ekom21

DIE ZUKUNFT DER VERWALTUNG

ERSTELLUNG VON SELBSTSIGNIERTEN CLIENT-ZERTIFIKATEN

Inhaltsverzeichnis

Versionsübersicht

Version	Datum	Autor/-in	Erläuterung
Ver. 0.1	19.03.2026	F. Heidrich	Erstellung des Dokumentes
Ver. 0.2	24.03.2026	C. Kurpanik	Überführung in ekom21 Vorlage, kleinere Korrekturen
Ver. 1.0	10.04.2026	C. Kurpanik	Veröffentlichung nach Lektorat Prüfung

1 Einleitung

Dieses Dokument bietet eine Anleitung zur Erstellung selbstsignierter Client-Zertifikate, die bei WebDAV-Kommunikationsproblemen aufgrund fehlender Client-Authentifizierung benötigt werden.

Beim Aufruf von Dokumenten über die WebDAV-Schnittstelle in civento kann es zu Problemen kommen: Das Dokument lässt sich in diesem Fall nicht in Word öffnen. Ursache kann ein nicht existierendes Client-Zertifikat sein.

Diese Anleitung beschreibt, wie ein selbstsigniertes Client-Zertifikat erstellt werden kann, ohne dass administrative Berechtigungen erforderlich sind. Das erzeugte Zertifikat enthält keine personenbezogenen Daten, da beim WebDAV Aufruf ausschließlich die Client-Authentifizierung geprüft wird. Die Berechtigung, das Dokument zu bearbeiten, wurde bereits intern durch die User-Anmeldung in civento sichergestellt . Das Zertifikat ist für ein Jahr gültig und muss danach verlängert werden.

Wichtig zu beachten: Sofern Sie innerhalb ihrer Organisation über eine eigene Zertifizierungsstelle verfügen, sollten Sie immer die eigene interne Zertifizierungsstelle nutzen. Wenden Sie sich diesbezüglich an Ihre interne IT-Abteilung.

2 Anleitung zur Zertifikatserstellung

2.1 Was für die Zertifikatserstellung benötigt wird

- Windows PowerShell Konsole (im Userkontext ausgeführt, keine Adminrechte notwendig)
- Microsoft Management Console (mmc) (im Userkontext ausgeführt, keine Adminrechte notwendig)
- PowerShell Befehl aus der offiziellen Microsoft Dokumentation („Example 4"): *https://learn.microsoft.com/en-us/powershell/module/pki/new-selfsignedcertificate?view=windowsserver2025-ps#example-4*

2.2 Aufruf der Microsoft Dokumentation

Wenn Sie den Link zur Dokumentation (siehe Kapitel 2.1) aufgerufen haben, sollte Ihnen „Example 4" angezeigt werden:

EXAMPLE 4

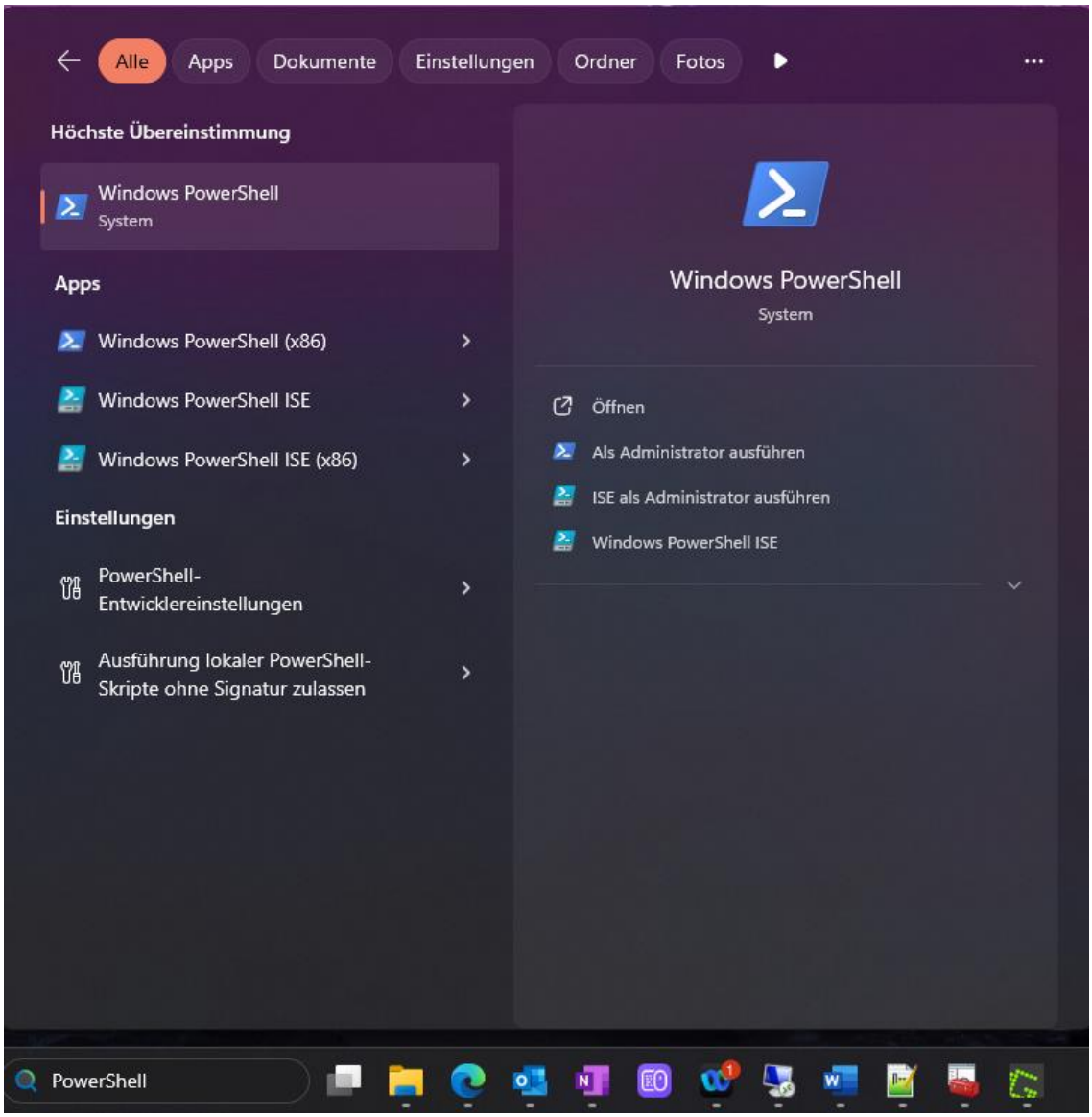
This example creates a self-signed client authentication certificate in the user `MY` store. The certificate uses the default provider, which is the `Microsoft Software Key Storage Provider`. The certificate uses an `RSA` asymmetric key with a key size of `2048` bits. The certificate has a subject alternative name of `pattifuller@contoso.com`.

The certificate expires in one year.

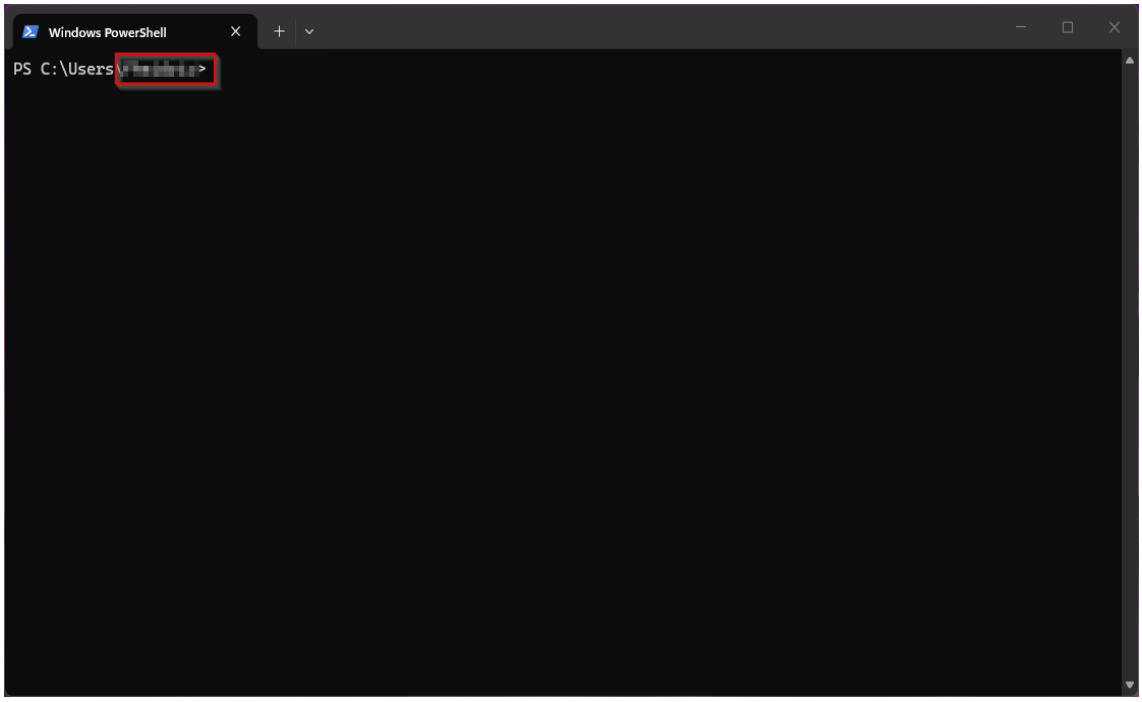
Nutzen Sie den Button „Copy", um den PowerShell Befehl in die Zwischenablage zu speichern. Der Befehl wird für den folgenden Schritt (Kapitel 2.3) benötigt.

2.3 Zertifikatserstellung via PowerShell Konsole

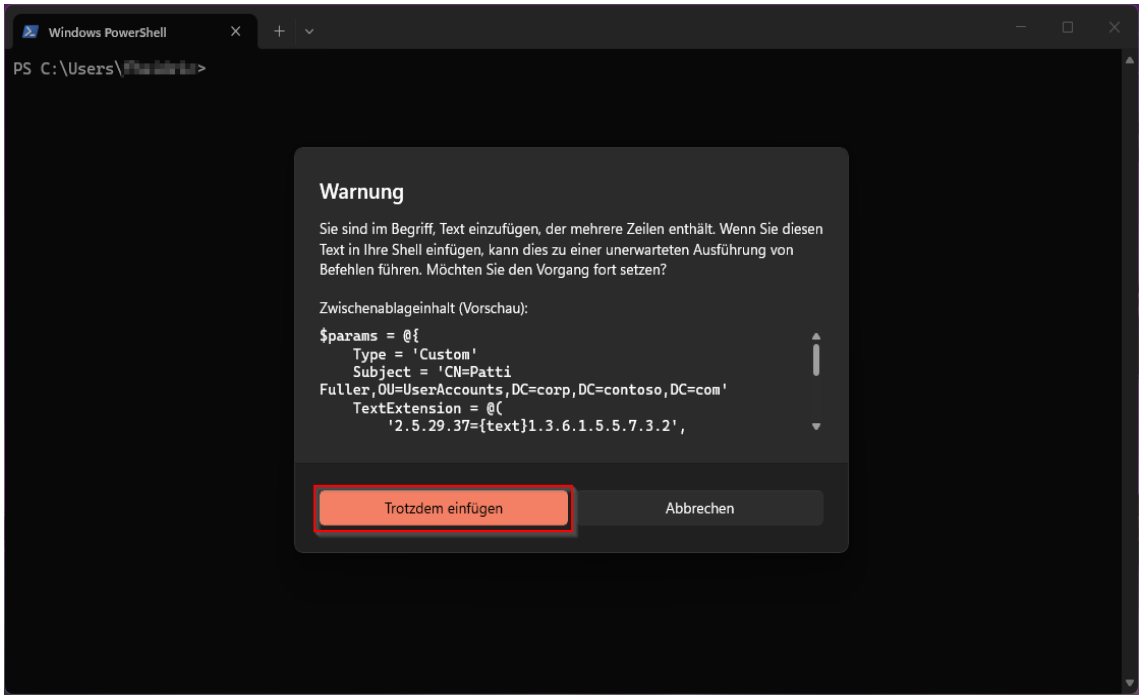
Geben Sie in der Windows Suchleiste „PowerShell" ein. Mit einem Klick auf „Windows PowerShell" oder auf „Öffnen" startet die Windows PowerShell Konsole.



In der Konsole sollten Sie hinter „PS C:\Users\...“ Ihren Benutzernamen sehen.

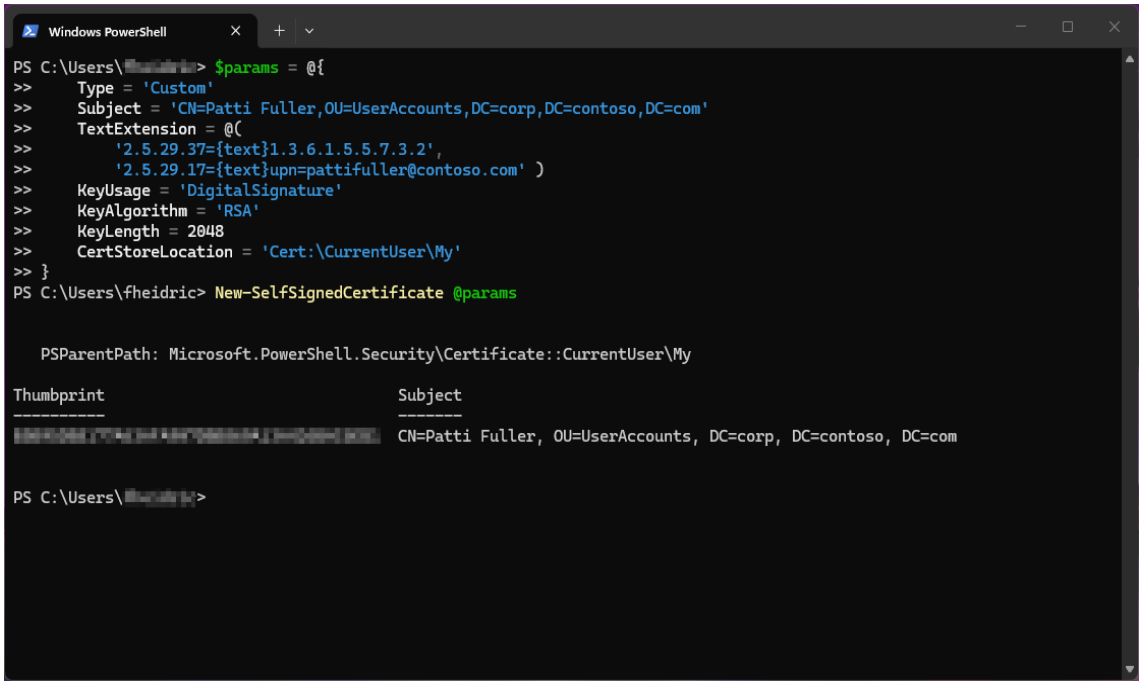


Durch einen Rechtsklick können Sie den vorab gespeicherten Befehl in der Konsole einfügen. Gegebenenfalls muss der Befehl nochmals in die Zwischenablage gespeichert werden (Kapitel 2.2). Nach dem Einfügen erscheint die folgende Warnung:



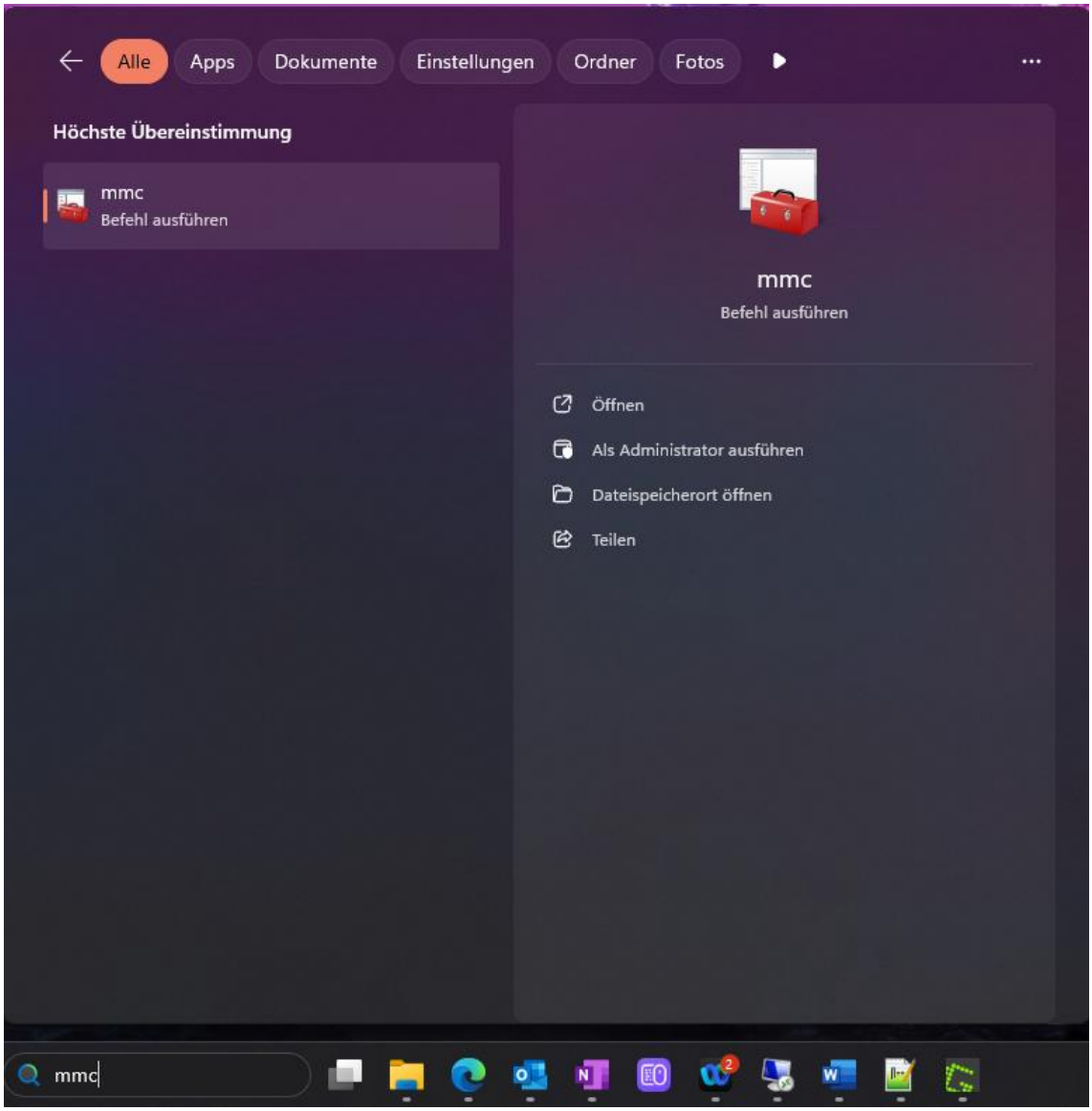
Bestätigen Sie die Warnung mit einem Klick auf „Trotzdem einfügen“. Nachdem Sie die Warnung bestätigt haben, werden Ihnen zwei PowerShell Eingaben angezeigt. Hier müssen Sie mit „Enter“ die letzte Eingabe ausführen.

Daraufhin sollten Sie folgende Ausgabe sehen:

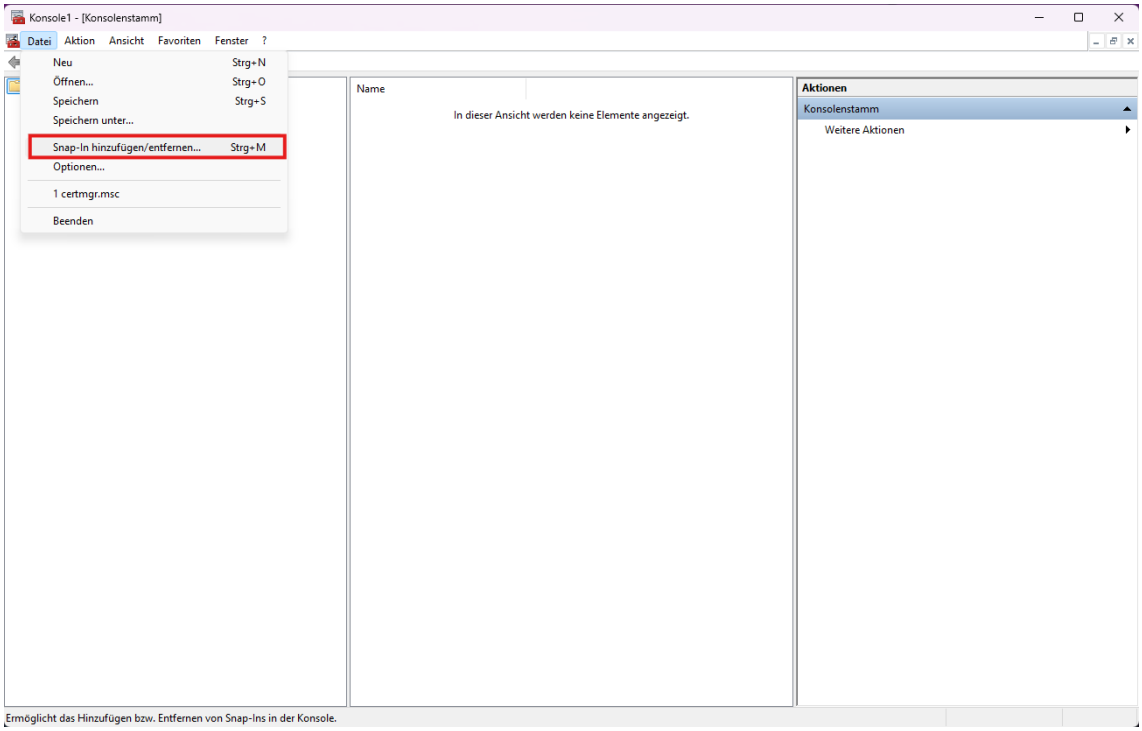


2.4 Überprüfung des erstellten Zertifikats

Um zum Abschluss zu überprüfen, ob das Zertifikat erfolgreich erstellt wurde, geben Sie in der Windows Suche „mmc" ein und klicken Sie auf „Öffnen". Die Microsoft Management Console öffnet sich.

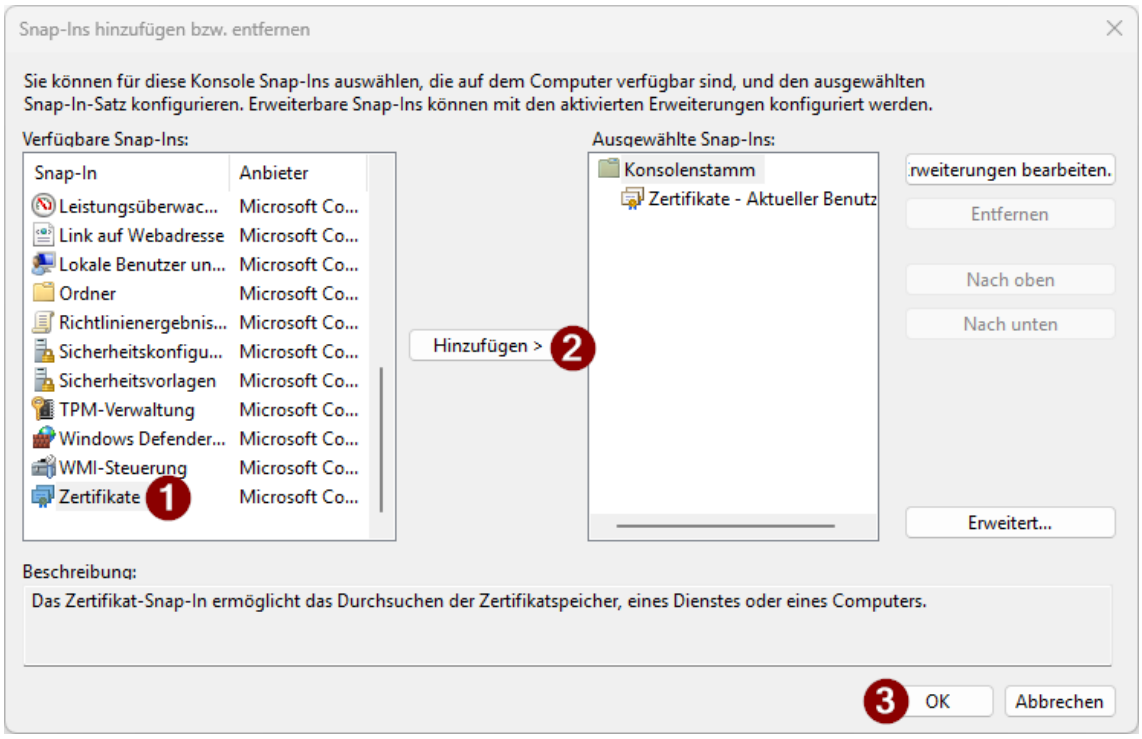


In der Konsole klicken Sie auf „Datei“ und anschließend auf „Snap-In hinzufügen/entfernen…“

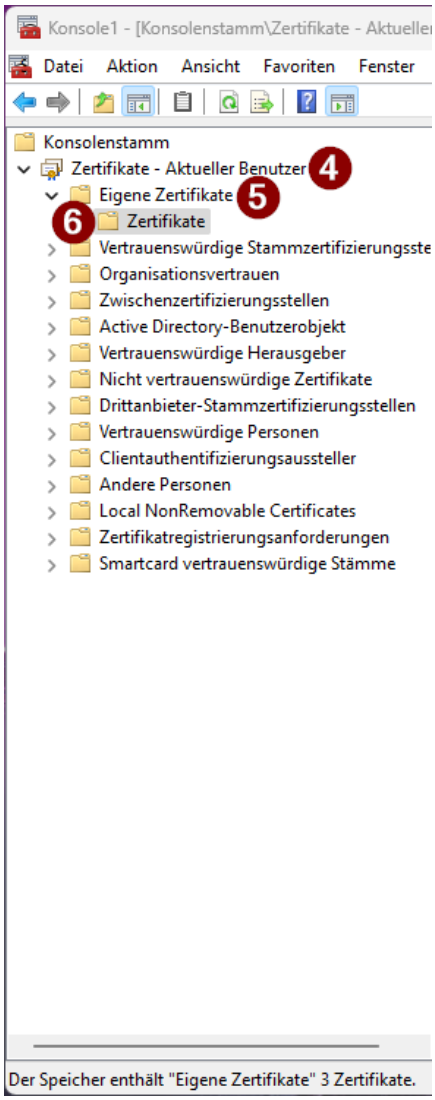


Anschließend wählen Sie in der Liste „Zertifikate“ (1) aus und klicken auf „Hinzufügen >“ (2) .

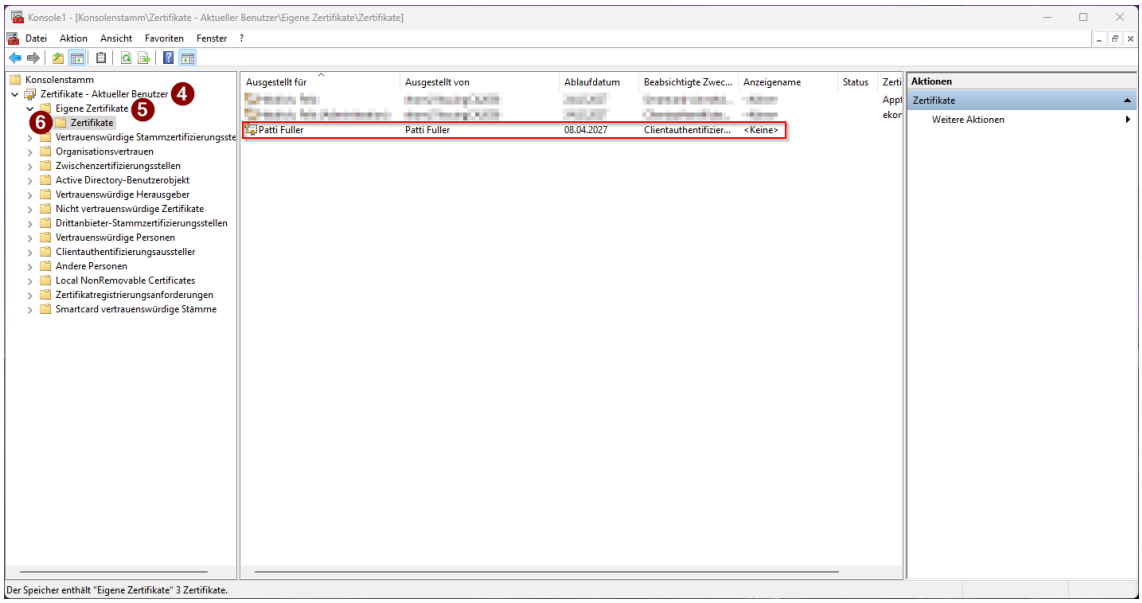
Mit Klick auf „OK“ (3) bestätigen Sie die Auswahl.



Daraufhin muss der Konsolenstamm erweitert werden. Klicken Sie auf „Zertifikate – Aktueller Benutzer" (4), „Eigene Zertifikate" (5) und zuletzt auf „Zertifikate" (6).



In der mittleren Spalte sehen Sie dann Ihr erstelltes Zertifikat mit Ihrem Benutzernamen (im Beispielbild „Patti Fuller"). Das Zertifikat ist ab dem Zeitpunkt der Erstellung ein Jahr gültig.



ekom21 – KGRZ Hessen

Körperschaft des öffentlichen Rechts

Carlo-Mierendorff-Straße 11

35398 Gießen

www.ekom21.de