## Including the VPN server certificate on Windows

Tb, 4.1.2021

To establish a secure SSTP VPN connection, the connection requester (private) computer explicitly requires the server certificate of the VPN server *fbivpn.informatik.uni-hamburg.de*. The reason for this is the situation that the VPN server of the computer science checks the login information of the users to the computer science user domain and also assigns special access rights on user/group-membership level. Therefore, a closed authentication process is mandatory. For the VPN server, "foreign certificates", such as .B certificates usually issued by the DFN Association for University Calculators, are not relevant.

The VPN server always presents its own computer/server certificate to the requesting VPN clients. In order for a requesting computer to successfully verify this certificate, the VPN server certificate must also be stored in the certificate store of the respective computer under "Trusted Root Certification Authorities".

Please download the *VPN server certificate* available from the web page <u>https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html</u> to your computer (via an existing Internet connection f.ex. from home, via a VPN connection, or via a pool computer and then offline via USB stick):

ABOUT US	IRZ ACCESS	INFRASTRUCTURE	IT SERVICES	SOF
scanner, library reso		on to access animersity while need		

On the VPN server's side a "Point to Point Tunneling Protocol (PPTP)" and the "Layer 2 Tunneling Protocol (L2TP) with preshared key" is supported.

The Microsoft-proprietary "Secure Socket Tunneling Protocol (SSTP)" is also available. The iRZ recommends they usage of SSTP connections for Windows clients. This enables an increased level of security as well as unobstructed access from every location because only default HTTP/HTTPS ports are used. However, **since 1/1/2021** it is necessary to store the (self signed) certificate of the Informatik VPN server fbivpn.informatik.uni-hamburg.de in your **computer**-certificate store under "Trusted Root Certification Authorities":



Instructions for how to add the vpn-server certificate to Windows.

The VPN server's address is:

fbivpn.informatik.uni-hamburg.de

For detailed tutorials on the VPN access configuration please choose the desired VPN client from the selection on the right-hand menu.

### Method 1: Install certificate directly

Using "right mouse button" -> Context menu "Install Certificate" on the just downloaded VPN server certificate you may store it in the "certificate store" of the computer directly:

A Quick access	^	Name V Earlier this week (1)		Date modifie	
Desktop	1	fbivpn.informatik.uni-hamburg.de			loo
🕹 Downloads	1		Open	-	09:
🗎 Documents	1	V Last month (6)	Install Certificate		
		The second of the second secon	<b>A A A A</b>		ho r

In the automatic installation process confirm the certificate to be been opened:



# Pay close attention to the procedure described below, as the default values of the automatic installation process may not produce the desired result !

Select the "Local Computer" entry as the location for the certificate:



If the selection of the "Local Computer" is not possible/visible here, this is due to the lack of administrator rights of your current login. In this case, use the method explained below via MMC !

Select the explicit selection of the storage space (1st),

ate stores are system areas where certif	Acates are kent	
	icates are kept.	
vs can automatically select a certificate s tificate.	tore, or you can :	specify a location for
Automatically select the certificate store h	based on the type	e of certificate
Place all certificates in the following store		
Certificate store:		
Trusted Root Certification Authorities	3.)	Browse
		2.)
	lificate. uutomatically select the certificate store lace all certificates in the following store Certificate store:	utomatically select the certificate store based on the typ lace all certificates in the following store Certificate store:

#### Use "Find" (2nd) to determine the *Trusted Root Certification Authorities* space (3rd).

Finally, the request is made again for confirmation of the selected storage space:

C	ompleting the Certific	cate Import Wizard
75	e certificate will be imported after	unu slisk Eisisk
11	e cerunicate will be imported after	you dick mish.
1.00	u have specified the following sett	
	Certificate Store Selected by User Content	Trusted Root Certification Authorities Certificate
	Jontent	Cel uncare
		_

The success of the import is now confirmed by the system:





Repeat the procedure that has just been performed (importing the root certificate by right mouse button) again for the "Local User" storage space:

Copy par Paste shi	🗧 🐉 Certificate Import Wizard	×
s PC > E Nam	Welcome to the Certificate Import Wizard	
n N N	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity	
E.	and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.  Store Location © Current User  O Local Machine	
	To continue, dick Next.	

Now, even with the VPN type "automatic", the Windows VPN client should always prefer to negotiate an SSTP connection.

### Method 2: Install certificate via MMC

The downloaded certificate (from <u>https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html</u>) of the VPN server can also be manually inserted into the Windows certificate store as follows. This procedure also allows control of the certificate store (if the above process did not succeed).

As an administrator, open a command line window (cmd.exe):



Now call the MMC tool (alternatively, you can also use Windows Search to start the "mmc" tool as an administrator):

a Administrator: Command Prompt	
Microsoft Windows [Version 10.0.19041.685] (c) 2020 Microsoft Corporation. All rights reserved.	
C:\WINDOWS\system32>mmc_	

In the management console that will appear, use the "File" tab to select the "Add snap-in" item:

New	Ctrl+N	
Open	Ctrl+0	
Save	Ctrl+S	There are no items to show in this view.
Save As		
Add/Remove Snap-	in Ctrl+M < 2.)	
Options		
Recent File		
Exit		

Select and add "Certificates" from the list of Windows management "snap-ins" :

Add or Remove Snap-ins

extensible snap-ins, you can configure which extensions are enabled. Available snap-ins: Selected snap-ins: Console Root Snap-in A Vendor ActiveX Control Microsoft Cor... Authorization Manager Microsoft Cor... 1.) Certificates ft Cor... Component Services Microsoft Cor... Computer Managem... Microsoft Cor... 🔒 Device Manager Microsof 2.) Add > 📅 Disk Management Microsof Event Viewer Microsoft Cor... Folder Microsoft Cor... Group Policy Object ... Microsoft Cor... Hvper-V Manager Microsoft Cor...

You can select snap-ins for this console from those available on your computer and configure the se

This must be done **twice**, a selection of certificate stores will appear when "adding" and both "My User Account" and "Computer Account" will be required.

First selection will be "My User Account" certificate store:



In the next step select "Certificates" -> "Add" again, but select "Computer Account":



The "Local Computer" must be selected again in an intermediate step:

Select the computer you want this sn	nap-in to manage.
This snap-in will always manage:	
Local computer: the compute	r this console is running on) <b>1.)</b>
O Another computer:	Browse
	b be changed when launching from the command line. This
only applies if you save the co	nsole.
only applies if you save the co	nsoie. 2.j

You will notice two certificate stores active in the management console:



After confirmation with "OK" you can now see the details of these certificate stores, please expand both ("current user" and "local computer") accordingly:



Important here are the directories for "Trusted Root CAs", expand them again and open the respective subdirectory "Certificates". The middle column contains the certificates that have already been (pre-)installed. "More Actions" -> "All Tasks"-> finally get to the crucial point "Import" of certificates:

• 🔿 🙇 📅 📋 🗟 🗟 🚺	1.11					
Console Root	Issued To	Issued By	Actions			
Certificates - Current User	AAA Certificate Services	AAA Certificate Servi	Certificates		▲ <sup>3:)</sup>	
Trusted Root Certification	Actalis Authentication Root CA	Actalis Authenticatio	More Actions 2.)	Import	All Tasks	
🗋 Certificates < 1:)	Add Trust External CA Root	AddTrust External CA AffirmTrust Commer			View	
Enterprise Trust     Intermediate Certification	Baltimore CyberTrust Root	Baltimore CyberTrust		4.)	New Window from Here	
Active Directory User Obi	Certum CA	Certum CA				
> Trusted Publishers	Certum Trusted Network CA	Certum Trusted Netv			New Taskpad View	
> Untrusted Certificates	🔄 Chambers of Commerce Root	Chambers of Comm			Refresh	
> 📔 Third-Party Root Certifica	🔄 Class 3 Public Primary Certificat	Class 3 Public Primar			Export List	
> 📔 Trusted People	COMODO ECC Certification Au	COMODO ECC Certil			Export Eistin	
> 📋 Client Authentication Issu	COMODO RSA Certification Au	COMODO RSA Certif			Help	
> 📋 Local NonRemovable Cer	Copyright (c) 1997 Microsoft C	Copyright (c) 1997 N				
> 🦰 Certificate Enrollment Rec	DESKTOP-NI6DB0H	DESKTOP-NI6DB0H			? 🖻 — 🗆 🔅	×

Please select the downloaded VPN server certificate, then follow the default procedure:

	o Import Specify the file you want to import.
1	File name:
)	C: \Users \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 (.P7B)
	Microsoft Serialized Certificate Store (.SST)
	_

Once again check for "Trusted Root Certification Authority" as target store in next step and confirm:

	te Store tificate stores are sy	ystem areas where certificates a	are kept.	
185-	4	ally select a certificate store, or		
the	certificate,	any select a ceruncate store, or	you can specify a location	101
	O Automatically sele	ect the certificate store based o	n the type of certificate	
	Place all certificat	tes in the following store		
	Certificate store:	and the second second		
1.)	Trusted Root C	ertification Authorities	Browse,	
			( 2.)	
			Next	Ci
	cate Import Wizard		Next	Ci
Con	pleting the o	Certificate Import W	Next	Ci
Con	pleting the o		Next	Ci
<b>Con</b> The ce You ha	rtificate will be impo	<b>Certificate Import W</b> rted after you dick Finish. lowing settings:	izard	Ci
Con The ce You ha	rtificate will be impo ave specified the foll ficate Store Selected	Certificate Import W rted after you click Finish. lowing settings: d by User Trusted Root Certific	izard	Ci
Con The ce You ha	rtificate will be impo ave specified the foll ficate Store Selected	Certificate Import W rted after you click Finish. lowing settings: d by User Trusted Root Certific Certificate	izard	

Hopefully you will finally get to "The import process was successful":

Finish

Cancel



It can now be checked again whether a valid certificate of the "fbivpn.informatik.uni-hamburg.de" with expiration date "30.12.2022" appears in the list:

🜇 Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

🗭 🛸 📶 🔏 🖬 🗙 🛅 1	🗟   🔽 📆			
Console Root ∧ ✓ ☑ Certificates - Current User	Issued To	Issued By	Expiration Date	Inte 🗥
> 📋 Personal	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA DigiCert Global Root CA	11/10/2031 11/10/2031	Clie Clie
Certificates	DigiCert Global Root G2	DigiCert Global Root G2 DigiCert Global Root G3	1/15/2038 1/15/2038	Clie Clie
> 2 Enterprise Trust > 2 Intermediate Certification	DigiCert High Assurance EV Ro	DigiCert High Assurance EV Root DownloadManager	11/10/2031	Clie < Al
Active Directory User Obj Trusted Publishers	DST Root CA X3	DST Root CA X3	9/30/2021	Clie
> Contrusted Certificates > Contrusted Certificates > Contrusted Certificates	D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009 D-TRUST Root Class 3 CA 2 EV 2009	11/5/2029 11/5/2029	Clie Clie
Trusted People Client Authentication Issue	Entrust Root Certification Auth	Entrust Root Certification Authority Entrust Root Certification Authori	11/27/2026	Clie
> Cocal NonRemovable Cer	Entrust.net Certification Author	Entrust.net Certification Authority	7/24/2029	Clie
> Certificate Enrollment Res > Certificate Enrollment Res > Certificate Enrollment Res	Equifax Secure Certificate Auth fbivpn.informatik.uni-hamburg	Equifax Secure Certificate Authority fbivpn.informatik.uni-hamburg.de	8/22/2018 12/30/2022	Cot <a< td=""></a<>
> 📔 VSWebPublishNAMEMA	GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Clie

#### Important:

After the certificate has been successfully added for "Current User", this integration flow must now be repeated again for the second certificate store "Local Computer" !

Now the console can be closed ("File"-> "stop", do not save settings),

and SSTP VPN should now work !!!