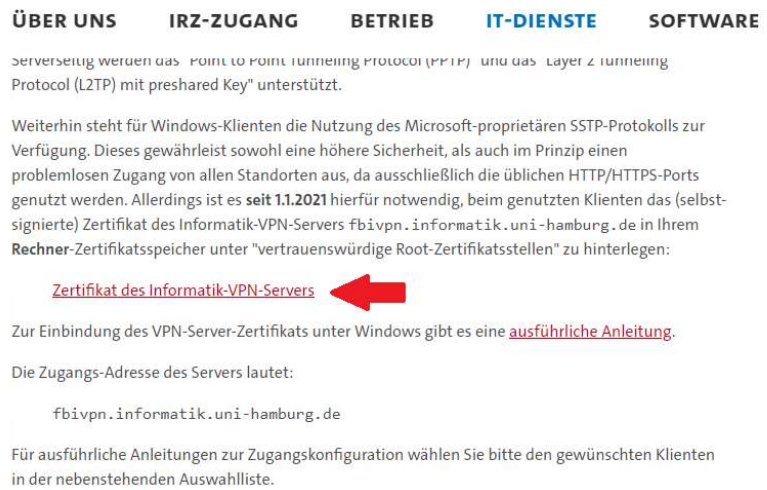
Einbinden des VPN-Server-Zertifikates unter Windows

Tb, 4.1.2021

Für die Einrichtung einer sicheren SSTP-VPN-Verbindung wird auf dem Verbindungsanfordernden (privaten) Rechner explizit das Server-Zertifikat des VPN-Servers *fbivpn.informatik.uni-hamburg.de* benötigt. Grund hierfür ist die Situation, dass der VPN-Server der Informatik die Anmelde-Informationen der Benutzer gegenüber der Informatik-Benutzerdomäne überprüft und auch besondere Zugangsrechte auf Informatik-Benutzer-/Gruppen-Ebene vergibt. Daher ist ein geschlossener Authentisierungsablauf zwingend. Für den VPN-Server sind „Fremdzertifikate“, wie z.B. die üblicherweise vom DFN-Verein für Universitäts-Rechner ausgestellten Zertifikate nicht von Belang.

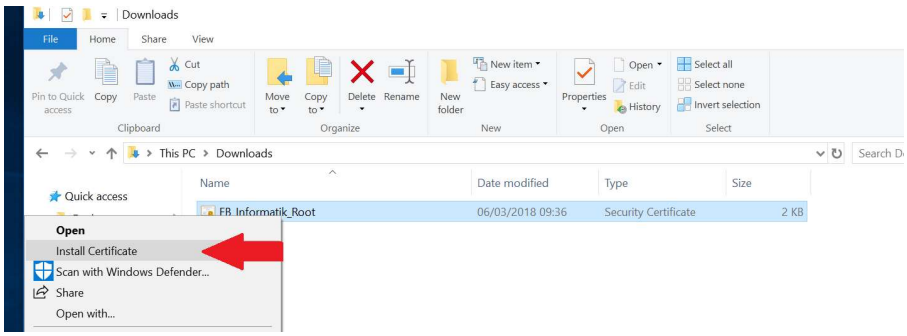
Gegenüber den anfragenden VPN-Clients präsentiert daher der VPN-Server immer sein eigenes Rechner-/Server-Zertifikat. Damit ein anfragender Rechner dieses Zertifikat erfolgreich verifizieren kann, muss das VPN-Server-Zertifikat auch im Zertifikatsspeicher des jeweiligen Rechners unter „Vertrauenswürdige Stammzertifizierungsstellen“ hinterlegt werden.

Speichern Sie daher von der Web-Seite https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html das dort verfügbare VPN-Server-Zertifikat auf Ihren Rechner (über eine bestehende Internet-Verbindung z.B. von zuhause, über eine VPN-Verbindung, oder über einen Pool-Rechner und anschließend offline via USB-Stick):

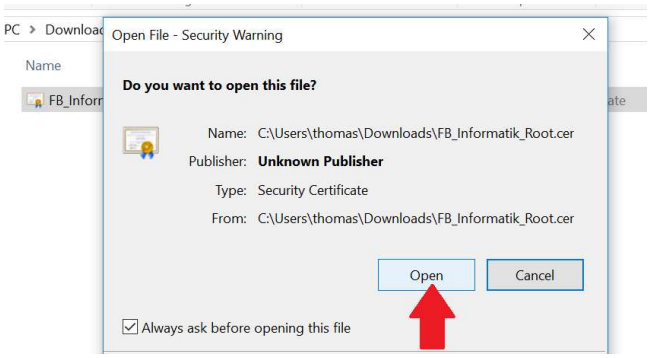


Methode 1: Zertifikat direkt installieren

Über „rechte Maustaste“ -> Kontextmenü „*Zertifikat installieren*“ kann das VPN-Server-Zertifikat direkt im Zertifikatsspeicher des Rechners abgelegt werden:

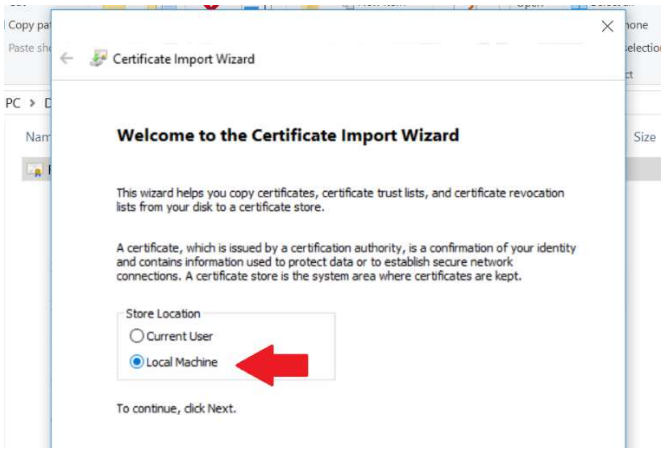


Bestätigen Sie im automatischen Installationsablauf nun das Öffnen des Zertifikats:



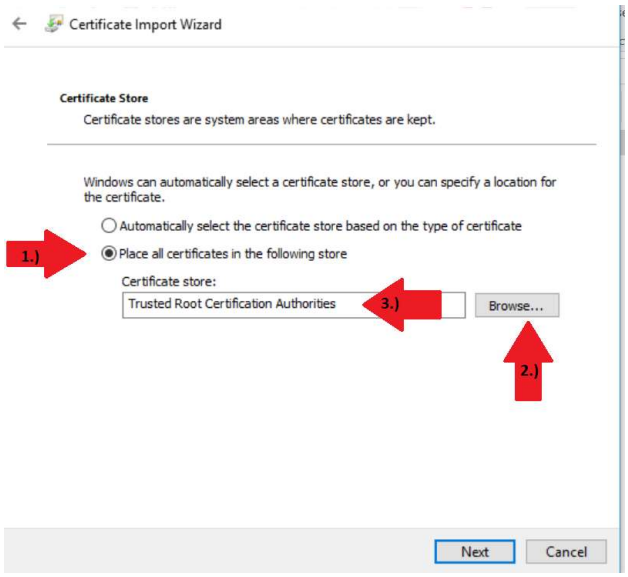
Beachten Sie genau den im Folgenden beschriebenen Ablauf, da die Standardwerte des automatischen Installations-Ablaufs nicht zum gewünschten Ergebnis führen !

Wählen Sie den Eintrag „Lokaler Computer“ als Speicherort für das Zertifikat:



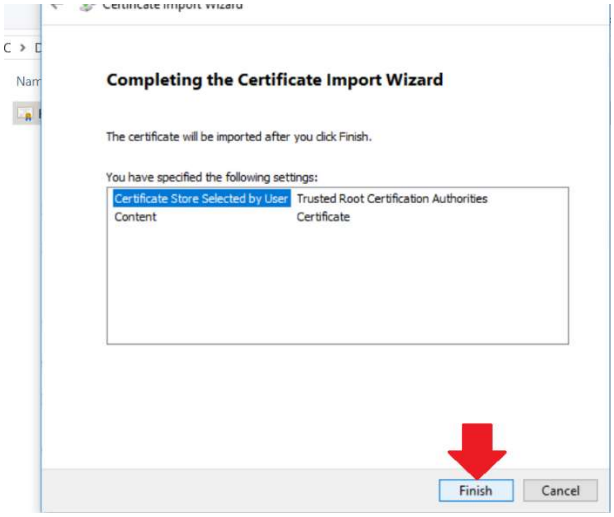
Ist die Auswahl des „Lokalen Computers“ hier nicht möglich/sichtbar, liegt dies an fehlenden Administrator-Rechten Ihrer derzeitigen Anmeldung. Nutzen Sie in diesem Fall die unten erläuterte Methode über MMC !

Wählen Sie die explizite Auswahl des Speicherplatzes (1.),

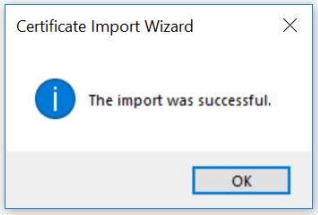


Ermitteln Sie über „suchen“ (2.) den Speicherplatz „Vertrauenswürdige Stammzertifizierungsstellen“ aus (3.).

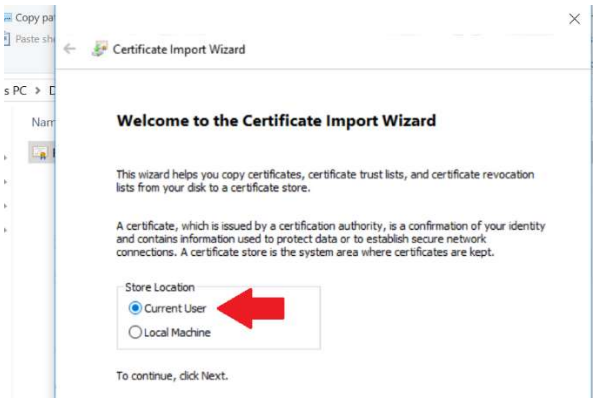
Abschließend wird noch einmal nach Bestätigung des ausgewählten Speicherplatzes gefragt:



Der Erfolg des Imports wird nun vom System bestätigt:



Wiederholen Sie den eben durchgeführten Ablauf (Import des Root-Zertifikats über rechte Maustaste) nun noch einmal für den Speicherplatz „Lokaler Benutzer“:

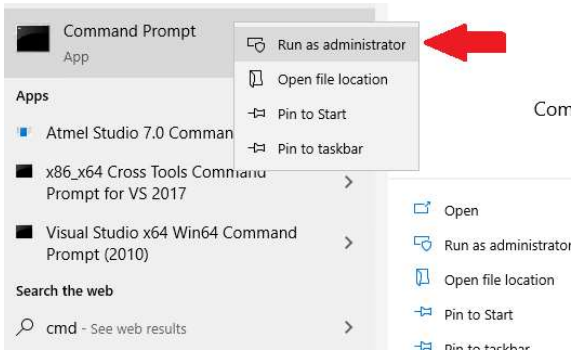


Nun sollte auch beim VPN-Typ „automatisch“ immer vom Windows-VPN-Klienten immer bevorzugt eine SSTP-Verbindung ausgehandelt werden.

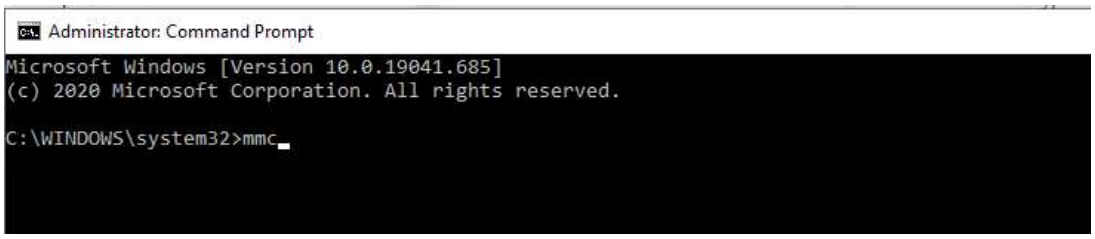
Methode 2: Zertifikat über MMC installieren

Das heruntergeladene (z.B. von https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html) Zertifikat des VPN-Servers kann wie folgt auch händisch in den Windows-Zertifikatsspeicher eingefügt werden. Über diesen Ablauf ist ebenfalls die Kontrolle des Zertifikatsspeichers möglich (falls der obige Ablauf nicht zum Erfolg geführt haben sollte).

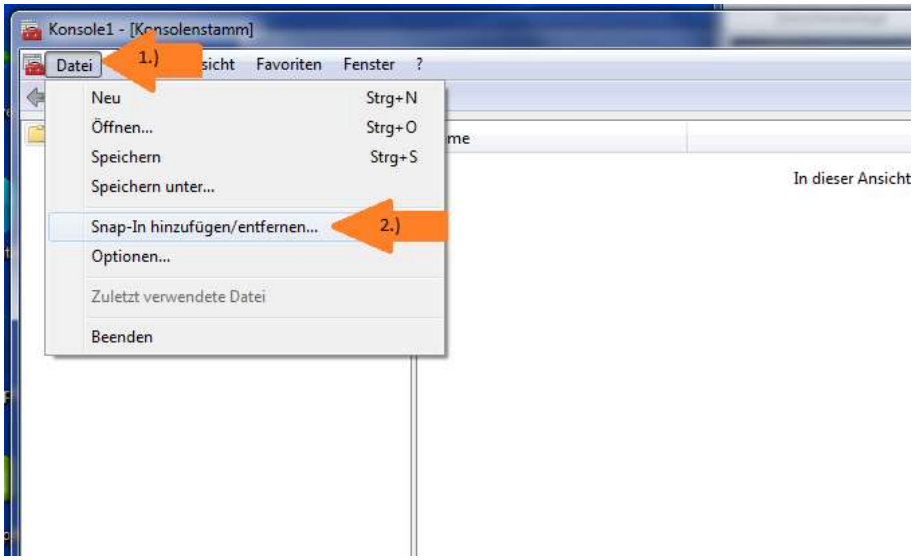
Öffnen Sie **als Administrator** ein Kommando-Zeilen-Fenster (cmd.exe):



Rufen sie dort nun das MMC-Tool auf (alternativ können Sie auch über die Windows-Suche das „mmc“-Tool **als Administrator** starten):

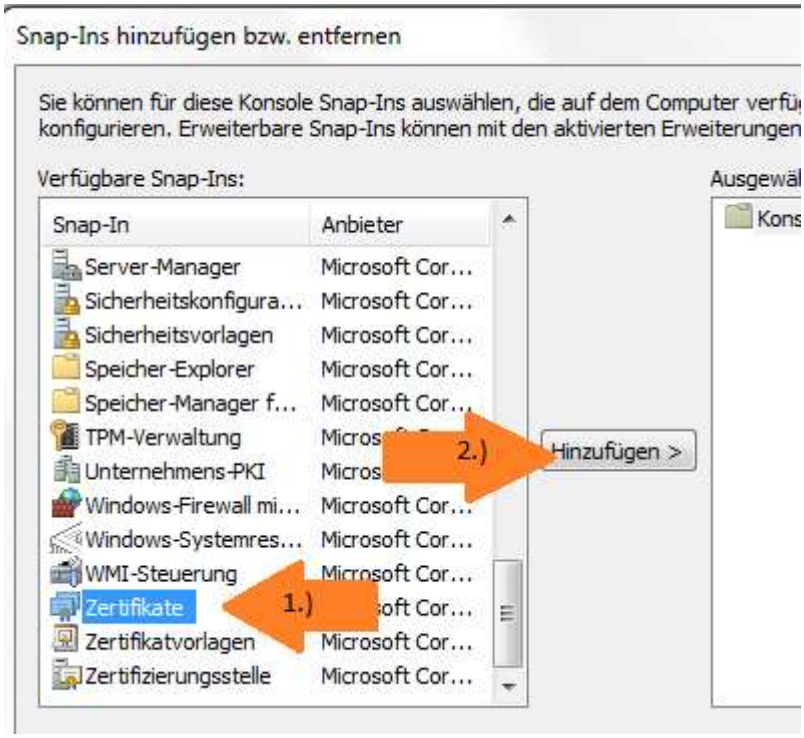


In der dann erscheinenden Verwaltungs-Konsole über den Reiter „Datei“ den Punkt „Snap-In hinzufügen“ anwählen:



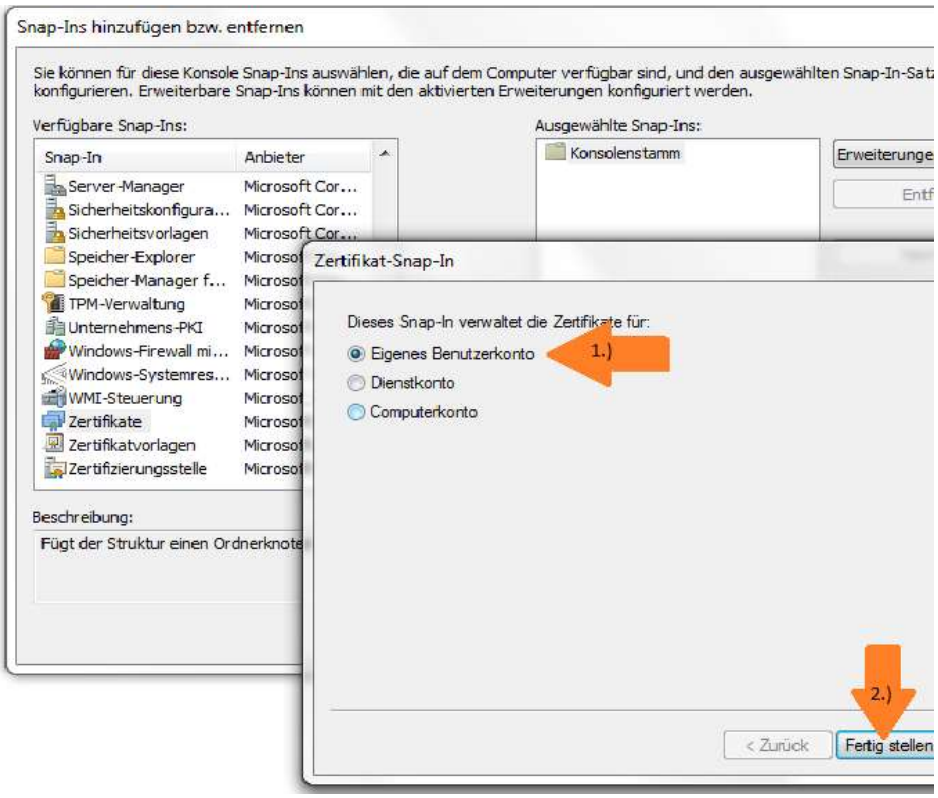
Die umfangreiche Liste der Windows-Verwaltungs-„Snap-Ins“ enthält auch die hier wichtige „Zertifikate“-Verwaltung, dafür bitte Links in der Liste der „verfügbaren Snap-Ins“ soweit nach

unten scrollen, bis die „Zertifikate“ erscheinen:

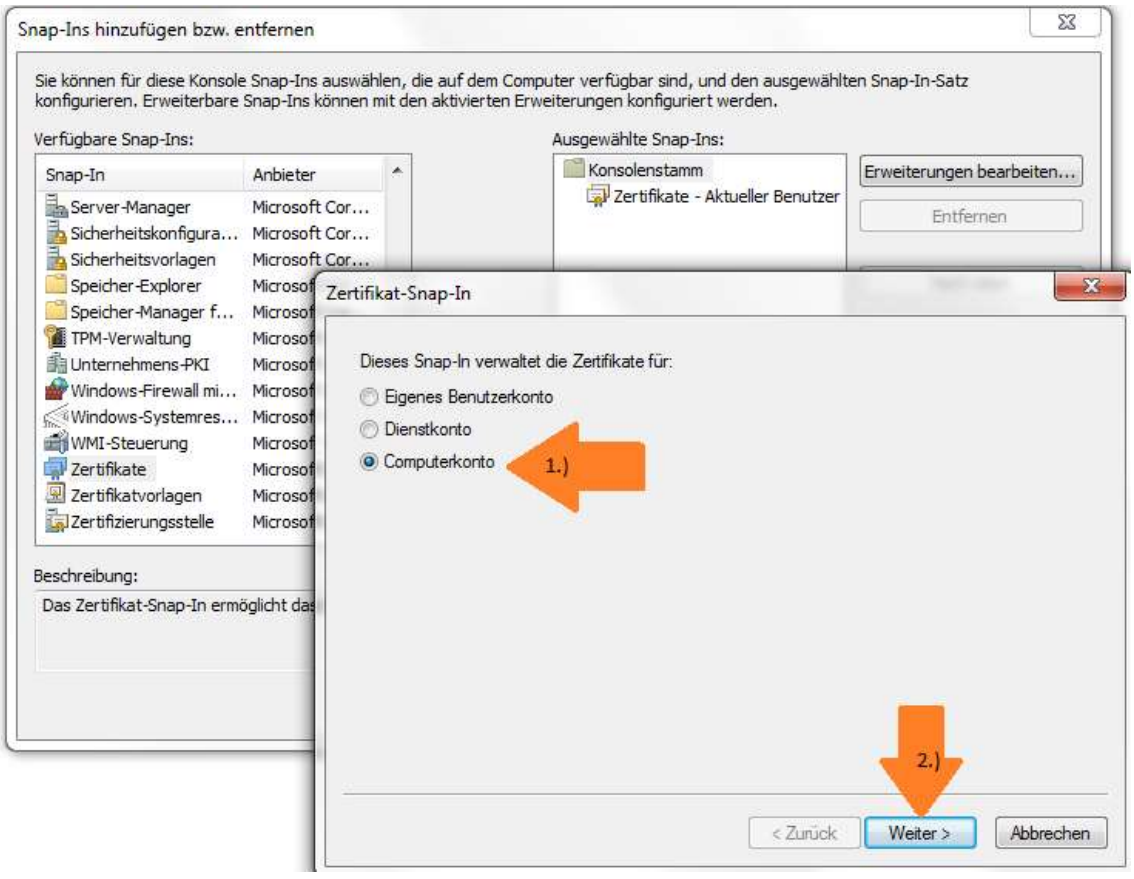


Dann „Zertifikate“ anwählen und über „Hinzufügen“ in die aktive Konsole übernehmen. Dies muss **zweimal** durchgeführt werden, es erscheint beim „Hinzufügen“ eine Auswahl an Zertifikatsspeichern, benötigt werden sowohl „Eigenes Benutzerkonto“ als auch „Computerkonto“.

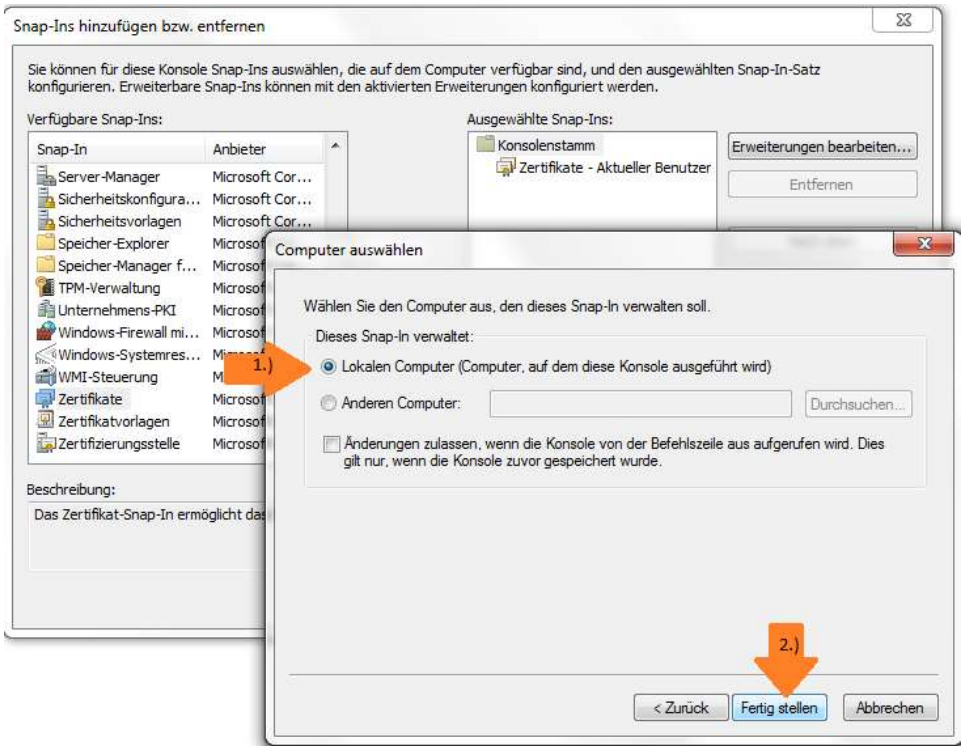
Daher erst den Speicher „Eigenes Benutzerkonto“ übernehmen:



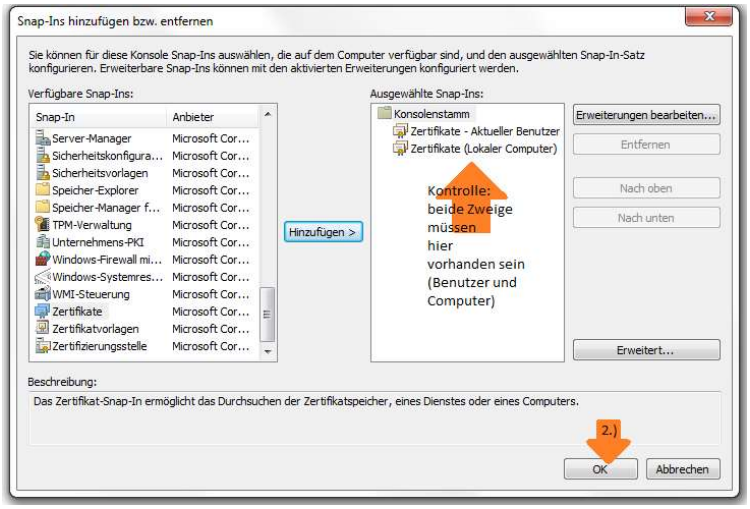
Anschließend nochmals „Zertifikate“ -> „Hinzufügen“, jetzt aber „Computerkonto“ auswählen:



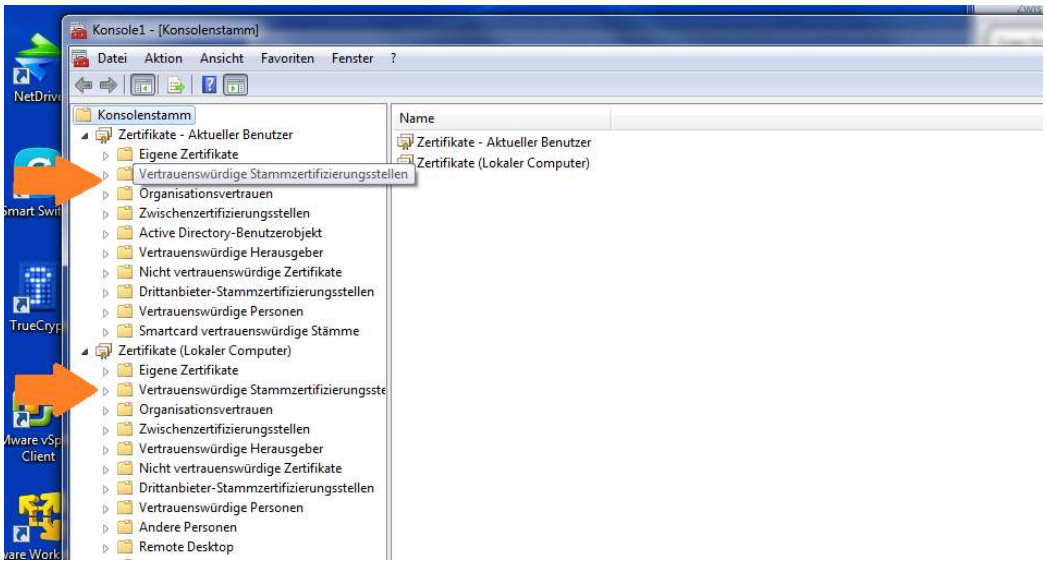
Hier muss in einem Zwischenschritt noch einmal der „Lokale Computer“ gewählt werden:



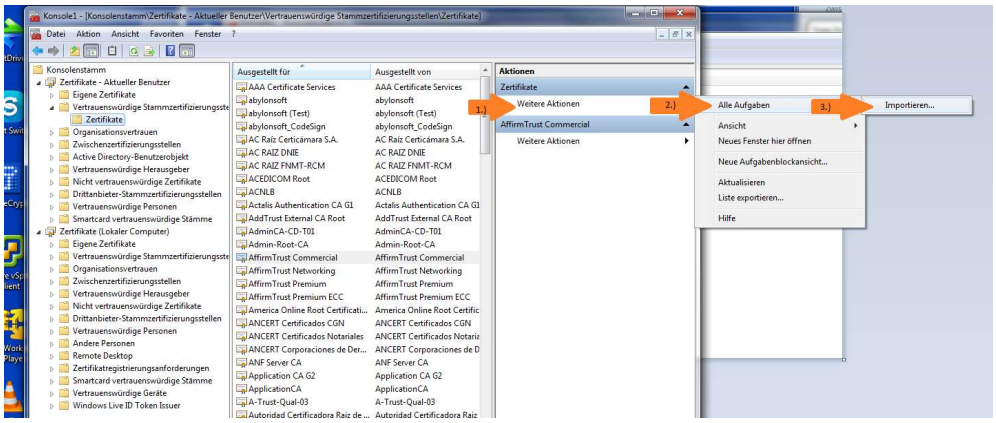
Es sind in der Verwaltungskonsole nun zwei Zertifikatsspeicher aktiv:



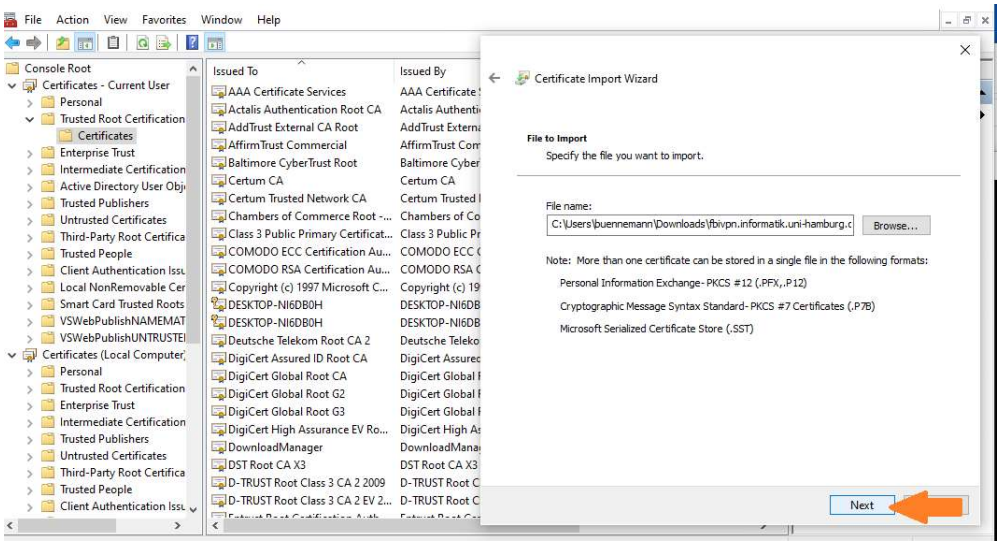
Nach Bestätigung mit „OK“ lassen sich nun die Details dieser Zertifikatsspeicher einsehen, bitte beide („aktueller Benutzer“ und „Lokaler Computer“) entsprechend erweitern:

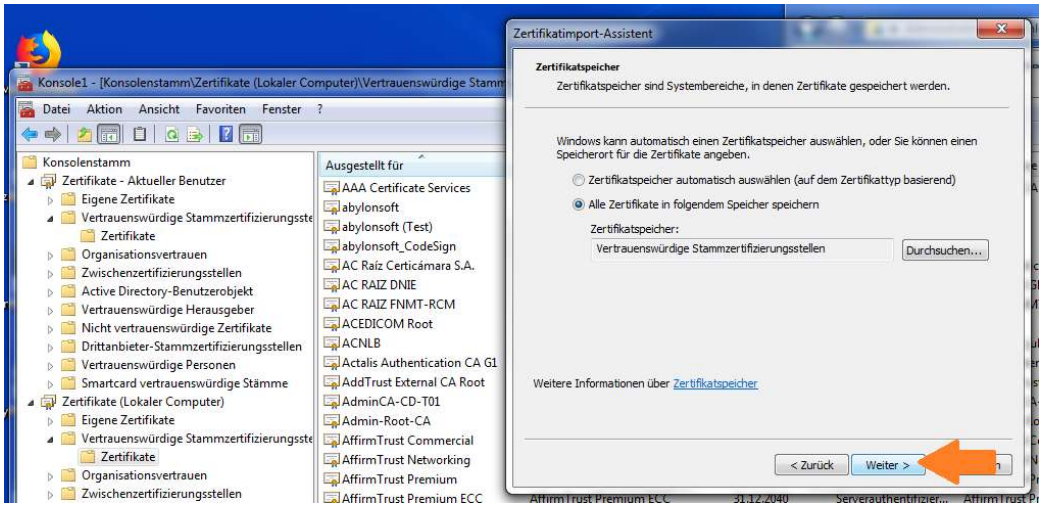


Wichtig sind hier die Verzeichnisse für „Vertrauenswürdige Stammzertifizierungsstellen“, diese nochmals erweitern und das jeweilige Unterverzeichnis „Zertifikate“ öffnen. In der mittleren Spalte finden sich die bereits (vor-)installierten Zertifikate. Über „Weitere Aktionen“ -> „Alle Aufgaben“-> kommt man nun endlich zum entscheidenden Punkt „Importieren“ von Zertifikaten:

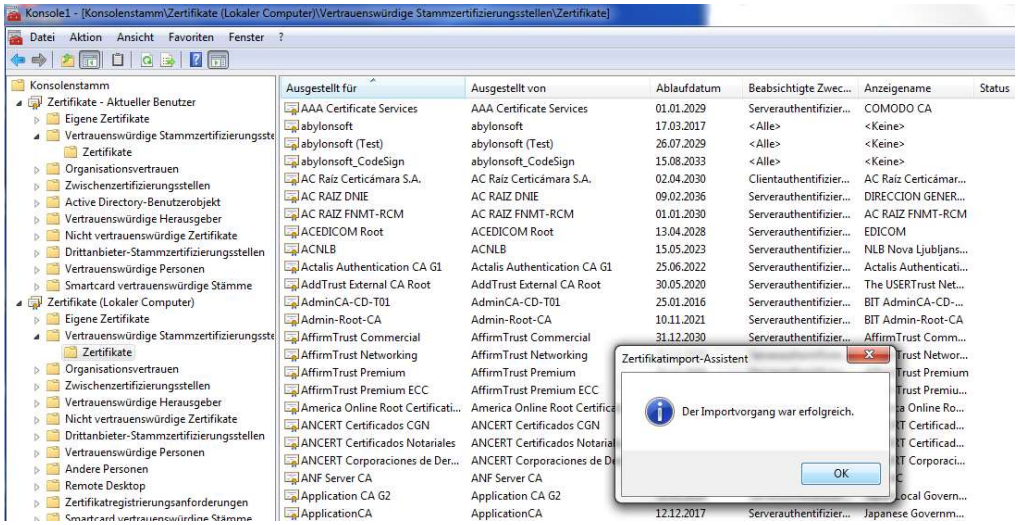


Hier kann das heruntergeladene VPN-Server-Zertifikat ausgewählt werden, es ist dann nur noch dem vorgegebenen Standard-Ablauf zu folgen:

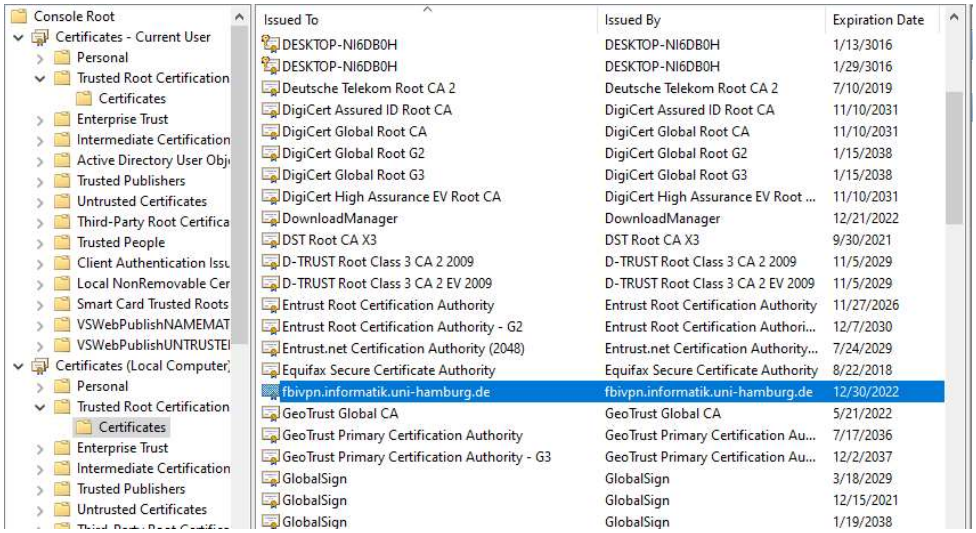




Hoffentlich gelangt man abschließend zu „Der Importvorgang war erfolgreich“:



Es kann nun noch einmal kontrolliert werden, ob auch wirklich ein gültiges Zertifikat der „Uni Hamburg, Informatik“ mit Ablaufdatum „30.12.2022“ mit in der Liste erscheint:



Wichtig:

Nachdem das Zertifikat erfolgreich für „Aktueller Benutzer“ hinzugefügt wurde, muss dieser Einbindungsablauf nun noch einmal für den zweiten Zertifikatsspeicher „Lokaler Computer“ wiederholt werden !

Nun kann die Konsole geschlossen werden („Datei“-> „beenden“, keine Einstellungen speichern),

und SSTP-VPN sollte ab jetzt funktionieren !!!