

Einbinden des Informatik-Root-Zertifikates unter Windows

Tb, 23.9.2019

Für die Einrichtung einer sicheren SSTP-VPN-Verbindung wird auf dem Verbindungsanfordernden (privaten) Rechner explizit das Informatik-Root-Zertifikat 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 von der Informatik-Domäne ausgestelltes Rechner-/Server-Zertifikat. Damit ein anfragender Rechner dieses Domänen-Zertifikat erfolgreich verifizieren kann, muss auch das Root-Zertifikat der Informatik-Domäne 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 Root-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):

Weiterhin steht für Windows-Klienten die Nutzung des Microsoft-proprietären SSTP-Protokolls zur Verfügung. Dieses gewährleistet sowohl eine höhere Sicherheit, als auch im Prinzip einen problemlosen Zugang von allen Standorten aus, da ausschließlich die üblichen HTTP/HTTPS-Ports genutzt werden. Allerdings ist es **ab 2018** hierfür notwendig, beim genutzten Klienten als Domänen-Root-Zertifikat der Informatik im Rechner-Zertifikatsspeicher unter "vertrauenswürdige Root-Zertifikatsstellen" zu hinterlegen:

Informatik_Root_Zertifikat

Informatik Root-Zertifikat



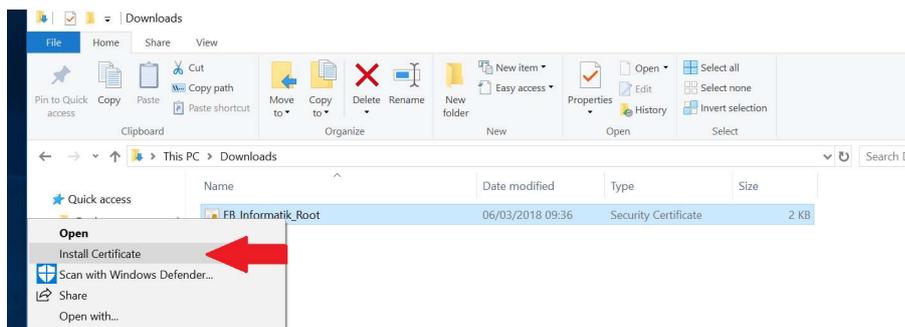
Die Zugangs-Adresse des Servers lautet:

fbivpn.informatik.uni-hamburg.de

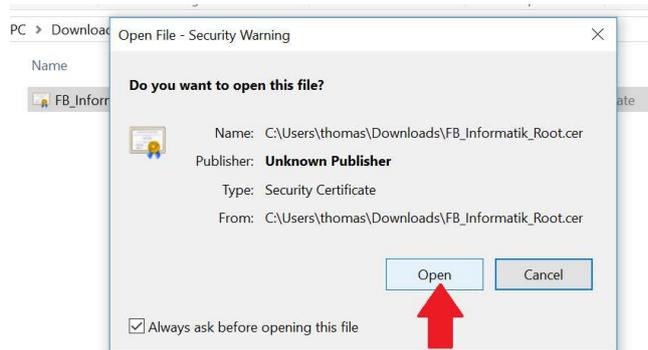
Für ausführliche Anleitungen zur Zugangskonfiguration wählen Sie bitte den gewünschten Klienten in der nebenstehenden Auswahlliste.

Methode 1: Zertifikat direkt installieren

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

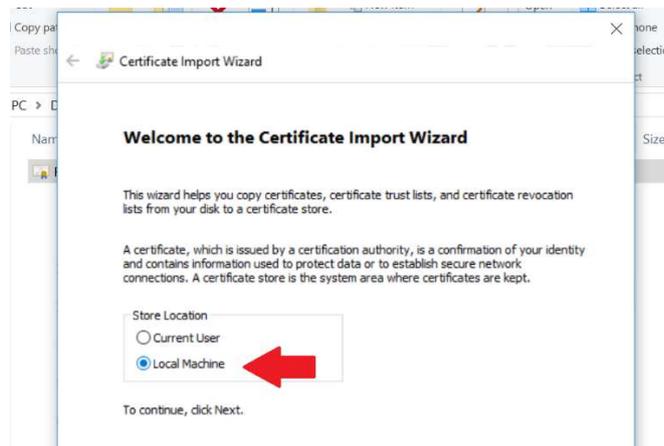


Bestätigen Sie im automatischen Installationsablauf nun das Öffnen des Zertifikats:

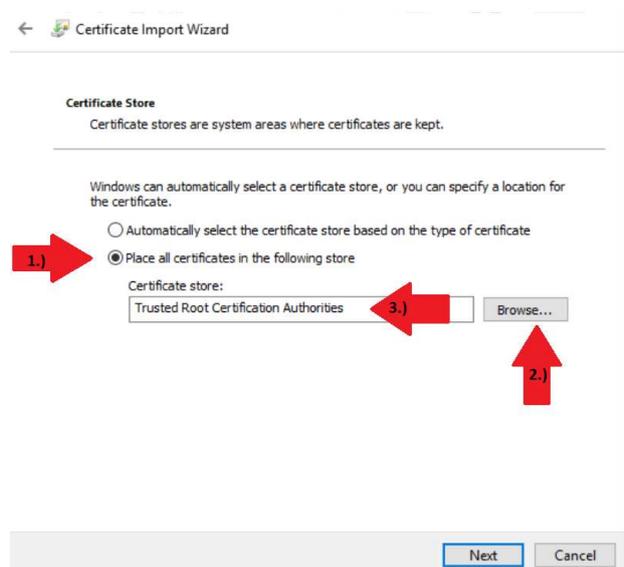


Beachten Sie genau den im Folgenden beschriebenen Ablauf, da die Standardwerte des automatischen Installations-Ablaufs nicht zum gewünschten Ergebnis führen !

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

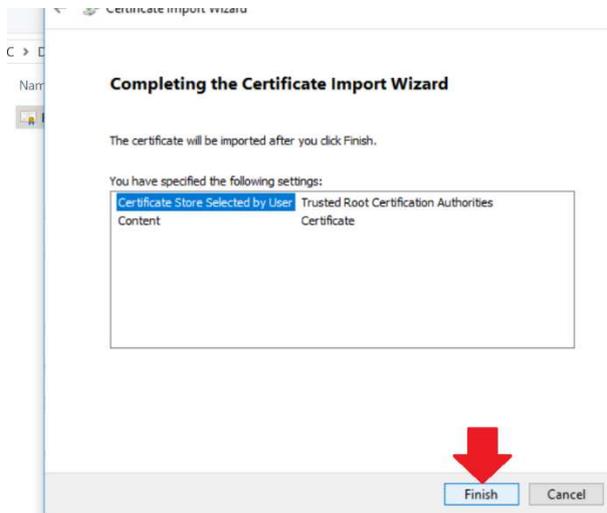


Wählen Sie die explizite Auswahl des Speicherplatzes (1.),



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

Abschließend wird noch einmal nach Bestätigung des ausgewählten Speicherplatzes gefragt:

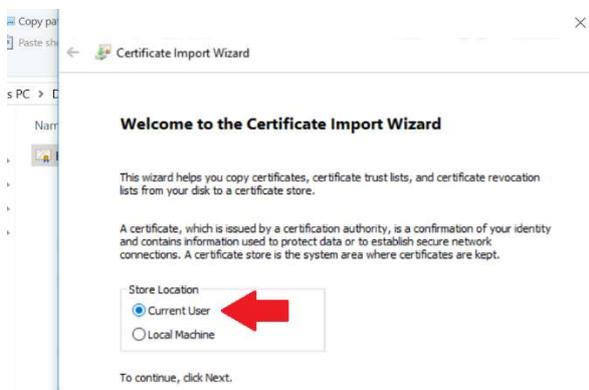


Der Erfolg des Imports wird nun vom System bestätigt:

Name	Date modified	Type
FB_Informatik_Root	06/03/2018 09:36	Security



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

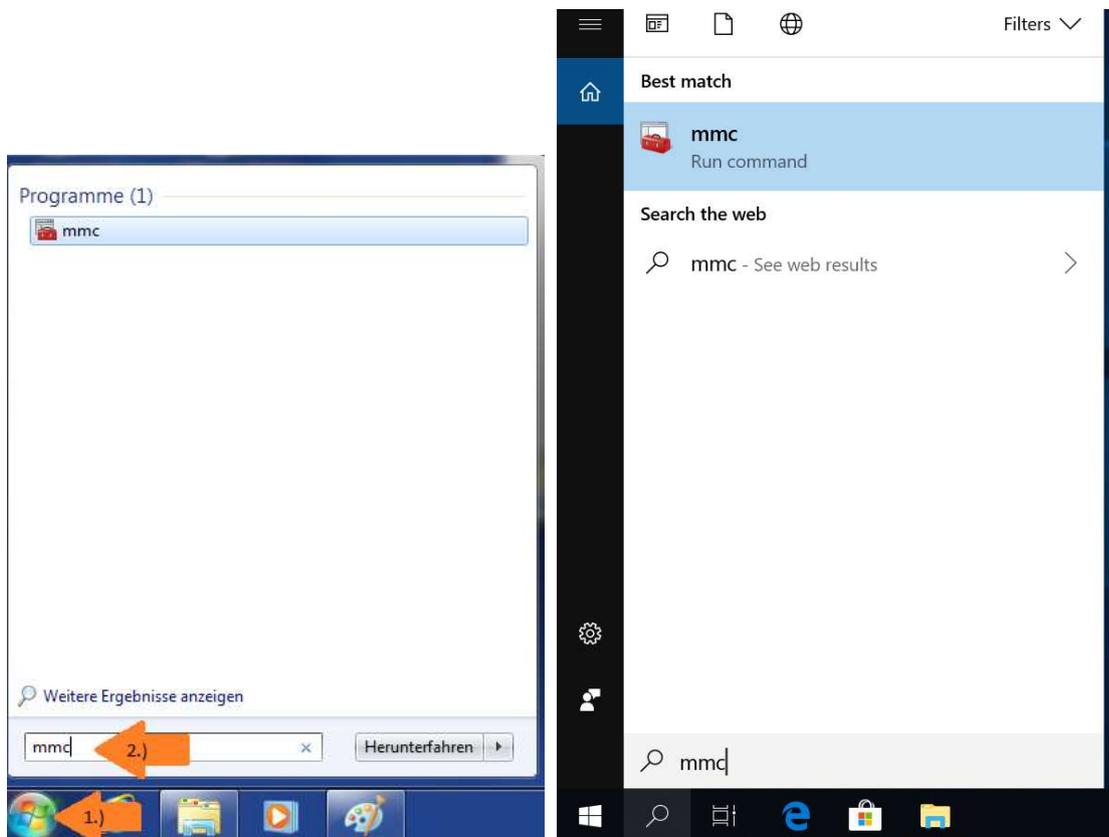


Nun sollte auch beim VPN-Typ „automatisch“ immer vom Windows-VPN-Klienten immer bevorzugt eine SSTP-Verbindung ausgehandelt werden.

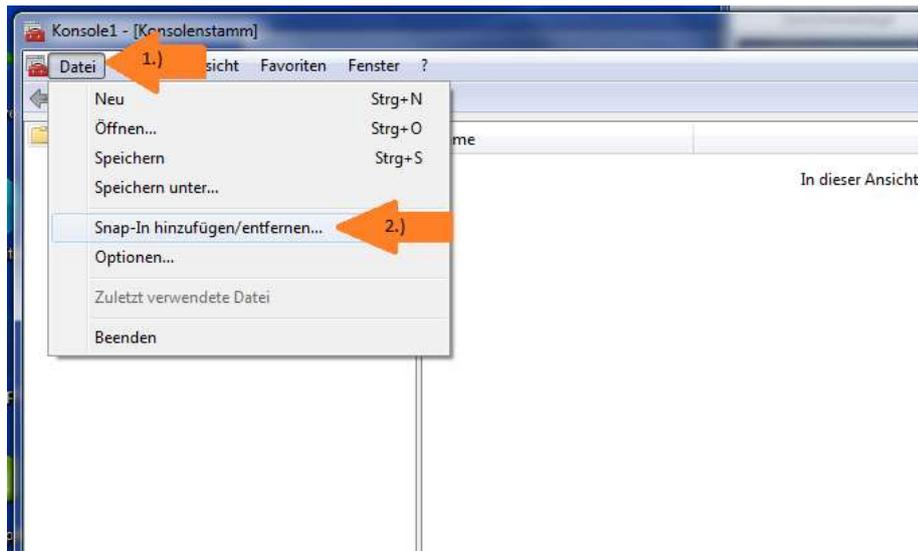
Methode 2: Zertifikat über MMC installieren

Das heruntergeladene (z.B. von <https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html>) Root-Zertifikat der Informatik 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).

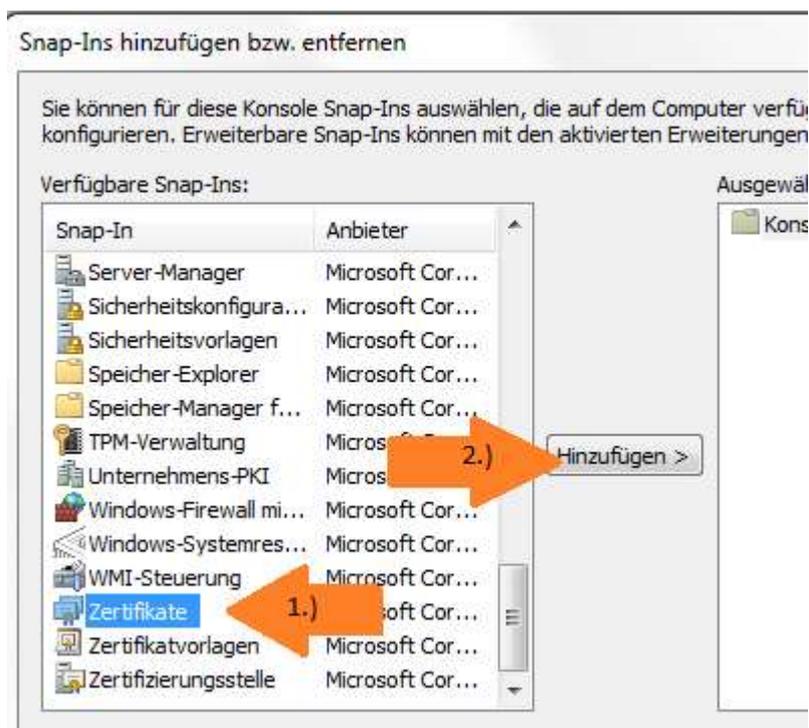
Über die Windows-Suchzeile das „mmc“-Verwaltungstool aufrufen:



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

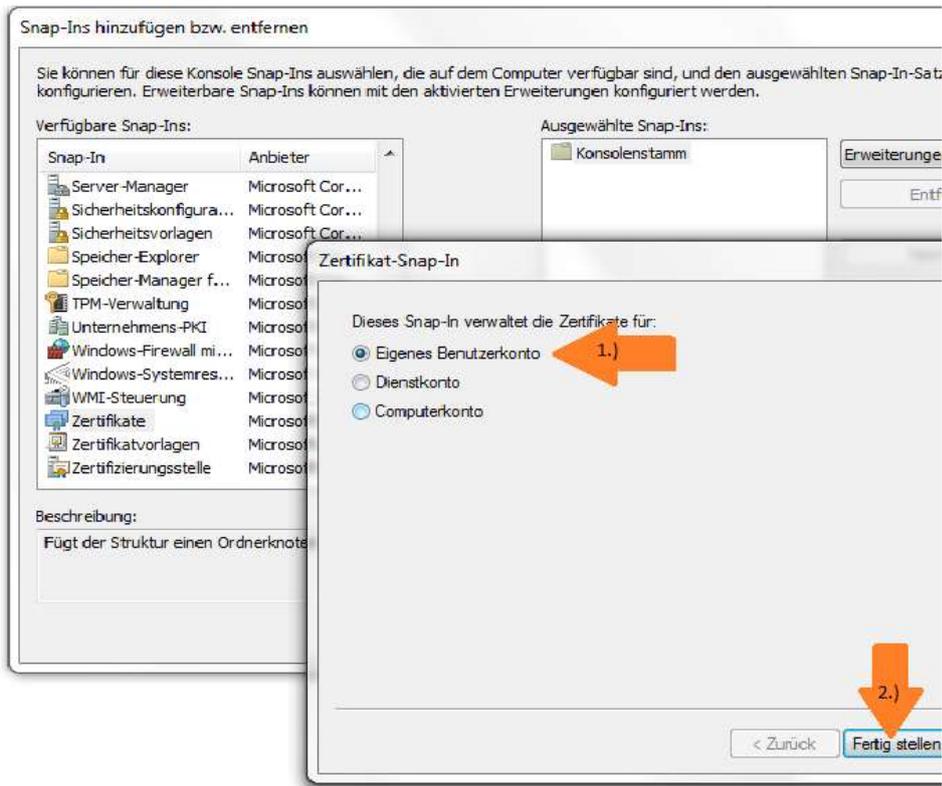


Die umfangreiche Liste der Windows-Verwaltungs-„Snap-Ins“ enthält auch die hier wichtige „Zertifikate“-Verwaltung, dafür bitte Links in der Liste der „verfügbaren Snap-Ins“ soweit nach unten scrollen, bis die „Zertifikate“ erscheinen:

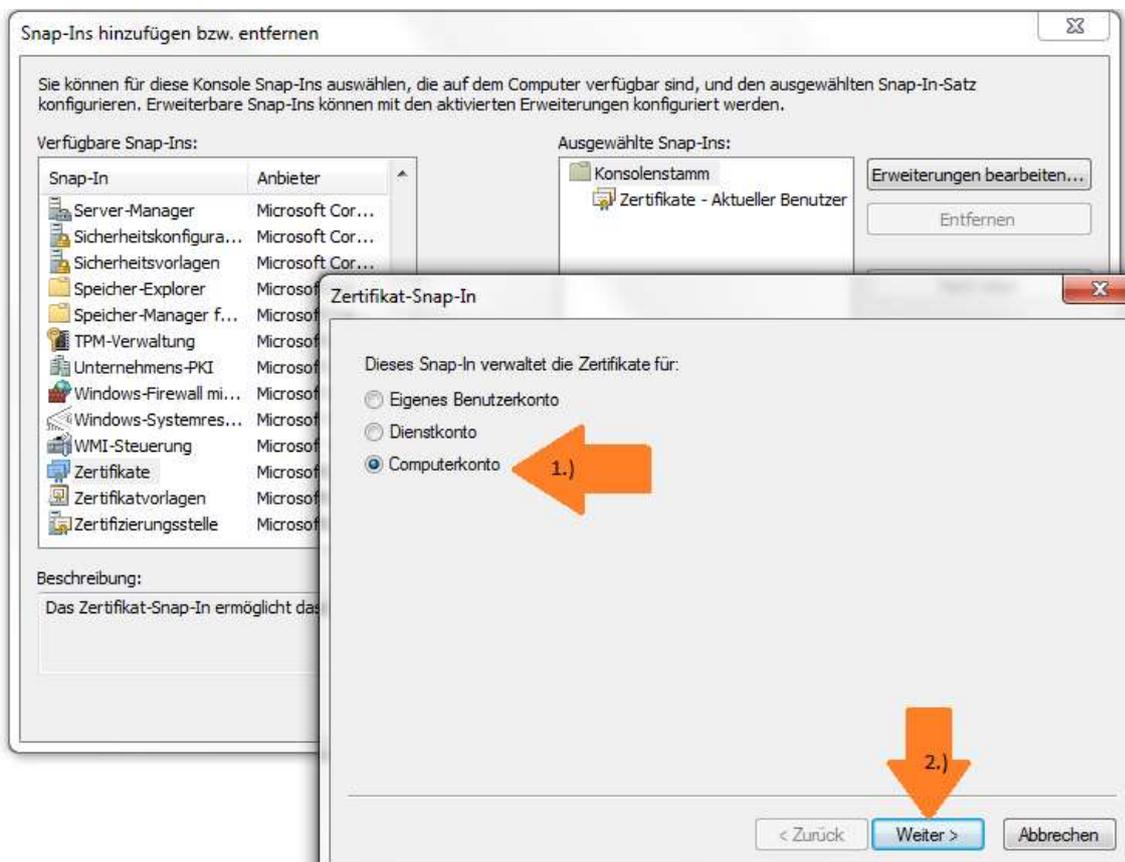


Dann „Zertifikate“ anwählen und über „Hinzufügen“ in die aktive Konsole übernehmen. Dies muss **zweimal** durchgeführt werden, es erscheint beim „Hinzufügen“ eine Auswahl an Zertifikatsspeichern, benötigt werden sowohl „Eigenes Benutzerkonto“ als auch „Computerkonto“.

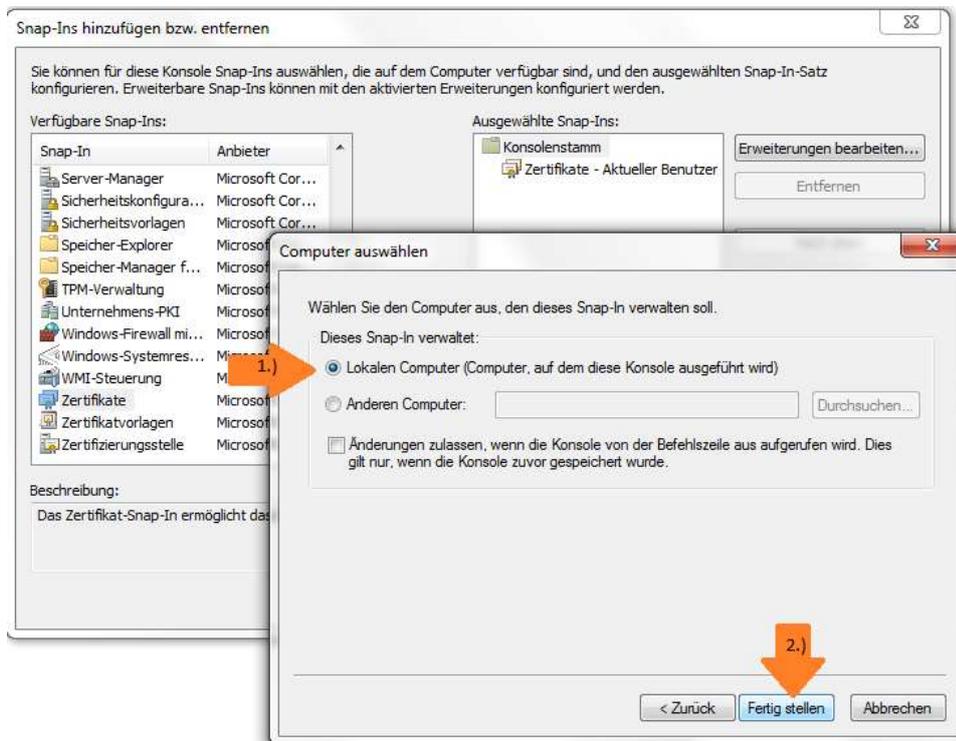
Daher erst den Speicher „Eigenes Benutzerkonto“ übernehmen:



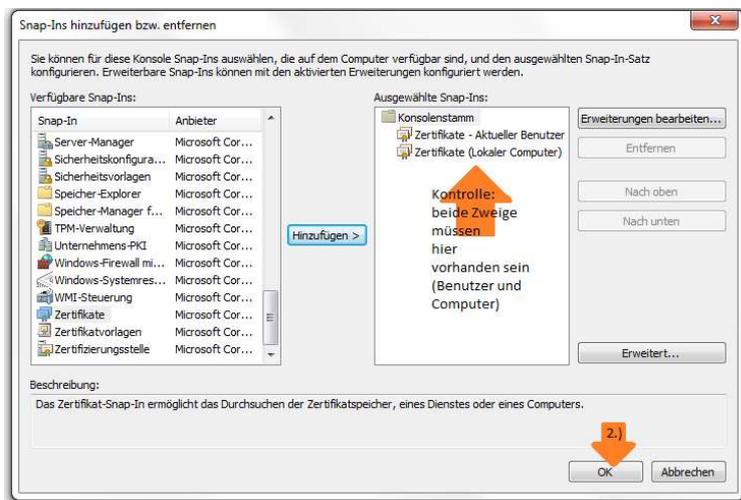
Anschließend nochmals „Zertifikate“ -> „Hinzufügen“, jetzt aber „Computerkonto“ auswählen:



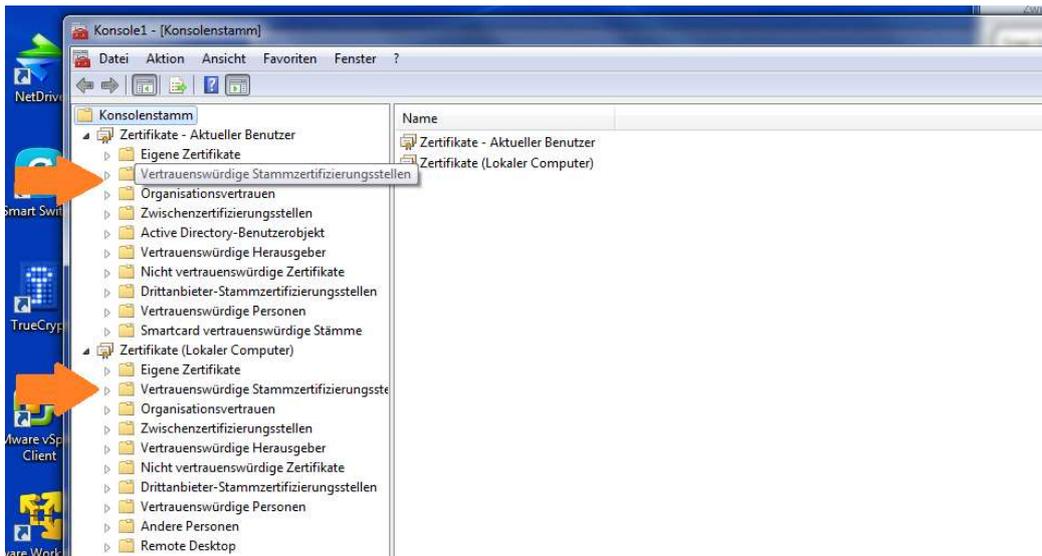
Hier muss in einem Zwischenschritt noch einmal der „Lokale Computer“ gewählt werden:



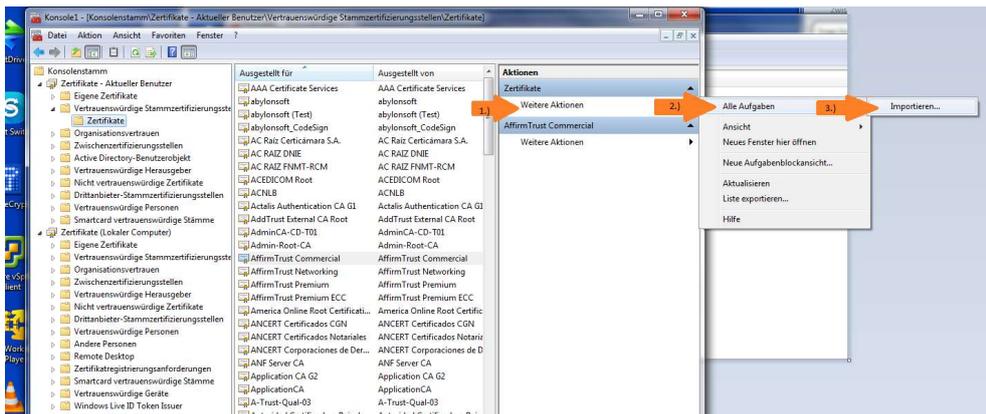
Es sind in der Verwaltungskonzole nun zwei Zertifikatsspeicher aktiv:



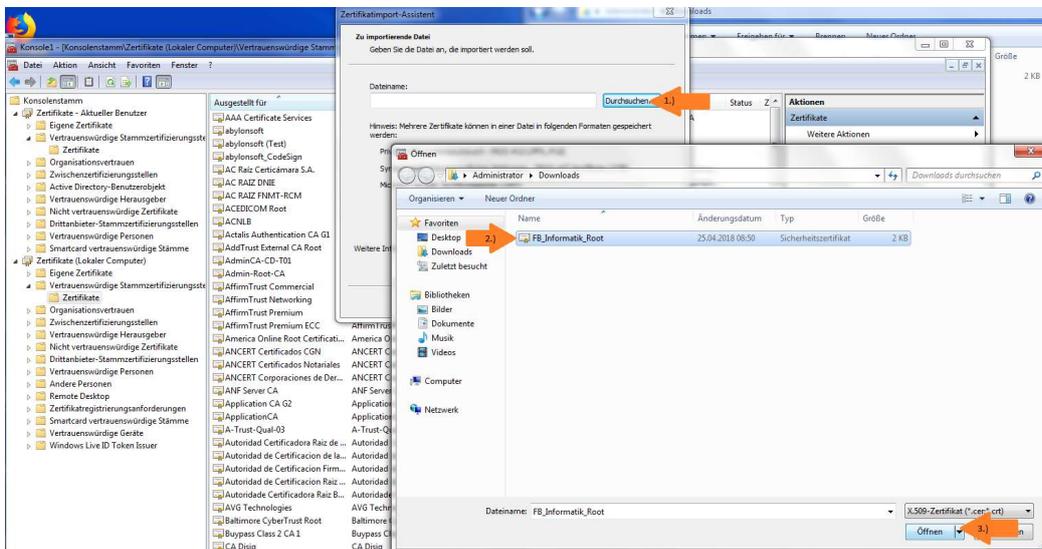
Nach Bestätigung mit „OK“ lassen sich nun die Details dieser Zertifikatsspeicher einsehen, bitte beide („aktueller Benutzer“ und „Lokaler Computer“) entsprechend erweitern:

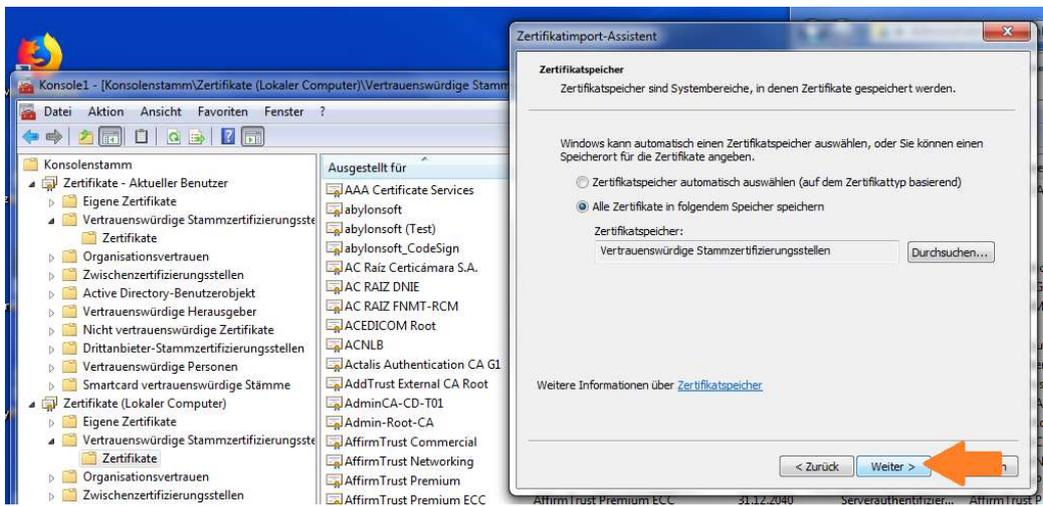
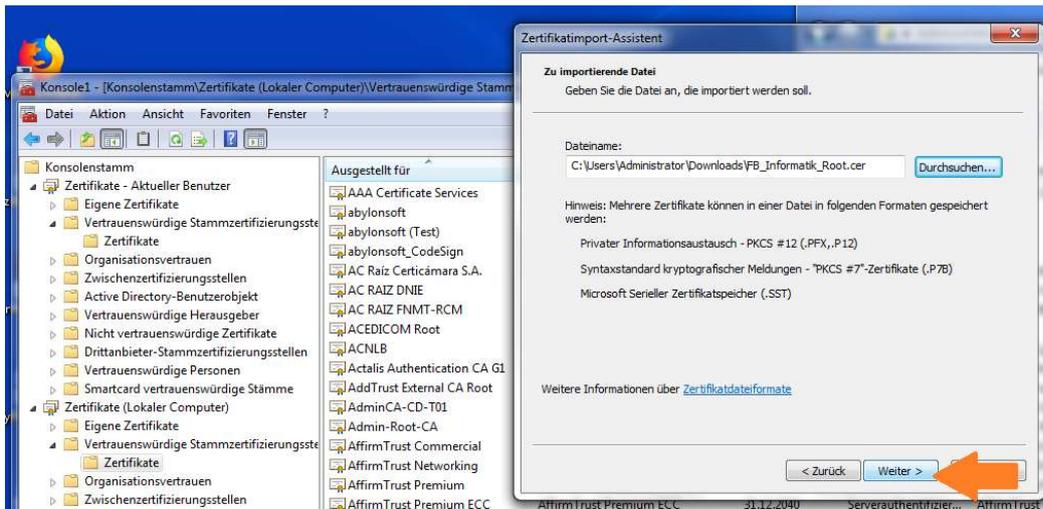


Wichtig sind hier die Verzeichnisse für „Vertrauenswürdige Stammzertifizierungsstellen“, diese nochmals erweitern und das jeweilige Unterverzeichnis „Zertifikate“ öffnen. In der mittleren Spalte finden sich die bereits (vor-)installierten Zertifikate. Über „Weitere Aktionen“ -> „Alle Aufgaben“-> kommt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

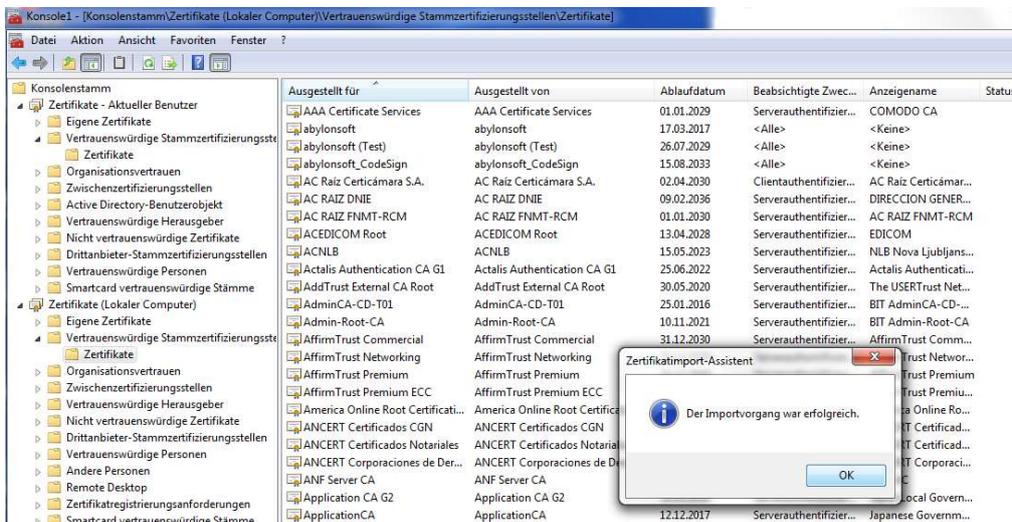


Hier kann das heruntergeladene Root-Zertifikat der Informatik ausgewählt werden, es ist dann nur noch dem vorgegebenen Standard-Ablauf zu folgen:





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 „11.07.2027“ mit in der Liste erscheint:

Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zweck...	Anzeigename	Status
Thawte Server CA	Thawte Server CA	01.01.2021	Serverauthentifizier...	thawte	
Thawte Timestamping CA	Thawte Timestamping CA	01.01.2021	Zeitstempel	Thawte Timestamp...	
Thawte Timestamping CA	Thawte Timestamping CA	01.01.2021	Zeitstempel	thawte	
Trustis FPS Root CA	Trustis FPS Root CA	21.01.2024	Serverauthentifizier...	Trustis FPS Root CA	
T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	02.10.2033	Serverauthentifizier...	T-TeleSec GlobalRo...	
TÜBITAK UEKAE Kök Sertifika H...	TÜBITAK UEKAE Kök Sertifika Hiz...	21.08.2017	Serverauthentifizier...	TÜBITAK Kamu SM	
TÜRKRUST Elektronik Sertifika ...	TÜRKRUST Elektronik Sertifika Hi...	22.12.2017	Serverauthentifizier...	TÜRKRUST Elektro...	
TWCA Root Certification Autho...	TWCA Root Certification Authority	31.12.2030	Serverauthentifizier...	TWCA Root Certific...	
TWCA Root Certification Autho...	TWCA Root Certification Authority	31.12.2030	Serverauthentifizier...	TWCA Root Certific...	
UCA Global Root	UCA Global Root	31.12.2037	Zeitstempel, IP-Sic...	UCA Global Root	
UCA Root	UCA Root	31.12.2029	Zeitstempel, IP-Sic...	UCA Root	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	06.01.2012	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	07.01.2016	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	08.06.2006	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	25.01.2008	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	11.07.2027	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	14.01.2010	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	07.06.2004	<Alle>	<Keine>	
Uni Hamburg, FB Informatik	Uni Hamburg, FB Informatik	03.01.2014	<Alle>	<Keine>	

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 !!!