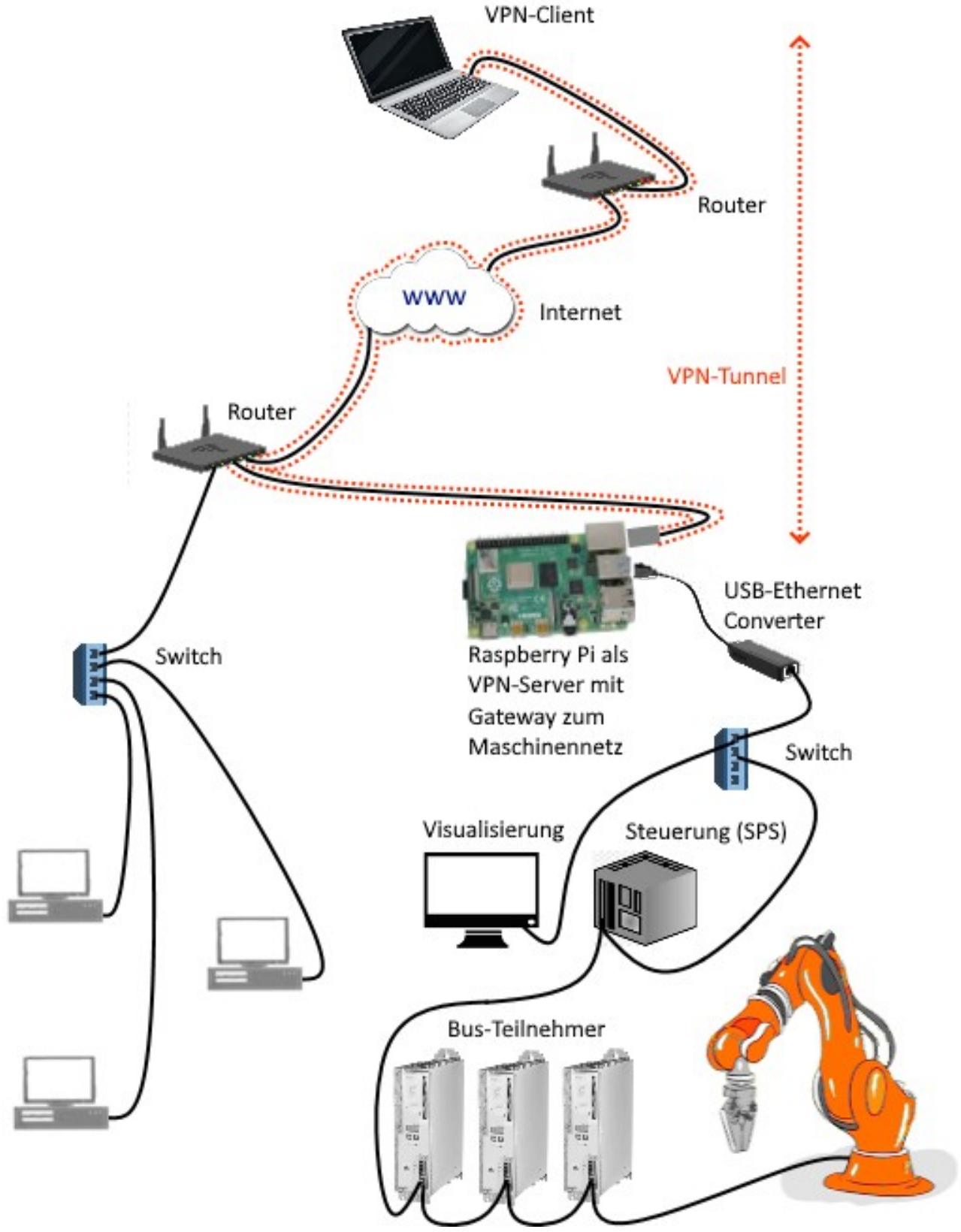
VPN-Tunnel zur Maschine

Wie mit einem VPN-Tunnel eine abgesicherte Verbindung über das Internet zu Ihrem Produktionsnetzwerk (oder ähnlichem) hergestellt werden kann.



Sichere Fernverbindungen über das Internet sind in Zeiten der Pandemie so wichtig wie nie zuvor. Ein bewährtes Verfahren ist dabei die Absicherung der kritischen Verbindungswege durch einen verschlüsselten Datenverkehr mit Hilfe eines VPN-Tunnels.

Im Gegensatz zu vielen anderen Lösungen läuft hier die Verbindung direkt zwischen Client und Server, d.h. es gibt keine zwischengeschaltete Cloud bzw. weitere Server der Anbieter ähnlicher Lösungen, an welchen Daten abgegriffen werden können.

Dazu wurde die quelloffene Software „OpenVPN“ zur Erstellung eine Virtuellen Privaten Netzwerkes über eine abgesicherte TLS-Verbindung (TLS = Transport Layer Security) zwischen VPN-Client und VPN-Server, gewählt.

Gründe, weshalb die Wahl auf OpenVPN fiel, sind:
- Verfügbar auf nahezu allen gängigen Betriebssystemen wie Windows, Linux, IOS, Android …
- Einfache Handhabung
- Freie Software
- Gute Verschlüsselung
- Authentisierung der Clients
- Verfügbar in den Paketlisten von Raspberry OS, einem Betriebssystem für Raspberry Pi Minicomputer

Als Hardware findet der Minicomputer Raspberry Pi Verwendung, weil er:
- im Preis-Leistungsverhältnis gut aufgestellt ist
- auf Grund seiner hohen weltweiten Verbreitung sicher beschafft werden kann
- mit dem freien Betriebssystem Raspberry OS betrieben werden kann
- mit seinem minimalen Energieverbrauch weder die Umgebung heizt, noch als Stromverbraucher in Industrieanlagen eine Rolle spielt.

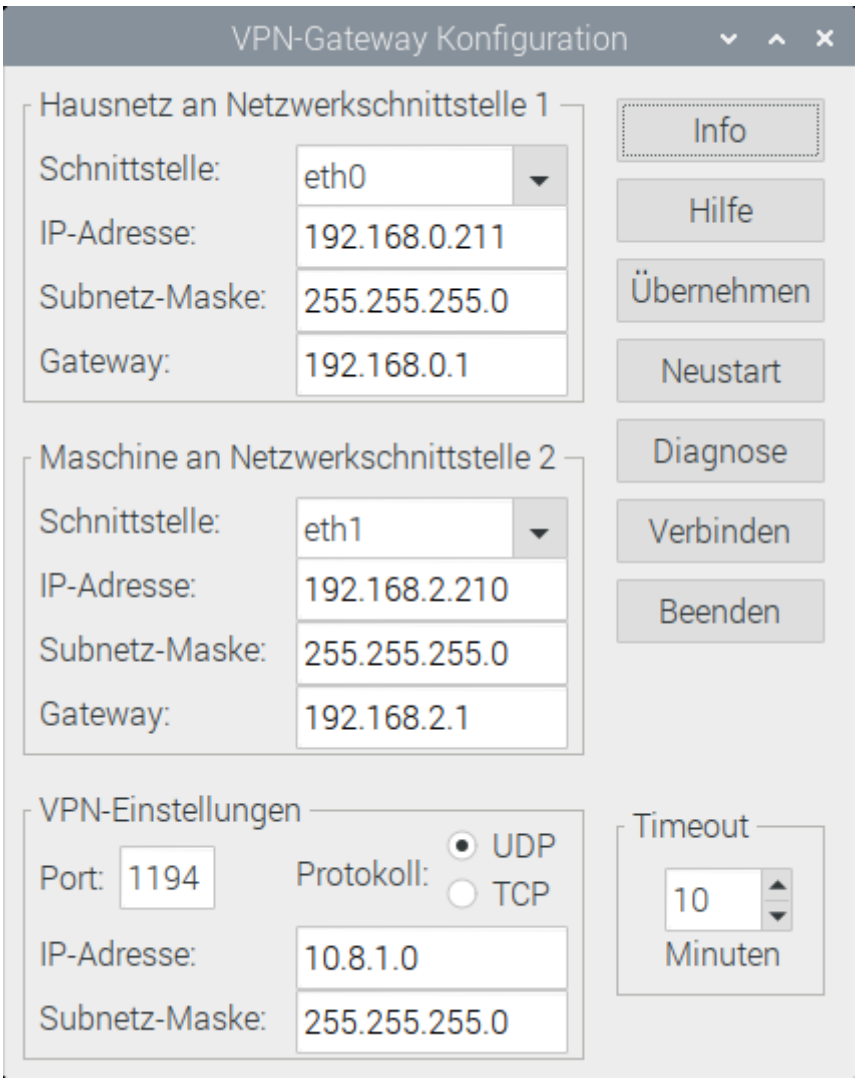
Trotzdem ist es möglich, auf Minicomputer anderer Hersteller auszuweichen.

Zusätzlich zur Funktion als VPN-Server ist noch eine Gateway-Funktion implementiert, welche die Daten aus dem in der Regel an das Hausnetz angeschlossenen Internet-Router in und aus dem Fertigungsnetzwerk weiterleitet.

Bei vielen Anbietern muss zusätzlich zur erforderlichen Hardware einen Zugang gemietet werden. Ist bereits ein PC an der Anlage vorhanden, kann auch auf reine Softwarelösungen (z.B.: TeamViewer) zurückgegriffen werden. Bei legaler Nutzung im kommerziellen Umfeld fallen dann ebenfalls weitere Kosten an.

Diese Zusatzkosten entstehen bei der hier vorgestellten Lösung nicht. Vorausgesetzt, dass eine Internet-Flatrate besteht, kann das VPN-Gateway 24/7 (24 Stunden am Tag, an allen 7 Wochentagen) betrieben werden.

Das Programm wird automatisch gestartet. Die Konfigurationsdaten sind als Textdateien auf einem USB-Stick abgelegt und können über eine einfach zu bedienende Benutzeroberfläche konfiguriert werden:



Sollen beide Netzwerkschnittstellen über Kabel mit den bekannten RJ45-Steckern angeschlossen werden, wird ein USB-Ethernet-Adapter verwendet.

Die Kontrolle über die Verbindung soll dem Anlagenbetreiber vorbehalten sein. Um nicht den Stecker ziehen zu müssen, um die Verbindung zu unterbrechen, ist die „Timout“-Funktion vorgesehen. Wird eine „0“ eingetragen, besteht die Verbindung dauerhaft. Sonst wird je nach Eingabe, X Minuten nachdem die externe Verbindung abgebaut wurde, der VPN-Server gestoppt. Über einen externen Taster kann diese bei Bedarf wieder gestartet werden. Eine Statusanzeige ist mittels einer Leuchtdiode realisiert.

- Leuchtdiode aus: Es besteht keine VPN-Verbindung
- Leuchtdiode blinkt langsam: VPN-Server ist bereit und wartet auf Verbindung
- Leuchtdiode blinkt schnell: Die externe Verbindung ist aktiviert

Von Extern kann nur zugegriffen werden, wenn der externe Benutzer ebenfalls über eine Konfigurationsdatei verfügt, in welcher die Kommunikationsparameter und die Zugangszertifikate für die verschlüsselte Verbindung enthalten sind. Zusätzlich muss er den Zugriff mit einem Passwort legitimieren.

Zusätzlich ist ein VNC-Server installiert. Innerhalb des Hausnetzwerks kann also mittels einer VNC-Client-Software eine Remote-Verbindung zum VPN-Gateway aufgebaut werden. Um also die externe Verbindung freizugeben oder zu unterbrechen, muss niemand mehr zur Anlage gehen, sondern kann diese über VNC fernsteuern. Für eventuelle Änderung der Konfiguration kann so auch auf den Anschluss von Monitor, Maus und Tastatur verzichtet werden.

Die Verwendung von VPN-Tunneln wird vom BSI (Bundesamt für Sicherheit in der Informationstechnik) empfohlenen. Bei sorgfältigem Umgang mit den Zertifikats- und Schlüsseldateien ist diese Art der Verbindung extrem sicher. Um das Einschleusen von Trojanern oder Viren zu verhindern, wird die Speicherkarte mit dem Betriebssystem und den Programmen schreibgeschützt. Während des Betriebs veränderte Dateien werden in einer RAM-Disk (flüchtiger Speicher) gehalten, die nach einem Neustart gelöscht ist. So wird auch erreicht, dass das Gerät ohne das übliche Herunterfahren einfach abgeschaltet werden kann. Alle Konfigurationsdateien sind auf einem USB-Stick gespeichert.

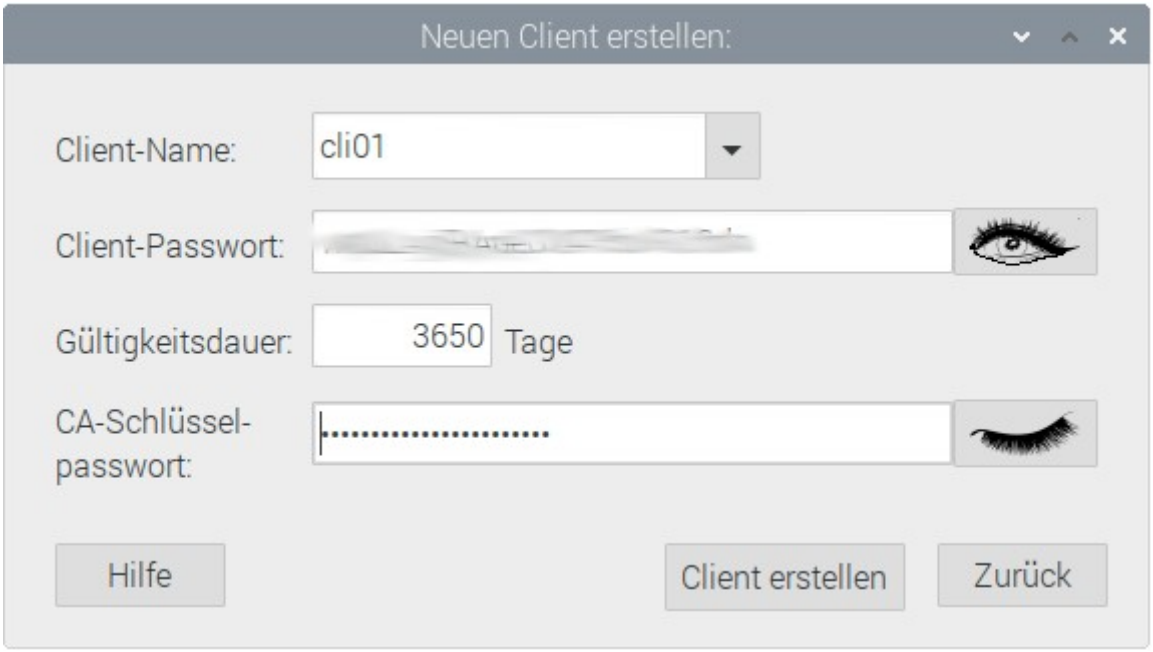
Clients verwalten

Um eine Verbindung mit dem VPN-Server herstellen zu können, müssen Clients angelegt werden (1). Diese sind in den Sicherheits- und Zertifikatsdateien des Servers gelistet. Nur gelistete Clients können sich verbinden. Dazu braucht ein Client eine Zugangsdatei („*.ovpn“-Datei) mit dem zugehörigen Passwort (3).

Weiterhin kann einem bereits gelisteten Client die Zugangsberechtigung durch dessen Annullierung wieder entzogen werden (2).

Für diese Aufgaben ist das Programm „vpnclient“ installiert:

1. Neuen Client erstellen



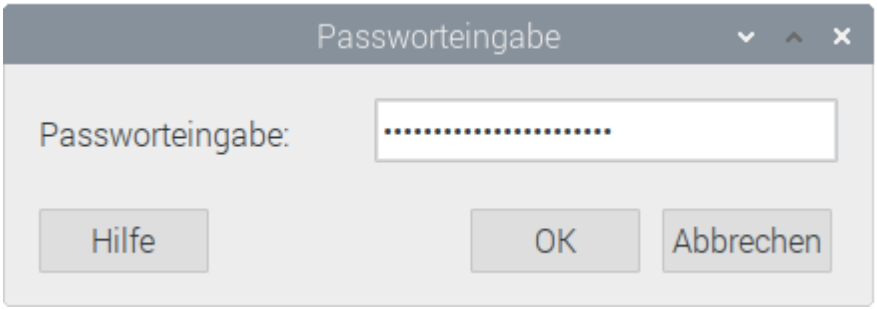
Zur Erstellung eines Clients sind folgende Schritte auszuführen:
- ein neuer Client-Name ist zu vergeben und einzutragen
- das Passwort für diesen Client ist festzulegen
- die Gültigkeitsdauer des Client-Zugangs ist anzugeben (max. 3650 Tage)
- das (Certificate Authority) CA-Schlüsselpasswort ist anzugeben (wird mit dem VPN-Server mitgeliefert)
- die Schaltfläche „Client erstellen“ ist zu betätigen.

Passworteingaben können sowohl sichtbar:

als auch verdeckt:

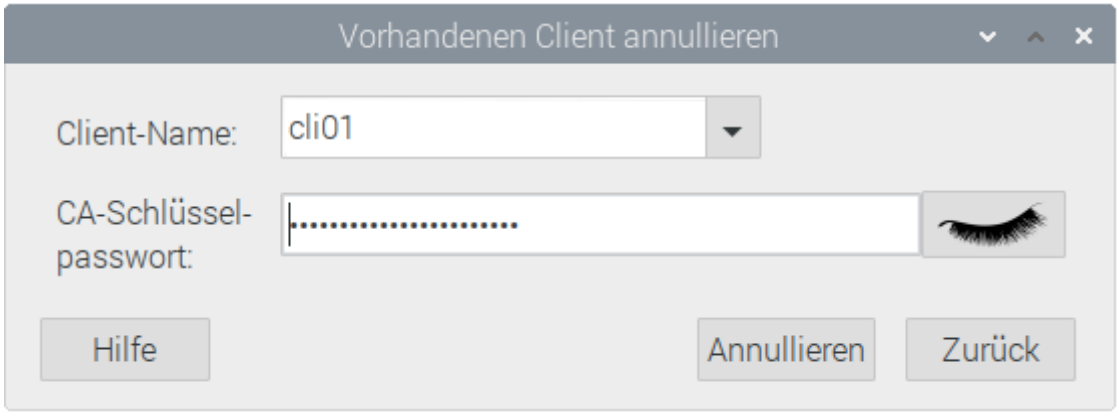
vorgenommen werden.

Bei verdeckter Eingabei öffnet sich der Passwort-Eingabe-Dialog:



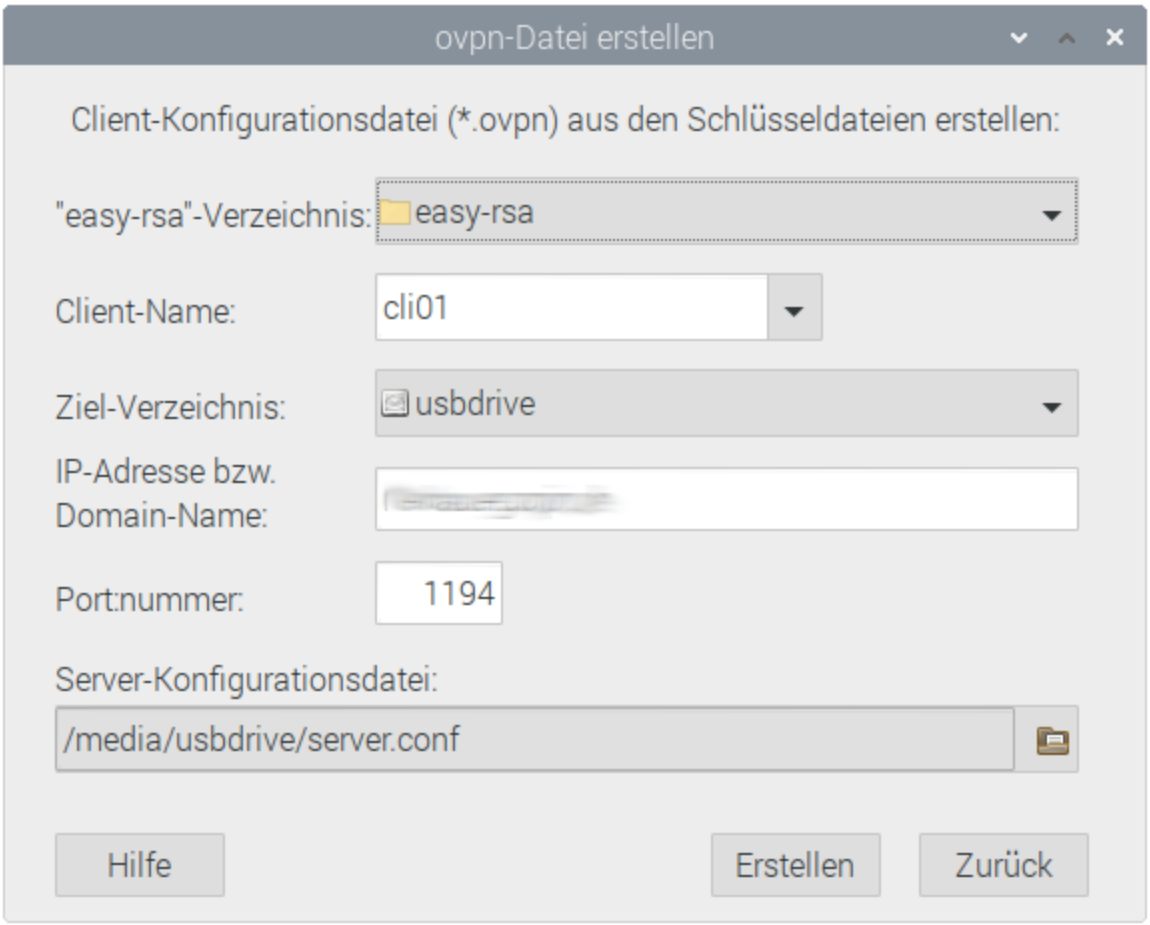
Die Eingabe muss dann zweimal erfolgen. Bei fehlerfreier Eingabe wird das Passwort übernommen.

2. Vorhandenen Client annullieren



Um eine vorhandene Client zu annullieren:
- ist der Client-Name aus der Klappliste (Combo Box) auszuwählen
- das (Certificate Authority) CA-Schlüsselpasswort ist anzugeben (wird mit dem VPN-Server mitgeliefert)
- die Schaltfläche „Annullieren“ ist zu betätigen.

3. „*.ovpn“-Datei erstellen



Aus den zu einem vorhandenen Client angelegten Zertifikats- und Schlüsseldateien kann dann die Zugangsdatei („*.ovpn“-Datei) erstellt werden.

Die Zertifikats- und Schlüsseldateien sind im „easy-rsa“-Verzeichnis und dessen Unterverzeichnissen abgelegt.

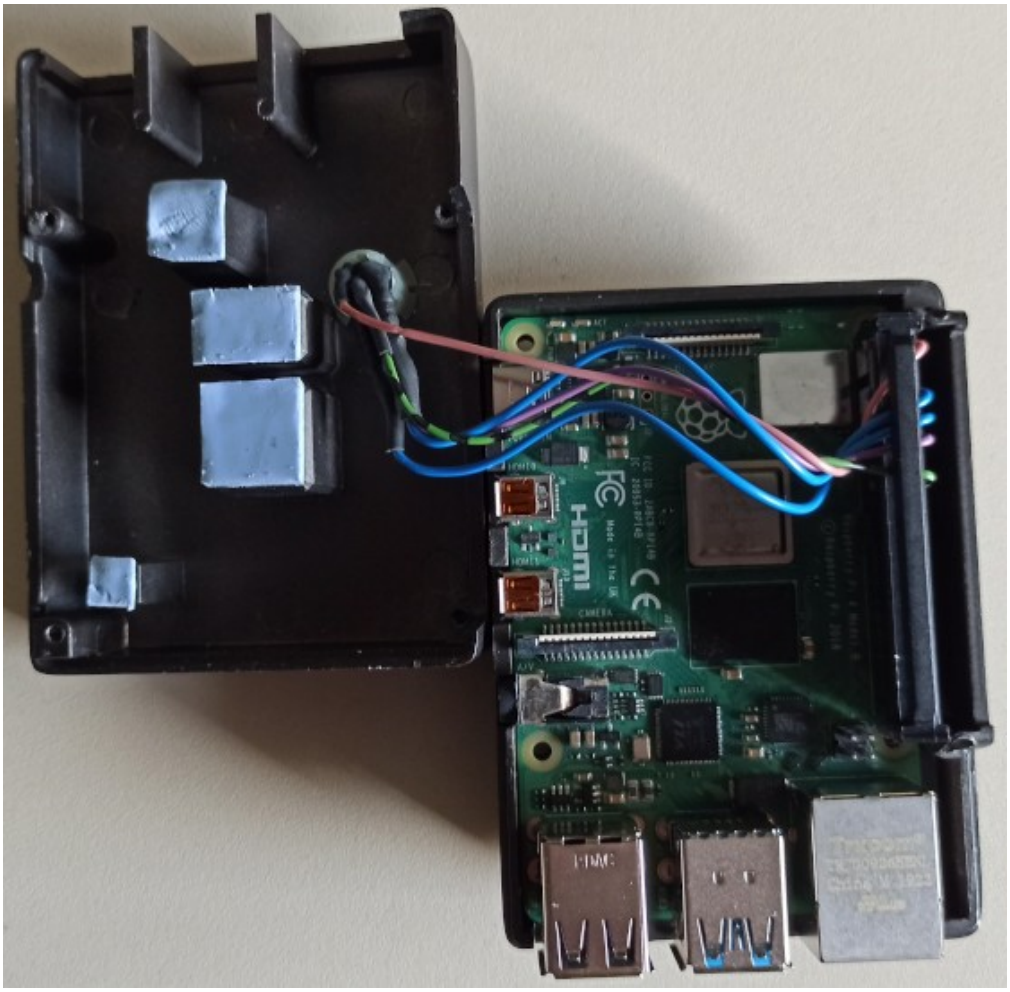
Die Zugangsdatei kann dann auf einem beliebigen Datenträger (z.B.: USB-Stick, USB-Festplatte, Netzwerklaufwerk …) erstellt werden.

Standardmäßig wird bei OpenVPN die Port-Nummer 1194 verwendet. Es kann aber auch jeder andere freie Port genutzt werden.

Das Client-Passwort und die Zugangsdatei sollten auf getrennten sicheren Wegen an den am entfernten Ort ansässigen Anwender versendet werden (z.B.: Zugangsdatei über eine SSH-Verbindung (SSH = Secure Shell oder Secure Socket Shell), Passwort per SMS).

Hardware

Das Gerät ist in ein Aluminium-Gehäuse eingebaut, das mittels eingegossener Blöcke und Wärmeleit-Pads die CPU sowie weitere Chips kühlt, d.h. es wird kein Lüfter benötigt. An der Rückseite des Gerätes ist eine Tragschienenadapter angebracht, so dass eine Montage im Schaltschrank mit einem Handgriff erledigt werden kann.




Verbatim
USB 3.0