## 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 <u>https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html</u> 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):

ÜBER UNS	IRZ-ZUGANG	BETRIEB	IT-DIENSTE	SOFTWARE
ODER OND	INE ECOAITO	DETRIED	IT DILITOTE	SOLLARE

serversettig werden das Point to Point funneling Protocol (PPTP) und das Layer 2 funneling Protocol (L2TP) mit preshared Key" unterstützt.

Weiterhin steht für Windows-Klienten die Nutzung des Microsoft-proprietären SSTP-Protokolls zur Verfügung. Dieses gewährleist 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 **seit 1.1.2021** hierfür notwendig, beim genutzten Klienten das (selbstsignierte) Zertifikat des Informatik-VPN-Servers fbivpn.informatik.uni-hamburg.de in Ihrem **Rechner**-Zertifikatsspeicher unter "vertrauenswürdige Root-Zertifikatsstellen" zu hinterlegen:

#### Zertifikat des Informatik-VPN-Servers

Zur Einbindung des VPN-Server-Zertifikats unter Windows gibt es eine ausführliche Anleitung.

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 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.),

Certificate	e Store	
Certi	ficate stores are system areas where certificates are kept.	
Wind the c	ows can automatically select a certificate store, or you can specif ertificate.	y a location for
C	Automatically select the certificate store based on the type of c	ertificate
	Place all certificates in the following store	
	Certificate store:	
	Trusted Root Certification Authorities 3.)	Browse
		2.)

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

Abschließend wird noch einmal nach Bestätigung des ausgewählten Speicherplatzes gefragt:

Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Certificate Store Selected by User Trusted Root Certification Authorities	
Concine Concine	

## Der Erfolg des Imports wird nun vom System bestätigt:

Name	Date modified	Туре
FB_Informatik_Root	06/03/2018 09:36	Securit
	Certificate Import Wizard $ imes$	
	The import was successful.	
	ОК	

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 <u>https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html</u>) 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:

				Ausger
Snap-In	Anbieter	1		K
Server-Manager Sicherheitskonfigura	Microsoft Cor… Microsoft Cor… Microsoft Cor…			
Speicher-Explorer	Microsoft Cor Microsoft Cor			
Unternehmens-PKI	Micros 2.)		Hinzufügen >	]
Windows-Systemres	Microsoft Cor			
WMI-Steuerung	Microsoft Cor			

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:

Snaphi       Hubble         Server-Manager       Microsoft Cor         Sicherheitskonfigura       Microsoft Cor         Sicherheitsvorlagen       Microsoft Cor         Speicher-Explorer       Microsoft Cor         Speicher-Explorer       Microsoft Cor         Speicher-Manager f       Microsoft Cor         Speicher-Explorer       Microsoft Cor         Dieses Snap-In       Dieses Snap-In verwaltet die Zettifikate für:         Windows-Firewall mi       Microsoft         Windows-Systemres       Microsoft         Windows-Systemres       Microsoft         Windows-Systemres       Microsoft         Zertifikate       Microsoft         Zertifikate       Microsoft         Zertifikate       Microsoft         Zertifikate       Microsoft         Zertifikate       Microsoft         Zertifikate       Microsoft         Sterifikate       Microsoft	Span Jo	Aphieter		Ausgewa	olenstamm	Frweiterur
Speicher-Explorer       Microso         Speicher-Manager f       Microso         IPH-Verwaltung       Microso         Unternehmens-PKI       Microso         Windows-Systemres       Microso         Windows-Systemres       Microso         Windows-Systemres       Microso         Zertifikate       Microso         Speider Struktur einen Ordnerknote       Speider Struktur einen Ordnerknote	Server-Manager Sicherheitskonfigura Sicherheitsvorlagen	Microsoft Cor Microsoft Cor Microsoft Cor				[E
	Speicher-Manager f TPM-Verwaltung Unternehmens-PKI Windows-Firewall mi Windows-Systemres WIDL-Steuerung Zertifikate Zertifikate Zertifikatovrlagen Zertifizierungsstelle Eigt der Struktur einen Or	Microsol Microsol Microsol Microsol Microsol Microsol Microsol Microsol Microsol Microsol	eses Snap-In v Eigenes Benu Dienstkonto Computerkont	erwaltet die Zertifik tzerkonto	ate für: .)	

# Anschließend nochmals "Zertifikate" -> "Hinzufügen", jetzt aber "Computerkonto" auswählen:

erfügbare Snap-Ins:			Ausgewählte Snap-Ins:			
Snap-In	Anbieter	*	Konsolenstamm		Erweiterungen bearbei	ten
Server-Manager Sicherheitskonfigura Sicherheitsvorlagen	Microsoft Cor Microsoft Cor Microsoft Cor		Zertifikate - Aktuelle من المحمد ا	er Benutzer	Entfernen	
Speicher-Manager f TPM-Verwaltung Unternehmens-PKI Windows-Firewall mi Windows-Systemres WMI-Steuerung Zertifikate Zertifikate Zertifikate Zertifikate	Microsof Microsof Microsof Microsof Microsof Microsof Microsof Microsof	eses Snap-In ve i Eigenes Benut; i Dienstkonto i Computerkonto	rwaltet die Zertifikate für: zerkonto			
Jas Zertifikat-Snap-In ermi	öglicht das					

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

nap-In	Anhieter	*	Konsolenstamm	Erweiterungen bearbeit	en
Server-Manager Sicherheitskonfigura	Microsoft Cor Microsoft Cor Microsoft Cor		🚽 Zertifikate - Aktueller Benutzer	r Entfernen	
Speicher-Manager f TPM-Verwaltung Windows-Firewall mi Windows-Systemres Windows-Systemres WMI-Steuerung Zertifikate Zertifikatvorlagen	Microsof Microsof Microsof Microsof Microsof Microsof Microsof	ihlen Sie den Dieses Snap-Ir O Lokalen C O Anderen C O Anderung	Computer aus, den dieses Snap-In verwalten soll n verwaltet: omputer (Computer, auf dem diese Konsole ausge computer: en zulassen, wenn die Konsole von der Befehlsze en die Konsole zuvor gesneichert wurde	führt wird) Durchsuch	en) s
schreibung: ias Zertifikat-Snap-In erm	öglicht das				

Es sind in der Verwaltungskonsole nun zwei Zertifikatsspeicher aktiv:

Snap-In	Anbieter		Konsolenstamm	Erweiterungen bearbeiten
Server-Manager	Microsoft Cor Microsoft Cor		Zertifikate - Aktueller Benutze	Entfernen
Sicherheitsvorlagen	Microsoft Cor Microsoft Cor		Kontrolle:	Nach oben
Speicher-Manager f	Microsoft Cor Microsoft Cor		beide Zweige	Nach unten
🔒 Unternehmens-PKI	Microsoft Cor		Hinzufügen > hier	
Windows-Firewall mi	Microsoft Cor		vorhanden sein	
Windows-Systemres	Microsoft Cor		(Benutzer und	
WMI-Steuerung	Microsoft Cor		(benuter)	
Zertifikate	Microsoft Cor	E	computery	
🖳 Zertifikatvorlagen	Microsoft Cor			
🙀 Zertifizierungsstelle	Microsoft Cor	+		Erweitert
eschreibung:			L	

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:

File Action View Favorites V	Window Help	_			- 5	×
Image: Second	Issued To Issued To Actalis Authenticatio Root CA Actalis Authentication Root CA Actalis Authentication Root CA Actalis Authentication Root Addinust External CA Root Centum Tusted Network CA Chambers of Commerce Root CoMODD RSC Certification Au COMODD RSC Certification Au COMODO RSC Certification Au COMODO RSC Certification Au COMOID RSC CERTIFICATION CONCERNING DigiCert Global Root CA 2 DigiCert Global Root C3 DigiCert Global Root C3 DigiCert Global Root C3 DigiCert High Assume EV Ro COMING MAManger DOST Root CA X3	Issued By AAA Certificate 1 Actalis Authenti AddTust Extern Baltimore Cyber Baltimore Cyber Certum CA Certum Trusted 1 Chambers of Co Class 3 Public Pr COMODO ESA C COMODO RSA C COMOTO RSA C COMOTO RSA C DIGICET Global I DigiCet Global I DigiCet Global I DigiCet High A DownloadMana, DST Root CA X3	÷	Certificate Import Wizard  File to Import Speafy the file you want to import.  File name:  C:\User'buennemann\Downloads\fbivpn.informatik.uni-hamburg.c  Browse  Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange-PKCS #12 (PFX, P12) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P78) Microsoft Serialized Certificate Store (.SST)	×	
> Client Authentication Issu	D-TRUST Root Class 3 CA 2 2009	D-TRUST Root C		Next		



Hoffentlich gelangt man abschließend zu "Der Importvorgang war erfolgreich":

📸 Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Co	mputer)\Vertrauenswürdige Stammzer	tifizierungsstellen\Zertifikate]				
The second secon	?					
💠 🔿 🔁 📅 📋 🖻 📑 🖬 🗊						
Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status
Gigen Zetrifikate - Aktueller Benutzer     Eigene Zetrifikate     Eigene Zetrifikate     Zetrifikate     Zetrifikate     Zetrifikate     Zovischenzentfüsierungstellen     Active Directory-Benutzerobjekt     Vertrauenswürdige Herausgeber     Nicht vertrauenswürdige Zetrifikate     Dirtinabieter-Stammertifizierungsstellen     Sonstandsterustfüsierungsstellen     Sonstandsterustfüsierungsstellen     Sonstandsterustfüsierungsstellen     Zetrifikate (Lokaler Computer)     Eigene Zetrifikate	AAA Certificate Services by Jonsoft by Jonsoft (Test) c aby Jonsoft (Cest) C ac Raiz Certiciamare S.A. C ac Raiz DNIE AC RAIZ DNIE AC RAIZ DNIE C ACLIS AUTHENTICA AC RAIS ACTUALS AC	AAA Certificate Services abylonsoft abylonsoft (Test) abylonsoft_CodeSign AC Raiz Certiciamars SA. AC RAIZ DNIE AC RAIZ FNIMT-RCM ACEDICOM Root ACCNLB Actalis Authentication CA G1 AddTrust External CA Root AdminCA-CD-T01 Admin-Root-CA	01.01.2029 17.03.2017 26.07.2029 15.08.2033 02.04.2030 09.02.2036 01.01.2030 13.04.2028 15.05.2023 25.06.2022 30.05.2020 25.01.2016 10.01.2021	Serverauthentifizier <alle> <alle> <alle> Clientauthentifizier Serverauthentifizier Serverauthentifizier Serverauthentifizier Serverauthentifizier Serverauthentifizier Serverauthentifizier Serverauthentifizier</alle></alle></alle>	COMODO CA <keine> <keine> <keine> AC Raiz Certicámar DIRECCION GENER AC RAIZ FNMT-RCM EDICOM NLB Nova Ljubljans Actalis Authenticat The USERTrust Net BIT Admin-Root-CA BIT Admin-Root-CA</keine></keine></keine>	
Verduelsvoluge samme indee inde	Affirm Trust Networking     Affirm Trust Premium     Affirm Trust Premium     Affirm Trust Premium ECC     America Online Root Certificatu.     ANCERT Certificados CGN     ANCERT Certificados Notariales     ANCERT Corporaciones de Der     ANF Server CA     Aoplication CA G2	Afrim Trust Commercial AffrimTrust Networking AffrimTrust Premium AffrimTrust Premium ECC America Online Root Certifica ANCERT Certificados GN ANCERT Certificados Notaria ANCERT Corporaciones de D ANF Server CA Application CA 62	Zertifikatimport-Assiste	vorgang war erfolgreich.	Trust Networ Trust Networ Trust Premium Trust Premium Tust Premium Tost Premium T Certificad T Certificad T Corporaci C occal Govern	
Electrifikatregistrierungsanforderungen Smartcard vertrauenswürdige Stämme	ApplicationCA	ApplicationCA	12.12.2017	Serverauthentifizier	Japanese Governm	

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:

🛗 Console Root 🔥 🔺	Issued To	Issued By	Expiration Date	^
✓ ☐ Certificates - Current User	Contraction Contractic	DESKTOP-NI6DB0H	1/13/3016	
> 📄 Personal	DESKTOP-NI6DB0H	DESKTOP-NI6DB0H	1/29/3016	
Trusted Root Certification	Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	7/10/2019	
Certificates	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	
> Enterprise irust	🗔 DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	
Active Directory User Obi	DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	
Tructed Publishers	DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	
Intrusted Certificates	DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root	11/10/2031	
Third-Party Root Certifica	DownloadManager	DownloadManager	12/21/2022	
Trusted People	DST Root CA X3	DST Root CA X3	9/30/2021	
Client Authentication Issu	D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	11/5/2029	
> 📋 Local NonRemovable Cer	D-TRUST Root Class 3 CA 2 EV 2009	D-TRUST Root Class 3 CA 2 EV 2009	11/5/2029	
> 🧾 Smart Card Trusted Roots	Entrust Root Certification Authority	Entrust Root Certification Authority	11/27/2026	
> 📔 VSWebPublishNAMEMAT	Entrust Root Certification Authority - G2	Entrust Root Certification Authori	12/7/2030	
> 📔 VSWebPublishUNTRUSTEI	Entrust.net Certification Authority (2048)	Entrust.net Certification Authority	7/24/2029	
✓	Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	
> 🧾 Personal	fbivpn.informatik.uni-hamburg.de	fbivpn.informatik.uni-hamburg.de	12/30/2022	
Trusted Root Certification	GeoTrust Global CA	GeoTrust Global CA	5/21/2022	-
Certificates	GeoTrust Primary Certification Authority	GeoTrust Primary Certification Au	7/17/2036	
> 🧾 Enterprise Trust	GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Au	12/2/2037	
> Intermediate Certification	GlobalSign	GlobalSign	3/18/2029	
> Irusted Publishers	GlobalSign	GlobalSign	12/15/2021	
<ul> <li>Ontrusted Certificates</li> <li>Third Date Date Certificates</li> </ul>	GlobalSign	GlobalSign	1/19/2038	

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 !!!