Root-CA für TightGate-Viewer unter Windows zentral bereit stellen

Sofern die Benutzer-Authentifizierung beim TightGate-Pro über einen Active-Directoty erfolgt, so muss bei der ersten Anmeldung dem Sicherheitszertifikat von TightGate-Pro vertraut werden. Dies ist notwendig, damit der TightGate-Viewer eine verschlüsselte Verbindung zum TightGate-Pro Server aufbauen kann.

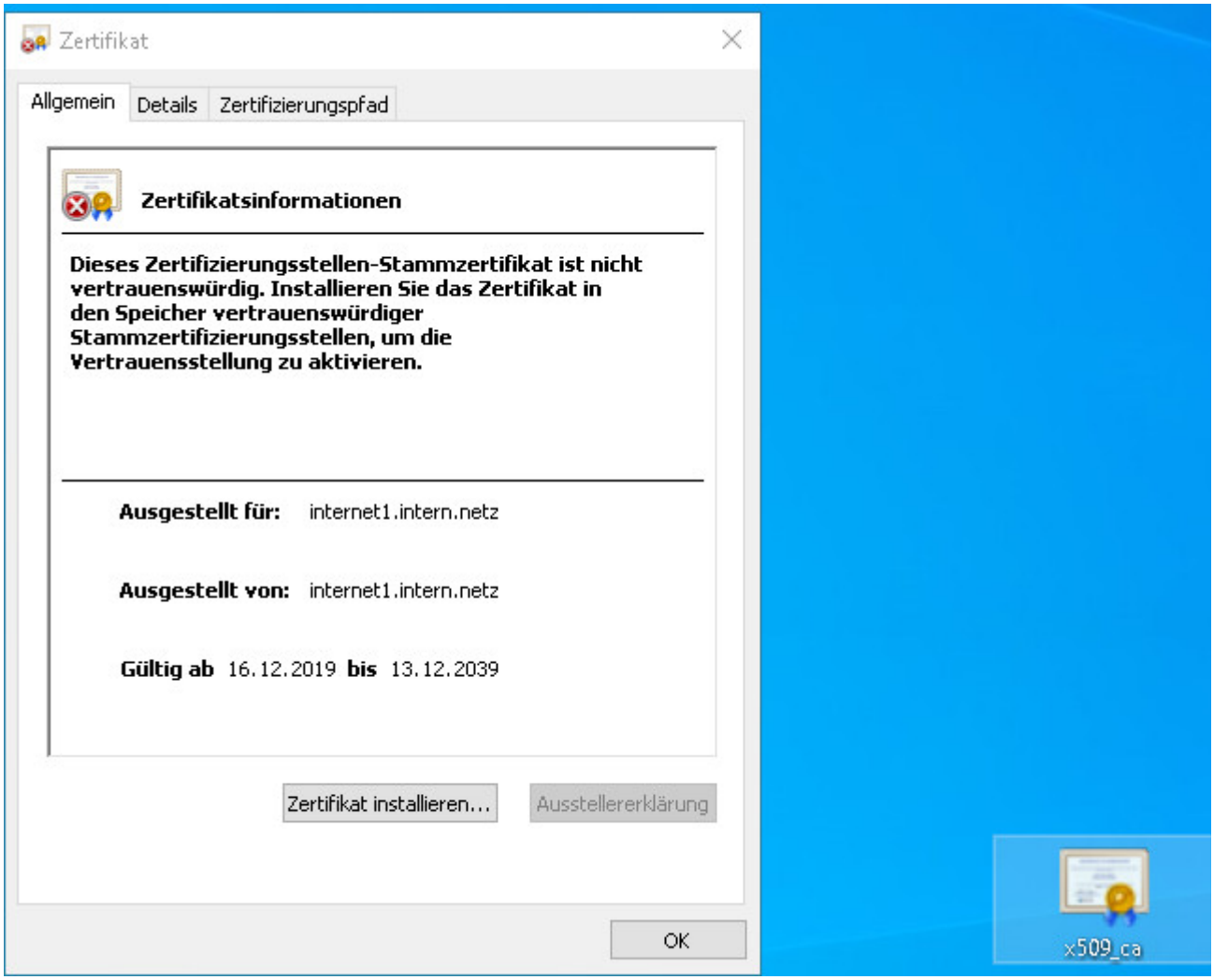
Möchte man vermeiden, dass die Frage zum Vertrauen der Anmeldung bei der ersten Anmeldung erscheint, so kann man das Root-CA-Zertifikat zentral im Windows Zertifikatsspeicher ablegen. Die nachfolgende Anleitung beschreibt die Vorgehensweise.

Root-CA exportieren

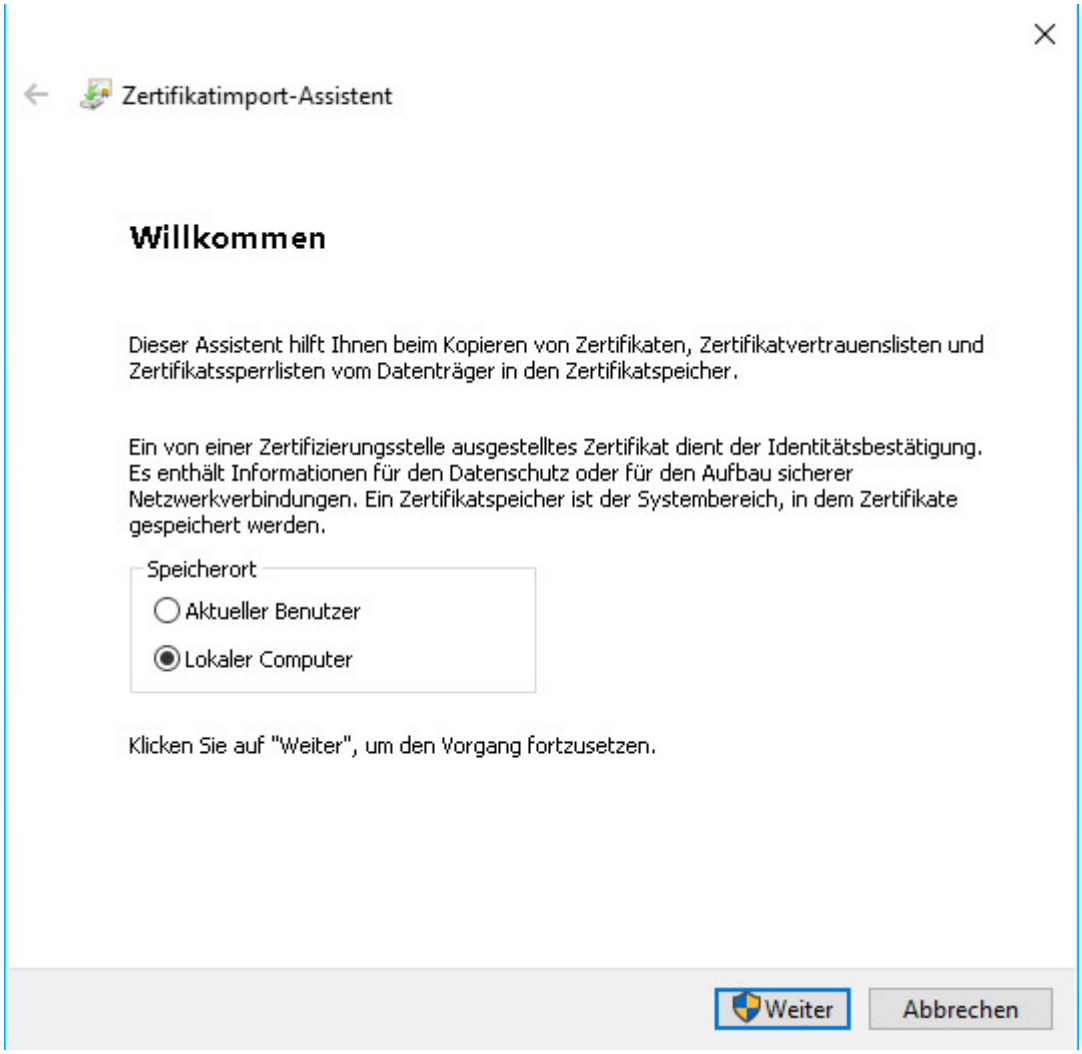
1. Bitte am TightGate-Pro als Administrator ***maint*** anmelden den Menüpunkt **Benutzerverwaltung > Erzeuge SSL-Schlüssel** aufrufen.
2. Einen bestehenden BENUTZER auswählen und den Dialog **SSL-Schlüssel wurde erzeugt oder aktualisiert für BENUTZER XYZ** mit **OK** bestätigen.
3. Die nachfolgende Frage **Sollen die Erstellten Zertifikate nun exportiert werden?** mit **Ja** bestätigen.
4. Verbinden Sie sich jetzt mit einem SFTP-Program (z.B. WinSCP) mit dem TightGate-Pro als Benutzer Administrator ***config***. Unter dem Verzeichnis **/home/user/.transfer/config/certs/BENUTZER** befindet sich nun die Datei **x509_ca.pem**.
5. Kopieren Sie diese Datei auf den Windows-Computer, in dessen Zertifikatsspeicher sie importiert werden soll.
6. Benennen Sie die Datei **x509_ca.pem** in **x509_ca.crt** um.

Zertifikatsdatei in den Windows-Zertifikatsspeicher importieren

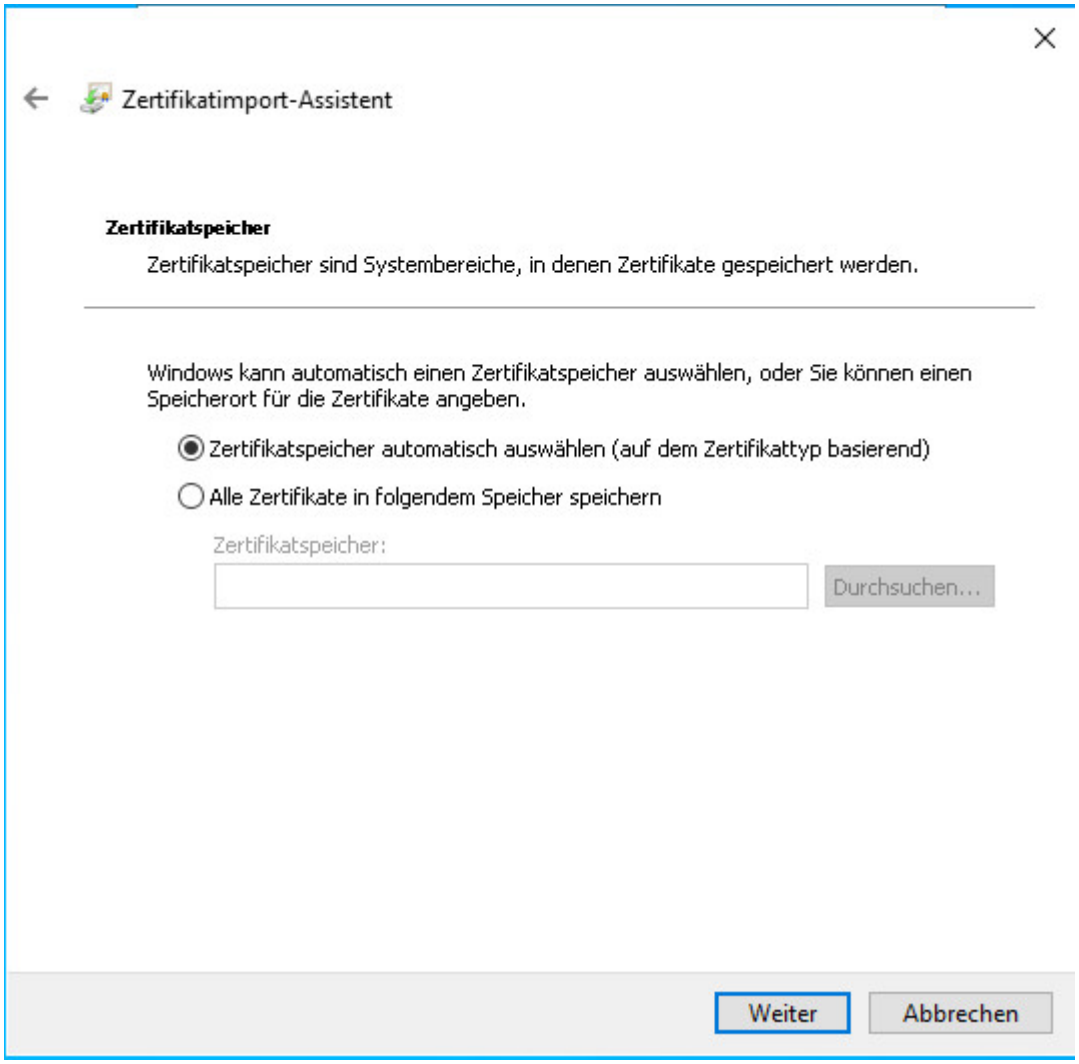
- Einen Doppelklick auf die Datei **x509_ca.crt** ausführen.
- Es öffnet sich das Zertifikat. Klicken Sie auf die Schaltfläche **Zertifikat installieren…**



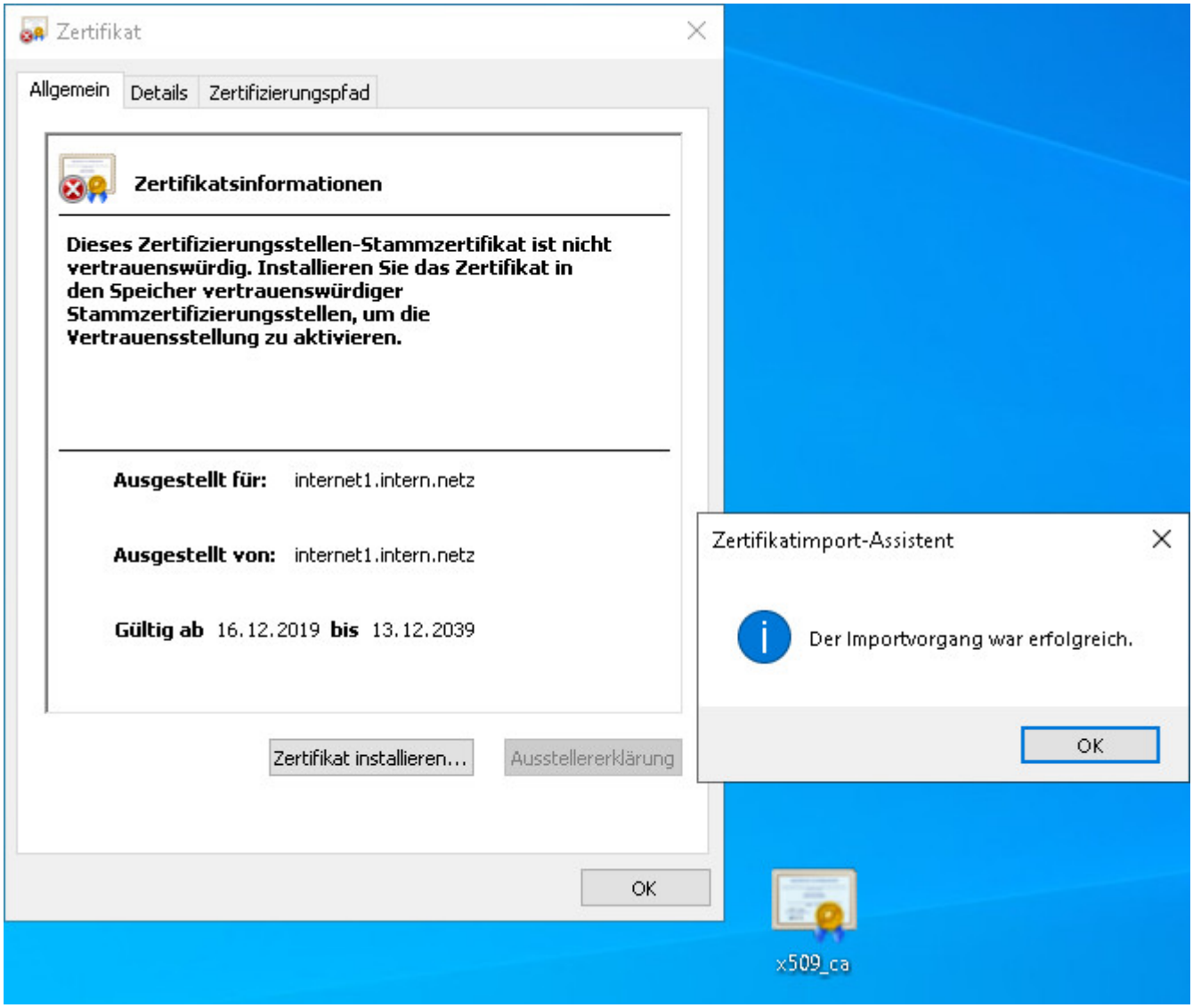
- Es öffnet sich der Assistent zum Zertifikatimport. Wählen Sie **Lokaler Computer** aus.



- Anschließend den bevorzugten Zertifikatsspeicher auswählen und anschließend auf Fertig stellen.



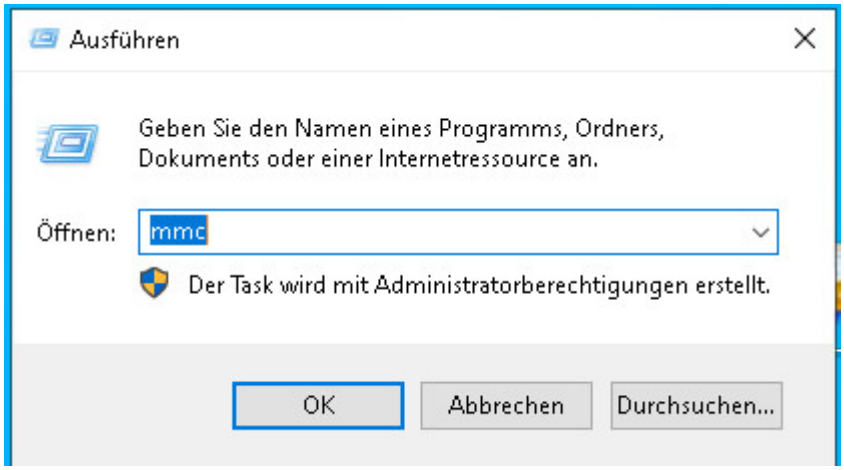
- Es sollte eine Nachricht zum erfolgreichen Import erscheinen.



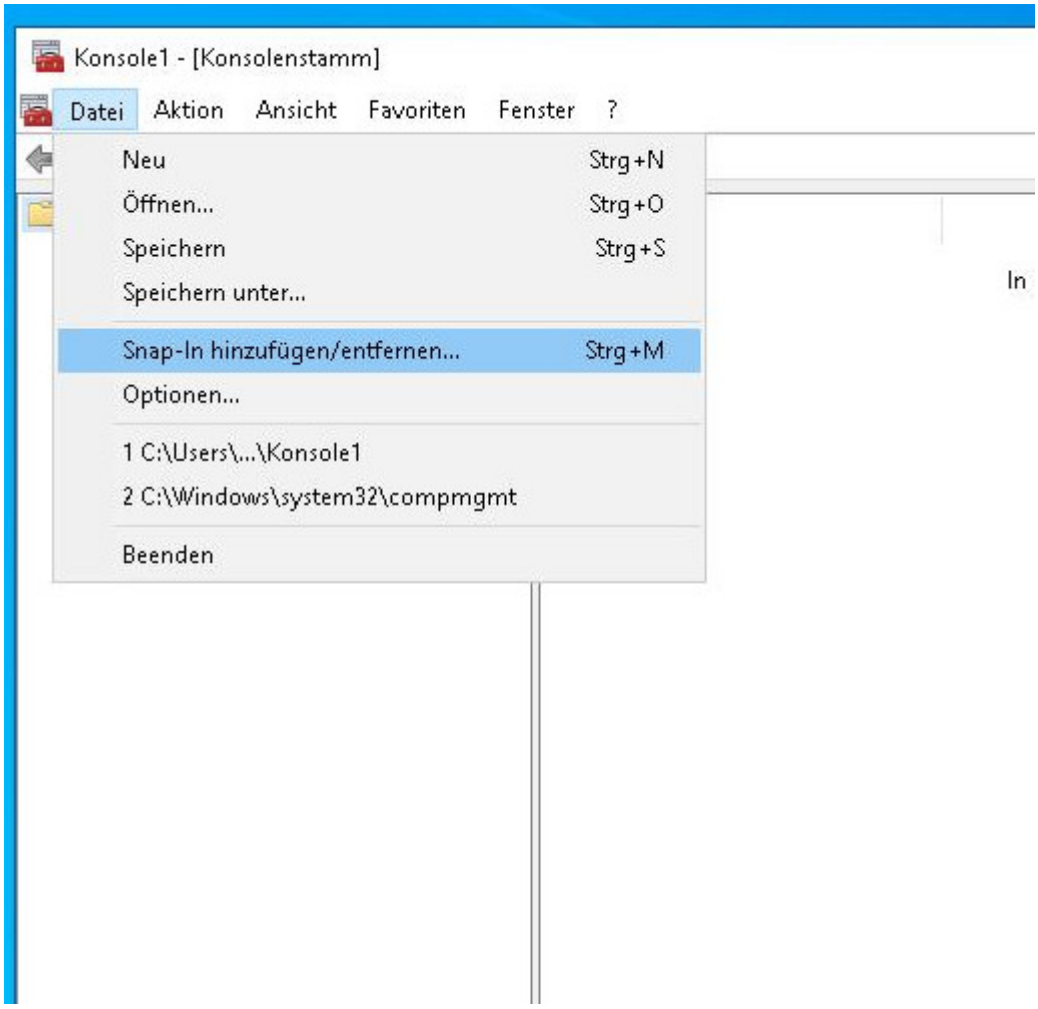
- Zum Schluss das Verzeichnis %APPDATA%\vnc löschen. Die SSO-Anmeldung mit AD sollte funktionieren, ohne dass die TLS-Bestätigungsmeldung erscheint. Die Datei **x509_savedcerts.pem** sollte nach dem Schließen des TightGate-Viewers nicht erstellt werden.

Entfernen der Zertifikatsdatei aus dem Windows-Zertifikatsspeicher

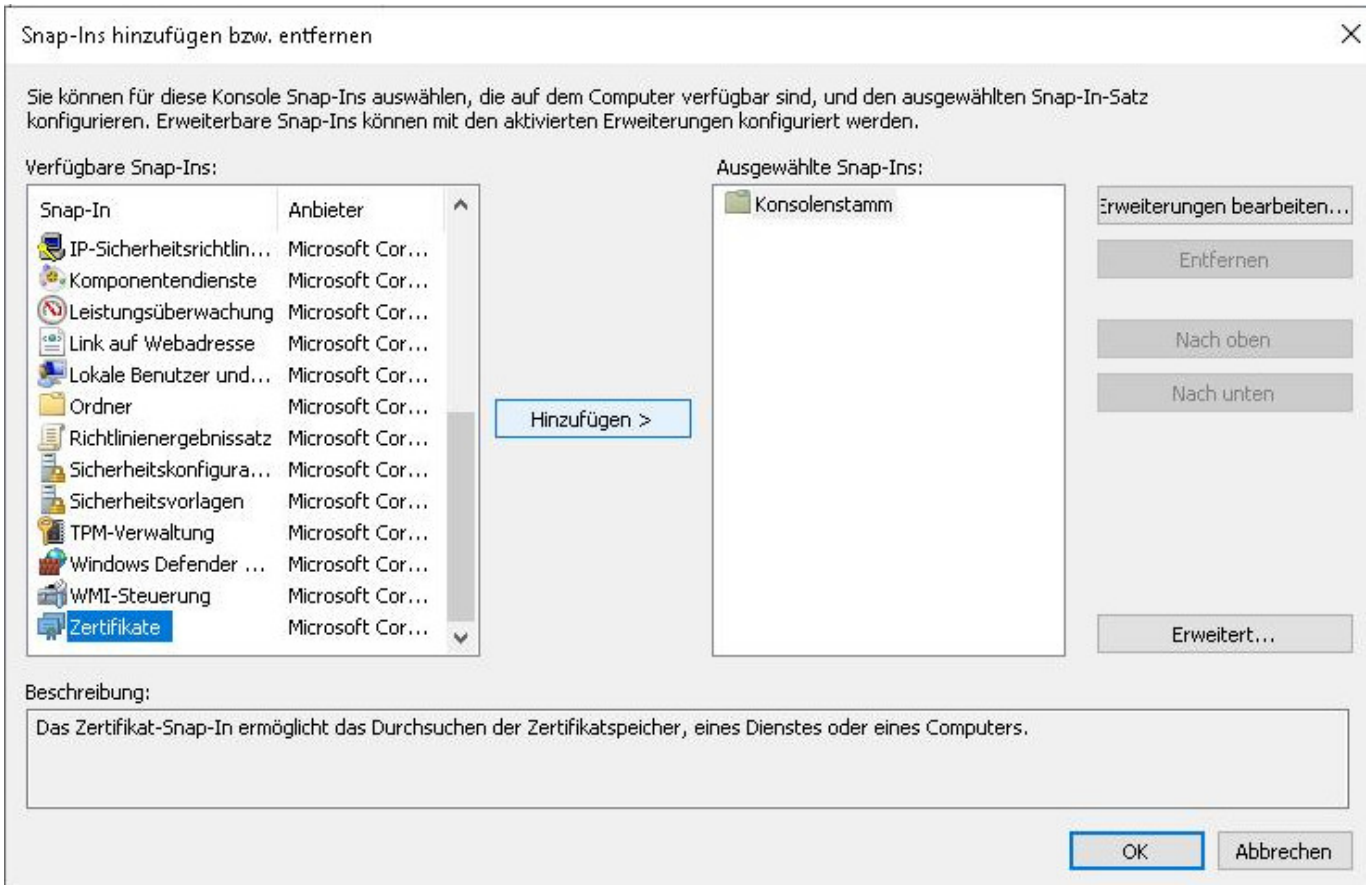
- Melden Sie sich als **Administrator** auf dem Windows-PC an.
- Rechtsklick auf das **Windows-Symbol > Ausführen**. Geben Sie **mmc** ein und bestätigen Sie mit **OK**.



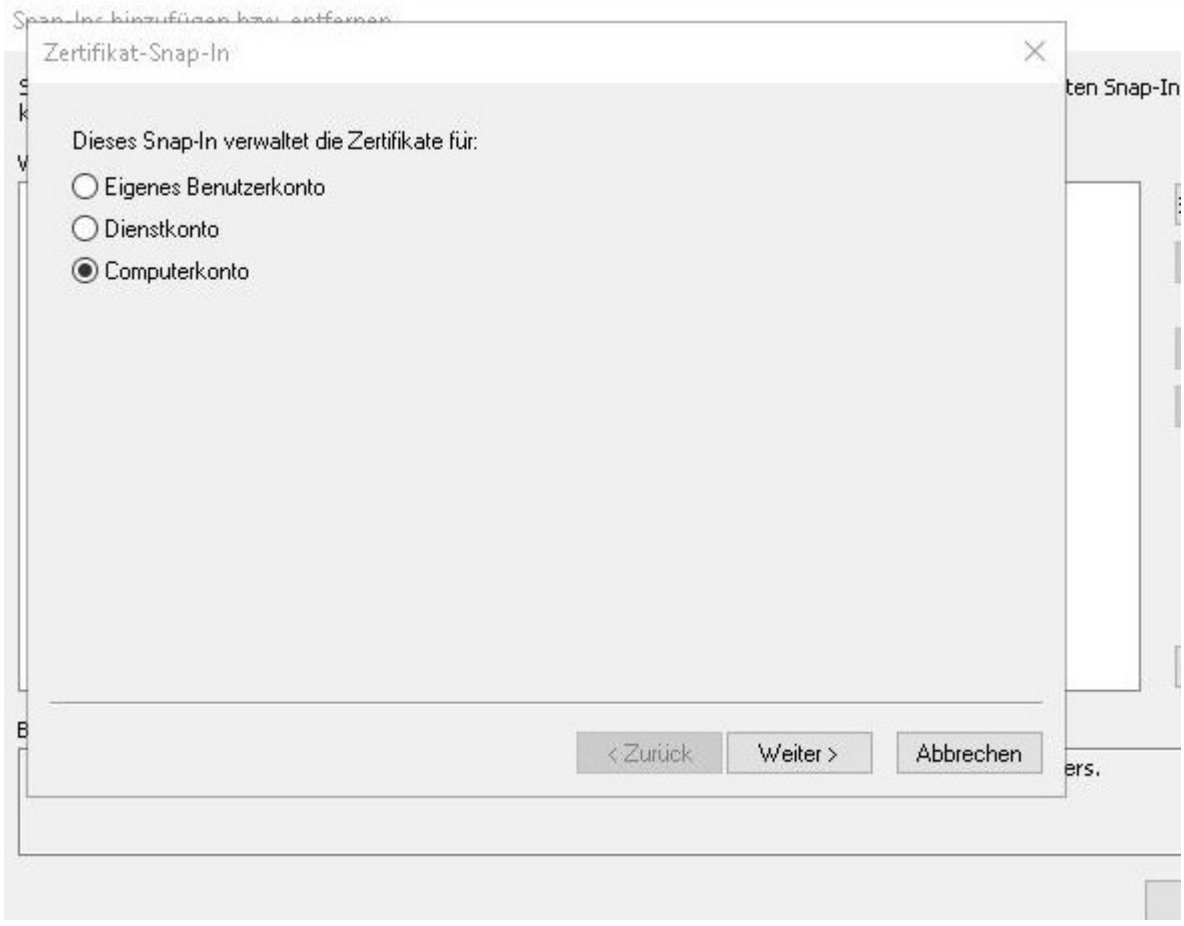
- Die **Microsoft Management Console** öffnet sich. In der Konsole bitte auf **Datei > Snap-In hinzufügen/entfernen...** klicken.



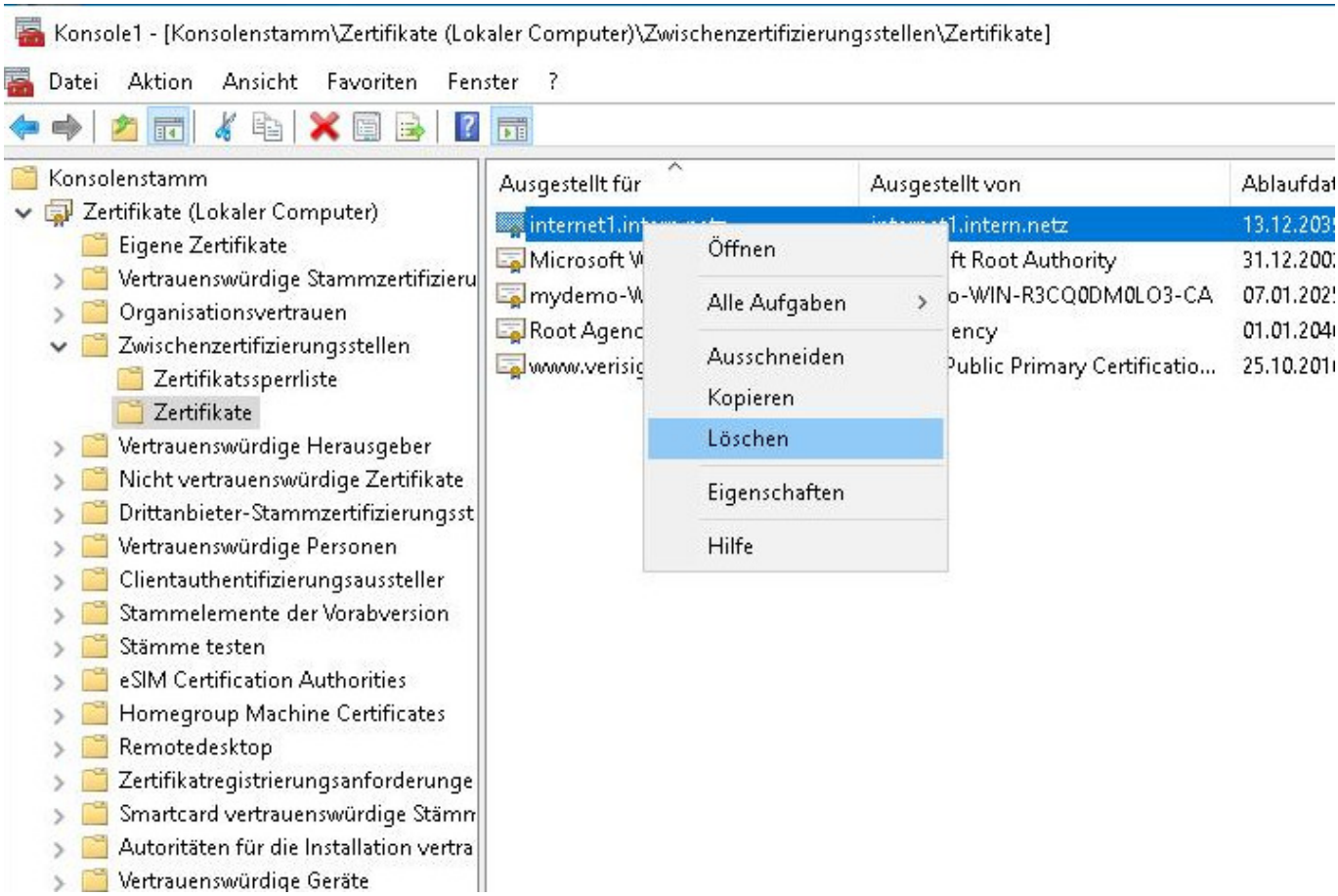
- Im folgenden Fenster im linken Unterfenster runterscrollen, das Snap-In **Zertifikate** auswählen und anschließend auf **Hinzufügen** klicken.



- Es öffnet sich ein weiteres Fenster, in dem **Computerkonto** auszuwählen ist und danach noch **Lokalen Computer**. Schließen Sie die Eingabe mit **OK** ab.



- Anschließend Rechtsklick auf **Eigene Zertifikate > Zertifikate** und Auswahl des Menüpunktes **Löschen**.



- **Nicht vergessen!** Zum Schluss die Microsoft Management Console-Session speichern mit **Datei > Speichern / Speichern unter ...**
- Fertig, nun sollte die TLS-Bestätigungsmeldung beim Starten von TightGate-Pro wieder angezeigt werden.

From:
https://help.m-privacy.de/ -

Permanent link:
https://help.m-privacy.de/doku.php/faq:tightgate_pro_root_ca

Last update: **2021/04/01 10:47**