

# VPN Homeworking

## Inhaltsverzeichnis

- 1 Wie funktioniert Homeworking?
- 2 VPN Kanal aufbauen
  - 2.1 Openvpn Connect
    - 2.1.1 Installation
      - 2.1.1.1 Windows
      - 2.1.1.2 Android
      - 2.1.1.3 iOS
      - 2.1.1.4 MacOS
      - 2.1.1.5 Linux
    - 2.1.2 Verwendung:
      - 2.1.2.1 mit App OpenVPNconnect
        - 2.1.2.1.1 Profil importieren
        - 2.1.2.1.2 Verbindung aufbauen
      - 2.1.2.2 Linux
        - 2.1.2.2.1 vom Terminal aus
        - 2.1.2.2.2 Mit NetworkManager
  - 2.2 Vpn Verbindung mit Bordmitteln
    - 2.2.1 Windows 10 (Pc/Laptop zu Hause)
      - 2.2.1.1 VPN Verbindung erstellen
      - 2.2.1.2 VPN verbinden
      - 2.2.1.3 Probleme
    - 2.2.2 Windows 8 (zu Hause) - geht auch für Windows 7
      - 2.2.2.1 VPN Verbindung erstellen
      - 2.2.2.2 VPN verbinden
    - 2.2.3 Vpn auf MAC
    - 2.2.4 Android
- 3 MFA: Erhöhte Sicherheit mit 2-Faktor-Authentifizierung
  - 3.1 Vorbereitung
    - 3.1.1 Anmeldung im mfa-Portal
    - 3.1.2 privacyIDEA Authenticator installieren
    - 3.1.3 Token ausrollen und in App importieren
  - 3.2 Authentifizierung beim Verbinden mittels 2-Faktor-Authentifizierung

- 4 Remotezugriff auf Pc der Körperschaft
  - 4.1 Konfiguration des Pc der Körperschaft
  - 4.2 Konfiguration Pc zu Hause

# Wie funktioniert Homeworking?

Vom Pc zu Hause wird auf dem PC im Büro zugegriffen, und zwar über Remotedesktop

1.) Es benötigt einen geschützten Kanal zum Büro, entweder

a) über Openvpn Connect oder

b) über Vpn - Ipsec von Windows

Die einfachere Variante ist Variante a) über openVPN. Sollte die nicht funktionieren, dann bitte die Variante b) benutzen.

2.) Nachdem der Kanal konfiguriert wurde und die Verbindung steht, kann per Remotedesktop über die Ipadresse des Bürorechners auf den Betriebsrechner zugegriffen werden.

## Berechtigung:

**Berechtigungen:** Jeder VPN-Benutzer muss zuerst vom EDV-Verantwortlichen der eigenen Körperschaft die Berechtigung erhalten, sich über VPN verbinden zu dürfen. Dies kann wie üblich mit <https://im.gvcc.net> erledigt werden:

Und zwar im Berechtigungsteil mit der Berechtigung "Homeworking VPN rdp".

Das betrifft Windows 10- Windows 8- Windows7-, Adroid, Linux, iPhone und Mac-Benutzer

## Zugang zur Dokumentation von zu Hause:

Auf Geminfo kann auch von zu Hause aus zugegriffen werden:

Daher könnt ihr die Dokumentation auch von zu Hause aus aufrufen.

Gebt folgenden Link ein:

<https://wiki.gvcc.net>

Die Anmeldung erfolgt mit eurem Benutzer und Kennwort.

Geht dort auf "Dokumentation" und dann auf "Vpn Homeworking"

# VPN Kanal aufbauen

## Openvpn Connect

**ACHTUNG!:** Username in OpenVPN ist immer **user\_gemeinde**, der Teil hinter dem "\_" z.B. **\_bruneck** muss mit angegeben werden.

## Installation

Für openVPN muss zuerst ein Clientprogramm installiert werden.

### Windows

Lade dazu **OpenVPN Connect for Windows V.3**: <https://openvpn.net/client-connect-vpn-for-windows/> (<https://openvpn.net/client-connect-vpn-for-windows/>) herunter und führe die Installation aus.

### Android

Google Play (<https://play.google.com/store/apps/details?id=net.openvpn.openvpn>)

### iOS

App Store (<https://apps.apple.com/us/app/openvpn-connect/id590379981>)

### MacOS

siehe <https://openvpn.net/vpn-server-resources/connecting-to-access-server-with-macos> (http

s://openvpn.net/vpn-server-resources/connecting-to-access-server-with-macos/)

## Linux

**openvpn** und eventuell **network-manager-openvpn** mit Paketmanager installieren.

## Verwendung:

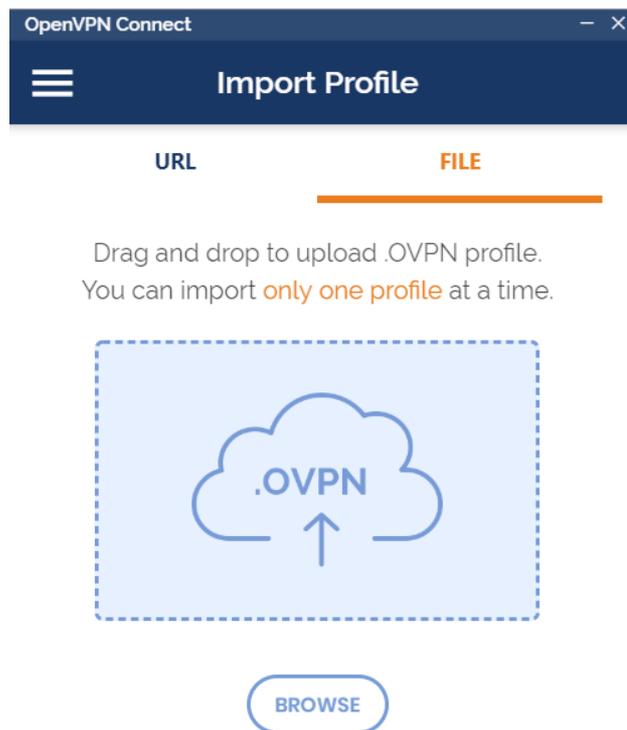
### mit App OpenVPNconnect

#### Profil importieren

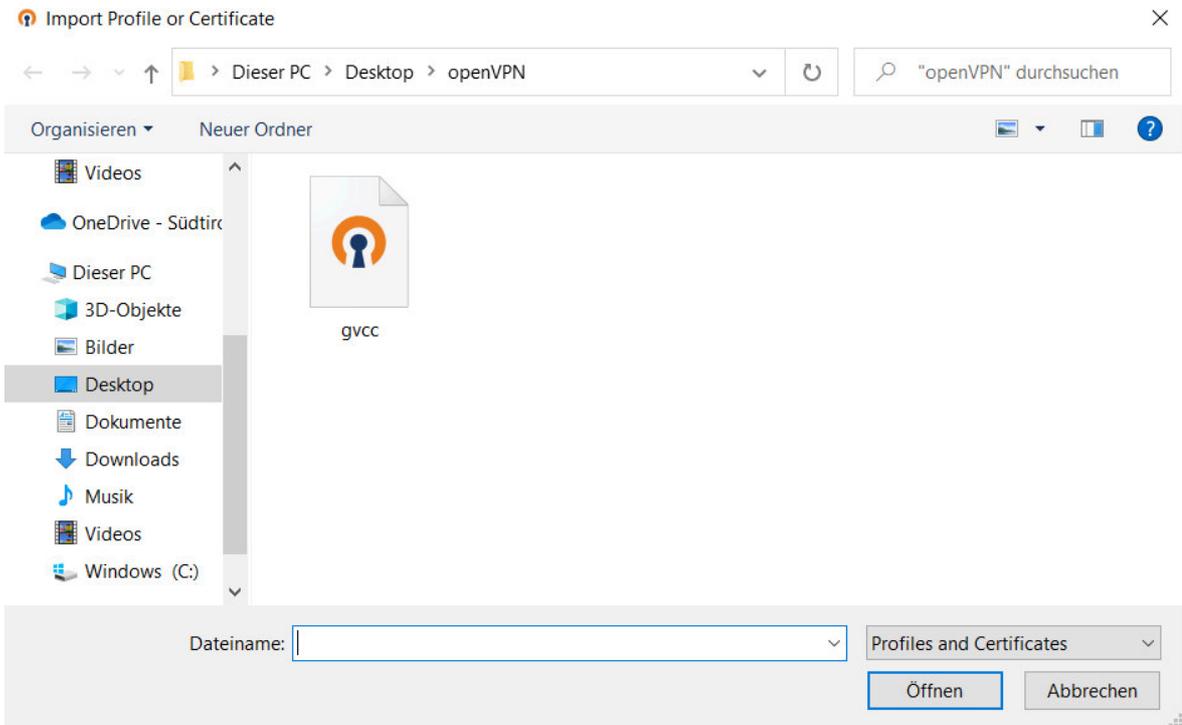
Nach erfolgter Intallation kann das Programm **openvpn connect** geöffnet werden. Du kannst folgende Datei herunterladen und entpacken:

gvcc.ovpn

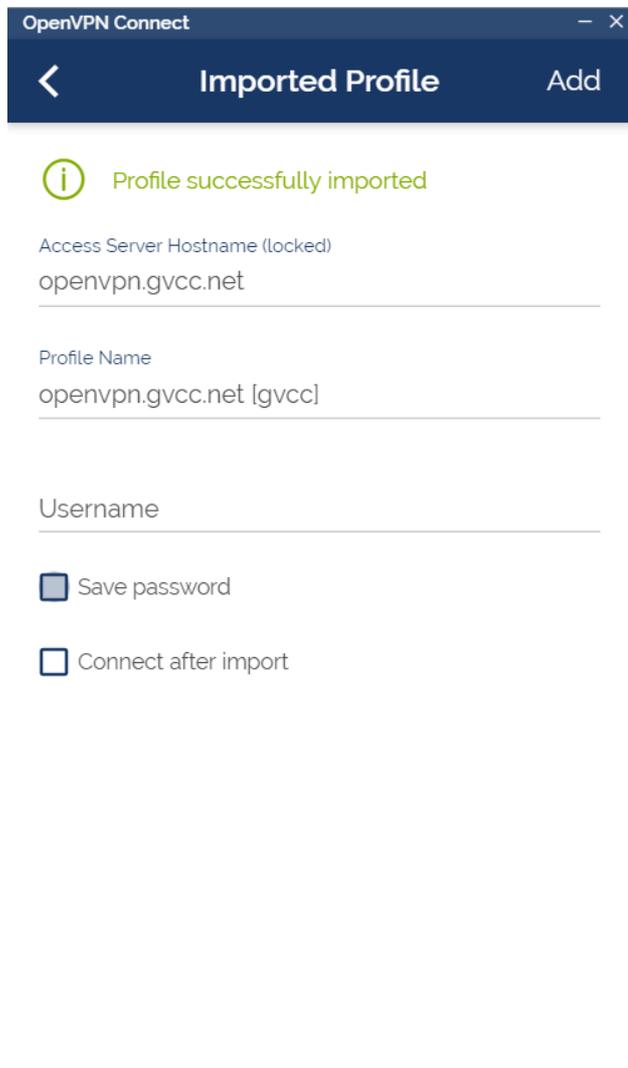
Beim ersten Öffnen des Programmes erscheint der Dialog zum Importieren des Profils:



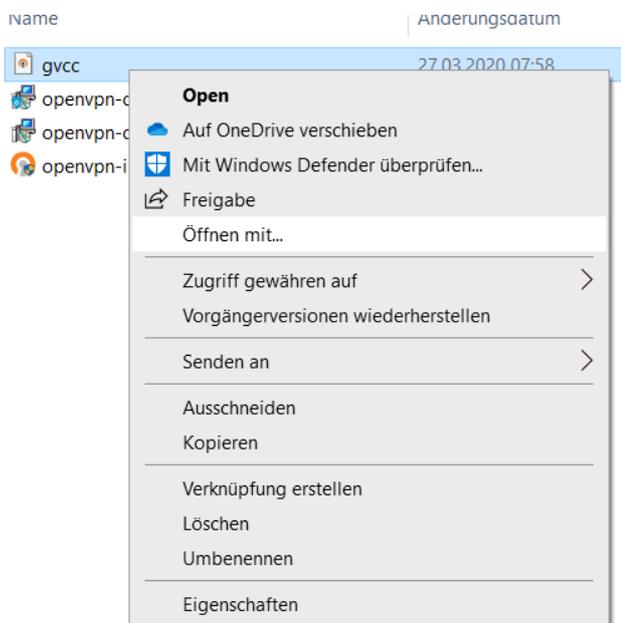
Die Config-Datei wählen:

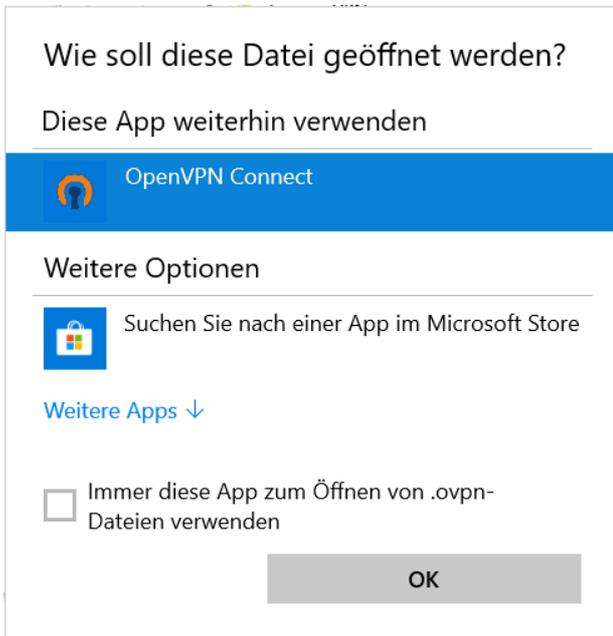


... und importieren...



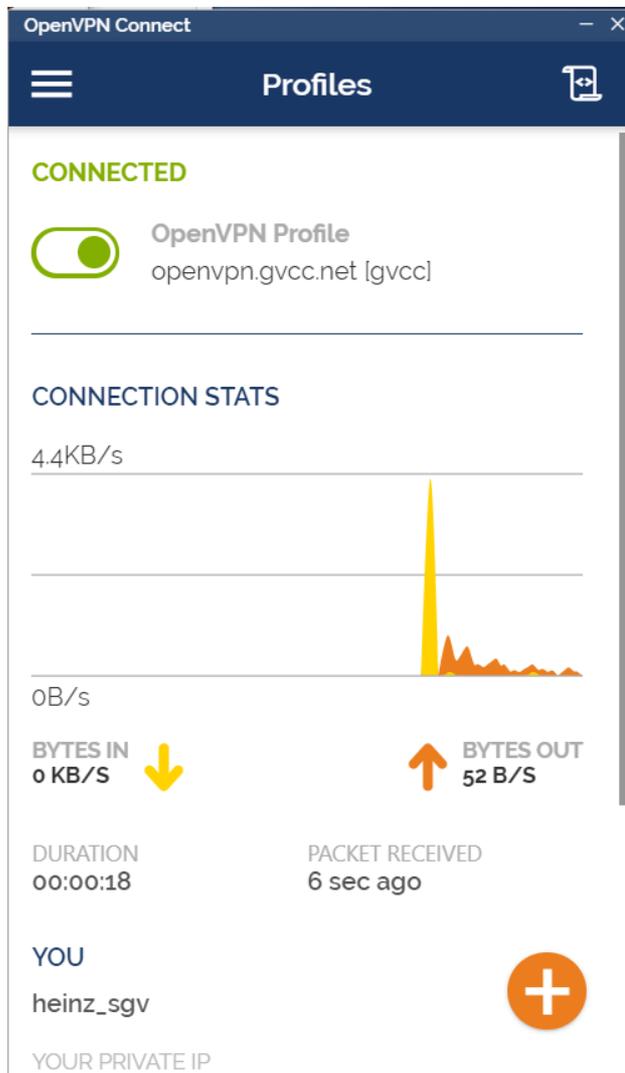
Alternativ: Zip entpacken und die Datei **gvcc.ovpn** mit Dateimanager öffnen:





## Verbindung aufbauen

Nach dem Import der Config kannst du den grünen Schalter zum Verbinden umlegen:



## Linux

### vom Terminal aus

Nach der Installation kannst du den Kanal mit **sudo openvpn --config gvcc.ovpn** aufbauen.

### Mit NetworkManager

Im **NetworkManager** auf **VPN hinzufügen** klicken und mit **aus Datei importieren** die **gvcc.ovpn** einlesen.

Eventuell **Diese Verbindung nur für Ressourcen in deren Netzwerk verwenden** auswählen.

Abbrechen gvcc VPN Anwenden

Details Identität IPv4 IPv6

**IPv4-Methode**

Automatisch (DHCP)  Nur Link-Local  
 Manuell  Deaktivieren  
 Für anderen Rechner freigegeben

**DNS** Automatisch

IP-Adressen durch Kommata trennen

**Routen** Automatisch

Adresse	Netzmaske	Gateway	Metrik
			🗑️

Diese Verbindung nur für Ressourcen in deren Netzwerk verwenden

# Vpn Verbindung mit Bordmitteln

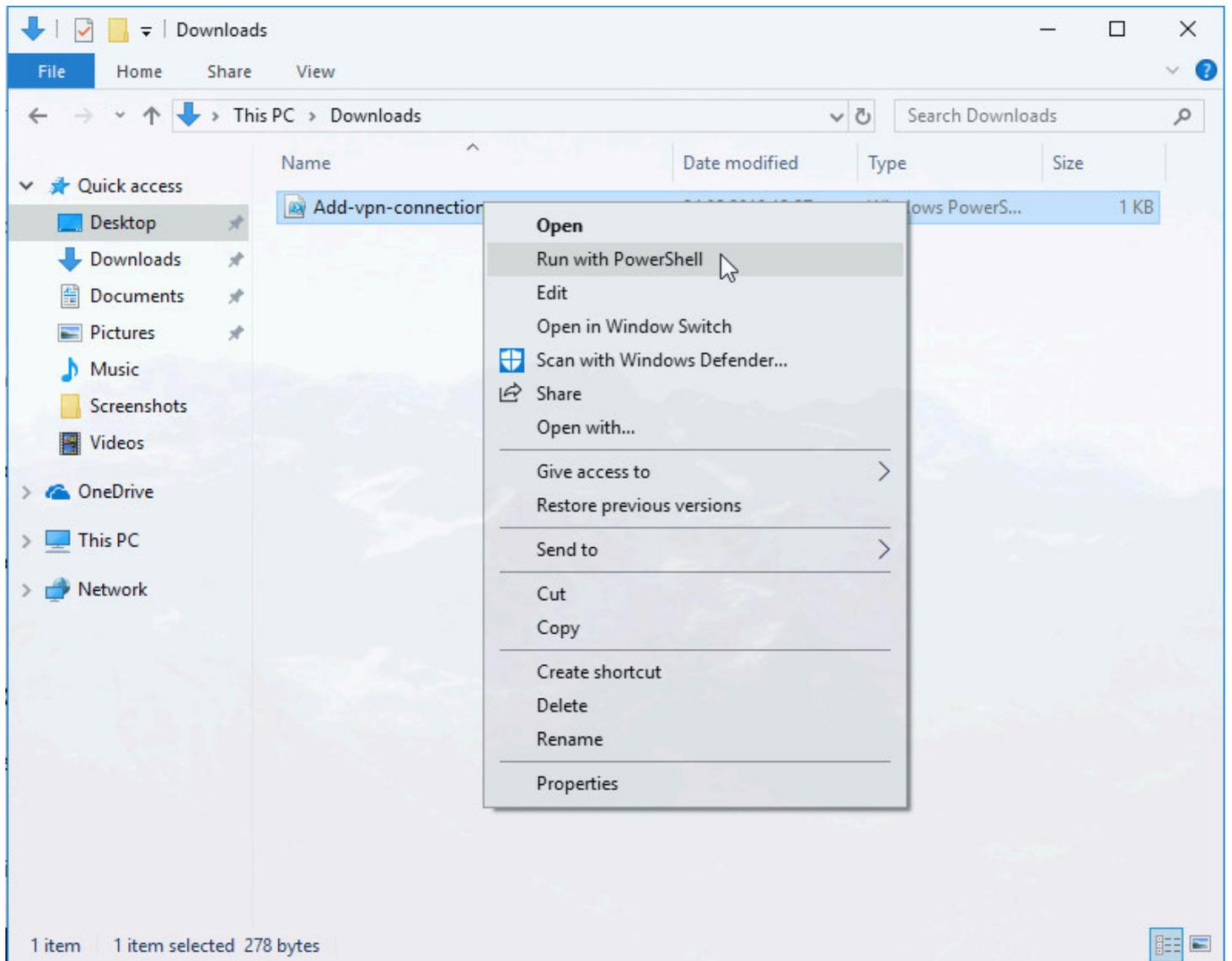
## Windows 10 (Pc/Laptop zu Hause)

### VPN Verbindung erstellen

Um eine VPN Verbindung mit Windows 10 einzurichten, kann folgender Powershell-Script ausgeführt werden:

add-vpn-connection.ps1 (1 KB)

Script herunterladen, mit Rechts-Klick öffnen, "mit PowerShell ausführen", jeweils mit Y bestätigen.



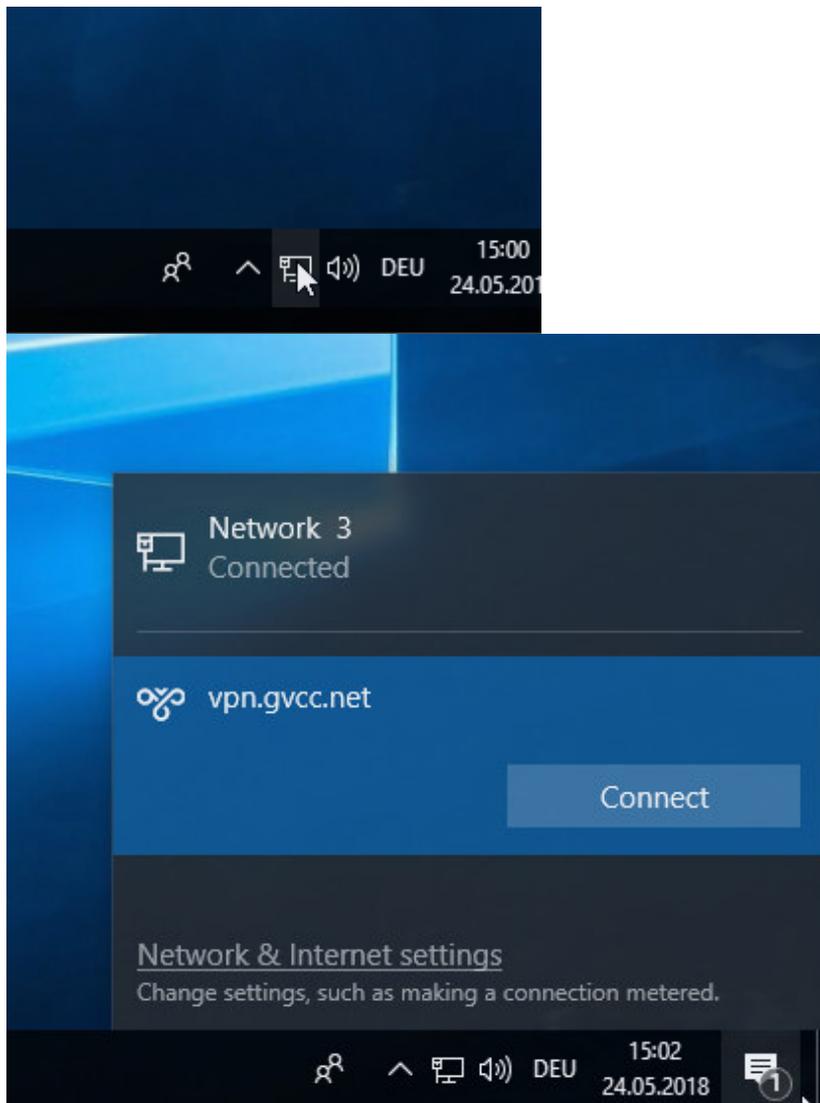
## VPN verbinden

Rechts unten auf die Internet-Ikone klicken, auf [vpn.gvcc.net](https://vpn.gvcc.net) und dann auf connect klicken.

**Benutzer** und **Passwort** eingeben.

**ACHTUNG:** Bei Körperschaften die über einen AD-Trust verbunden sind, die Domain voranstellen:

Z.B.: **BZGEIS.IT\anne\_bzgeis** oder **bzgeis\anne\_bzgeis**



Jetzt zu Punkt 3 Remotezugriff auf Pc der Körperschaft

## Probleme

Bei so einigen Windows-Versionen gibt es Bugs bez. VPN. Sollte der PC betroffen sein, Windows-Update anstoßen, alle Updates durchführen, reboot. - Geduld

## Windows 8 (zu Hause) - geht auch für Windows 7

**Achtung!:** Windows 7 bekommt seit Jänner keine Sicherheitsupdates von Microsoft, der Pc ist daher ungeschützter als Windows 8 oder Windows 10, ein solches System wird vom Gemeindenverband nicht empfohlen und daher bitte nur für die derzeitige Ausnahmesituation des Coronavirus zu verwenden.

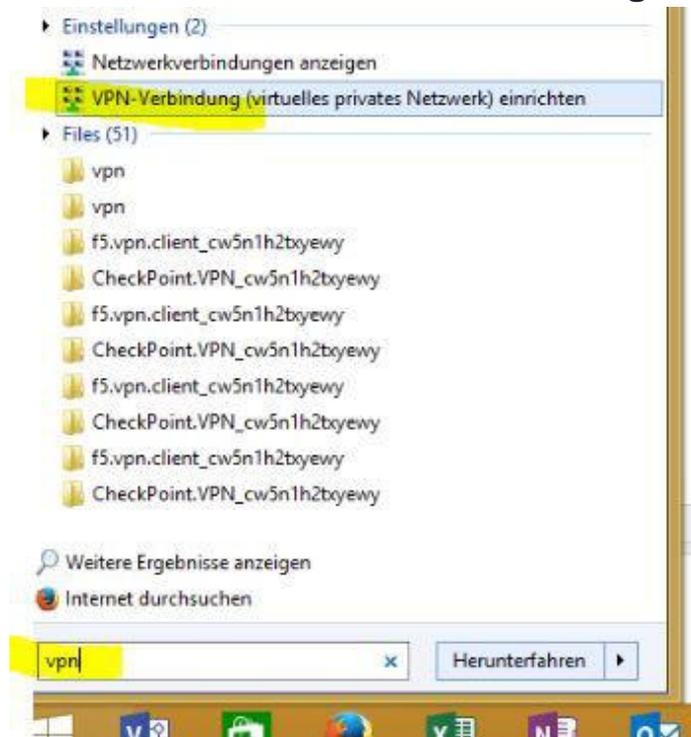
Ansonsten kann die Einrichtung ganz ähnlich wie bei Windows 8 vorgenommen werden.

Einzig Punkt "Jetzt nicht verbinden, sondern für spätere Einrichtung konfigurieren" bei der

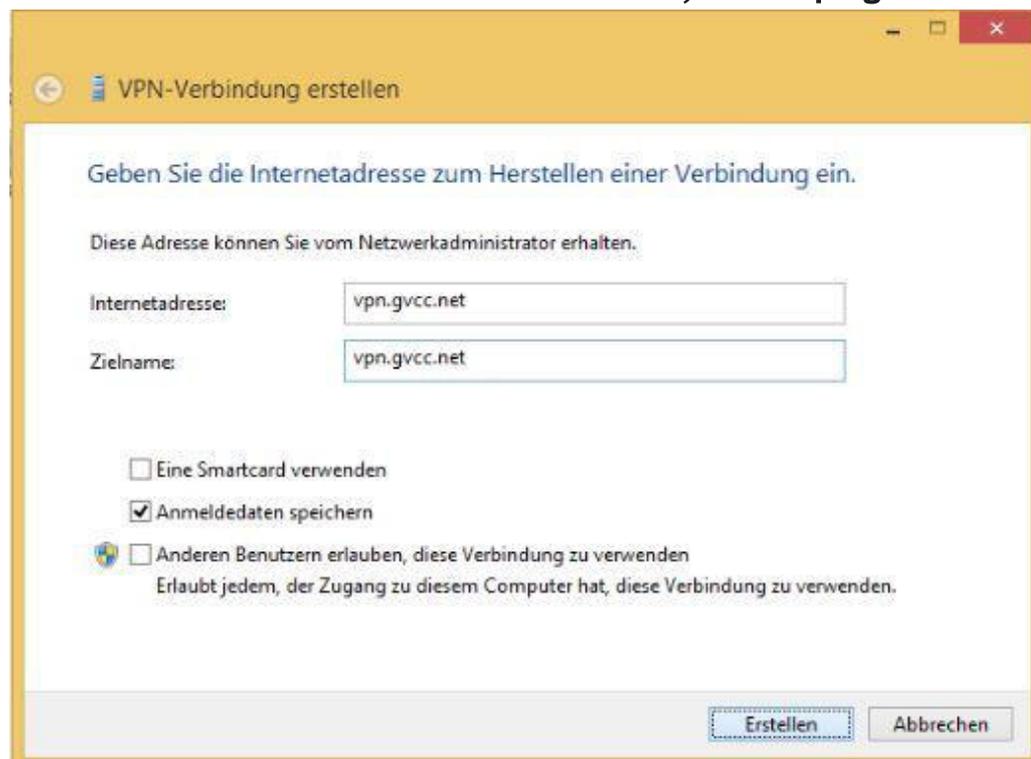
Einrichtung aktivieren und dann beim nächsten Punkt Benutzer und Kennwort hinterlegen. Die restlichen Schritte sind wie bei Windows8

## VPN Verbindung erstellen

Links unten auf das Start-Symbol klicken, in die Befehlszeile **vpn** eingeben, und in der erscheinenden Liste auf "**VPN-Verbindung (virtuelles privates Netzwerk) einrichten**" klicken

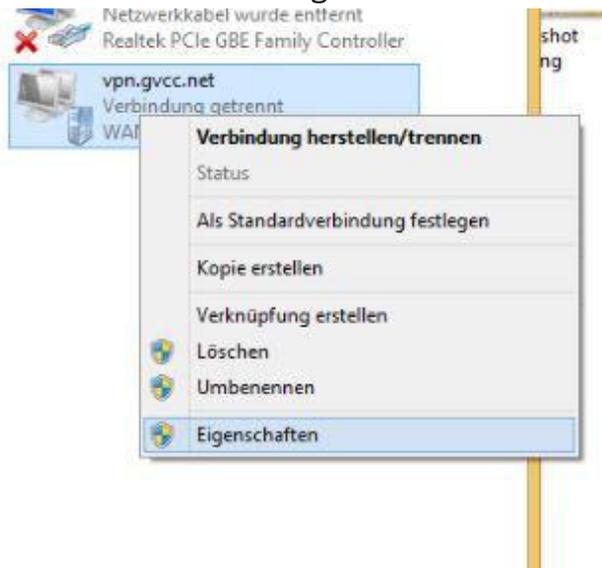


In den Feldern Internetadresse und Zielname jeweils **vpn.gvcc.net** eintragen und speichern

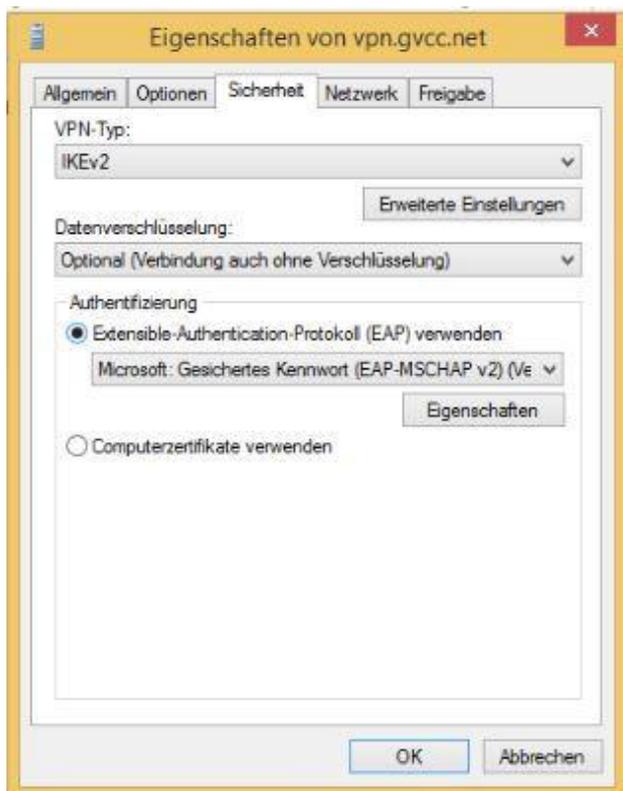


Nochmals unten links auf das Start-Symbol klicken, in die Befehlszeile **Netzwerk** eingeben und in

der erscheinenden Liste auf **Netzwerkverbindungen anzeigen** klicken (bei Windows7: **Netzwerk- und Freigabecenter** und dann **Adaptoreinstellungen**). Auf der Verbindung "**vpn.gvcc.net**" rechts-klicken und Eigenschaften wählen.

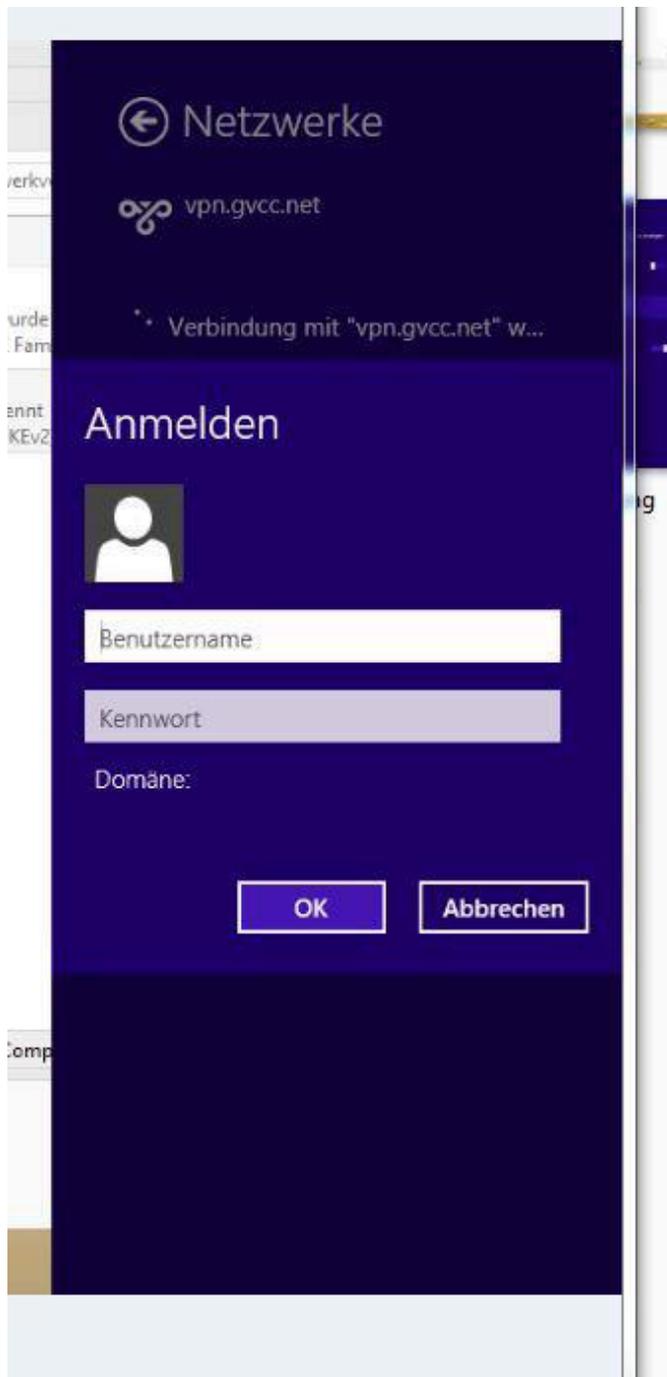


Im Reiter "Sicherheit" VPN-Typ: **IKEv2** wählen, den Authentifizierung Radioknopf auf '*Extensible-Authentication-Protokoll (EAP) verwenden*' stellen und "**Microsoft: Gesichertes Kennwort (EAP-MSCHAP v2)**" auswählen.



# VPN verbinden





**ACHTUNG:** Bei Körperschaften die über einen AD-Trust verbunden sind, die Domain voranstellen:  
Z.B.: **BZGEIS.IT\anne\_bzgeis** oder **bzgeis\anne\_bzgeis**

**Jetzt zu Punkt 3** Remotezugriff auf Pc der Körperschaft

## Vpn auf MAC

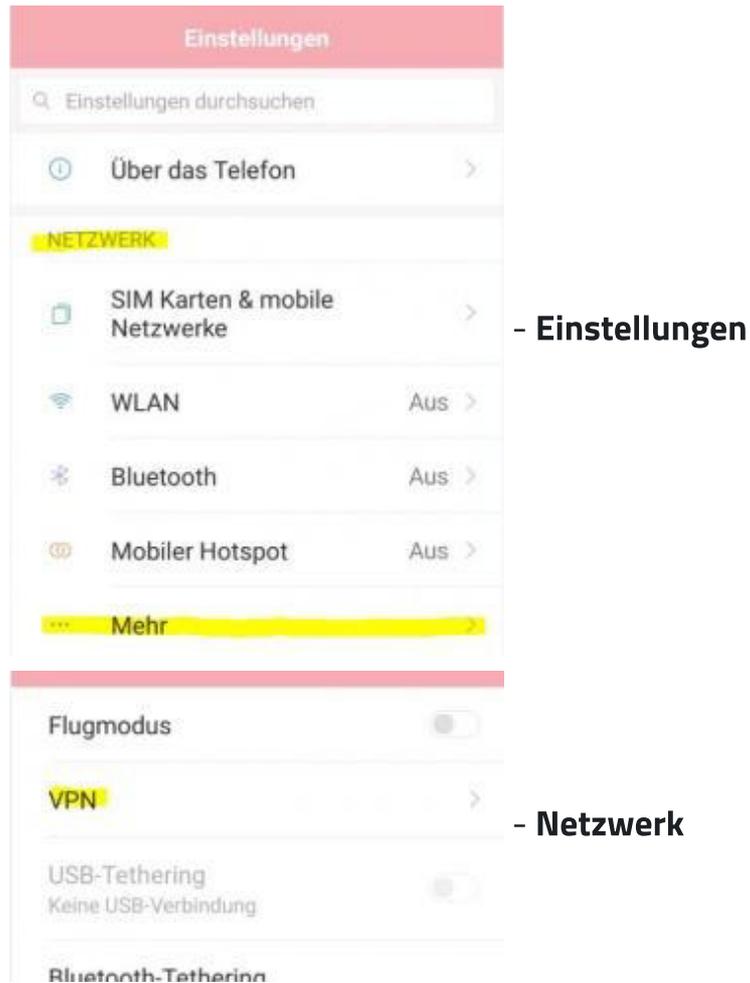
freundlicherweise von Rene Schmid zur Verfügung gestellt  
Installation\_IPSec\_VPN\_auf\_MacOS.pdf (800 KB)

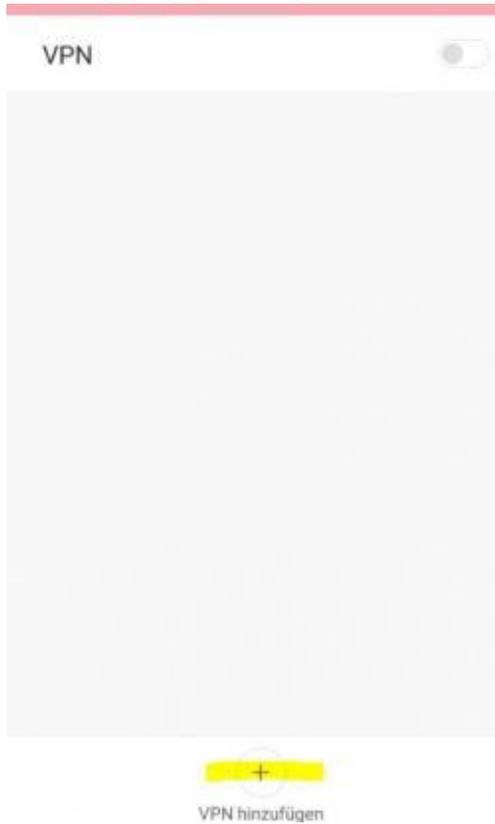
Anleitung2.pdf

**Jetzt zu Punkt 3** Remotezugriff auf Pc der Körperschaft : Unterschied! Auf MAC-OS muss der "Microsoft Remote Desktop" konfiguriert bzw. installiert werden!

Anleitung.pdf

## Android





- VPN - VPN hinzufügen

Name	Gvcc
TYP	
IPSec Xauth PSK	>
Serveradresse	vpn.gvcc.net
IPSec-ID	(nicht verwendet)
Vorinstallierter IPSec-Schlüssel	*****
<input type="radio"/> Erweiterte Optionen einblenden	
Nutzername	gerti_gemeinde
Passwort	*****

Name: **frei wählbar**

Typ: **IPSec Xauth PSK**

Serveradresse: **vpn.gvcc.net**

Vorinstallierter Schlüssel oder Pre-shared key: **home2gvcc**

IPSec-ID: **nicht verwenden**

Benutzername: der übliche Benutzername z.B. **evi\_martell**

**ACHTUNG:** Bei Körperschaften die über einen AD-Trust verbunden sind, die Domain voranstellen:

Z.B.: **BZGEIS.IT\anne\_bzgeis** oder **bzgeis\anne\_bzgeis**

# MFA: Erhöhte Sicherheit mit 2-Faktor-Authentifizierung

Um die Sicherheit gegenüber Hackerangriffen zu erhöhen, verlangt diese Methode beim Aufbau der VPN-Verbindung nach der Eingabe des Ldap-Passwortes zusätzlich eine Bestätigung über die App **privacyIDEA Authenticator**.

- Authentifizierungsfaktor 1: Username/Password (ldap/ADS)
- Authentifizierungsfaktor 2: Bestätigung per **privacyIDEA Authenticator** App am Smartphone.

Ablauf: Nach der Eingabe des Ldap-Passwortes erscheint in der APP eine Pushbenachrichtung, in welcher das Verbinden über VPN akzeptiert werden kann. Wird diese nicht bestätigt, kann der VPN-Kanal nicht aufgebaut werden.

**ACHTUNG!:** Diese 2-Faktor-Authentifizierung ist noch nicht aktiv. Die Aktivierung wird mittels Rundschreiben angekündigt werden und es wird für die Vorbereitung genügend Zeit eingeräumt.

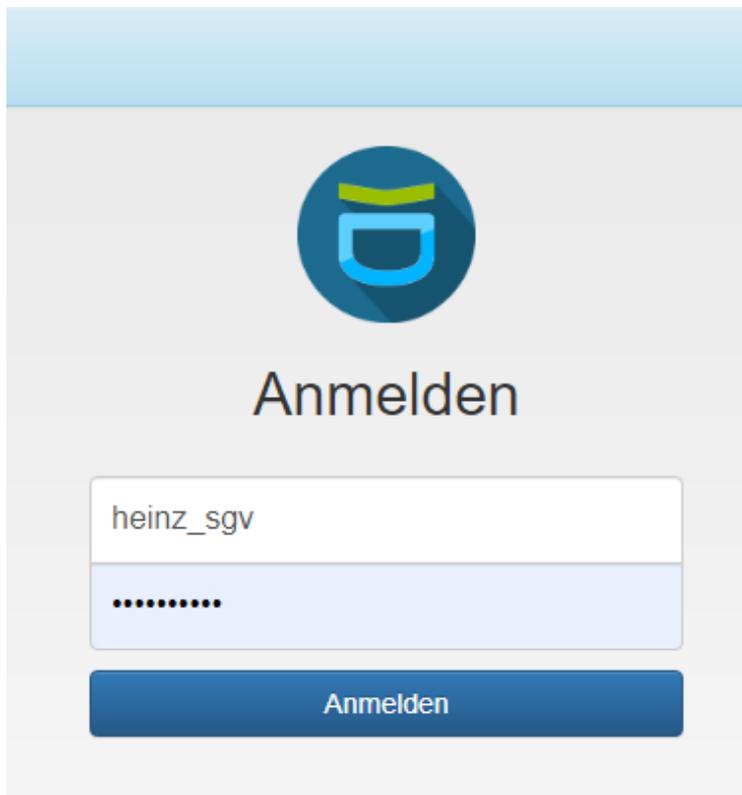
## Vorbereitung

### Anmeldung im mfa-Portal

in <https://mfa.gvcc.net/> (<https://mfa.gvcc.net/>) einsteigen, Anmeldung erfolgt mit z.B heinz\_sgv.

Mit Benutzer und Ldap-Passwort anmelden.

Aus Sicherheitsgründen funktioniert das nur von der Gemeinde / BZG aus oder über einen bereits geöffneten VPN-Kanal. Das Portal ist nicht vom Internet aus erreichbar.



## privacyIDEA Authenticator installieren

- Links oben im Menu auf **Token ausrollen** klicken.
- Es erscheinen 2 QR für die Installation der **privacyIDEA Authenticator-App**, einer für Android, der andere Für iOS. Scannt man mit dem Smartphone den entsprechenden QR für Android oder iOS, gelangt man direkt zum entsprechenden App-Store, und zur App **privacyIDEA Authenticator-App**, die man hiermit installieren kann.

**ACHTUNG!:** Nach der Installation der APP, muss mit genau dieser App noch der QR des Token gescannt und damit importiert werden.

Alle Token

Token ausrollen

## Neuen Token ausrollen

PUSH: Sendet eine Push Nachricht an ein Smartphone.

Mit dem PUSH Token sendet privacyIDEA eine Benachrichtigung an das registrierte Smartphone. Auf dem Smartphone kann der Benutzer die Anmeldung bestätigen oder verwerfen.

Für den Initialisierungsprozess und auch während der Anmeldung benötigt Ihr Smartphone eine Netzwerkverbindung, um privacyIDEA zu erreichen.



Laden Sie die Authenticator App für Android.

Laden Sie die Authenticator App für iOS.

Token ausrollen

# Token ausrollen und in App importieren

Nach erfolgreicher Installation der APP unten auf den Button **Token ausrollen** klicken. Dies erzeugt einen neuen QR (das ist der **QR des Token**), der mit der **privacyIDEA App** gescannt werden muss. Dies importiert den soeben generierten Token in die App.

## Neuen Token ausrollen

Der Token mit der Seriennummer **TOTP00156DD4** wurde erfolgreich ausgerollt.



**ACHTUNG!:** Der QR muss sofort nach dem generieren mit der App gescannt werden, er wird nur 1 mal angezeigt.

# Authentifizierung beim Verbinden mittels 2-Faktor-Authentifizierung

Wird ein Vpnkanal aufgebaut, so muss man sich zuerst mittels ldap-username und ldap-passwort authentifizieren. Danach muss man die **privacyIDEA App** am Handy öffnen. Hier wird man aufgefordert die VPN-Verbindung zu akzeptieren oder abzulehnen.

**ACHTUNG!:** Sollte diese Aufforderung nicht innerhalb von ein paar Sekunden erscheinen, muss ein **refresh** (im Display nach unten wischen) gemacht werden.

Nachdem auf **akzeptieren** getippt wurde, wird der VPN-Kanal innerhalb der nächsten Sekunden aufgebaut und der **Remotezugriff** kann verwendet werden.

# Remotezugriff auf Pc der Körperschaft

## Konfiguration des Pc der Körperschaft

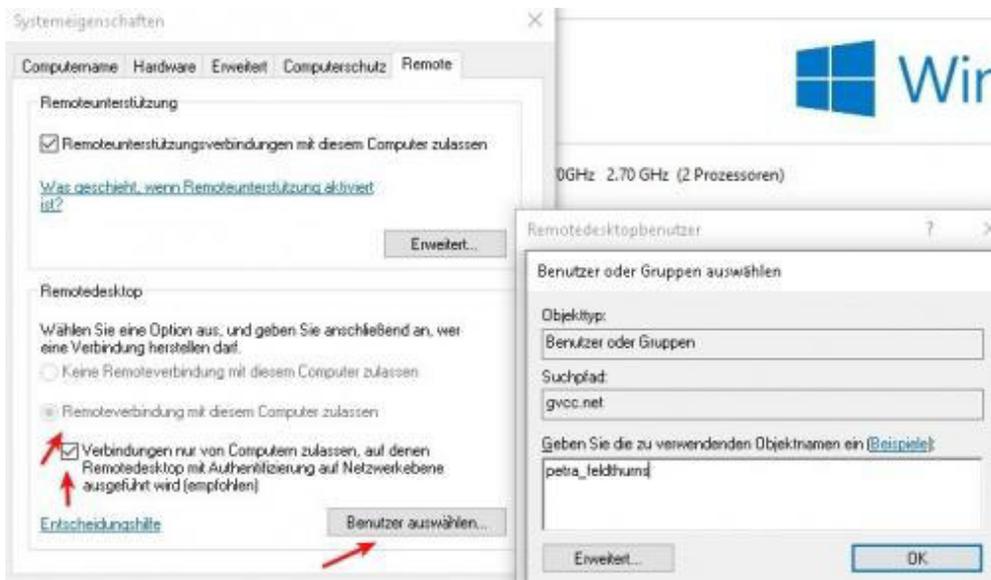
Damit kann per Remotedesktop über Vpn oder Openvpn auf den Pc in der Körperschaft zugegriffen werden.

Dazu muss Remotedesktop auf dem Pc im Betrieb freigegeben werden:

Die Windows-Taste + R drücken und in dem Ausführendialog: "sysdm.cpl" eingeben



Auf Remoteeinstellungen wechseln:



"Remoteverbindung mit diesem Computer zulassen" muss aktiviert sein, sonst aktivieren (wenn ausgegraut, aber aktiv ist das in Ordnung)

Die Option "Authentifizierung auf Netzwerkebene" ist empfehlenswert, aber falls die Verbindung von zu Hause nicht klappt, dann bitte deaktivieren.

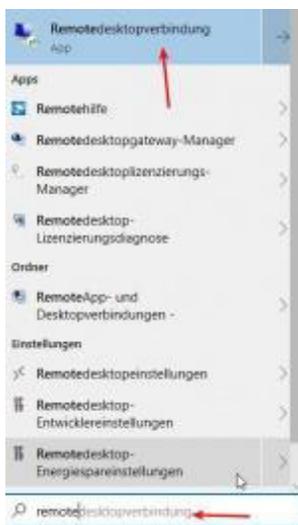
Dann "Benutzer auswählen" klicken, "hinzufügen" und den entsprechenden Benutzer hinzufügen und die Dialoge abschließen

Damit von zu Hause aus zugegriffen werden kann, benötigt es die Ipadresse des Rechners (über Teamviewer wird sie kurzfristig angezeigt oder über Fernwartung Vnc starten)

## Konfiguration Pc zu Hause

Jetzt kann vom Pc/Laptop zu Hause zugegriffen werden, wenn das Gerät bereits mit Vpn oder Openvpn verbunden ist.

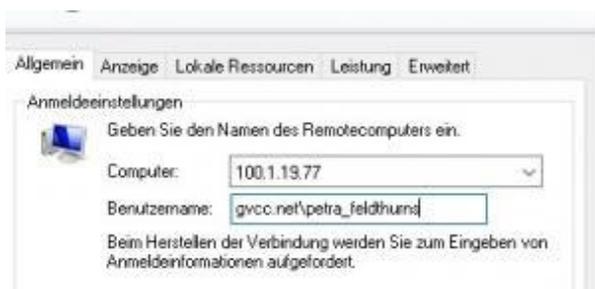
Dazu im Startmenü schreiben: remotedesktop und dann die Remotedesktopverbindung öffnen



Dann die Ipadresse des Computers in der Körperschaft eingeben (im Feld Computer)  
Auf "Optionen einblenden" klicken und als Benutzername in der Regel: gvcc.net\<>benutzer>  
eingeben, bei älteren Rechnern in der Körperschaft könnte es auch <corp>\<benutzer> sein, z.B:  
feldthurns\petra\_feldthurns

Viele Windows 8 Rechner sind noch "kerberoisiert", dann lautet die richtige Syntax:  
<benutzer>@GVCC.NET (GVCC.NET großgeschrieben)

mögliche Probleme: Manche Betriebsrechner sind im öffentlichen Netz, dann blockiert die Firewall die Remoteverbindung. In diesem Fall sollte die Firewall auf dem Betriebsrechner deaktiviert werden.



**Warnung:** Wenn zu Hause ein Gerät der Gemeinde/Körperschaft verwendet wird, und es sind dort die Körperschaftsdrucker konfiguriert, dann funktioniert die Verbindung nicht oder erst nach langer Wartezeit.

Abhilfe schafft hier das Deaktivieren der Druckerumleitung: Bei Remotedesktopverbindung "Optionen einblenden" anklicken, auf Reiter "lokale Ressourcen" wechseln und dort "Drucker" deaktivieren.

**Digitale Unterschrift über Homeworking:** Der Stick muss zu Hause angeschlossen werden (am ArbeitsPc funktioniert es nicht!) und es muss die Software des Sticks ("Autorun.exe" als Administrator starten, dann Utilità , Import Certificato) auf dem Pc zu Hause installiert werden. (installiert die Software Bit4Id)

Siehe dazu Doku auf /mw/index.php/Digitale\_Unterschrift - Bereich: Download - Digitale Unterschrift - Punkt 1 Installation des USB-Sticks mit Digitaler Unterschrift...