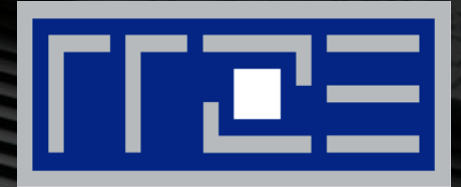


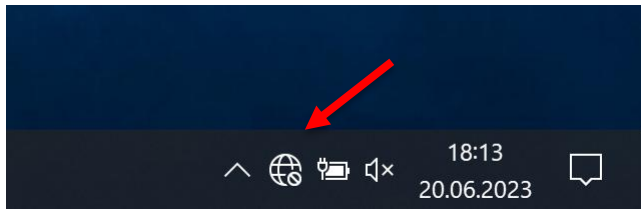
# REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



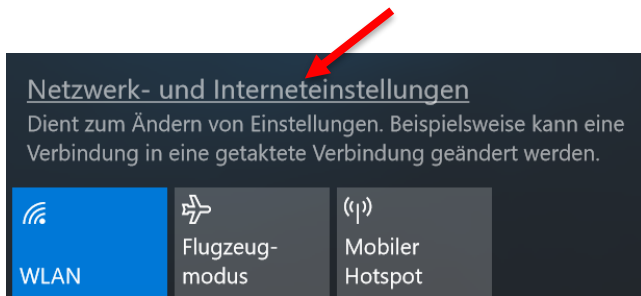
## Wireless LAN

Konfiguration von FAU-Event unter Windows

# Netzwerk- und Freigabecenter öffnen

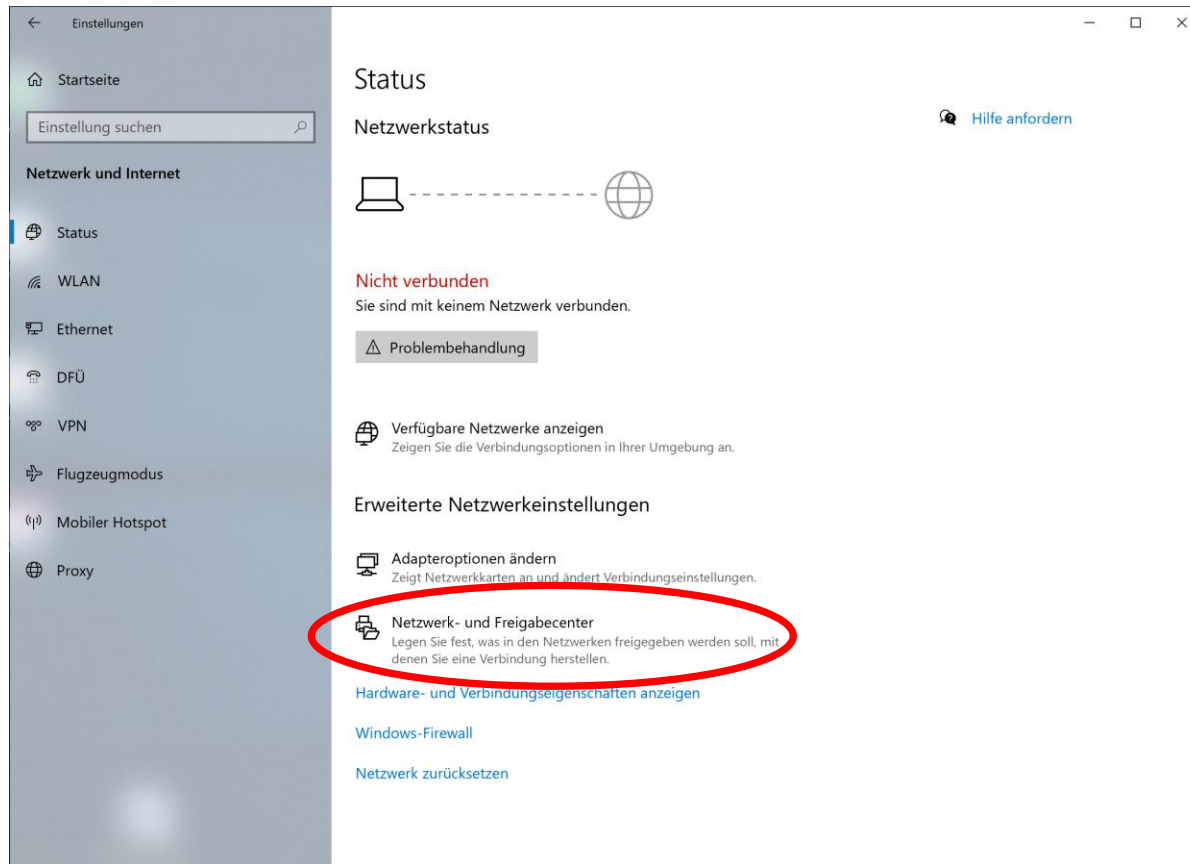


- Auf dem Desktop unten rechts Klick auf das Netzwerk-Symbol



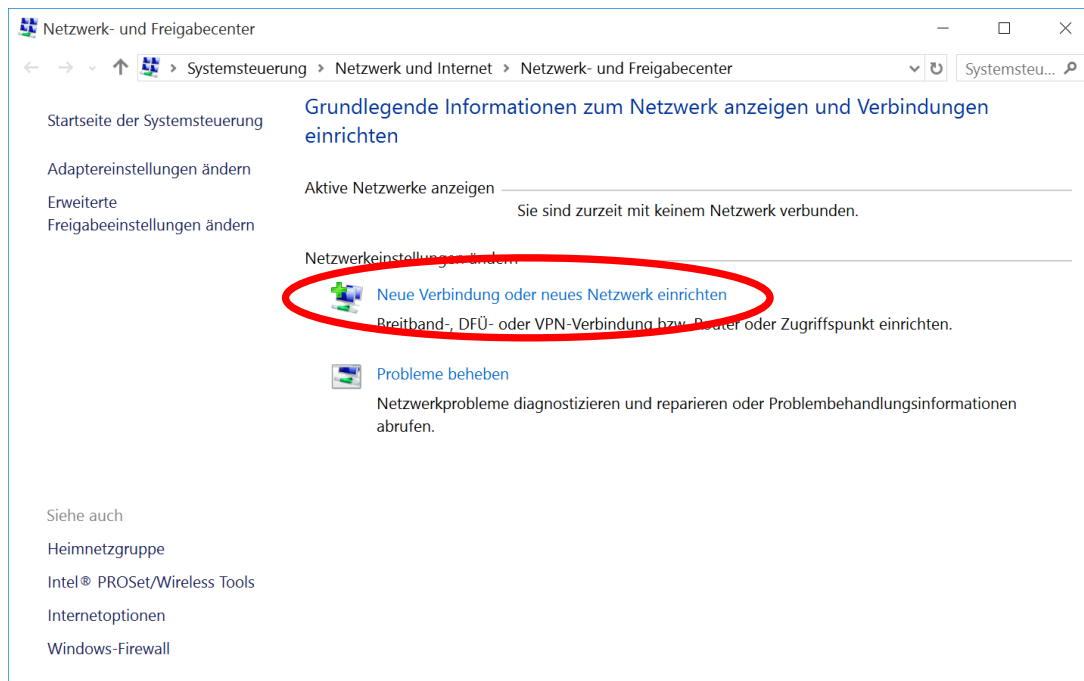
- Klick auf „**Netzwerk- und Interneteinstellungen**“

# Netzwerk- und Freigabecenter öffnen



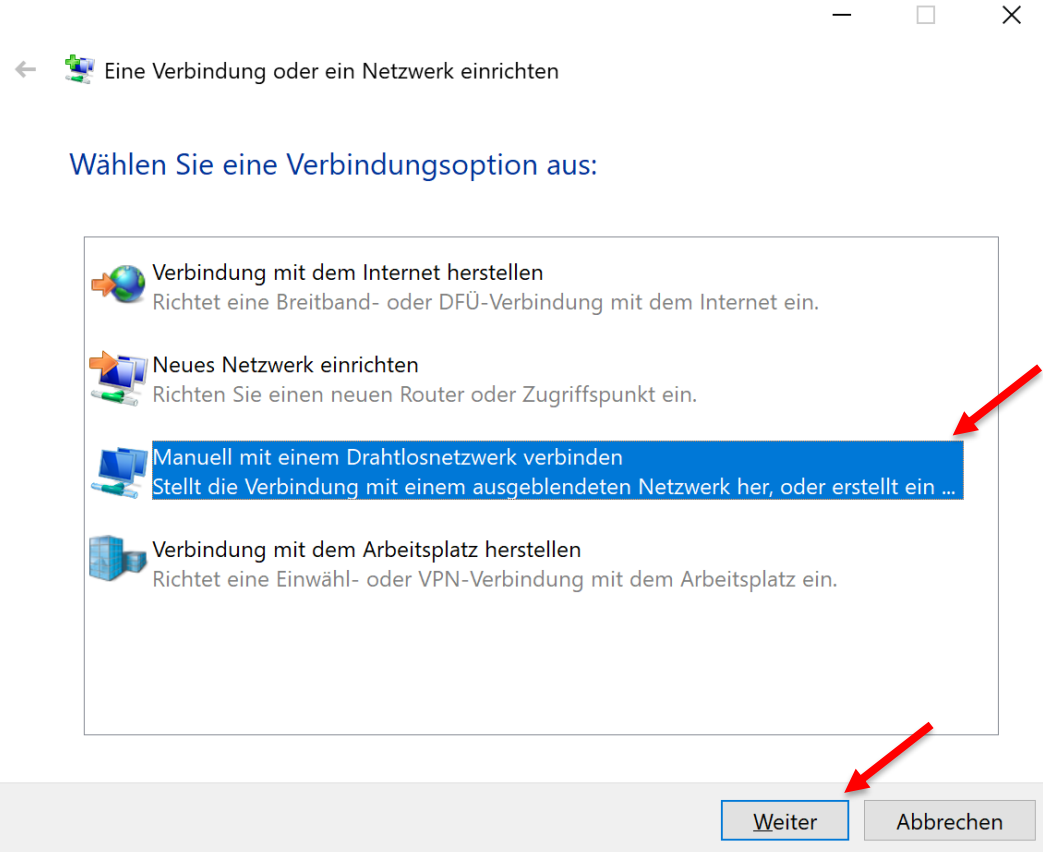
- Klick auf „Netzwerk- und Freigabecenter“

# Neue Verbindung einrichten



- Im „Netzwerk- und Freigabecenter“  
klick auf „**Neue Verbindung oder  
neues Netzwerk einrichten**“

# Manuell mit einem Funknetzwerk verbinden



- Klick auf „**Manuell mit einem Drahtlosnetzwerk verbinden**“
- Klick auf „**Weiter**“

# Manuell mit einem Funknetzwerk verbinden

← Manuell mit einem Funknetzwerk verbinden

Geben Sie Informationen für das Drahtlosnetzwerk ein, das Sie hinzufügen möchten.

Netzwerkname: FAU-Event

Sicherheitstyp: WPA2-Enterprise

Verschlüsselungstyp: AES

Sicherheitsschlüssel:  ☐ Zeichen ausblenden

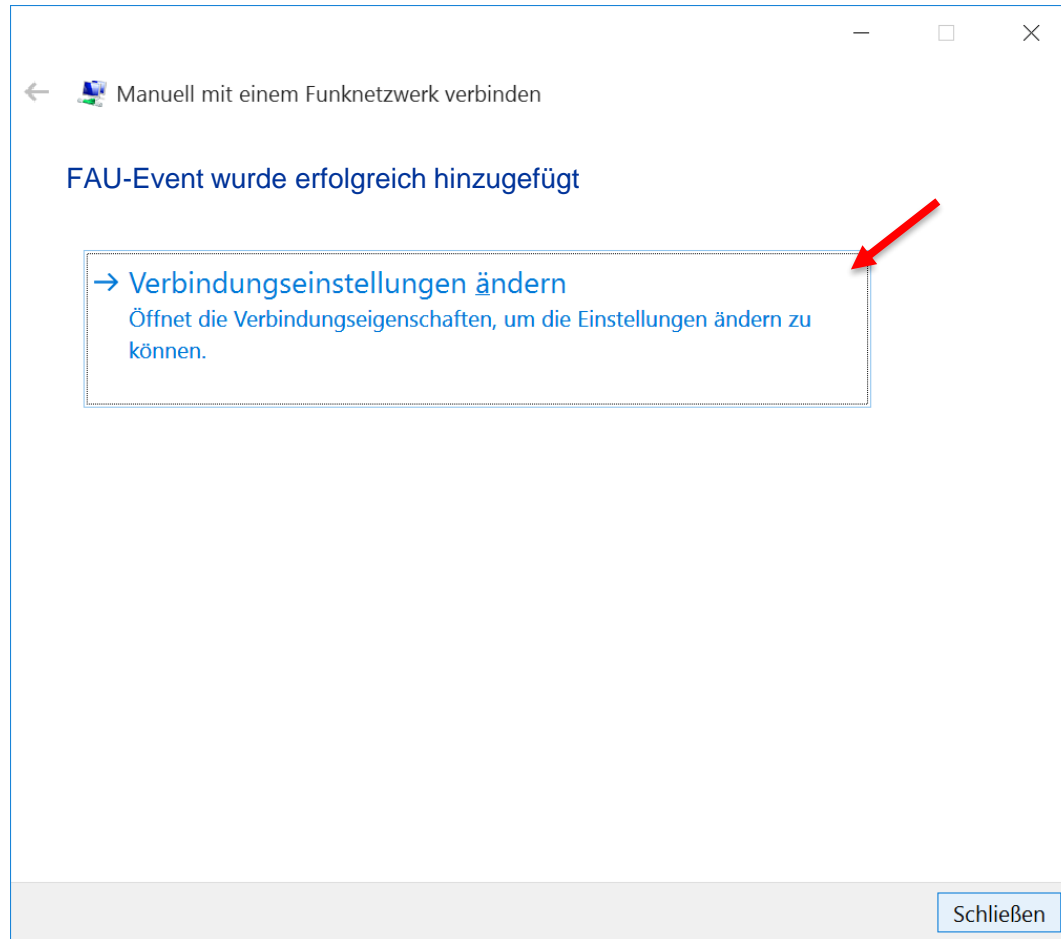
☒ Diese Verbindung automatisch starten

☐ Verbinden, selbst wenn das Netzwerk keine Kennung aussendet

Warnung: Bei Auswahl dieser Option ist der Datenschutz dieses Computers ggf. gefährdet.

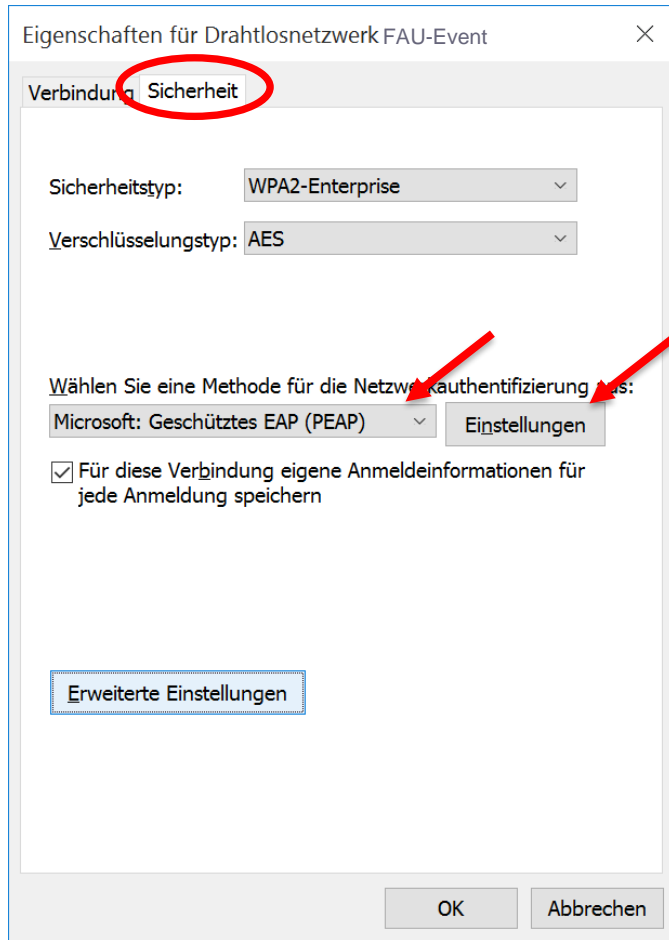
- Unter „Netzwerkname“ „**FAU-Event**“ eingeben
- „Sicherheitstyp“ „**WPA2-Enterprise**“ auswählen
- „Verschlüsselungstyp“ „**AES**“ auswählen
- Klick auf „**Weiter**“

# Verbindungseinstellungen ändern



- Klick auf „**Verbindungseinstellungen ändern**“

# Eigenschaften für Drahtlosnetzwerk FAU-Event



- Reiter „**Sicherheit**“
- „Methode für die Netzwerkauthentifizierung“: „**Microsoft: Geschütztes EAP (PEAP)**“ auswählen
- Klick auf „**Einstellungen**“



# Eigenschaften für geschütztes EAP

Eigenschaften für geschütztes EAP

Beim Herstellen der Verbindung:

- ☒ Identität des Servers mittels Zertifikatprüfung überprüfen
- ☒ Verbindung mit folgenden Servern herstellen (Beispiele: "srv1", "srv2", ".\*\srv3\com"):  
radius.rrze.uni-erlangen.de

Vertrauenswürdige Stammzertifizierungsstellen:

- ☒ HARICA TLS RSA Root CA 2001
- ☐ Baltimore CyberTrust Root
- ☐ Blizzard Battle.net Local Cert
- ☐ Certification Authority of WoSign
- ☐ Certum CA
- ☐ Certum Trusted Network CA
- ☐ Class 3 Public Primary Certification Authority
- ☐ COMODO RSA Certification Authority

Benachrichtigungen vor der Verbindungsherstellung:

Benutzer benachrichtigen, wenn die Serveridentität nicht überprüft ☐

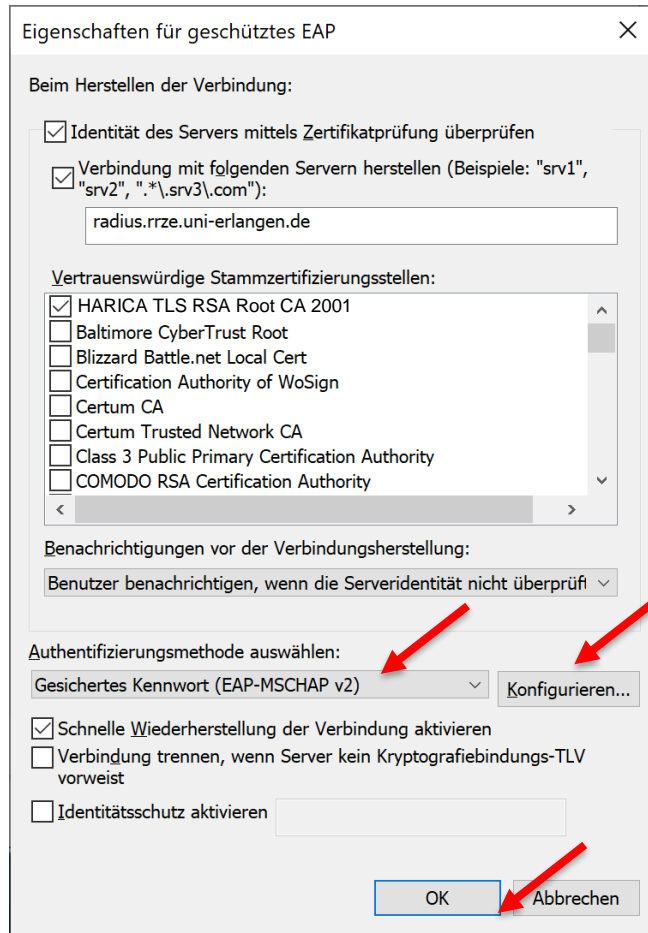
Authentifizierungsmethode auswählen:

Gesichertes Kennwort (EAP-MSCHAP v2)

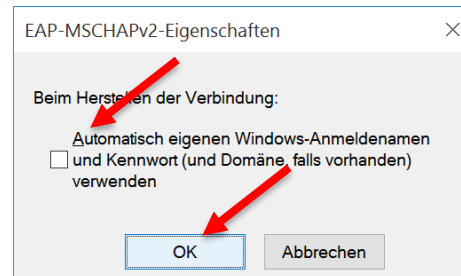
- ☒ Schnelle Wiederherstellung der Verbindung aktivieren
- ☐ Verbindung trennen, wenn Server kein Kryptografiebindungs-TLV vorweist
- ☐ Identitätsschutz aktivieren

- Haken setzen: „**Identität des Servers mittels Zertifikatprüfung überprüfen**“
- Haken setzen: „**Verbindung mit folgenden Servern herstellen**“
- Eintragen: „**radius.rrze.uni-erlangen.de**“
- Haken setzen: „**HARICA TLS RSA Root CA 2021**“
- Sollte das Zertifikat nicht vorhanden sein, siehe [Exkurs: Wurzelzertifikat installieren](#)

# Eigenschaften für geschütztes EAP



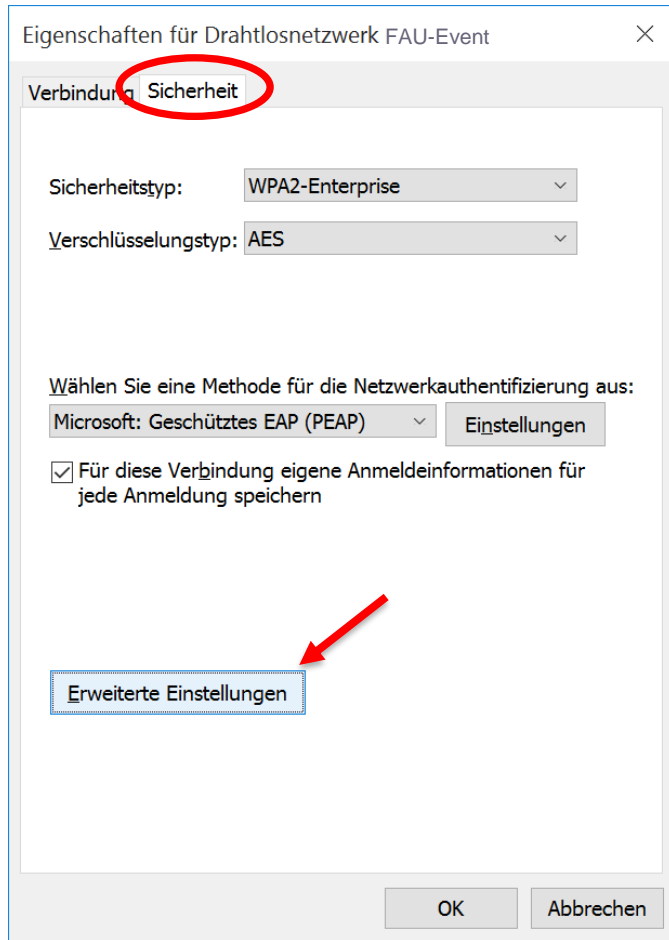
- „Authentifizierungsmethode“ „**Gesichertes Kennwort (EAP-MSCHAP v2)**“ auswählen
- Klick auf „**Konfigurieren**“



- › Haken entfernen: „**Automatisch eigenen Windows-Anmeldenamen und Kennwort [...] verwenden**“
- › Klick auf „**OK**“

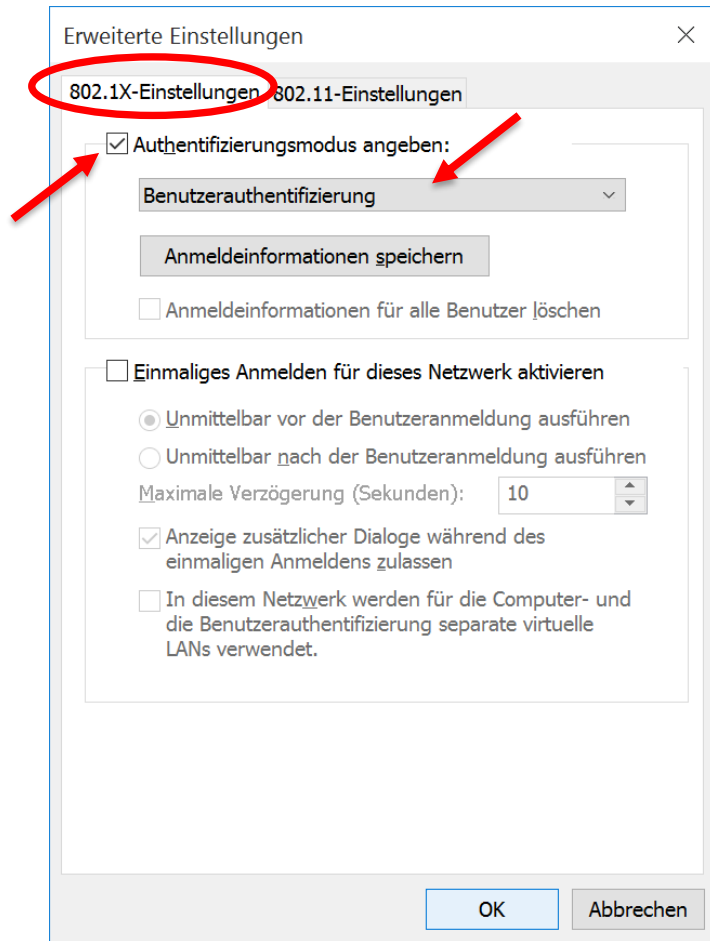
- Klick auf „**OK**“

# Eigenschaften von Drahtlosnetzwerk FAU-Event



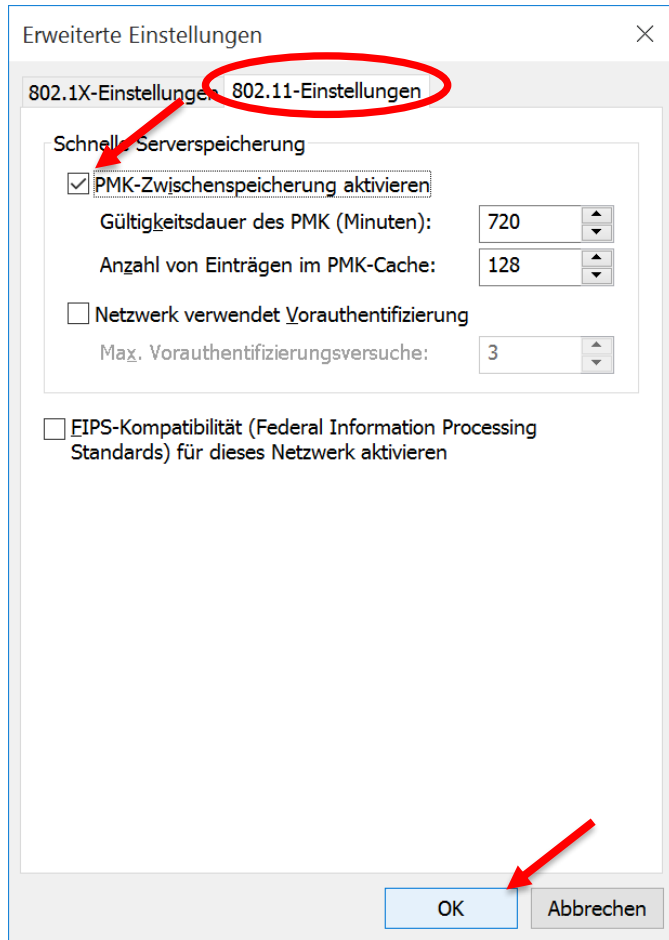
- Reiter „Sicherheit“
- Klick auf „Erweiterte Einstellungen“

# Erweiterte Einstellungen



- Reiter „**802.1X-Einstellungen**“
- Haken setzen:  
„**Authentifizierungsmethode angeben**“
- „**Benutzerauthentifizierung**“ auswählen

# Erweiterte Einstellungen



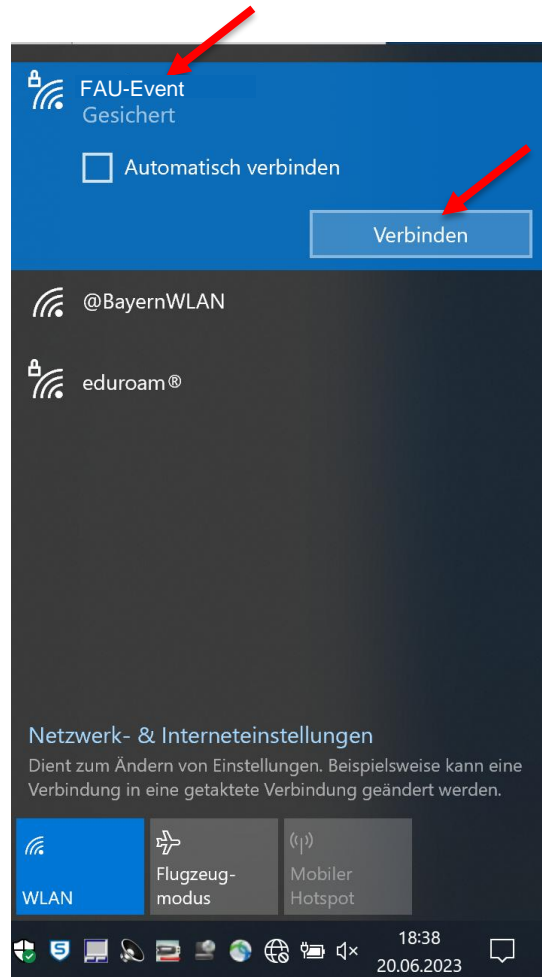
- Reiter „**802.11-Einstellungen**“
- Haken setzen: „**PMK-Zwischenspeicherung aktivieren**“
- Klick auf „**OK**“
- Im vorigen Fenster ebenfalls Klick auf „**OK**“

# Netzwerkverbindungen öffnen



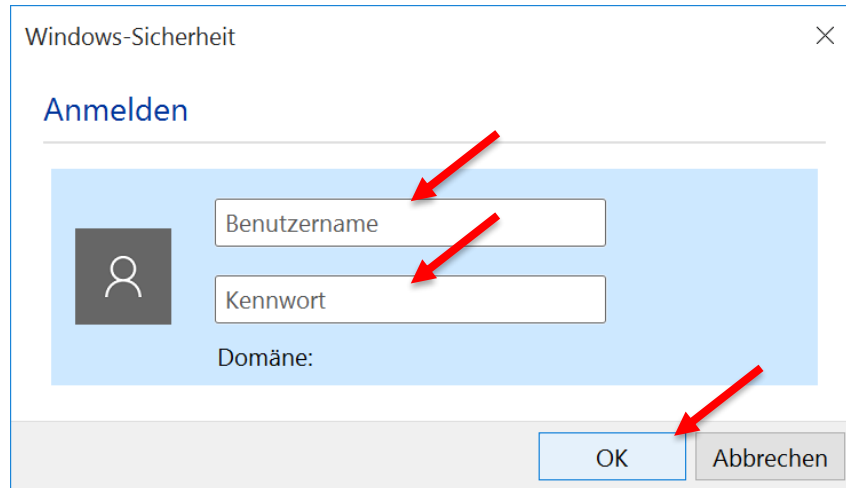
- Auf dem Desktop Klick auf das WLAN-Symbol

# Verbinden mit FAU-Event



- Netzwerk „**FAU-Event**“ auswählen
- Klick auf „**Verbinden**“

# Benutzername und Passwort eingeben

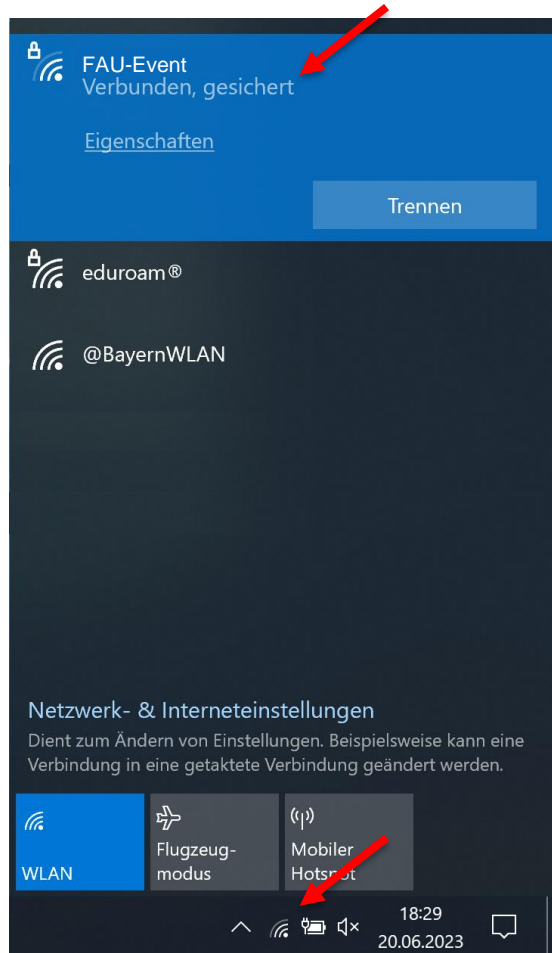


The screenshot shows a Windows Security dialog box titled "Windows-Sicherheit" with a close button (X) in the top right corner. Below the title is the word "Anmelden". The main area is a light blue box containing a user icon, a "Benutzername" (Username) text box, a "Kennwort" (Password) text box, and a "Domäne:" (Domain) label. Three red arrows point to the "Benutzername" text box, the "Kennwort" text box, and the "OK" button at the bottom right of the dialog.

- Geben Sie Ihre **IdM-Benutzerkennung**
- Geben Sie Ihr **IdM-Passwort** ein
- Oder falls Sie die Passwort-synchronisation im IdM für WLAN deaktiviert haben[\*]:
  - Geben Sie Ihr **WLAN-Passwort** ein
- Klick auf „**OK**“



# Verbindung herstellen



- Die Verbindung wird hergestellt

# Links

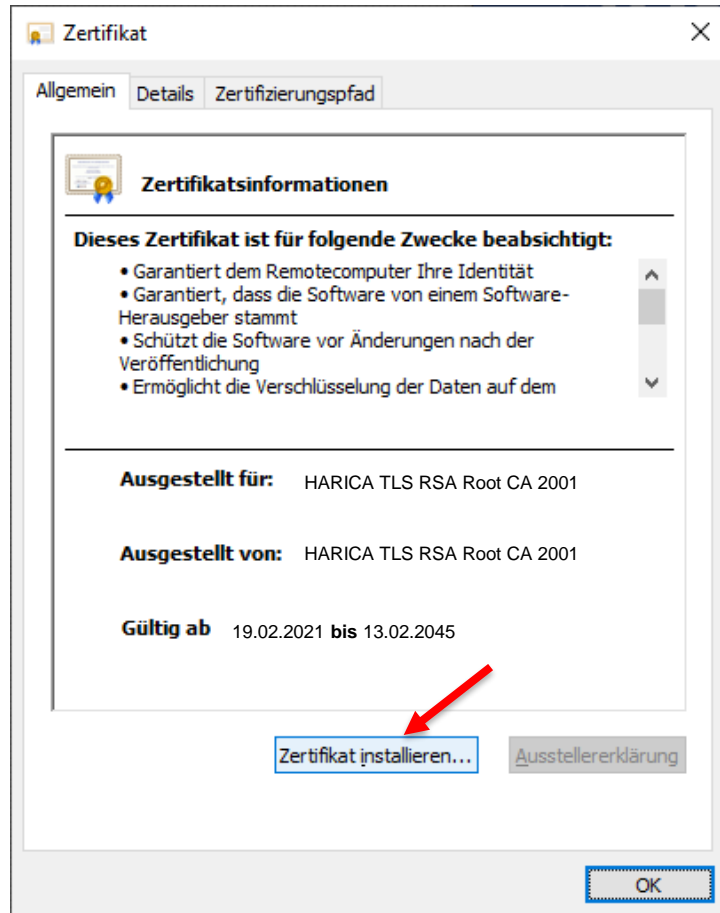
- Identity Management (IdM) Self Service

<https://www.idm.fau.de/>

- WLAN am RRZE

<https://www.rrze.fau.de/internet-e-mail/internet-zugang/wlan/>

# Exkurs: Wurzelzertifikat installieren



- Download des Wurzelzertifikats über folgenden Link:  
<https://crt.sh/?d=4147041876>
- Nach dem Download Doppelklick auf die Datei  
**„4147041876.crt“**
- Klick auf **„Zertifikat installieren...“**

# Exkurs: Wurzelzertifikat installieren

← 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

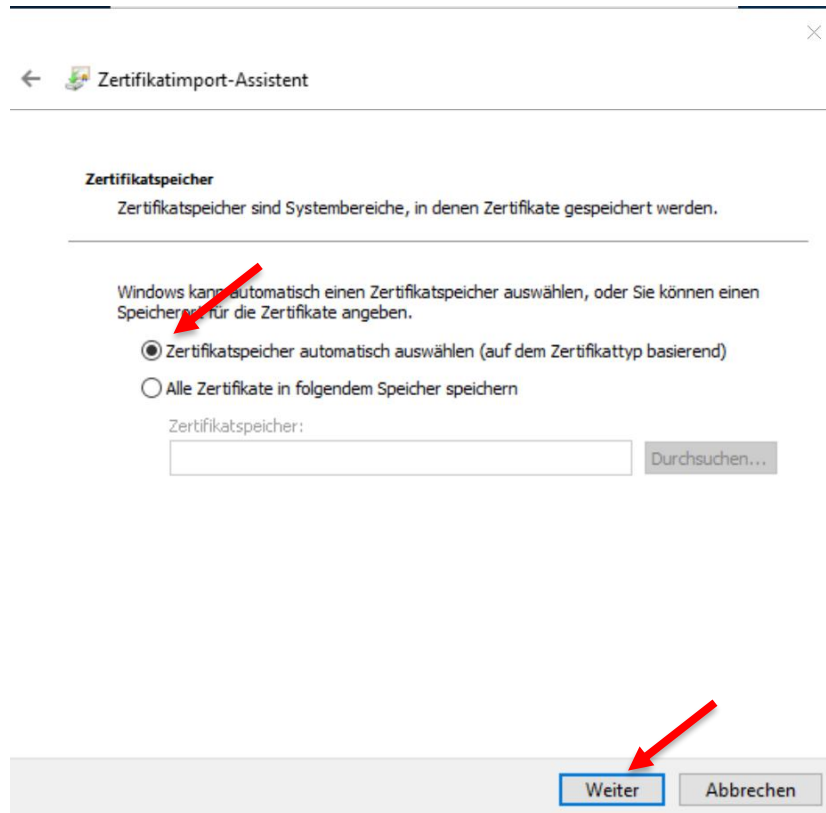
☐ Lokaler Computer

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

Weiter Abbrechen

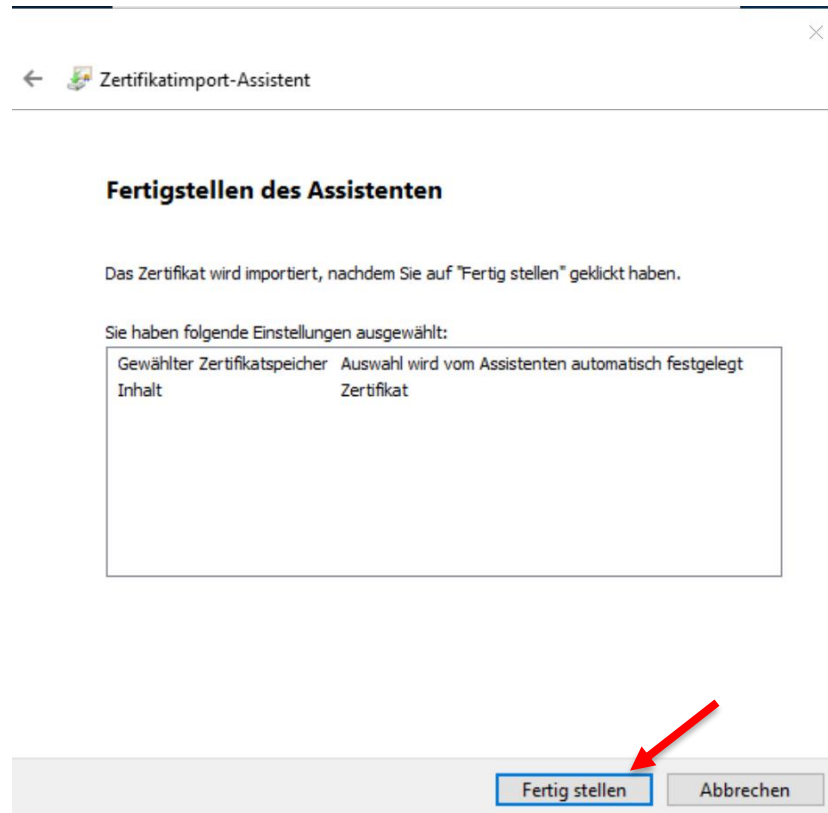
- Klick auf „**Weiter**“

# Exkurs: Wurzelzertifikat installieren



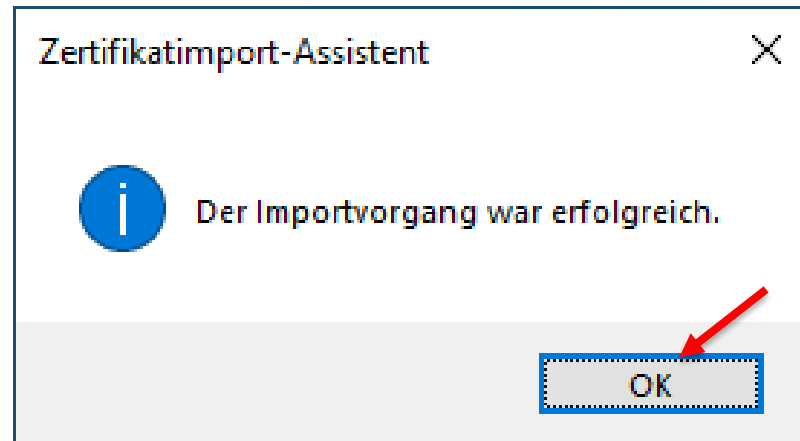
- Anwählen von „**Zertifikatspeicher automatisch auswählen**“
- Klick auf „**Weiter**“

# Exkurs: Wurzelzertifikat installieren



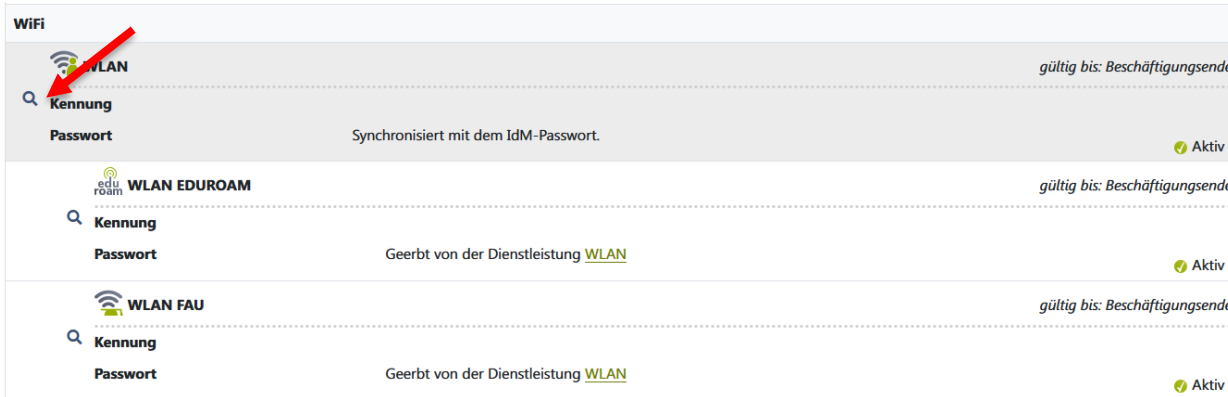
- Klick auf „Fertig stellen“

# Exkurs: Wurzelzertifikat installieren

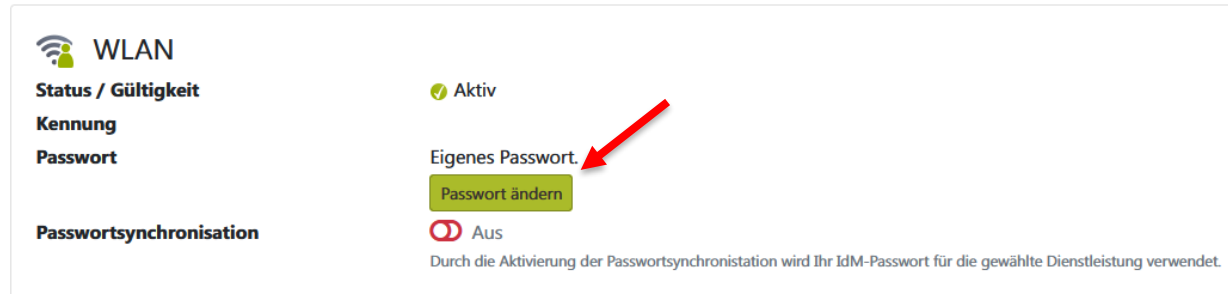
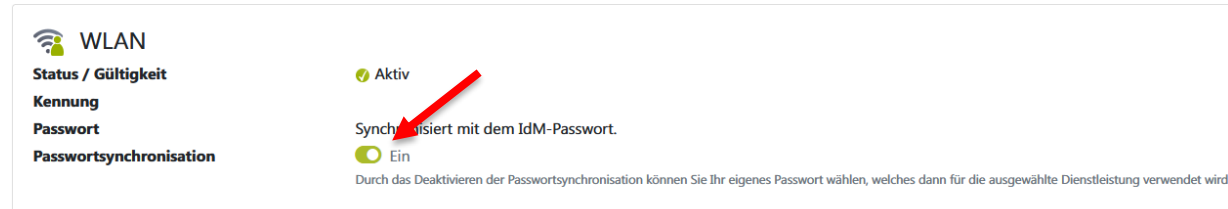


- Das Zertifikat wurde installiert
- [Hier geht es zurück zur Konfiguration](#)

# Exkurs: Passwortsynchronisation im IdM deaktivieren



## Dienstleistung: WLAN



[Zurück zur Übersicht](#)

## Exkurs: Passwortsynchronisation ändern:

- Im IdM-Portal unter Datenübersicht -> WiFi -> WLAN auf die Lupe klicken
- Dann „Passwortsynchronisation auf „Aus“ stellen
- „**Passwort ändern**“ wählen und ein neues Passwort für WLAN vergeben
- „**Passwort ändern**“ klicken damit die Änderung gespeichert wird
- Ihr WLAN-Passwort ist nun unabhängig vom IdM-Passwort