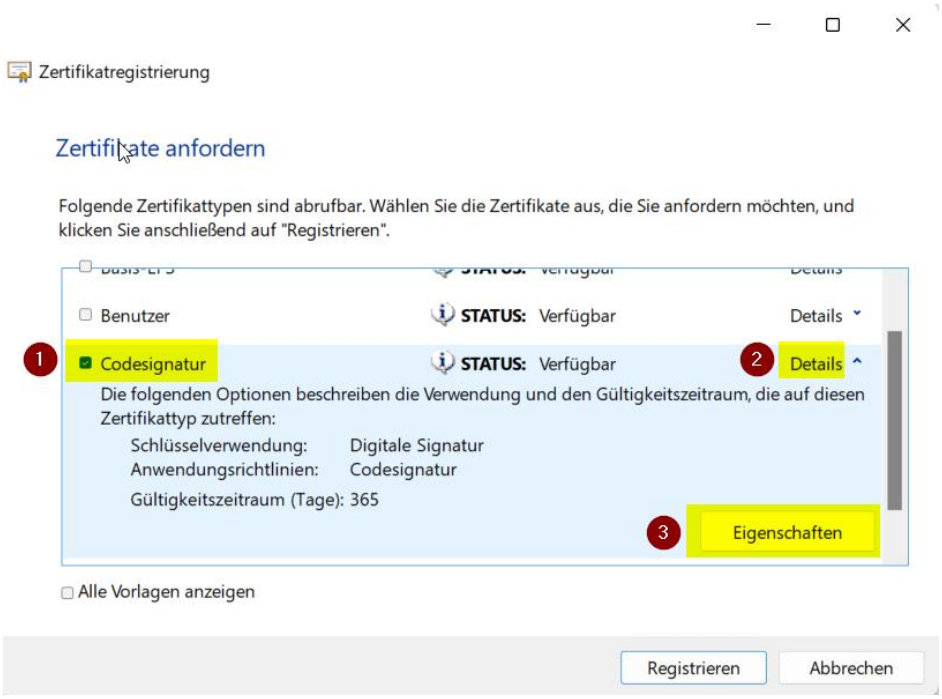
Danach mit der rechten Maustaste auf "Zertifikate → Alle Zertifikate(1) → Neues Zertifikat anfordern(2)"



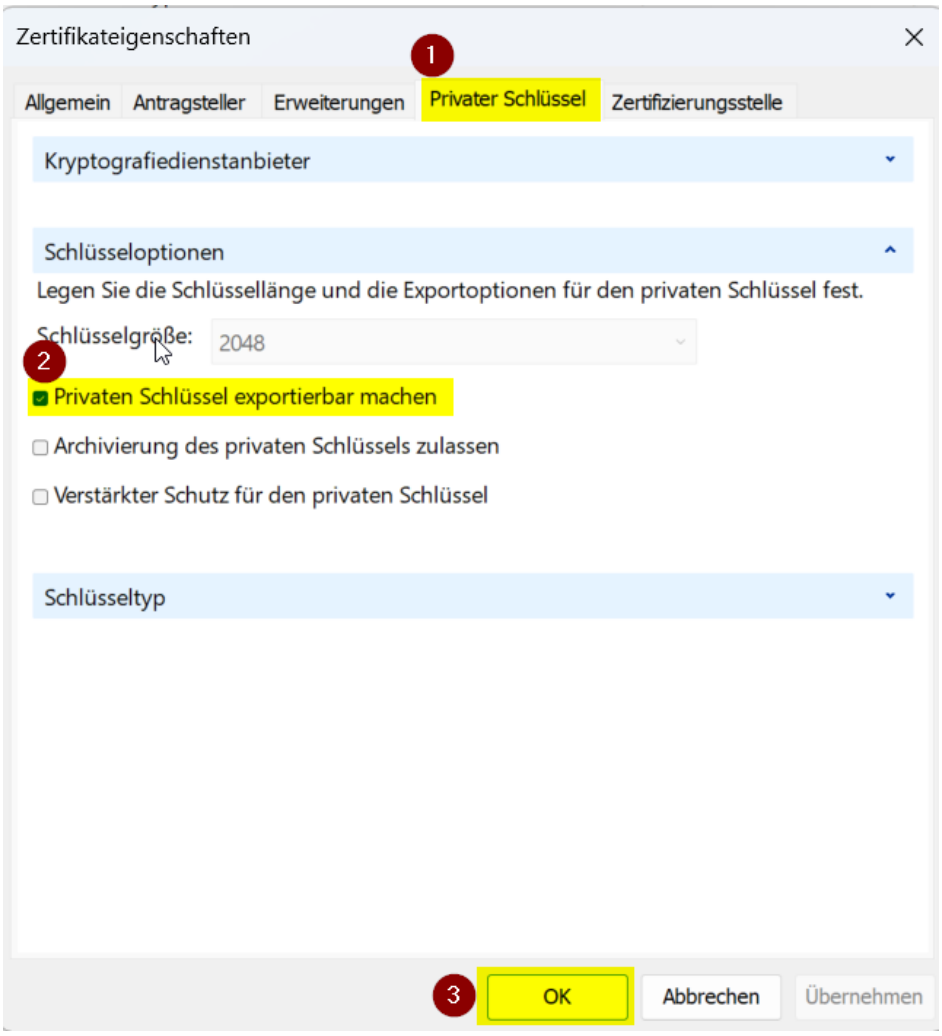
Man wählt die "Active Directory-Registrierungsrichtlinie"(1) und dann auf "Weiter"(2)



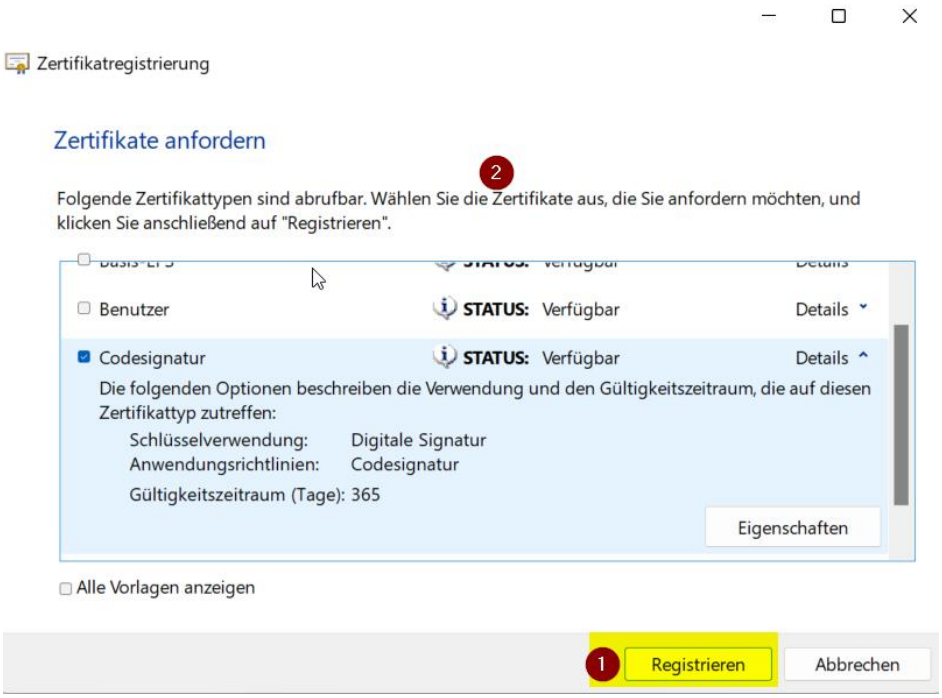
Im folgende Screen wählen wir die Vorlage "Codesignatur"(1) aus, klicken auf "Details"(2) und dann auf "Eigenschaften"(3)



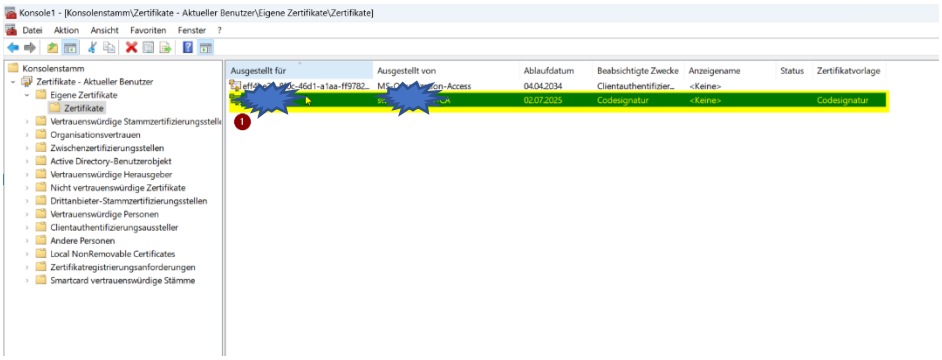
Jetzt markiert man noch den privaten Schlüssel(1) als exportierbar(2) und klickt auf OK(3)



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



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



2.) Skript signieren

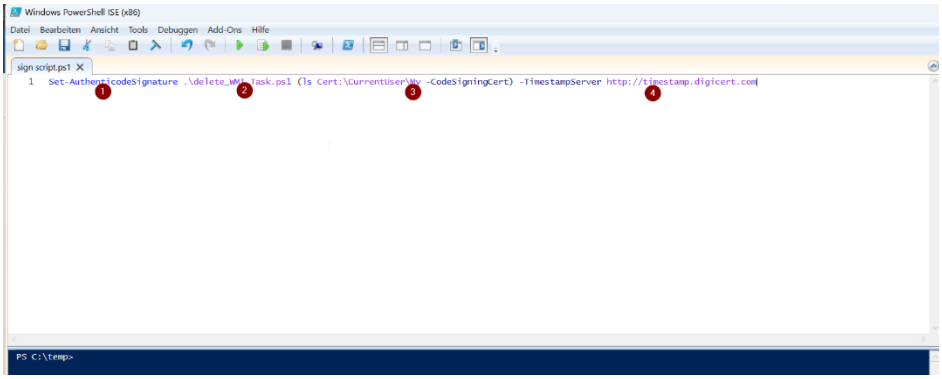
Das eigentliche Signieren ist mit nur einer Zeile erledigt. Der Befehl ist in 4 Bereiche gegliedert

(1) Das CMDlet

(2) das zu signierende Skript

(3) das zu verwendende Zertifikat

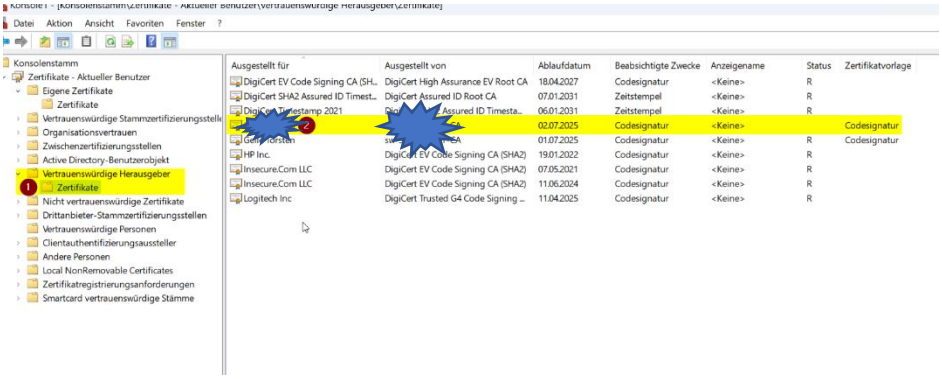
(4) der Timstampserver. Dieser ist nötig, damit die Skripte unbegrenzt gültig und dem Signierer auf unbestimmte Zeit vertraut wird.



3.) Vertrauenswürdige Herausgeber hinzufügen

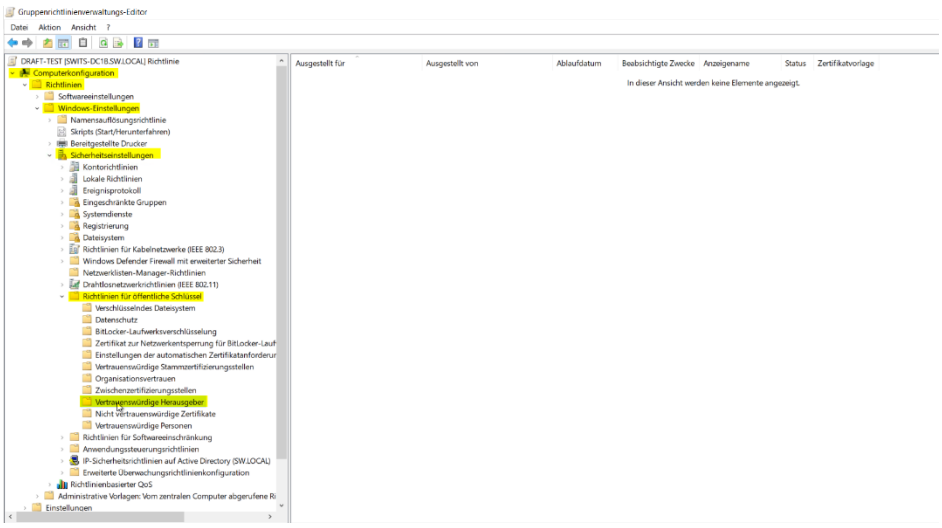
Führt man ein signiertes Skript erstmalig aus, so erhält man eine Warnung, dass der Signierer nicht vertrauenswürdig sei. Dies lässt sich manuell bestätigen. Dadurch wird der Signierer im

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



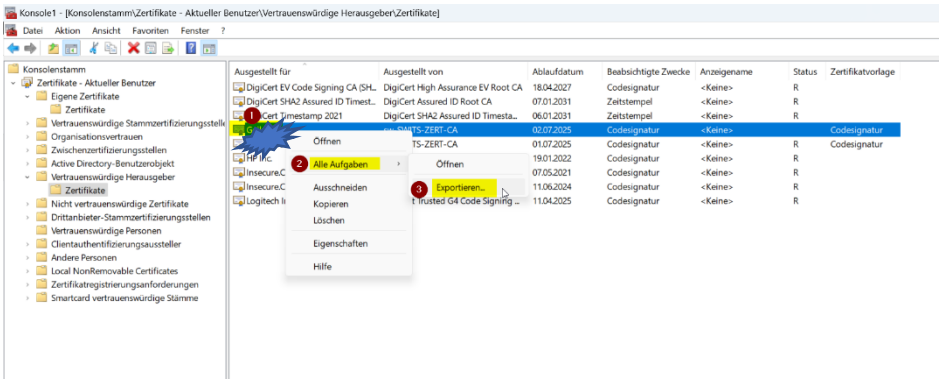
Einfacher ist es jedoch, den "Vertrauenswürdigen Herausgeber" via GPO zu verteilen. So steht er allen im Scope befindlichen Objekten zur Verfügung und muss nicht manuell bestätigt werden.

Innerhalb des GPO ist folgender Bereich zuständig

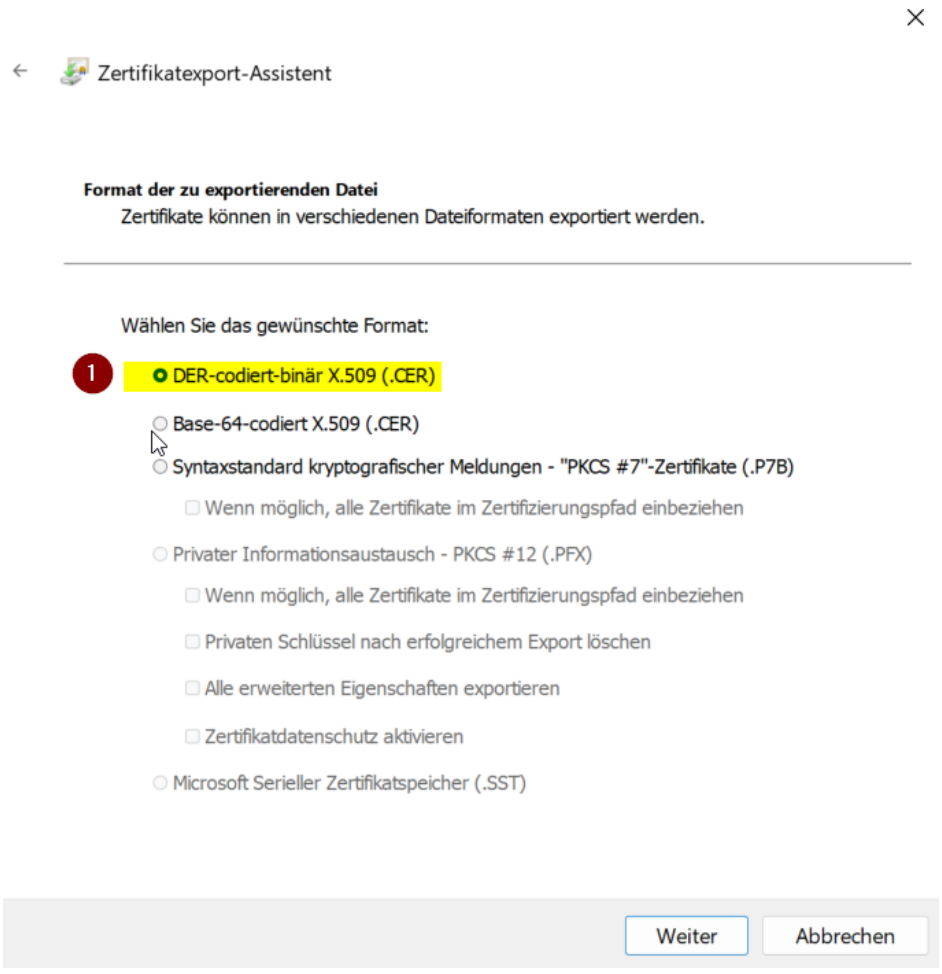


Dort lässt sich das eigene Zertifikat hinterlegen, welches man vorher am eigenen PC exportiert hat. Der Exportvorgang wird wie folgt durchgeführt:

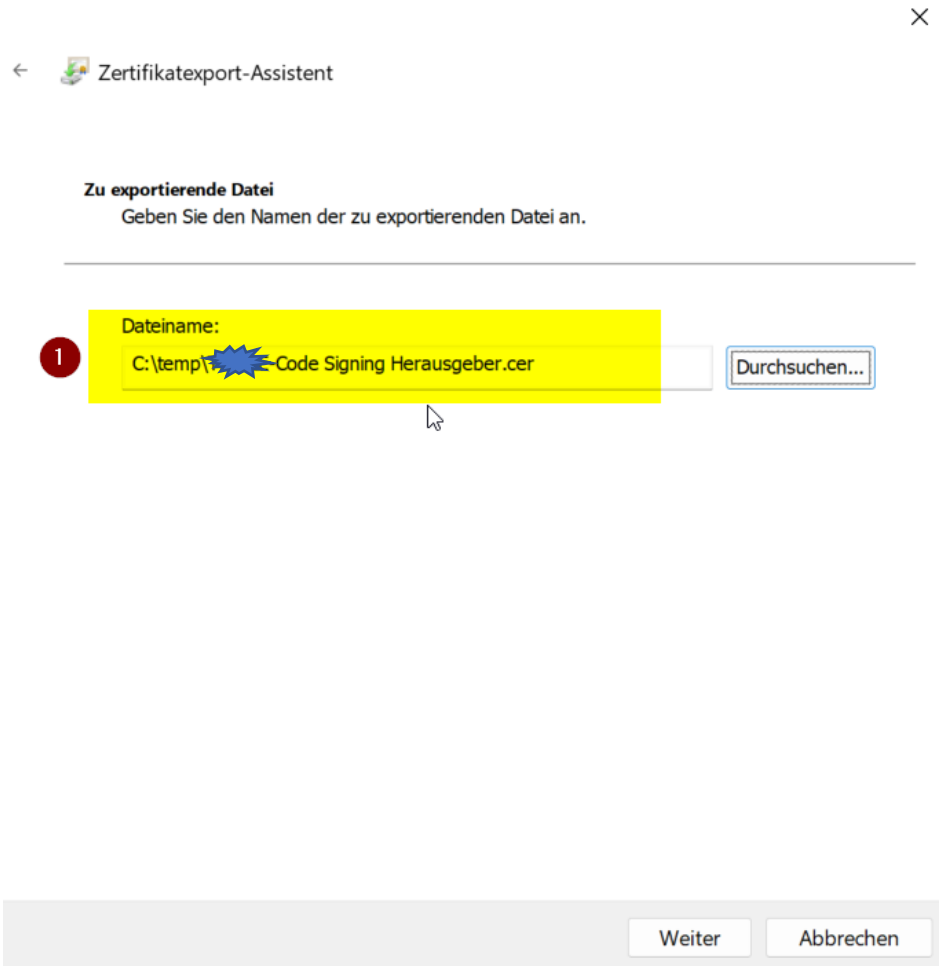
Man wählt im Zertifikatsspeicher das eigene Codesigning Zertifikat aus(1) und klickt mit rechts auf "Alle Aufgaben"(2) und wählt "Exportieren"(3).



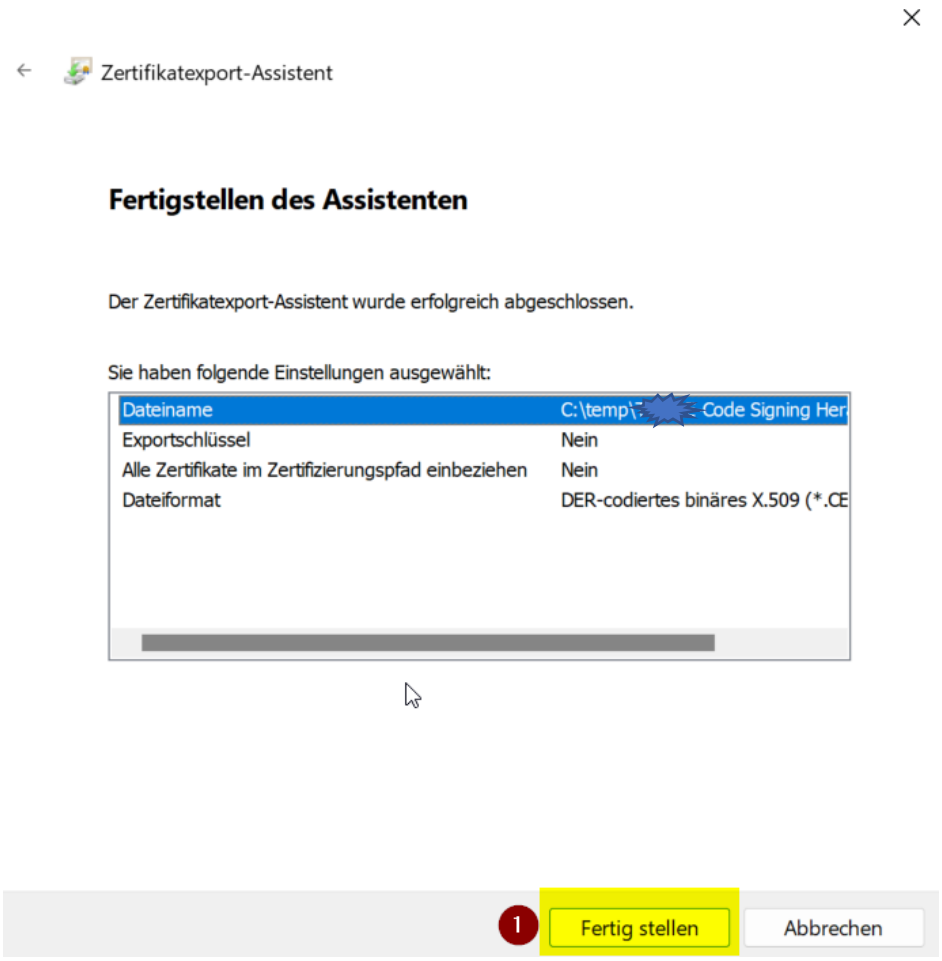
Die Voreinstellung(1) kann man so belassen



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



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



Das exportierte Zertifikat lässt sich dann in das GPO laden.