

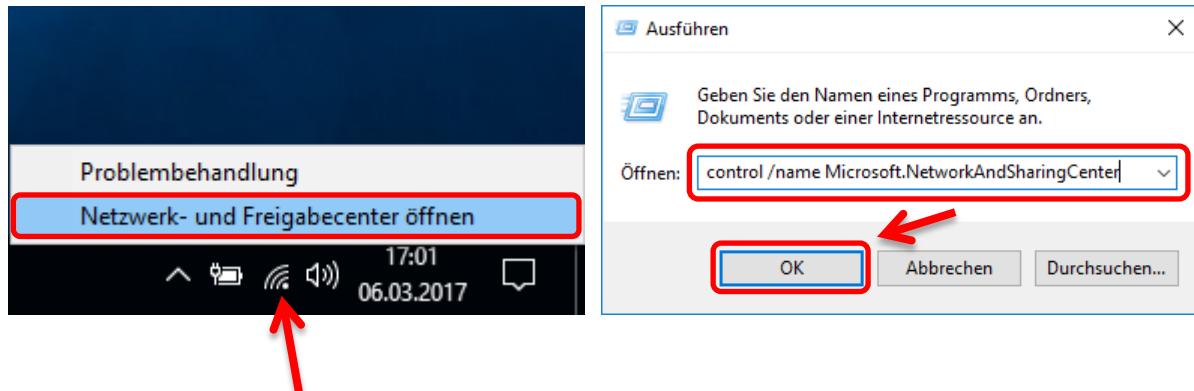
Rechenzentrum

# **Einrichten der Eduroam-Verbindung unter Windows 10**

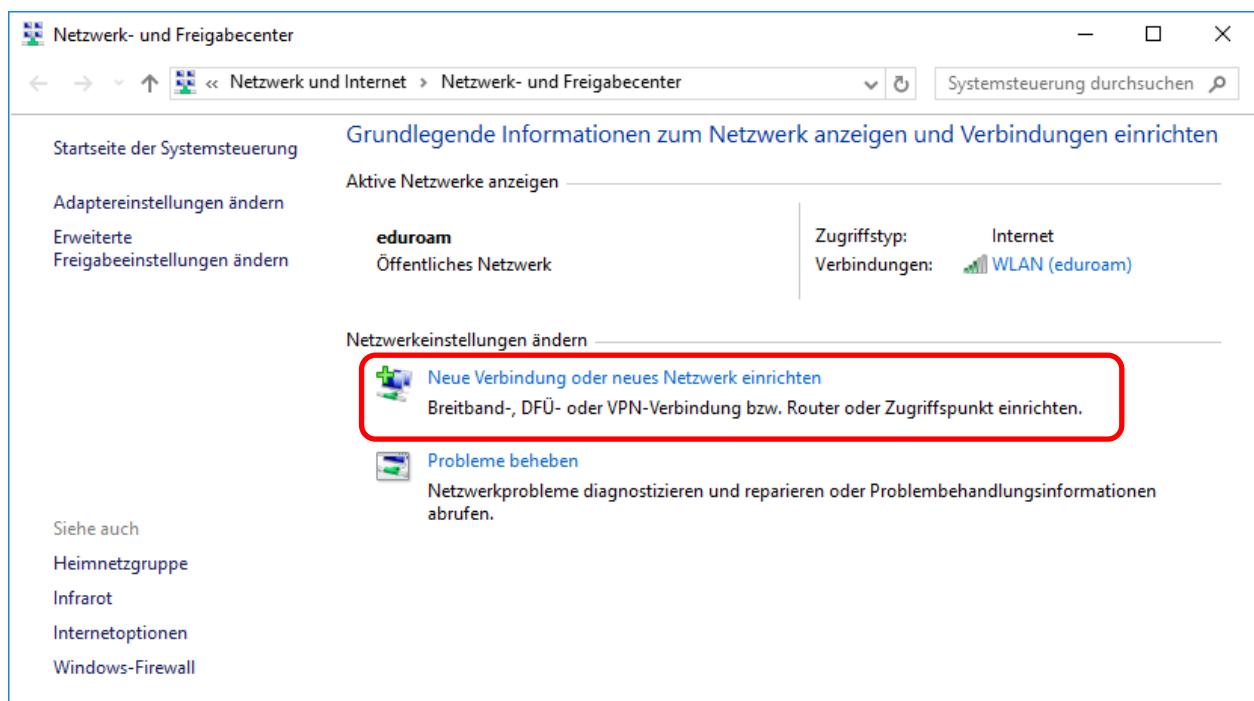
Rechtsklick auf das Netzwerksymbol in der Taskleiste und anschließend die Option „Netzwerk- und Freigabecenter öffnen“ auswählen:

Alternativ:

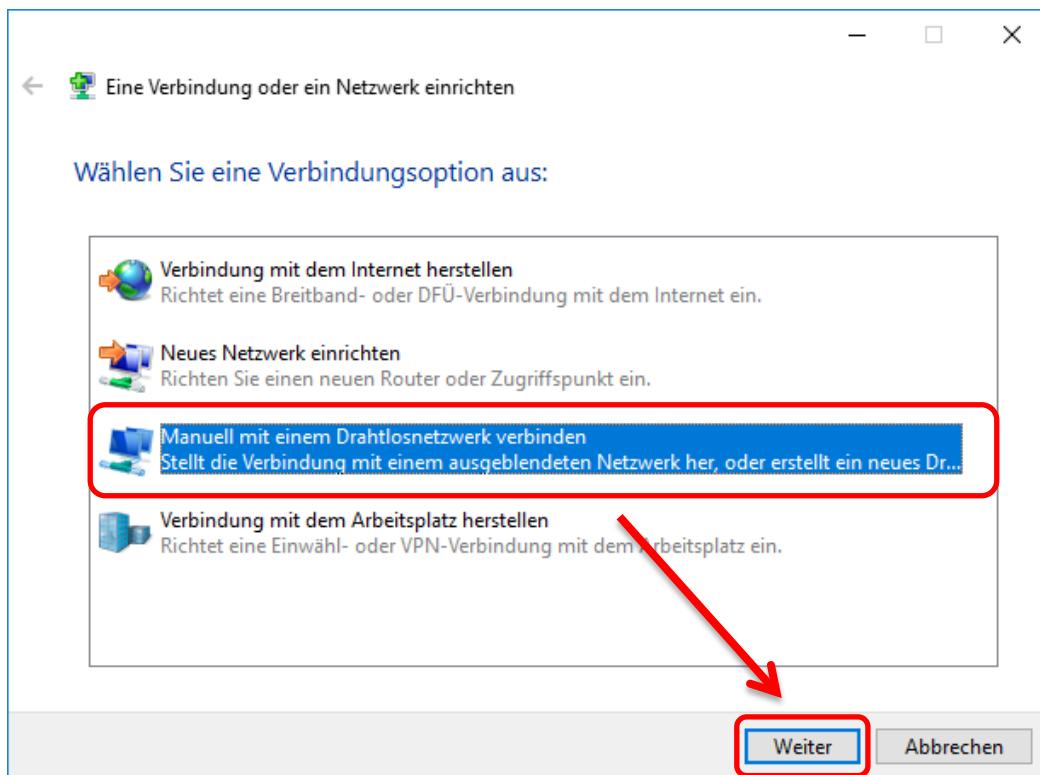
„Windows-Taste + R“ drücken und Folgendes eintragen:  
control /name Microsoft.NetworkAndSharingCenter



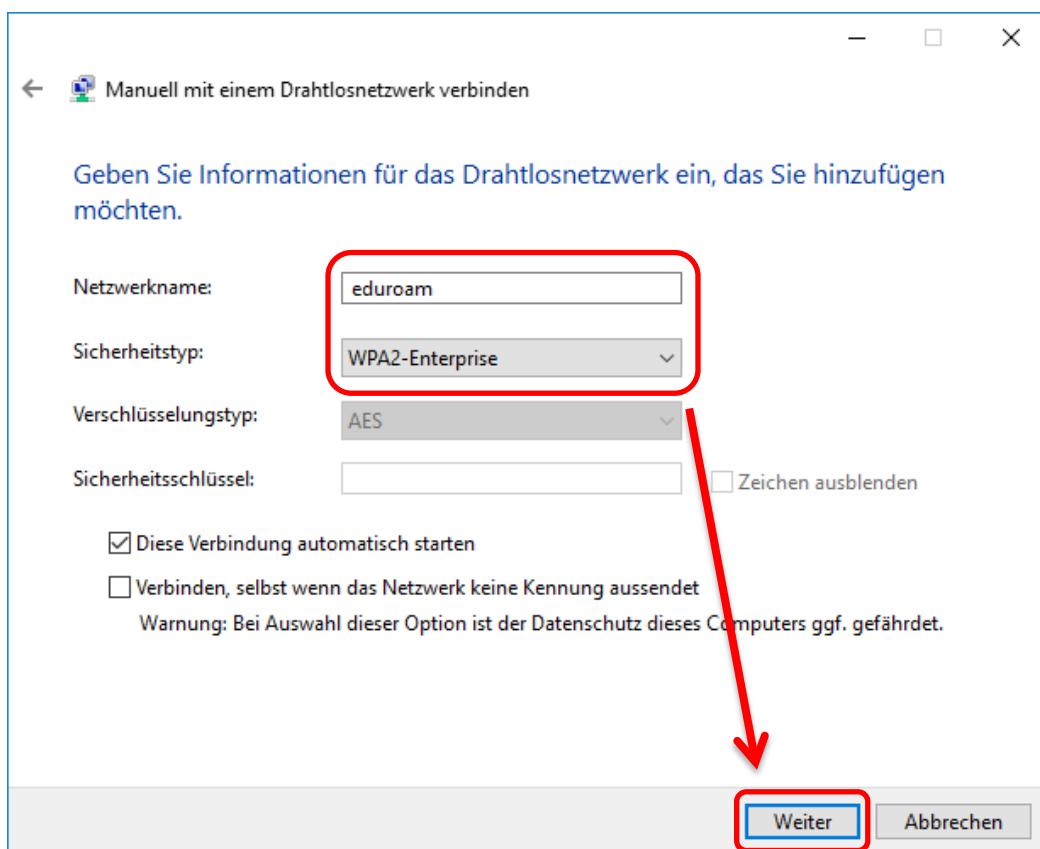
„Neue Verbindung oder neues Netzwerk einrichten“ auswählen:



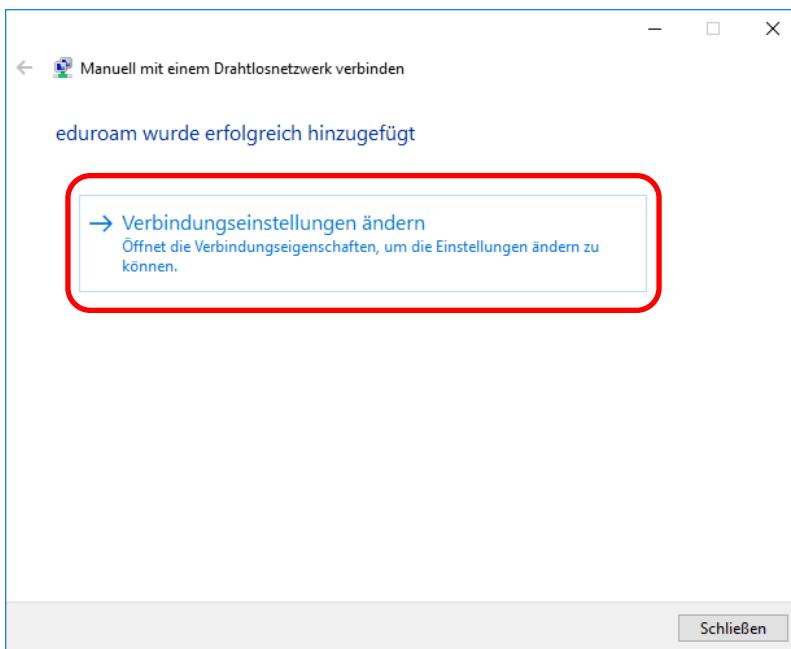
„Manuell mit einem Drahtlosnetzwerk verbinden“ auswählen und auf „Weiter“ klicken:



„Eduroam“ als Netzwerknamen und „WPA2-Enterprise“ als Sicherheitstyp konfigurieren:



Nach Hinzufügen des WLANs „Verbindungseinstellungen ändern“ auswählen:

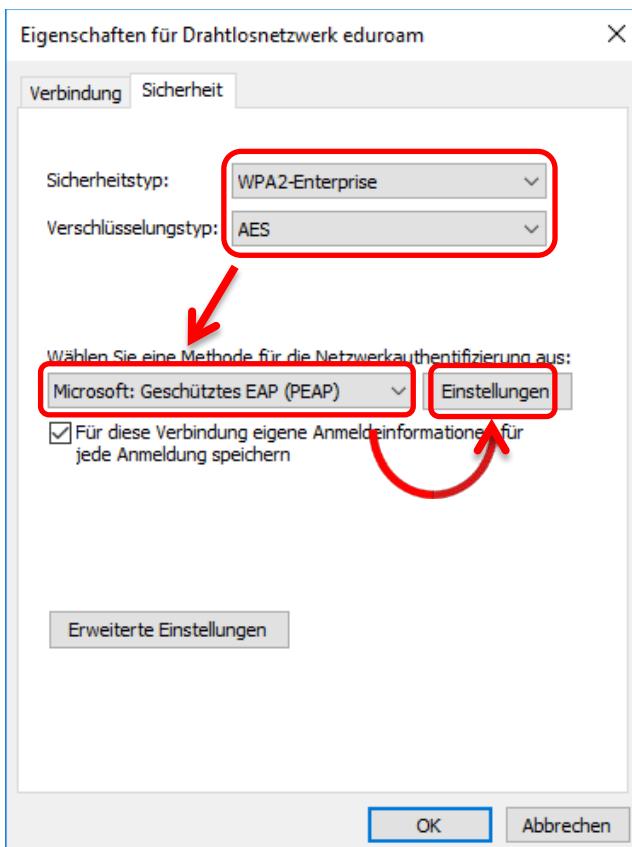


Im Reiter Sicherheit folgende Konfiguration vornehmen und auf „Einstellungen“ klicken:

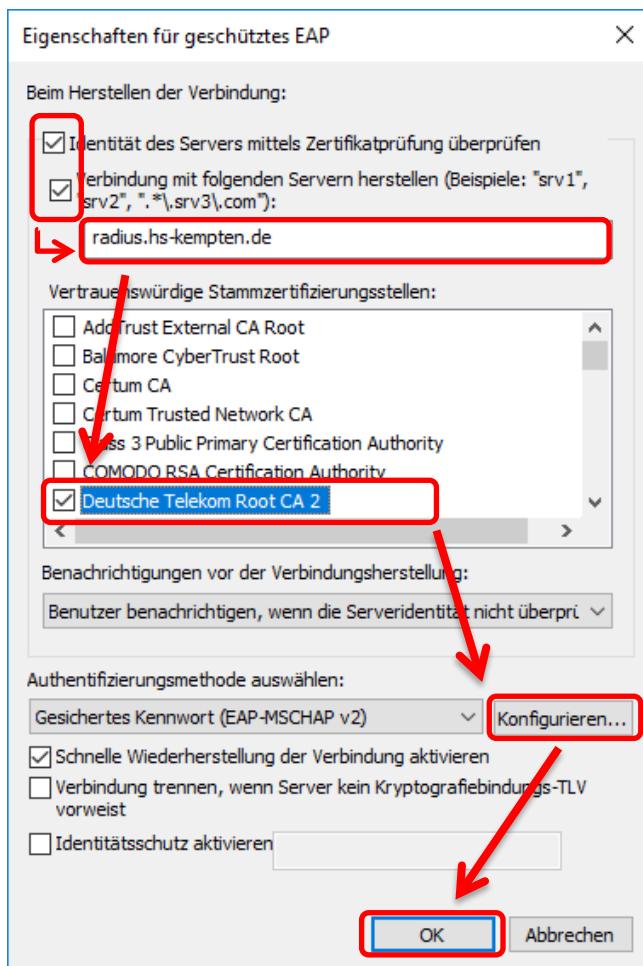
Sicherheitstyp: **WPA2-Enterprise**

Verschlüsselungstyp: **AES**

Methode für Netzwerkauthentifizierung: **Microsoft: Geschütztes EAP (PEAP)**



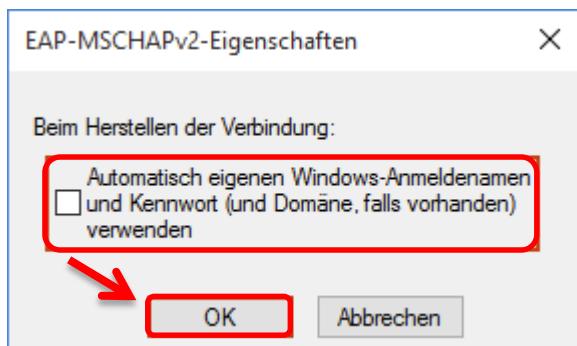
Abgebildete Häkchen setzen und folgenden Server eintragen: **radius.hs-kempten.de**  
 Vertrauenswürdige Stammzertifizierungsstelle aktivieren: **Deutsche Telekom Root CA 2**  
 Anschließend auf „Konfigurieren“ klicken:



Falls das Zertifikat „Deutsche Telekom Root CA 2“ nicht vorhanden ist, bitte dieses zuerst herunterladen und installieren. Genaue Anweisungen dazu gibt es ab

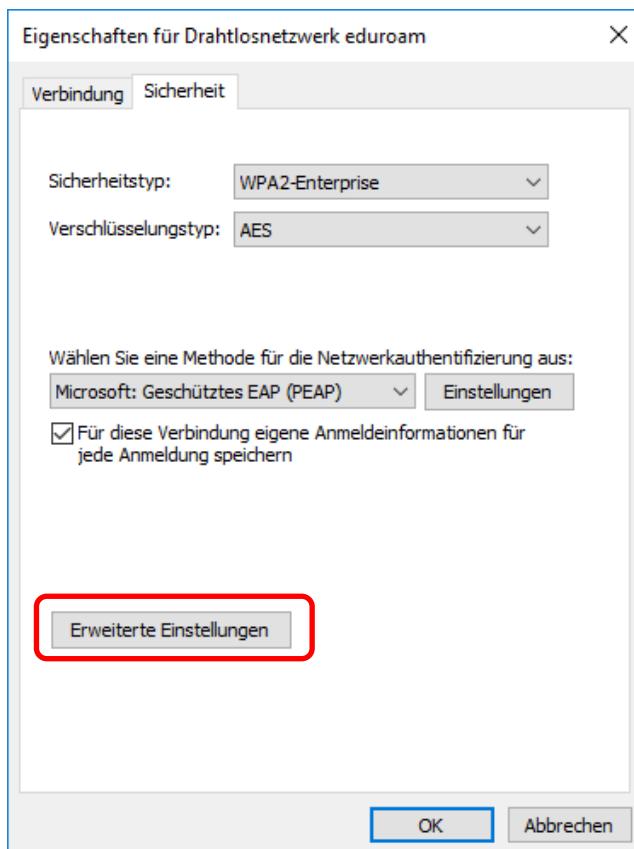
**Seite 9**

Häckchen entfernen (falls gesetzt) und auf „OK“ klicken:

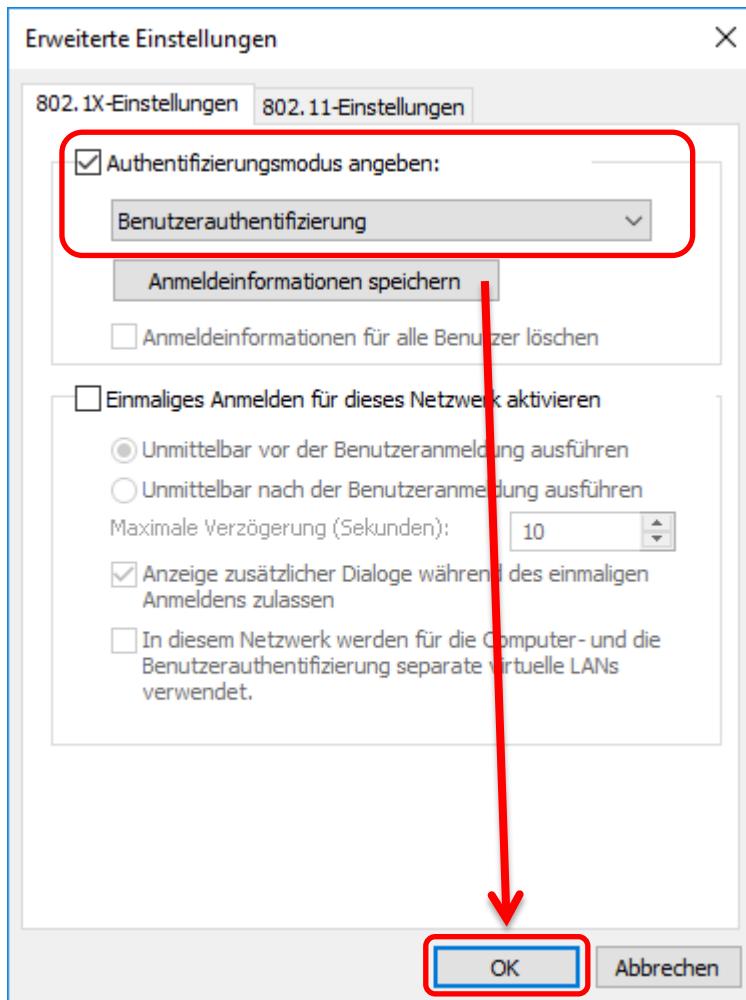


Das Fenster „Eigenschaften für geschütztes EAP“ durch Klicken auf „OK“ schließen.

Im Fenster „Eigenschaften für Drahtlosnetzwerk eduroam“ auf „Erweiterte Einstellungen“ klicken:



Häkchen für „Authentifizierungsmodus angeben“ setzen und „Benutzeroauthentifizierung“ auswählen:



Zum Schluss alle Fenster durch Klicken auf „OK“ schließen und einen Neustart von Windows durchführen.

Nach dem Neustart von Windows die Verbindung zum WLAN **eduroam** herstellen:



Als Benutzernamen die Hochschulkennung eintragen, z.B.: [stmustter@hs-kempten.de](mailto:stmustter@hs-kempten.de)  
und anschließend durch Klicken auf „OK“ bestätigen:



Bei Erfolg wird der Begriff „**Verbunden**“ unter der Verbindung angezeigt.

**FERTIG!**

**Optional: Zertifikat herunterladen und installieren**

Falls das Telekom-Zertifikat nicht vorhanden ist, muss dieses zuerst importiert werden, hierzu folgende Adresse im Webbrowser aufrufen und auf abgebildeten Link klicken:

<https://www.pki.dfn.de/root/globalroot/>



Überblick DFN-PKI

Die CAs im DFN

Grid Zertifikate

DFN-AAI Zertifikate

Zeitstempeldienst

Policies

Wurzelzertifikate

Wurzel- und CA-Zertifikate im Sicherheitsniveau Global

1. Wurzelzertifikat Deutsche Telekom Root CA 2

2. CA-Zertifikat DFN-Verein PCA Global - G01 (altes CA-Zertifikat mit Signatur)

3. CA-Zertifikat DFN-Verein PCA Global - G01 (neues CA-Zertifikat mit Signatur)

4. Fehlerhaft ausgestelltes CA-Zertifikat DFN-Verein PCA Global - G01

Wurzelzertifikat Deutsche Telekom Root CA 2

Zertifikatdatei „.crt“ mit der **rechten Maustaste** anklicken und „**Ziel speichern unter...**“ auswählen:



Policies

Wurzelzertifikate

Global (Generation 2)

Global (Generation 1)

Classic

Grid

SLCS

Basic

Validierungsdienste (CRL und OCSP)

FAQ DFN-PKI

Kontakt und Support

DFN-PKI Blog

DFN-Verein

Wurzelzertifikat Deutsche Telekom Root CA 2

Dieses Wurzelzertifikat ist in den unter [Integration DFN-PKI](#) aufgeführten Anwendungen verwendbar.

**Gültigkeit**

- Jul 9 12:11:00 1999 GMT bis Jul 9 23:59:00 2019 GMT

**Formate**

- Das Zertifikat im Binärformat (DER-Format) zum Import in Anwendungen (Windows-Datei-Extensions: **.crt**)
- Text: Das Zertifikat in Textform
- PEM: Das Zertifikat in PEM-Format

**Seriennummer**

38 bzw. hexadezimal 0x26

**Fingerprint**

SHA1 Fingerprint - 05:AA:00

Öffnen

In neuer Registerkarte öffnen

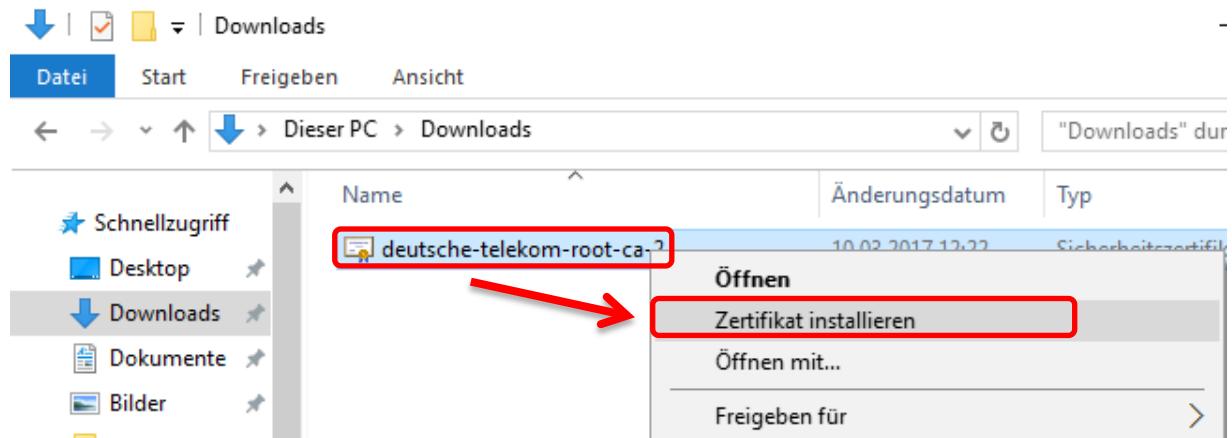
In neuem Fenster öffnen

Ziel speichern unter...

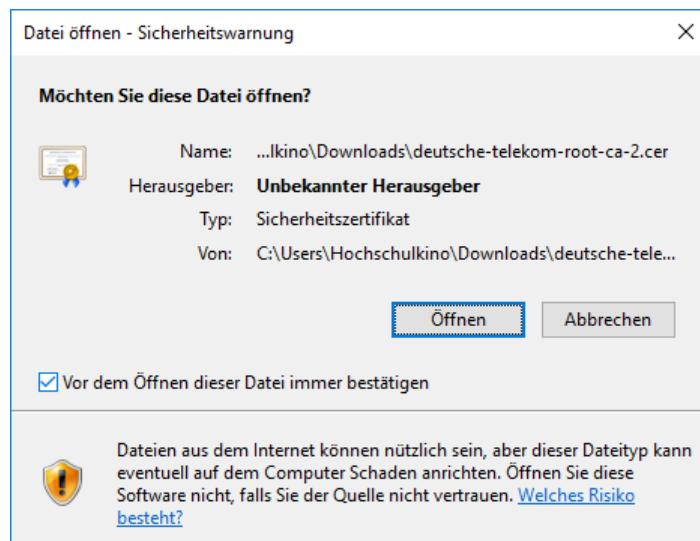
Ziel drucken

Windows Explorer starten und zum Verzeichnis der Zertifikat-Datei wechseln.

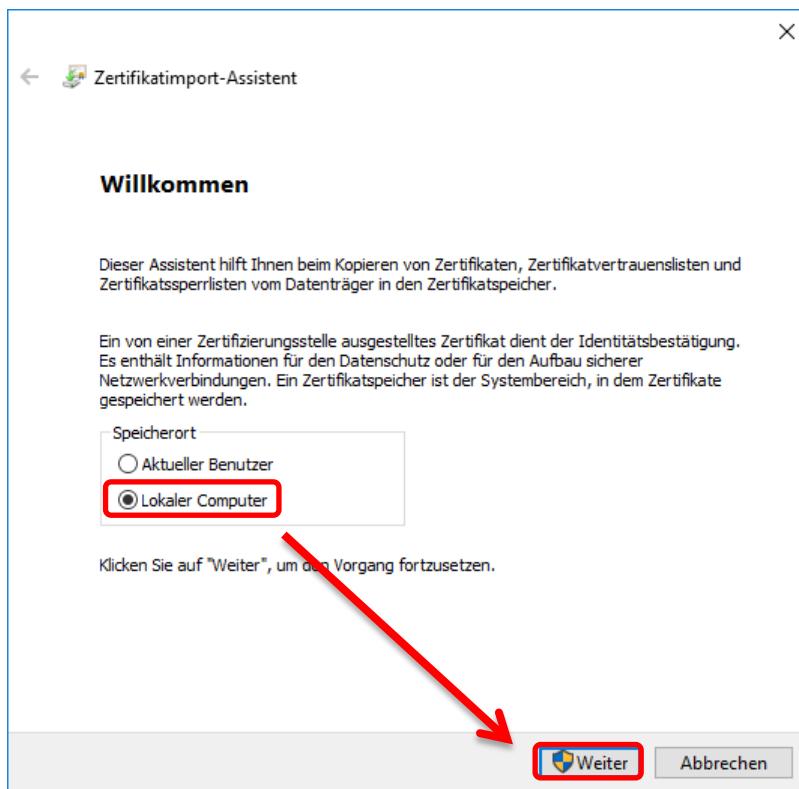
Datei mit der rechten Maustaste anklicken und „**Zertifikat installieren**“ auswählen:



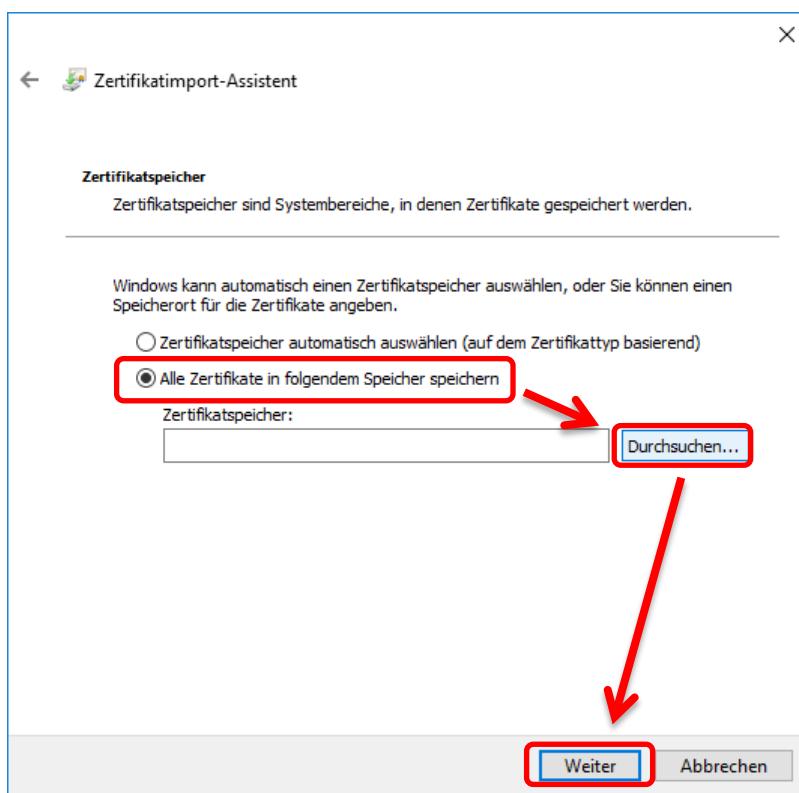
Bei einer eventuell auftretenden Sicherheitswarnung auf „**Öffnen**“ klicken:



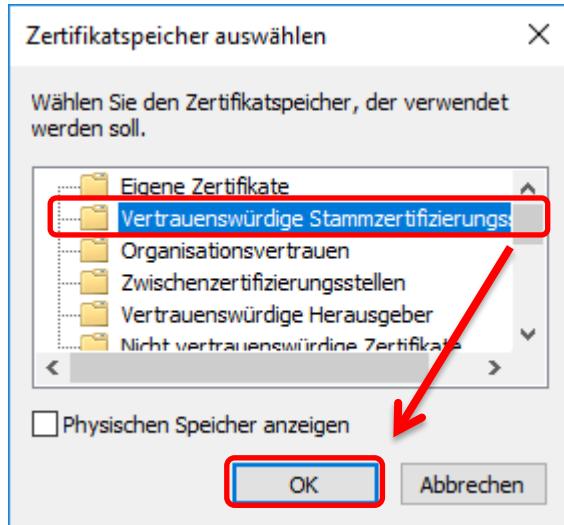
„Lokaler Computer“ auswählen und auf „Weiter“ klicken:



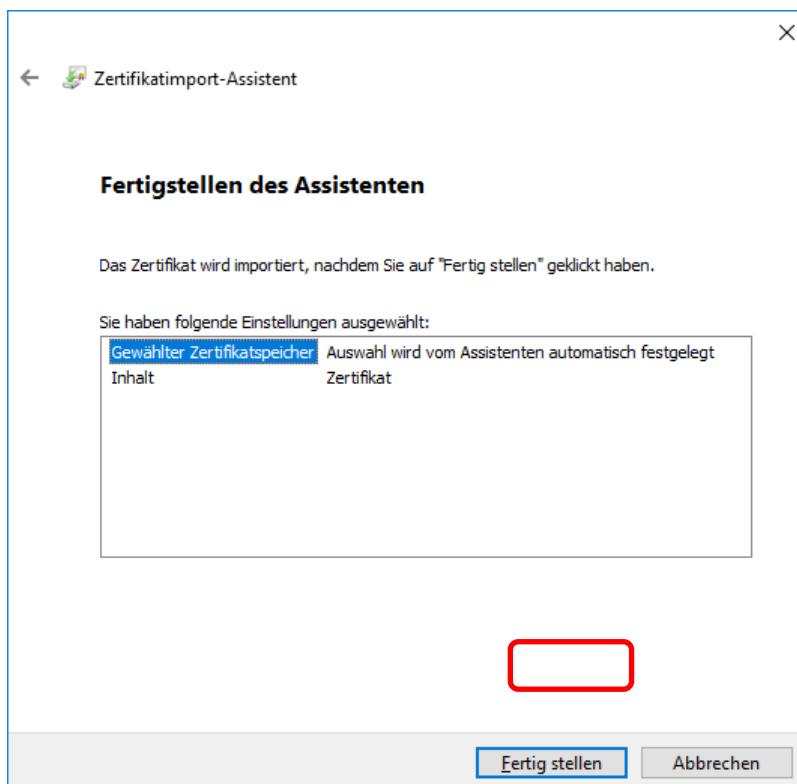
„Alle Zertifikate in folgendem Speicher speichern“ auswählen und auf „Durchsuchen“ klicken:



„Vertrauenswürdige Stammzertifizierungsstellen“ markieren und auf „OK“ und „Weiter“ klicken:



Auf „Fertigstellen“ klicken:



Die Meldung „Der Importvorgang war erfolgreich“ mit „OK“ bestätigen:

