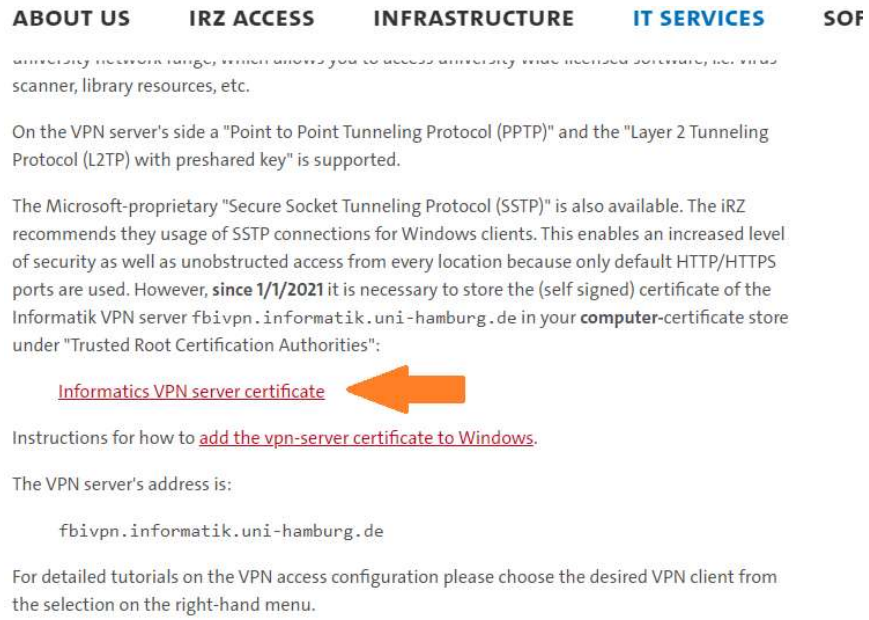
Including the VPN server certificate on Windows

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".

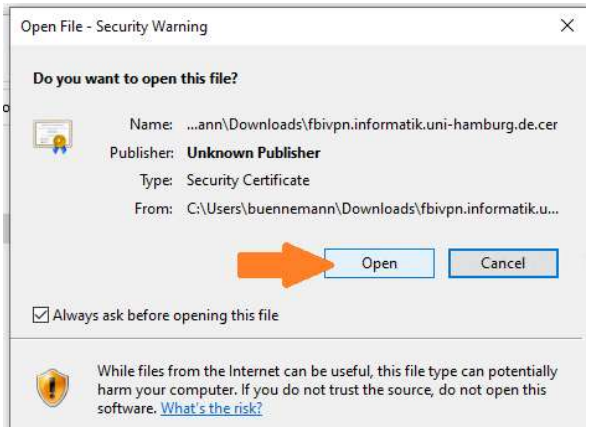
Please download the ***VPN server certificate*** available from the web page https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html to your computer (via an existing Internet connection f.ex. from home, via a VPN connection, or via a pool computer and then offline via USB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



Method 1: Install certificate directly

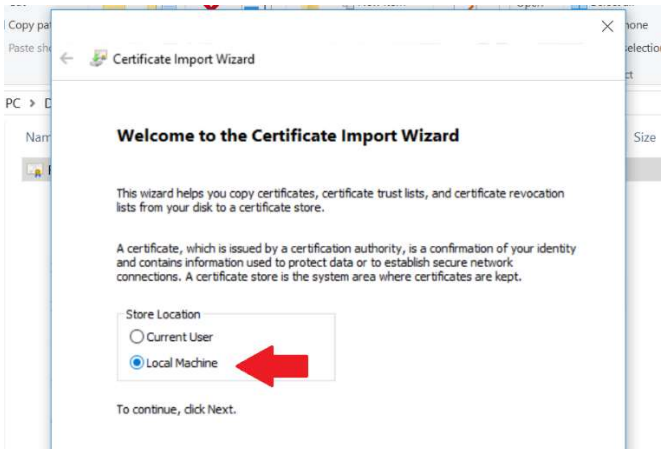
Using "right mouse button" -> Context menu *"Install Certificate"* on the just downloaded VPN server certificate you may store it in the “certificate store” of the computer directly:

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



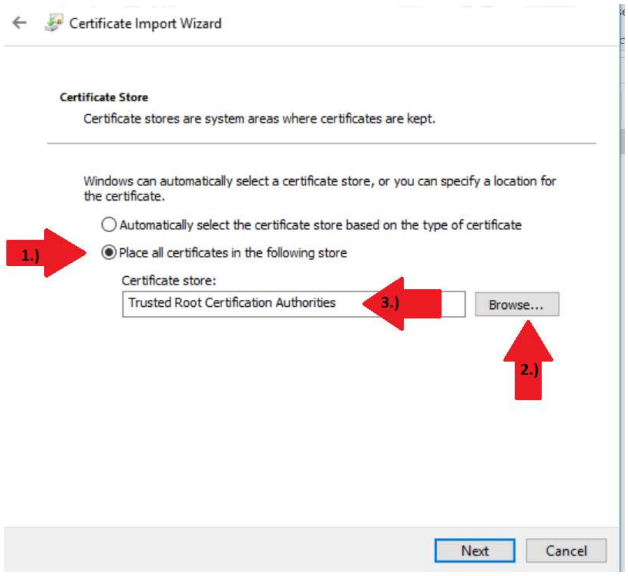
Pay close attention to the procedure described below, as the default values of the automatic installation process may not produce the desired result !

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



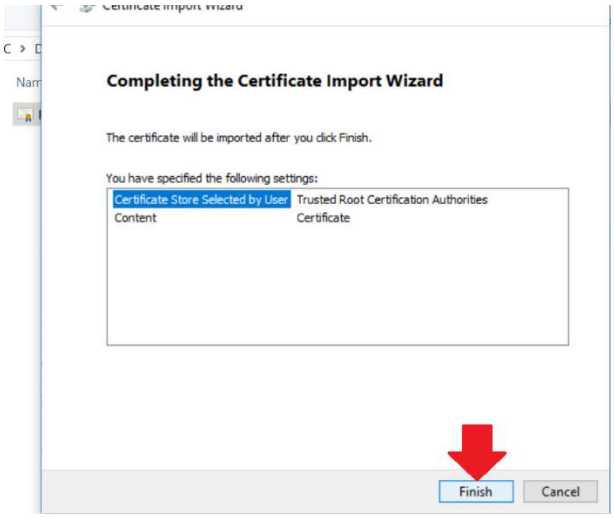
If the selection of the "Local Computer" is not possible/visible here, this is due to the lack of administrator rights of your current login. In this case, use the method explained below via MMC !

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

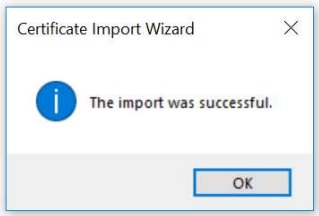


Use "Find" (2nd) to determine the ***Trusted Root Certification Authorities*** space (3rd).

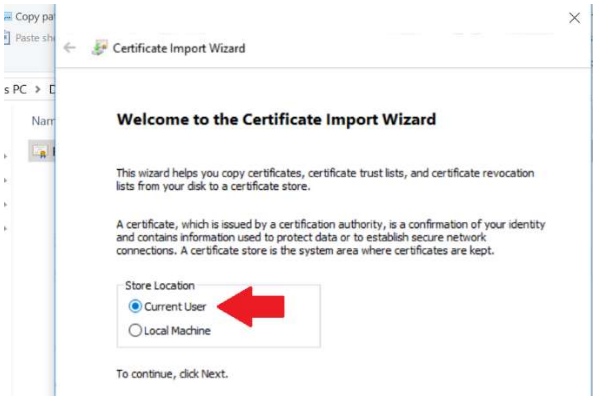
Finally, the request is made again for confirmation of the selected storage space:



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:

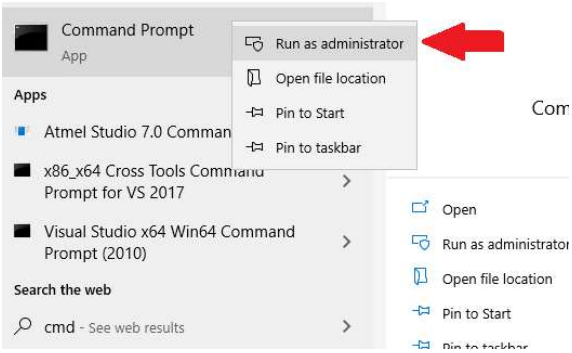


Now, even with the VPN type "automatic", the Windows VPN client should always prefer to negotiate an SSTP connection.

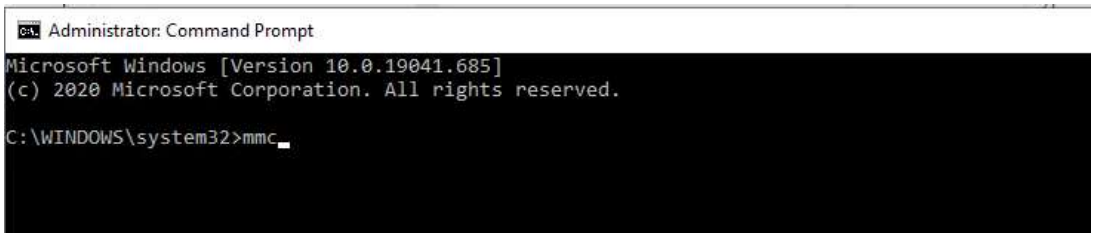
Method 2: Install certificate via MMC

The downloaded certificate (from https://www.inf.uni-hamburg.de/inst/irz/it-services/private-devices/vpn-clients.html) 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).

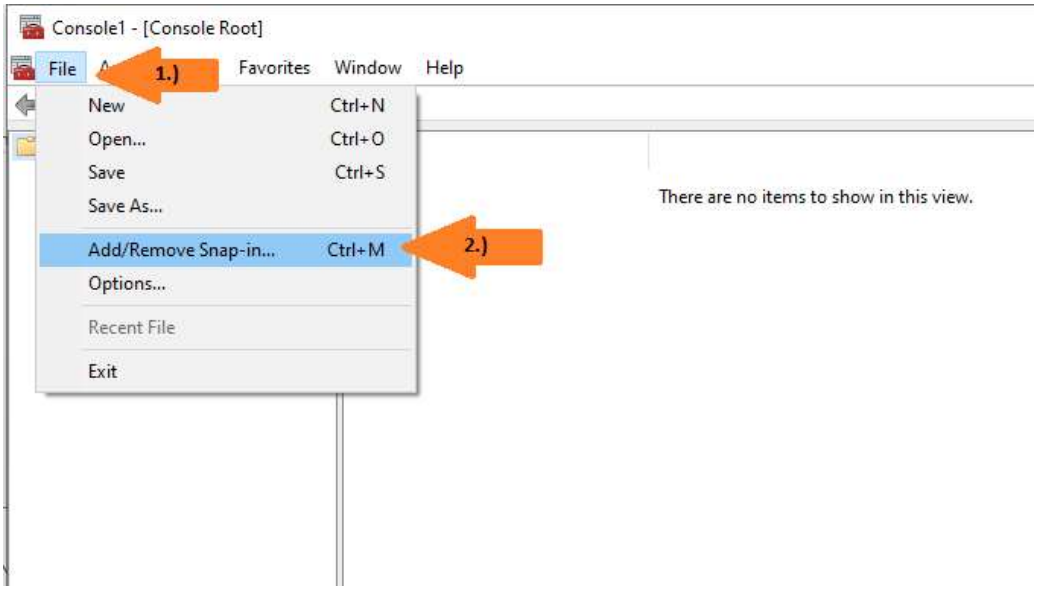
As **an administrator,** open a command line window (cmd.exe):



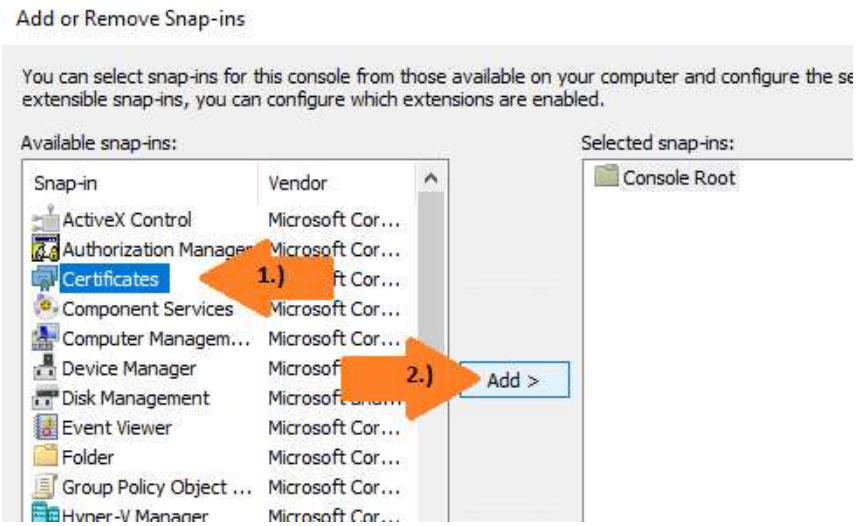
Now call the MMC tool (alternatively, you can also use Windows Search to start the "mmc" tool **as an administrator):**



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

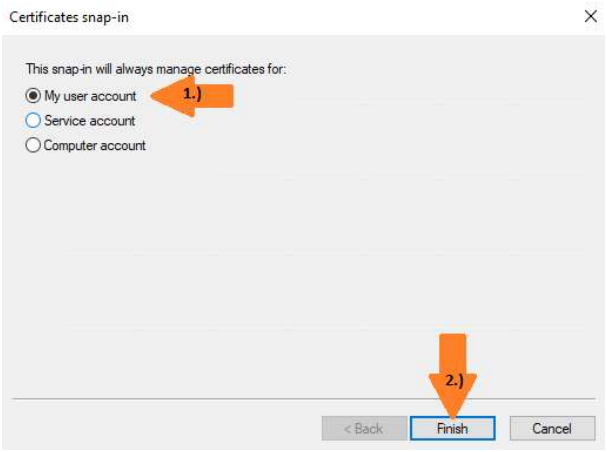


Select and add “Certificates” from the list of Windows management "snap-ins" :

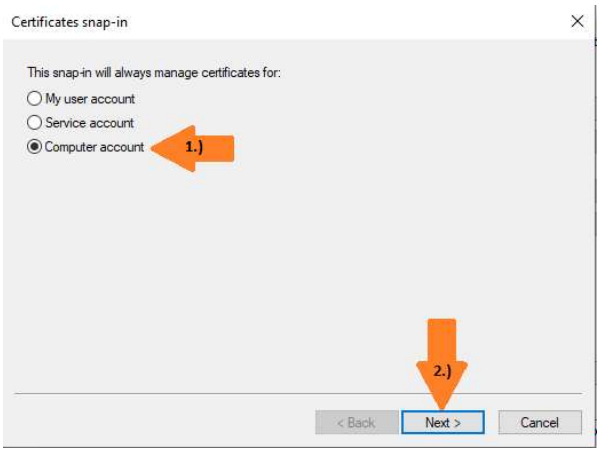


This must be done **twice,** a selection of certificate stores will appear when "adding" and both "My User Account" and "Computer Account" will be required.

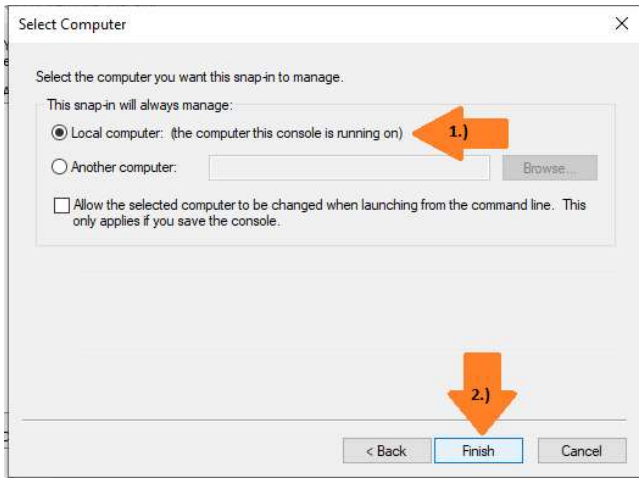
First selection will be "My User Account" certificate store:



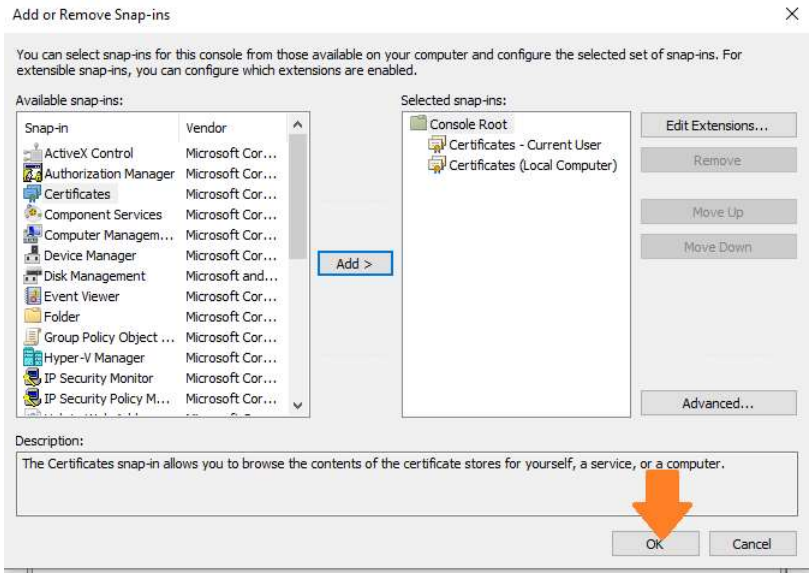
In the next step select "Certificates" -> "Add" again, but select "Computer Account":



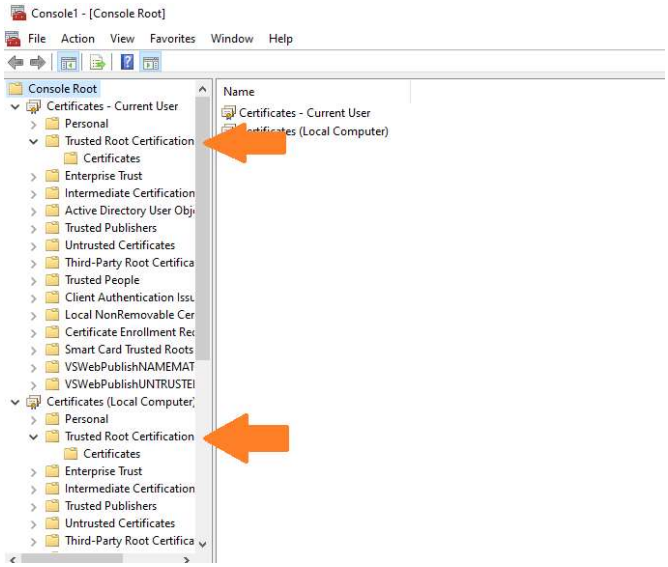
The "Local Computer" must be selected again in an intermediate step:



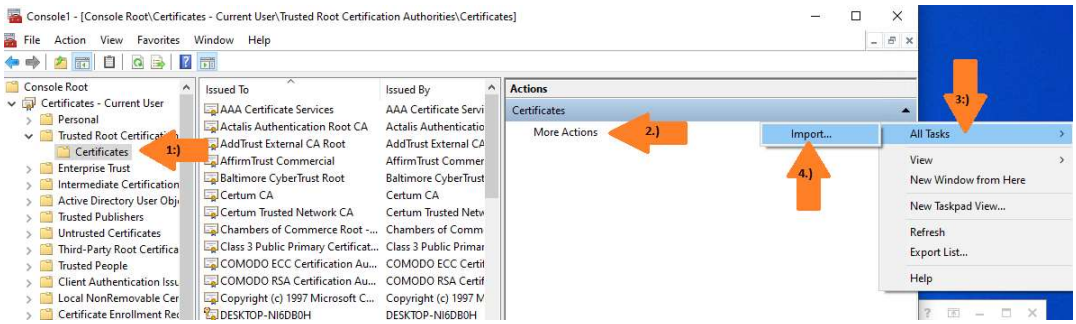
You will notice two certificate stores active in the management console:



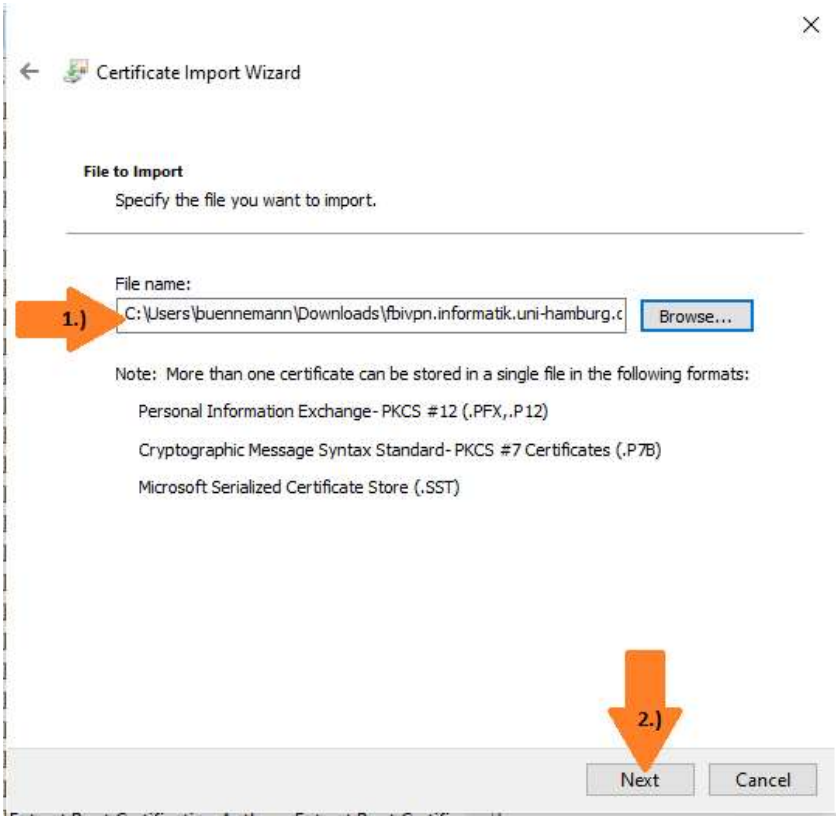
After confirmation with "OK" you can now see the details of these certificate stores, please expand both ("current user" and "local computer") accordingly:



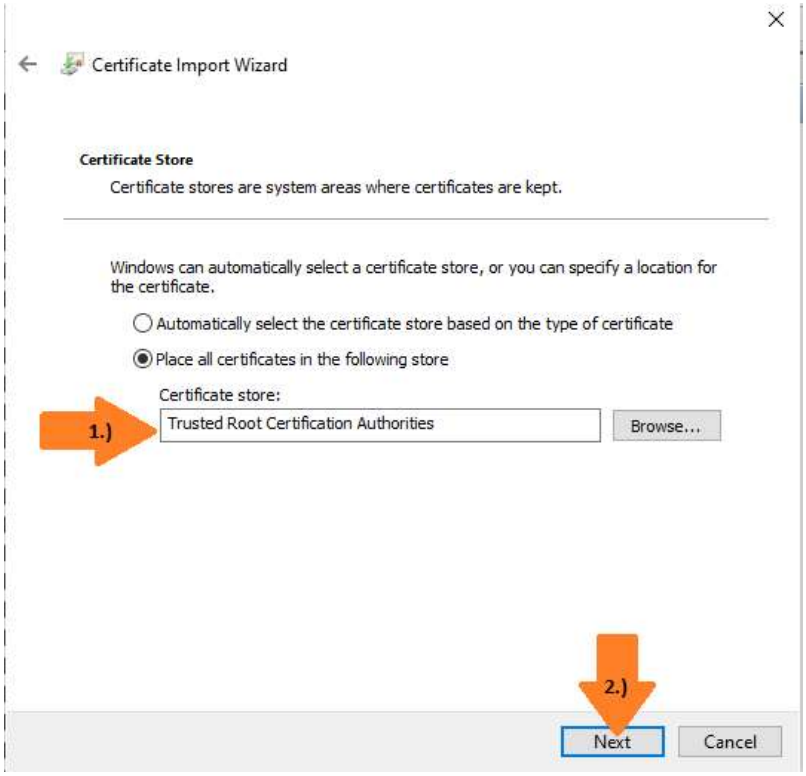
Important here are the directories for "Trusted Root CAs", expand them again and open the respective subdirectory "Certificates". The middle column contains the certificates that have already been (pre-)installed. "More Actions" -> "All Tasks"-> finally get to the crucial point "Import" of certificates:

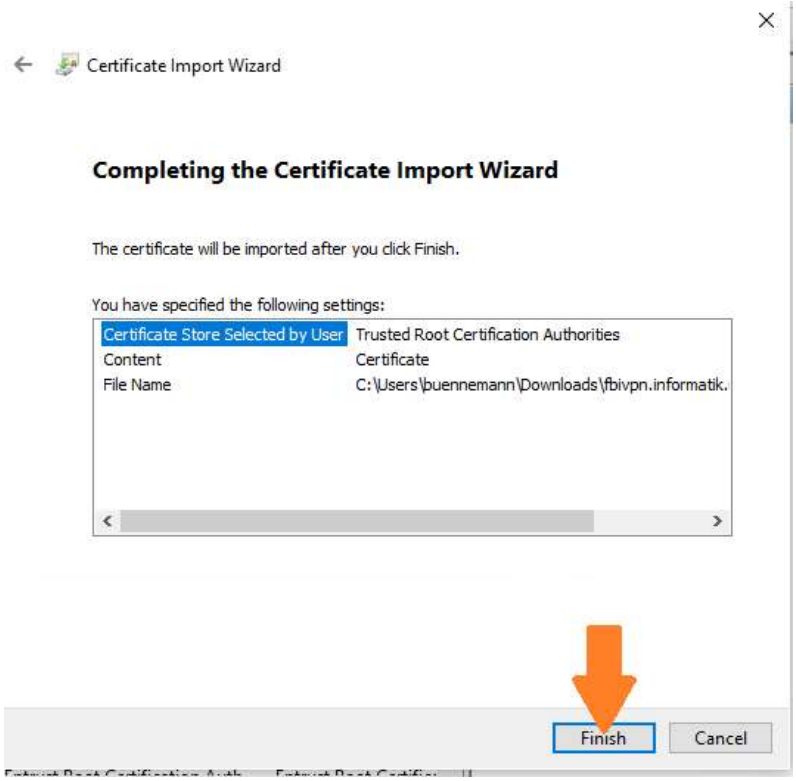


Please select the downloaded VPN server certificate, then follow the default procedure:

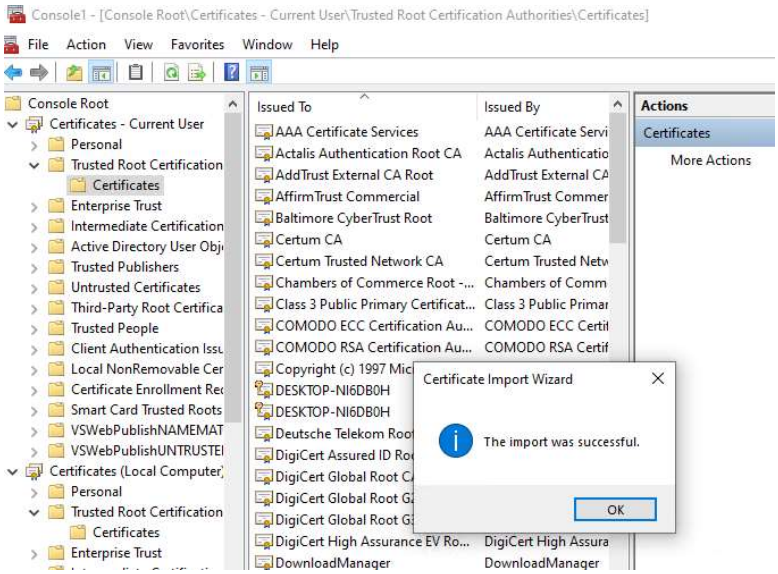


Once again check for “Trusted Root Certification Authority” as target store in next step and confirm:

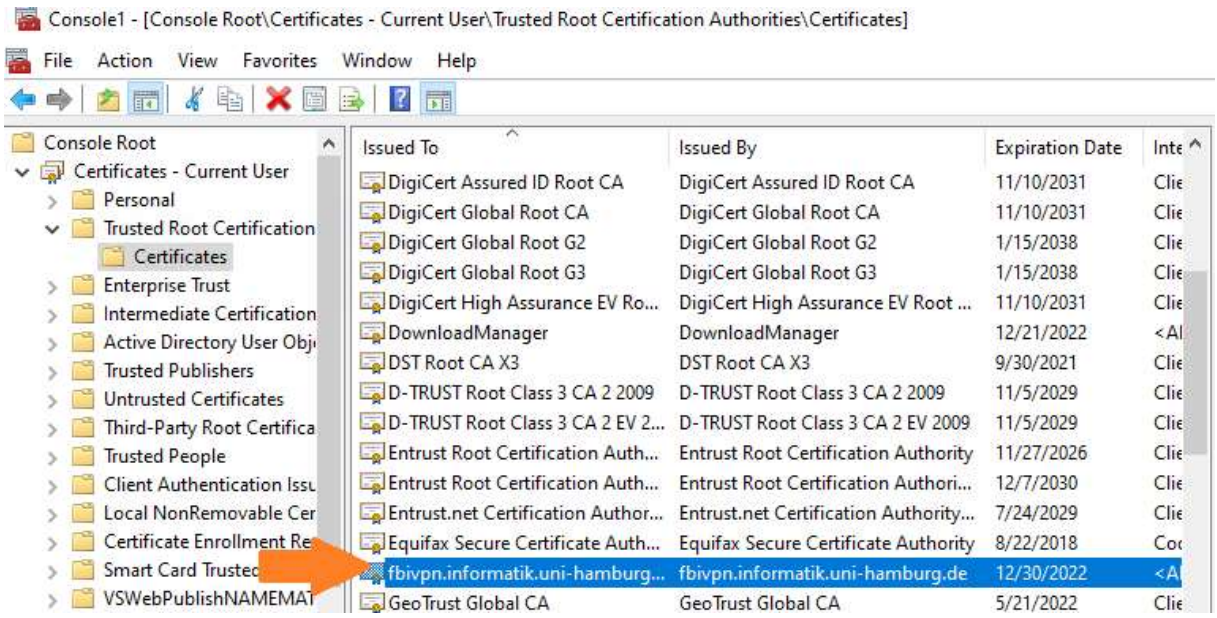




Hopefully you will finally get to "The import process was successful":



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:



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 !!!