

VPN-Dienst der HamCloud

Am Dreiländersysopotreffen vom 11. Februar 2023 in Engen wurde von IP-Koordinator DL, Jann Traschewski DG8NGN der neue HamCloud VPN-Dienst vorgestellt. Eine Installationsanleitung findet sich unter vpn.hc.r1.ampr.org

Der HamCloud VPN-Dienst ermöglicht Funkamateuren die Teilnahme am HAMNET über das Internet. Es gibt zwei Möglichkeiten den VPN-Dienst zu nutzen:

- a) Für Mitglieder des DARC
- b) Für Nutzer des ARRL Logbook of the World-Programms

Für den Funkamateure sind folgende Schritte dafür notwendig:

1. Authentifizierung als Funkamateure gegenüber dieser Webseite:
 - o [Als Mitglied des Amateurfunk Verbands DARC e.V. über Single-Sign-On](#)
oder
 - o [Als Teilnehmer am „ARRL Logbook of the World“-Programm mittels Browserzertifikat](#)
2. [Bezug der VPN-Einwahldaten von dieser Webseite](#)
3. [Einrichten der VPN-Verbindung](#)

Authentifizierung wie unter 1. beschrieben:

[Authentifizierung über Single-Sign-On \(DARC\)](#)

[Authentifizierung über Browserzertifikat \(ARRL Logbook of the World\)](#)

Version: März 2023

Folgende Anleitung basiert auf der aktuelle WEB-Version für:

Microsoft Windows 10 und 11 sowie dem
Browserzertifikat «ARRL Logbook oft the World»

d. h. für alle OM's in HB9 und HB0, die nicht Mitglied des DARC's sind.

b: Für Nutzer des ARRL Logbook of the World-Programms

HamCloud VPN Hilfe – LoTW-Zertifikat

Als Teilnehmer des „ARRL Logbook of the World“-Programms muss das eigene LoTW-Zertifikat in das Betriebssystem importiert werden, bevor es zur Authentifizierung gegenüber dieser Webseite verwendet werden kann.

Logbook of the World: Getting Started with LoTW

<http://www.arrl.org/quick-start>

Bevor Sie QSOs an Logbook of the World (LoTW) senden können, müssen Sie die kostenlose Anwendung TQSL auf Ihrem Computer installieren. Mit TQSL können Sie ein Rufzeichen-Zertifikat erhalten, das Sie als Quelle der von Ihnen eingereichten QSOs ausweist. Außerdem können Sie einen Stationsstandort definieren, der die geografischen Details Ihres Betriebsstandorts angibt. Ein Flussdiagramm, das diese Schritte veranschaulicht, finden Sie hier.

Die von Ihnen übermittelten QSOs werden bestätigt, wenn Ihre QSO-Partner passende QSOs übermitteln. Bevor Sie diese Bestätigungen für DXCC-, VUCC-, WAS-, WAZ- oder WPX-Auszeichnungen einreichen können, müssen Sie die Verknüpfung zwischen LoTW und den von Ihnen angestrebten Auszeichnungsfamilien einrichten.

Erste Schritte bei der Einreichung von QSOs

Hinweis: Wenn Ihr primäres Rufzeichen in den Vereinigten Staaten ausgestellt wurde, die bei der Federal Communications Commission (FCC) registrierte Postadresse jedoch nicht aktuell ist, aktualisieren Sie diese über die FCC ULS-Website, bevor Sie fortfahren.

Beginnen Sie mit dem Herunterladen und Installieren von TQSL und fordern Sie damit ein Rufzeichen-Zertifikat für Ihr aktuelles Rufzeichen an.

1. [Herunterladen und Installieren von TQSL](#)
2. [Beantragen Sie Ihr erstes Rufzeichenzertifikat und Ihr LoTW-Kontopasswort](#)

Der nächste Schritt hängt davon ab, ob Sie in den Vereinigten Staaten lizenziert sind oder nicht.

Wenn Ihr primäres Rufzeichen in den Vereinigten Staaten ausgestellt wurde, schickt die ARRL eine Postkarte an die in Ihrer FCC-Lizenz angegebene Postadresse. Auf der Postkarte ist ein 8-stelliges "Postkarten-Passwort" angegeben. Navigieren Sie mit Ihrem Webbrowser [hierher](#) und geben Sie Ihr "Postkarten-Passwort" ein. Daraufhin sendet Ihnen die ARRL eine E-Mail mit Ihrem LoTW-Kontopasswort und Ihrem Rufzeichen-Zertifikat.

Wenn Ihr primäres Rufzeichen nicht in den Vereinigten Staaten ausgestellt wurde, haben Sie drei Möglichkeiten:

1. Senden Sie eine Kopie Ihrer Amateurfunk-Betriebsgenehmigung und eine Kopie eines anderen staatlich ausgestellten Dokuments, aus dem Ihr Name und Ihre Adresse hervorgehen (z. B. ein Führerschein oder eine Stromrechnung), per E-Mail an die ARRL unter: LoTW-help@arrl.org Sie können alle sensiblen Informationen auf dem von der Regierung ausgestellten Dokument schwärzen, wie z.B. eine Lizenznummer oder eine

Kontonummer. Wenn die ARRL Ihre Unterlagen erhält, wird sie Ihnen eine E-Mail mit Ihrem LoTW-Kontopasswort und Ihrem Rufzeichen-Zertifikat schicken.

2. Legen Sie Ihre Dokumente persönlich bei einem ARRL-DXCC-Kartenprüfer im Land vor. Der Kartenprüfer prüft Ihre Dokumente und informiert, wenn er sie akzeptiert, die LoTW-Mitarbeiter der ARRL, dass die Identität und die Lizenz des Antragstellers überprüft wurden. Die ARRL schickt Ihnen dann eine E-Mail mit Ihrem LoTW-Kontopasswort und Ihrem Rufzeichen-Zertifikat im Anhang. Schicken Sie Ihre Dokumente nicht per E-Mail an den Card Checker.

Nicht jede DXCC-Einheit hat DXCC-Card-Checker, und Card-Checker sind nicht verpflichtet, an diesem Verifizierungsprozess teilzunehmen. Daher sollten Sie sich im Voraus mit einem Card Checker in Ihrem Land in Verbindung setzen und fragen, ob er bereit ist, Ihre Identität und Lizenzdokumente zu überprüfen. Eine Liste der DXCC Card Checkers finden Sie hier.

3. Schicken Sie eine Kopie Ihrer Amateurfunk-Betriebsgenehmigung und eine Kopie eines anderen von der Regierung ausgestellten Dokuments, aus dem Ihr Name und Ihre Adresse hervorgehen (z.B. ein Führerschein oder eine Stromrechnung) an die ARRL. Sie können alle sensiblen Informationen auf dem von der Regierung ausgestellten Dokument schwärzen, wie z. B. eine Lizenznummer oder eine Kontonummer. Wenn die ARRL Ihre Unterlagen erhält, schickt sie Ihnen eine E-Mail mit Ihrem LoTW-Kontopasswort und Ihrem Rufzeichen-Zertifikat im Anhang.

Weisen Sie TQSL an, das Rufzeichen-Zertifikat zu akzeptieren, das Sie von der ARRL erhalten haben:

4. [Akzeptieren Sie Ihr erstes Rufzeichen-Zertifikat](#)

Geben Sie als nächstes einen Stationsstandort an, der den Ort beschreibt, von dem aus Sie unter Ihrem aktuellen Rufzeichen arbeiten. Wenn Sie von mehr als einem Standort aus operiert haben, beginnen Sie mit der Definition eines Stationsorts für Ihren aktuellen Standort; Sie können [später weitere Stationsorte](#) definieren.

5. [Definieren Sie Ihren ersten Stationsstandort](#)

Bevor Sie TQSL oder Ihre Logging-Anwendung verwenden, um QSOs an LoTW zu übermitteln, verwenden Sie den Benutzernamen und das Passwort aus der E-Mail, die Sie von der ARRL erhalten haben, um zu überprüfen, ob Sie sich in Ihr LoTW-Konto einloggen können. Merken Sie sich diesen Benutzernamen und dieses Passwort, da Sie mit Ihrem LoTW-Konto bestätigen können, dass die von Ihnen an LoTW gesendeten QSOs akzeptiert wurden, feststellen können, welche Ihrer gesendeten QSOs über LoTW bestätigt wurden, und Bestätigungen für Award Credit einreichen können.

6. [Melden Sie sich bei Ihrem LoTW-Konto an](#)

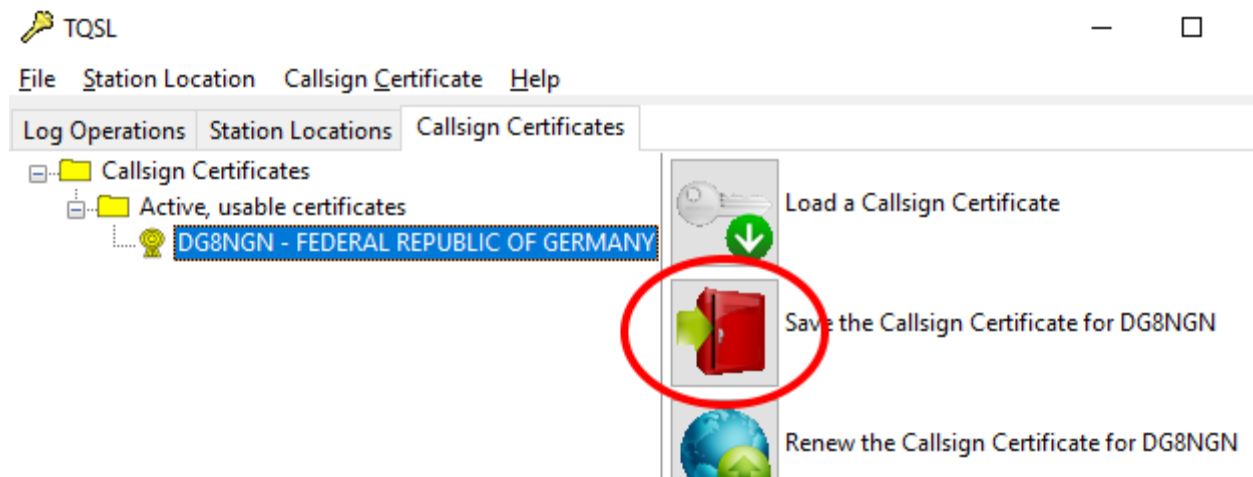
[Jetzt können Sie QSOs an LoTW senden!](#)

Wenn Sie QSOs mit anderen Stationsrufzeichen oder von anderen Standorten aus gemacht haben, können Sie nach Annahme eines Rufzeichen-Zertifikats für Ihr aktuelles Rufzeichen weitere Rufzeichen-Zertifikate erhalten und zusätzliche Stationsstandorte definieren.

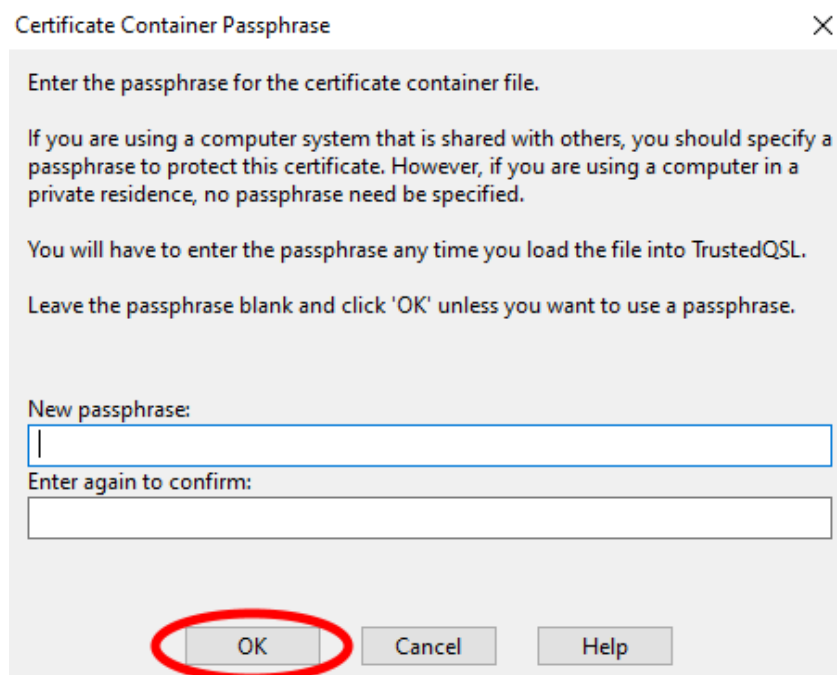
Jedes Rufzeichen-Zertifikat läuft nach 3 Jahren ab, kann aber vor Ablauf der Gültigkeitsdauer leicht erneuert werden. Sie erhalten einige Wochen vor Ablauf eines Ihrer Rufzeichen-Zertifikate eine E-Mail-Nachricht von der ARRL.

LoTW-Zertifikat in das Betriebssystem Microsoft Windows importieren

- Öffnen der Trusted QSL Applikation.
- Im Tab „Callsign Certificates“ das aktuelle Zertifikat auswählen und „Save the Callsign Certificate for CALLSIGN“ anklicken.



- Zertifikat auf dem Desktop speichern.
- Kein Passwort für der Zertifikat vergeben und OK anklicken.





- Das Zertifikat (Dein Call.p12) auf dem Desktop doppelt anklicken.

×

←  Zertifikatimport-Assistent

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Datenträger in den Zertifikatspeicher.

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Speicherort

☒ Aktueller Benutzer

☐ Lokaler Computer

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Weiter

Abbrechen

- Das Zertifikat mit „Weiter“ für den aktuellen Benutzer speichern.

Zu importierende Datei

Geben Sie die Datei an, die importiert werden soll.

Dateiname:

C:\Users\jann\Desktop\DG8NGN.p12

Durchsuchen...

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

Privater Informationsaustausch - PKCS #12 (.PFX,.P12)

Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)

Microsoft Serieller Zertifikatspeicher (.SST)

Weiter

Abbrechen

- Den Dateinamen mit „Weiter“ bestätigen.

Schutz für den privaten Schlüssel

Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:

|

☐ Kennwort anzeigen

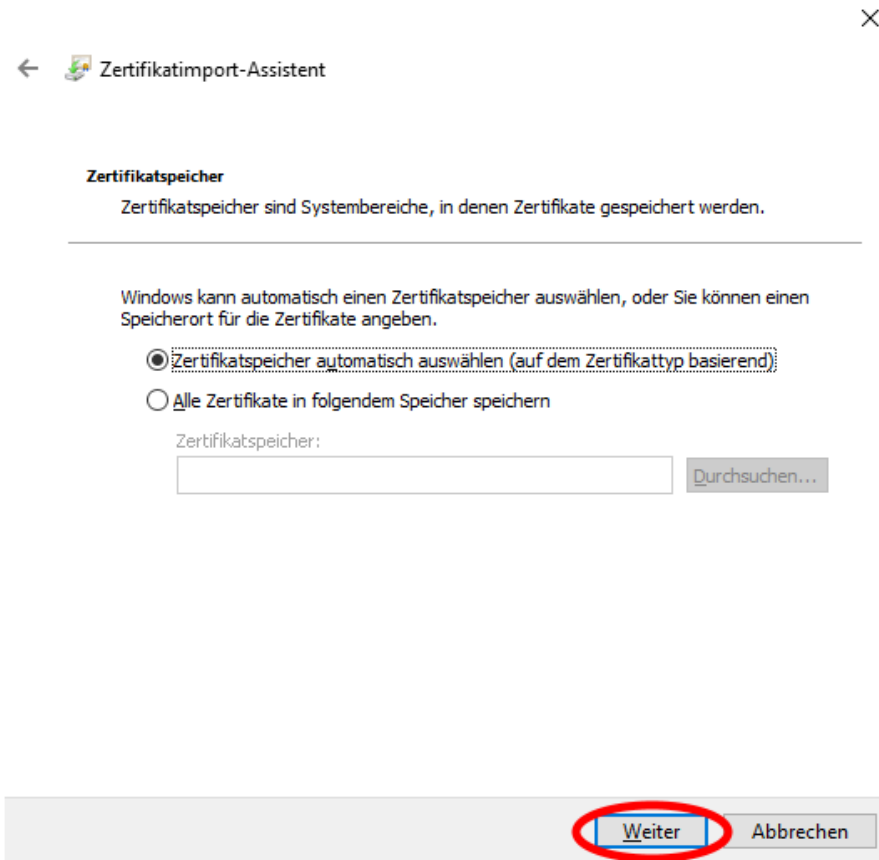
Importoptionen:

- ☐ Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
- ☐ Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
- ☐ Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
- ☒ Alle erweiterten Eigenschaften mit einbeziehen

Weiter

Abbrechen

- Das Zertifikat mit „Weiter“ importieren.



- Den Zertifikatspeicher mit „Weiter“ automatisch auswählen.

Fertigstellen des Assistenten

Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.

Sie haben folgende Einstellungen ausgewählt:

Gewählter Zertifikatspeicher	Auswahl wird vom Assistenten automatisch festgelegt
Inhalt	PFX
Dateiname	C:\Users\jann\Desktop\DG8NGN.p12

Fertig stellen

Abbrechen

- Den Prozess mit „Fertig stellen“ abschließen.

Sicherheitswarnung



Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:

Logbook of the World Root CA

Es wird nicht bestätigt, dass das Zertifikat wirklich von "Logbook of the World Root CA" stammt. Wenden Sie sich an "Logbook of the World Root CA", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:

Fingerabdruck (sha1): F6C51F0D 79638823 3B37D728
16B7CCC1 CC17DBF7

Warnung:

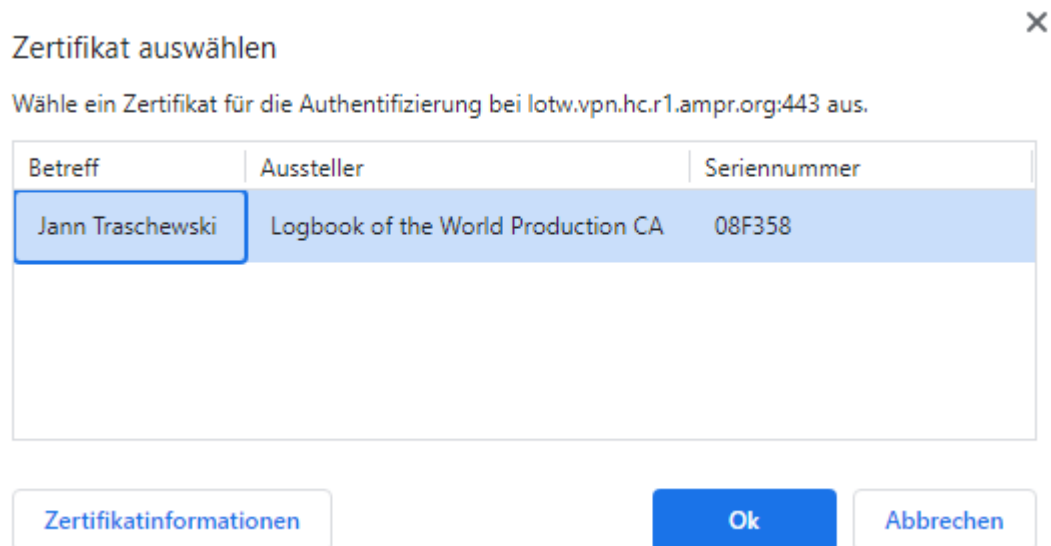
Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.

Möchten Sie dieses Zertifikat installieren?

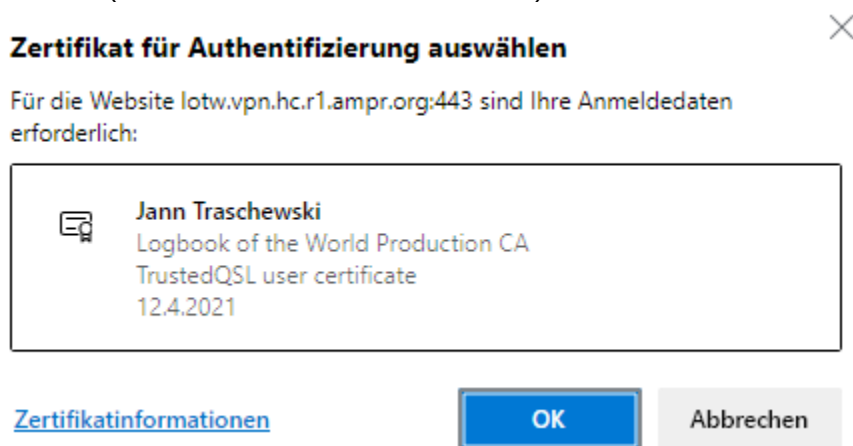
Ja

Nein

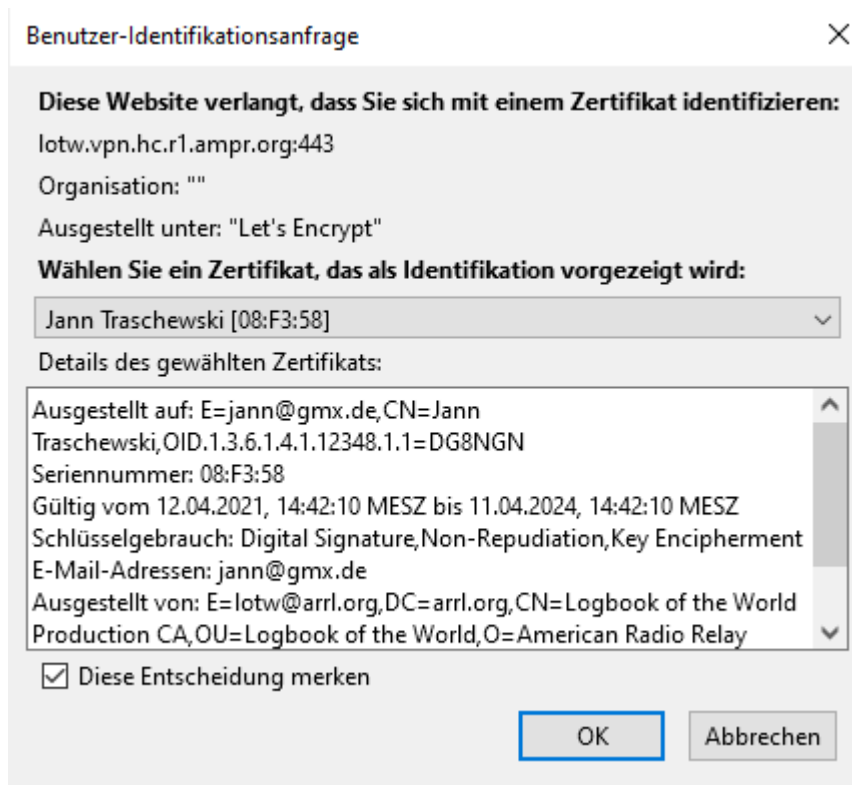
- Die Sicherheitswarnung zur Installation des Root-Zertifikats der Logbook of the World Root Zertifizierungsstelle mit „Ja“ akzeptieren.
- Das Zertifikat auf dem Desktop löschen.
- Anschließend folgt man dem Link „Anmelden über Zertifikat (ARRL Logbook of the World)“ auf der Hauptseite und wählt das Zertifikat aus. Die Abfrage schaut je nach gewählten Web Browser unterschiedlich aus:



- Chrome (Version 107.0.5304.107 64-Bit) unter Windows



- (Version 107.0.1418.42 64-Bit) unter Windows



Mozilla Firefox (Version

106.0.5 64-bit) unter Windows

HamCloud VPN Hilfe – Bezug der Einwahldaten

Je nach VPN-Technologie werden Login Daten benötigt:

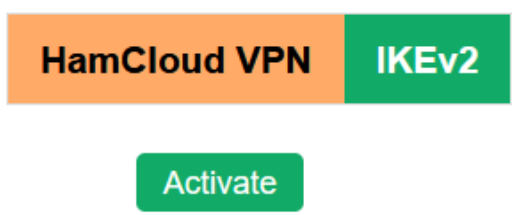
IKEv2:

Nach der Authentifizierung muss auf den IKEv2 Knopf gedrückt werden:



Hi dg8ngn

Wenn noch kein Passwort generiert worden ist oder das Passwort abgelaufen ist, dann kann durch Drücken von „Aktivieren“ ein Passwort erzeugt werden.



Es sind mehrere Verbindungen zum VPN-Server gleichzeitig möglich. Jeder Client muss einen eigenen Benutzernamen verwenden. Dazu kann man mit dem „+“-Knopf zusätzliche Benutzernamen anlegen.

HamCloud VPN	IKEv2	Wireguard	SSH Forward
user name	password	expiry date	delete
dg8ngn		2024-01-07	-
dg8ngn-1		2024-01-07	-
+			

Das Passwort ist ein Jahr gültig. Die Gültigkeit verlängert sich automatisch, sobald man sich auf der HamCloud VPN Seite einloggt und auf IKEv2 klickt.

Einrichten der VPN-Verbindung

Für jede VPN-Technologie gibt es mehrere Anleitungen:

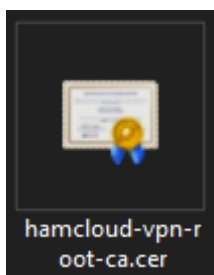
IKEv2:

Diese VPN-Methode benutzt IPsec mit dem modernen Schlüsselaustauschprotokoll IKEv2. Die Schlüssel werden über UDP Port 500 ausgetauscht. Die eigentlichen IPsec-Pakete werden über UDP Port 4500 getunnelt. Dieser Server authentifiziert sich gegenüber dem Client mit einem Zertifikat. Damit der Client das Zertifikat überprüfen kann muss auf dem Client das HamCloud VPN Root CA Zertifikat installiert werden.

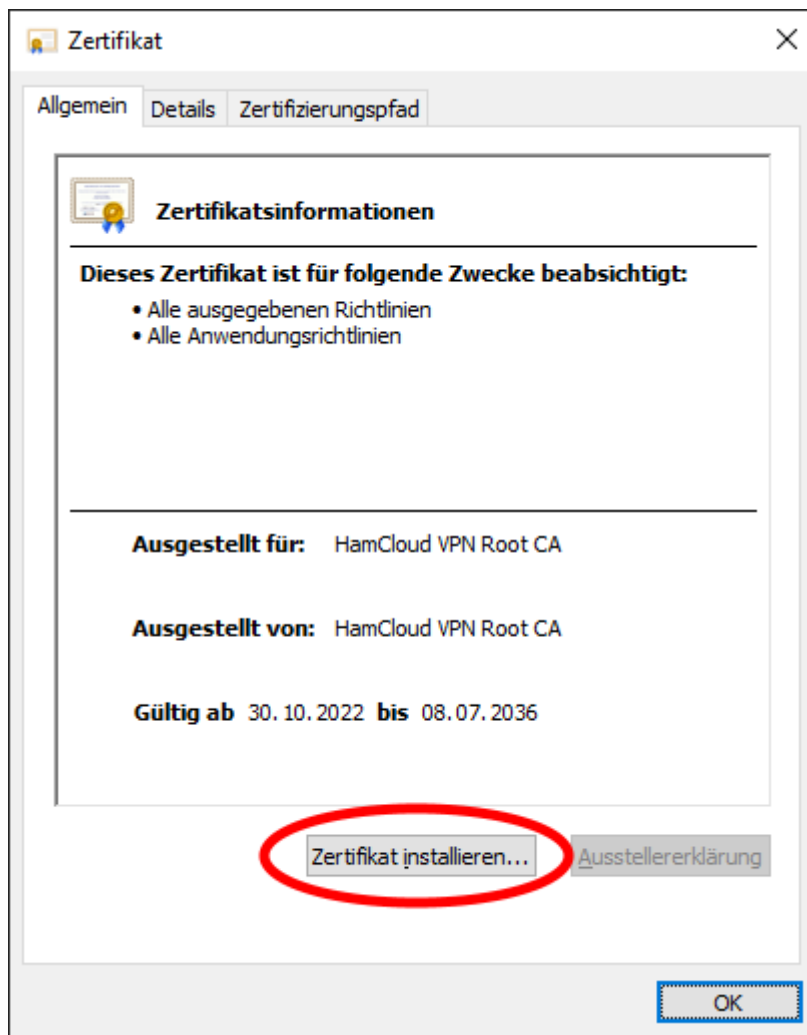
IKEv2 – Windows 10

Im ersten Schritt muss das Root-Zertifikat des HamCloud VPN-Servers importiert werden:

- Das Root-Zertifikat [hier](#) herunterladen und auf dem Desktop speichern.



- Das Zertifikat „hamcloud-vpn-root-ca.cer“ auf dem Desktop doppelt anklicken.



- Auf „Zertifikat“ installieren klicken.

Willkommen

Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrenlisten vom Datenträger in den Zertifikatspeicher.


Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.

Speicherort

☐ Aktueller Benutzer

☒ Lokaler Computer

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

 Weiter

- „Lokaler Computer“ auswählen und auf „Weiter“ klicken.

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

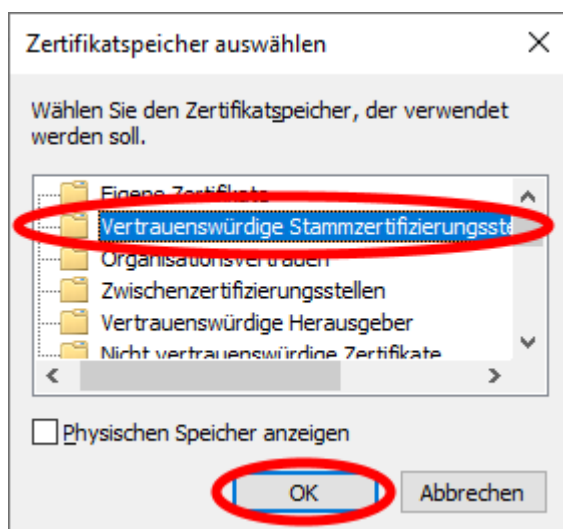
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

☐ Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)

☒ Alle Zertifikate in folgendem Speicher speichern:

Zertifikatspeicher:

- „Alle Zertifikate in folgendem Speicher speichern“ wählen und auf „Durchsuchen“ klicken.



- „Vertrauenswürdige Stammzertifizierungsstellen“ auswählen und auf „OK“ klicken.

Zertifikatspeicher

Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

- ☐ Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
- ☒ Alle Zertifikate in folgendem Speicher speichern

Zertifikatspeicher:

Vertrauenswürdige Stammzertifizierungsstellen

Durchsuchen...

Weiter

Abbrechen

- Auf „Weiter“ klicken.

Fertigstellen des Assistenten

Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.


Sie haben folgende Einstellungen ausgewählt:

Vom Benutzer gewählter Zertifikatspeicher	Vertrauenswürdige Stammzertifizierungsstelle
Inhalt	Zertifikat

Fertig stellen Abbrechen

- Auf „Fertig stellen“ klicken.

Zertifikatimport-Assistent

 Der Importvorgang war erfolgreich.

OK

- Auf „OK“ klicken und mit „OK“ das Zertifikat schließen.

Im zweiten Schritt wird eine neue VPN-Verbindung mit Hilfe der Powershell erstellt:

- Das Windows Start Symbol anklicken, „powershell“ eingeben und anschließend die Windows PowerShell App starten.



- Folgende Befehle (am besten mit Kopieren & Einfügen [Steuerung + v]) eingeben und mit Enter ausführen:

Add-VPNConnection -Name "HamCloud VPN" -ServerAddress "vpn.hc.r1.ampr.org" -TunnelType "Ikev2" -RememberCredential -SplitTunneling -EncryptionLevel Maximum -Force

Add-VpnConnectionRoute -ConnectionName "HamCloud VPN" -DestinationPrefix "44.128.0.0/10"

A screenshot of a Windows PowerShell terminal window. The title bar says "Windows PowerShell". The window content shows the PowerShell prompt "PS C:\Users\jann>" followed by the command "Add-VPNConnection -Name 'HamCloud VPN' -ServerAddress 'vpn.hc.r1.ampr.org' -TunnelType 'Ikev2' -RememberCredential -SplitTunneling -EncryptionLevel Maximum -Force". The prompt then changes to "PS C:\Users\jann>" and the second command "Add-VpnConnectionRoute -ConnectionName 'HamCloud VPN' -DestinationPrefix '44.128.0.0/10'" is entered. The prompt returns to "PS C:\Users\jann>" after the second command.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

PS C:\Users\jann> Add-VPNConnection -Name "HamCloud VPN" -ServerAddress "vpn.hc.r1.ampr.org" -TunnelType "Ikev2" -RememberCredential -SplitTunneling -EncryptionLevel Maximum -Force
PS C:\Users\jann>
PS C:\Users\jann> Add-VpnConnectionRoute -ConnectionName "HamCloud VPN" -DestinationPrefix "44.128.0.0/10"
PS C:\Users\jann>
```

- Das Fenster schließen.

Im dritten Schritt muss die VPN-Verbindung noch angepasst werden, so dass nur Pakete an das HAMNET die VPN-Verbindung nutzen:

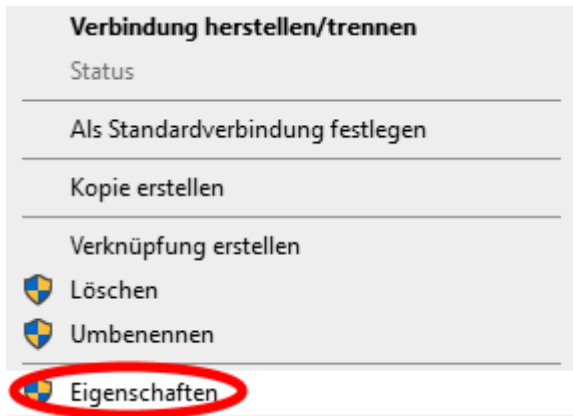
- Das Windows Start Symbol anklicken, „ncpa.cpl“ eingeben und anschließend das Systemsteuerungselement öffnen.



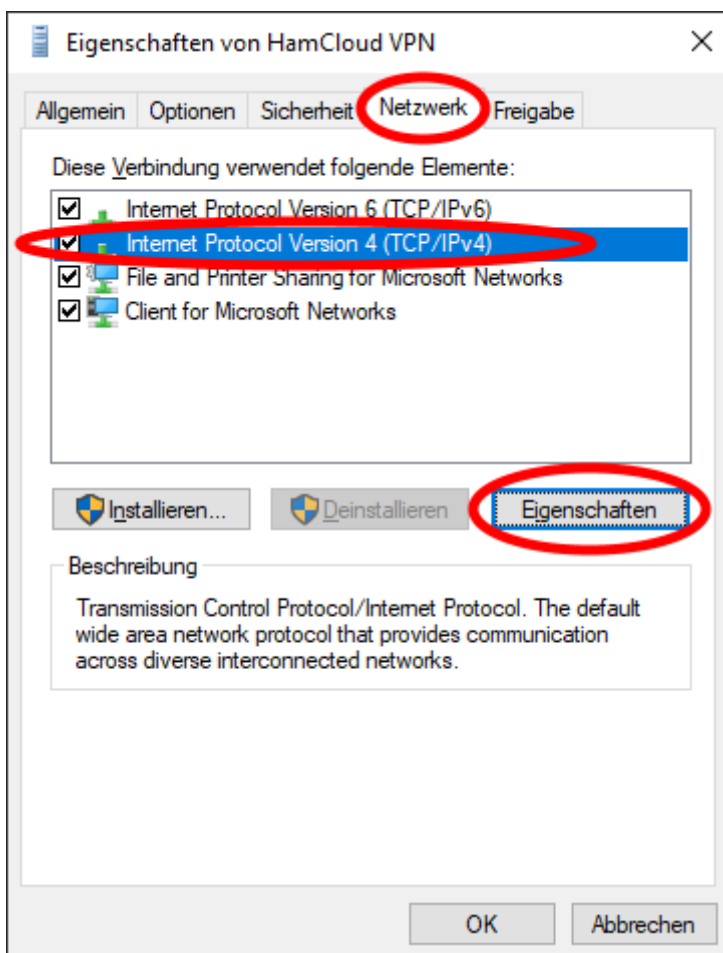
- Die Verbindung „HamCloud VPN“ mit der rechten Maustaste anklicken.



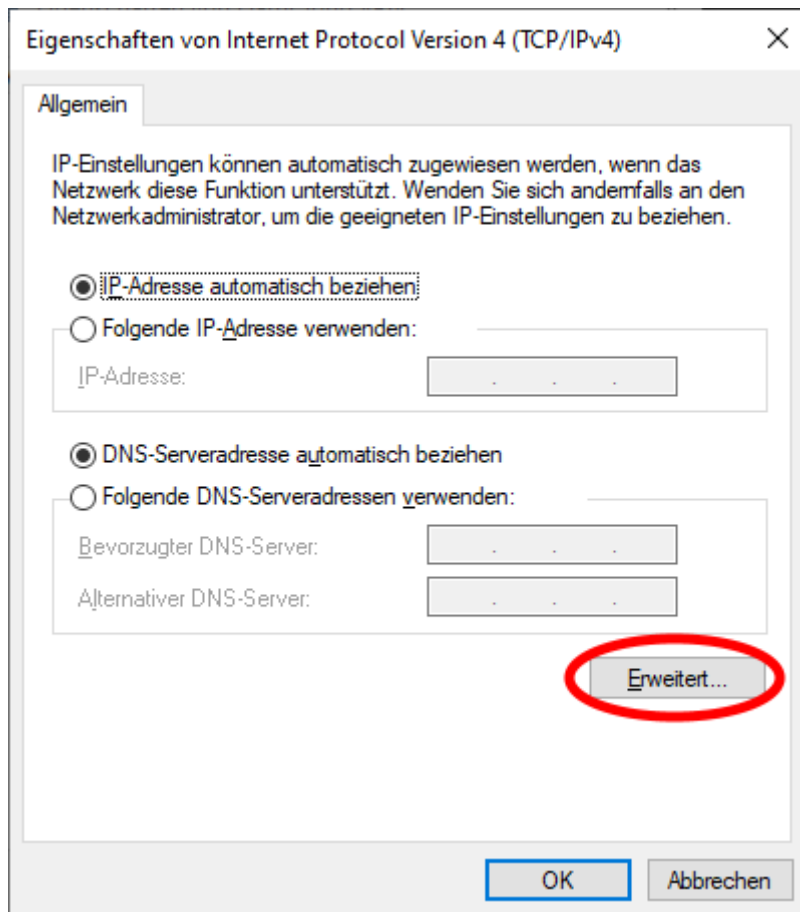
- „Eigenschaften“ auswählen.



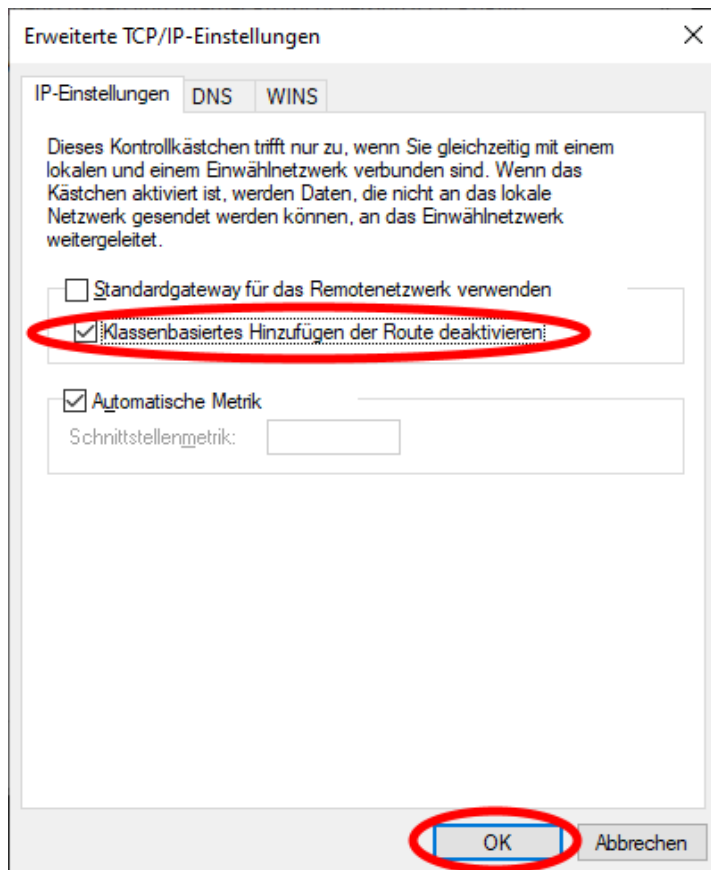
- Den Tab „Netzwerk“ auswählen, das Element „Internet Protokoll Version 4 (TCP/IPv4)“ auswählen und auf „Eigenschaften“ klicken.



- Auf „Erweitert“ klicken.



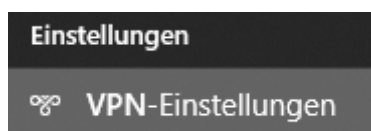
- „Klassenbasiertes Hinzufügen der Route deaktivieren“ auswählen und auf „OK“ klicken.



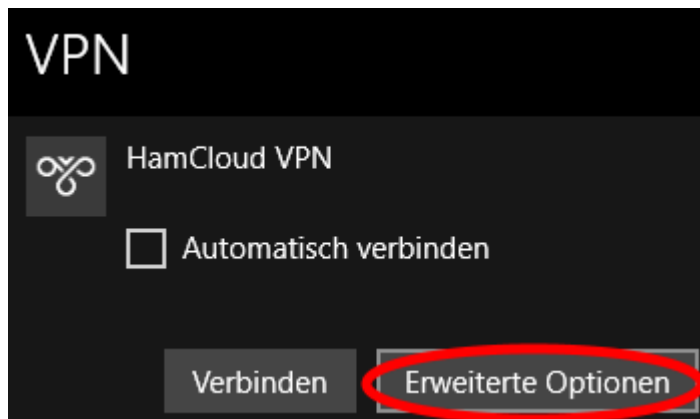
- Weitere 2x auf „OK“ klicken und anschließend das Systemsteuerungselement „Netzwerkverbindungen“ wieder schließen.

Im letzten Schritt wird für die VPN-Verbindung der Username und das Passwort gespeichert:

- Das Windows Start Symbol anklicken, „vpn“ eingeben und anschließend unter den Einstellungen „VPN-Einstellungen“ öffnen:



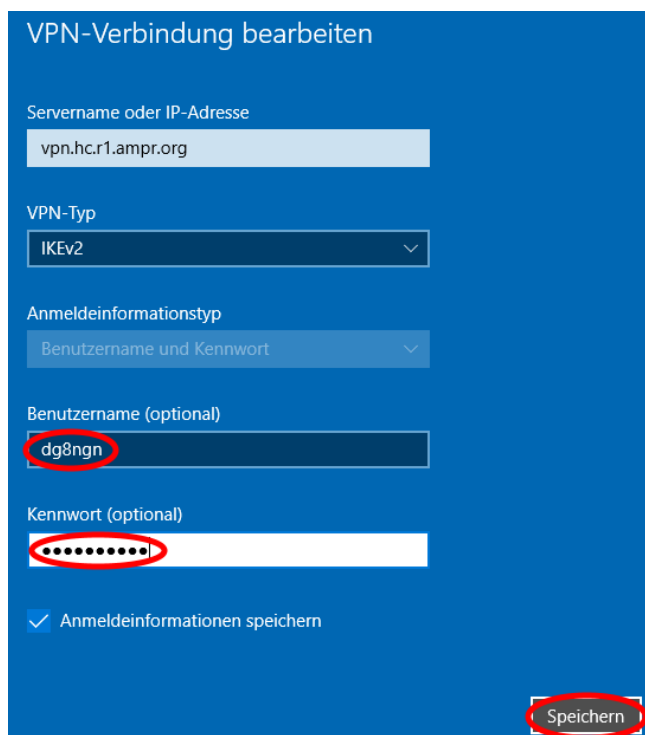
- Die Verbindung „HamCloud VPN“ anklicken und auf „Erweiterte Optionen“ klicken.



- Die Verbindungseigenschaften durch Klick auf „Bearbeiten“ anpassen.



- Der von «HamCouud VPN – IKEv2» erstelle Benutzernamen und dort generierte Kennwort, eingeben und anschließend auf „Speichern“ klicken.



- Das Fenster oben rechts mit Klick auf „X“ schließen.

Nun kann die VPN-Verbindung genutzt werden:

- Auf das Netzwerksymbol in der Windows Taskbar klicken.



- Die Verbindung „HamCloud VPN“ anklicken und auf „Verbinden“ klicken.

