FORSCHUNGSZENTRUM JÜLICH GmbH
Jülich Supercomputing Centre

JuNet-IP Helpdesk, Tel. (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0408
Markus Meier, Thomas Schmühl
09.02.2023

Wireless-LAN im Forschungszentrum Jülich

1. Regelung

Das WLAN im Forschungszentrum Jülich ist in die bestehende Netzwerk-Infrastruktur auf dem Campus integriert. Alle Einrichtungen, die über eine Switch-basierte Verkabelung an das Campus-Netz angeschlossen sind, können am WLAN teilnehmen.

Als Schnittstelle zwischen Funk- und Kabelgebundenem Netz dienen Access-Points (APs). Die Installation, Konfiguration und das Monitoring der AP's erfolgt ausschließlich durch das JSC. Die Kosten der Hardwarebeschaffung trägt die jeweilige Einrichtung. Um einen stabilen und sicheren Betrieb weitestgehend sicherstellen zu können, dürfen keine anderen WLANs innerhalb des Campus installiert oder betrieben werden, weder mit noch ohne APs.

Das WLAN ist innerhalb des Campus nicht flächendeckend verfügbar. Die aktuelle Abdeckung des WLAN kann unter

https://junet-portal.fz-juelich.de/cgi-bin/public/wlan_abdeckung.cgi

eingesehen werden. Jeder in Reichweite befindliche WLAN-Adapter kann am WLAN teilnehmen.

Alle Regelungen des JuNet (https://intranet.fz-juelich.de/de/tools/interneregelungen/it-sicherheitsregeln_fuer_den_grundschutz_ir_119-1/) gelten analog auch für das WLAN innerhalb des Forschungszentrums. Es ist zu beachten, dass an einem Rechner die Kommunikation über das kabelgebundene JuNet und das WLAN nicht parallel betrieben werden dürfen, da hier Routing- und Sicherheitsprobleme entstehen können.

Auf dem Campus stehen verschiedene WLAN-Netze zur Verfügung. Gäste-Netze (SSIDs fzj, eduroam und fzjguest) für Besucher oder Mitarbeiter bieten uneingeschränkten Zugang zum INTERNET, regulieren aber durch die zentrale Firewall den Zugang zum internen Netz. Das Mitarbeiter-Netz (sfzj) bietet vollen Zugang zum internen Netz, so dass alle internen Dienste nutzbar sind.

1.1. SSID: fzj, Gäste-WLAN

Das Gäste-Netz `fzj` soll Besuchern und Mitarbeitern einen schnellen Zugang zum INTERNET bieten. Für nach außen (INTERNET) gerichtete Verbindungen gibt es so gut wie keine Einschränkungen. Die einzigen Einschränkungen resultieren aus Filterregeln, um akuten Sicherheitsbedrohungen entgegenzuwirken und werden je nach Bedarf angepasst. Die Kommunikation ins Intranet wird durch die zentrale Firewall gefiltert. Die erlaubten Kommunikationsbeziehungen basieren auf dem Regelwerk für Verbindungen vom INTERNET ins Intranet.

Das Gäste-Netz `fzj` verwendet keine Verschlüsselung, d.h. wenn auf höherer Schicht im OSI-Modell keine Verschlüsselung erfolgt, kann der Datentransfer leicht mitgelesen werden. Zugriff zum Gäste-Netz `fzj` wird allein durch die Authentifizierung der Hardware-Adresse des WLAN-Adapters reglementiert. Die Zuweisung der Netzwerkparameter erfolgt im Gäste-Netz dynamisch per DHCP.

1.2. SSID: sfzj, Mitarbeiter-WLAN

Seit Mitte 2008 steht in Teilen des Forschungszentrums ein Mitarbeiter-WLAN zur Verfügung. Die Nutzung interner Dienste ist hier ohne Hilfsmittel (wie z.B. VPN) möglich. Die Adressvergabe erfolgt statisch ausschließlich per DHCP mit festen Adressen aus dem offiziellen Klasse-B IP-Adressbereich des FZJ. Die Authentifizierung und Autorisierung geschieht sowohl auf Server- als auch auf Clientseite nach IEEE 802.1X Standard durch X.509 Zertifikate. Für eine sichere Übertragung werden die Daten mittels WPA2/AES verschlüsselt.

1.3. SSID: eduroam, WLAN-Zugang unterwegs

Durch die Teilnahme am eduroam-Dienst wird es Mitarbeitern des Forschungszentrums ermöglicht, unter Verwendung der persönlichen FZJ-Mailadresse mit zugehörigem Passwort, Zugang zum *eduroam*-WLAN (Internetzugang) an allen partizipierenden Organisationen zu erhalten. Der vom DFN

angebotene Roaming-Dienst DFN-Roaming ist inzwischen in die europäische Initiative eduroam eingebettet.

Umgekehrt können sich auch Gäste aus Einrichtungen, die an `eduroam` teilnehmen, im Forschungszentrum ohne die für Gäste sonst notwendige Registrierung durch einen FZJ-Mitarbeiter unmittelbar mit dem WLAN verbinden. Sie nutzen dabei die SSID `eduroam` und die von Ihrer Heimateinrichtung gewohnte Authentisierung. Einrichtungen, die an `eduroam` teilnehmen, sind untereinander auskunftspflichtig, so dass die Nutzer im Fall von Betriebsstörungen oder IT-Sicherheitsproblemen identifiziert werden können. Damit erfüllt dieser Dienst eine wichtige Voraussetzung für die Teilnahme innerhalb des JuNet.

> **Sicherheit: Vertraulichkeit**
>
> **Die Authentifizierung aller FZJ-Mitarbeiter erfolgt stets durch die Server des Forschungszentrums, sofern das teilnehmende WLAN-Gerät ordnungsgemäß konfiguriert ist.** Durch eine Ende-zu-Ende-Verschlüsselung der Authentifizierung (EAP-PEAP) zwischen WLAN-Gerät und Server im JSC ist die Vertraulichkeit gewährleistet. Für die Absicherung des Datenverkehrs sind die Verschlüsselungsmethoden WPA oder WPA2 vorgeschrieben.
> **Konfigurieren Sie Ihr WLAN-Gerät unbedingt wie in den folgenden Abschnitten beschrieben. Geben Sie Ihre Zugangsdaten E-Mail UserID und Passwort insbesondere niemals in andere Authorisierungssysteme wie z.B. Web-Zugangs-Portale ein.**

Mit der Teilnahme an `eduroam` verpflichten sich die Einrichtungen zur Einhaltung bestimmter Spielregeln (eduroam-Policy), die einen sicheren und störungsfreien Betrieb garantieren sollen. Dazu gehören neben der oben erwähnten Auskunftspflicht und der Ende-zu-Ende-Verschlüsselung auch, dass sich Nutzer bei Problemen zunächst an den Support in ihrer Heimateinrichtung wenden. Kontaktieren Sie daher bei Problemen immer zuerst einen Netzwerk-Ansprechpartner im JSC.

Weiter ist zu beachten, dass man sich in anderen Einrichtungen in einer fremden Netzwerkinfrastruktur befindet. Der erlaubte Netzwerkverkehr richtet sich daher nach den Regelungen der externen Einrichtung. Die eduroam-Policy empfiehlt aber, Standardanwendungen wie Web-Surfen zu ermöglichen.

1.4. SSID: fzjguest, Gäste-WLAN

Das WLAN fzjguest bietet Gästen einen schnellen Zugang zum INTERNET. Der Zugriff auf externe Services ist im Allgemeinen erlaubt. Der Zugriff ins Intranet wird durch die zentrale Firewall reglementiert. Die für den Zugriff notwendigen Berechtigungen (Coupons) können von jedem Mitarbeiter erstellt werden:

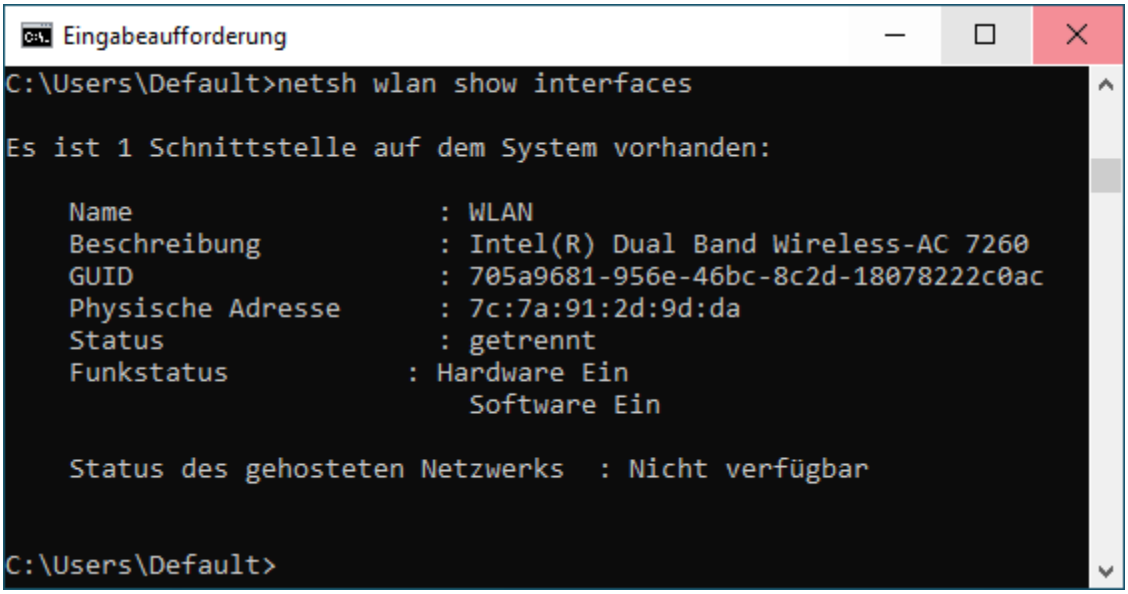
https://junet-portal.fz-juelich.de/wlan-fzjguest

2. Zugang

2.1. Windows 10

2.1.1. fzj

Um das WLAN-Gästenetz nutzen zu können muss die Physikalische Adresse des Drahtlos-Adapters wie in Kapitel 3.1 beschrieben registriert werden. Die Physikalische Adresse kann in der Windows Eingabeaufforderung mit dem Befehl `netsh wlan show interfaces` abgelesen werden:

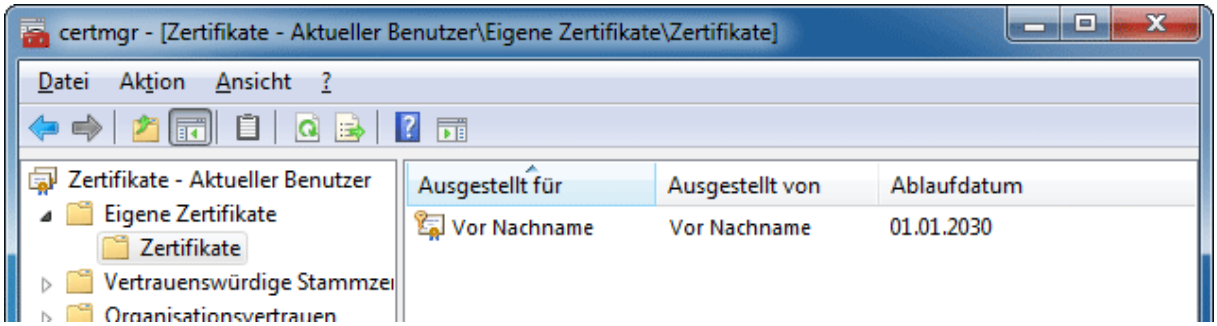


Wenn die entsprechende Adresse registriert ist, kann durch Auswahl des Drahtlosnetzwerkes `fzj` der Zugang hergestellt werden. (Windows 10 erkennt alle Parameter zum Gästenetz automatisch)

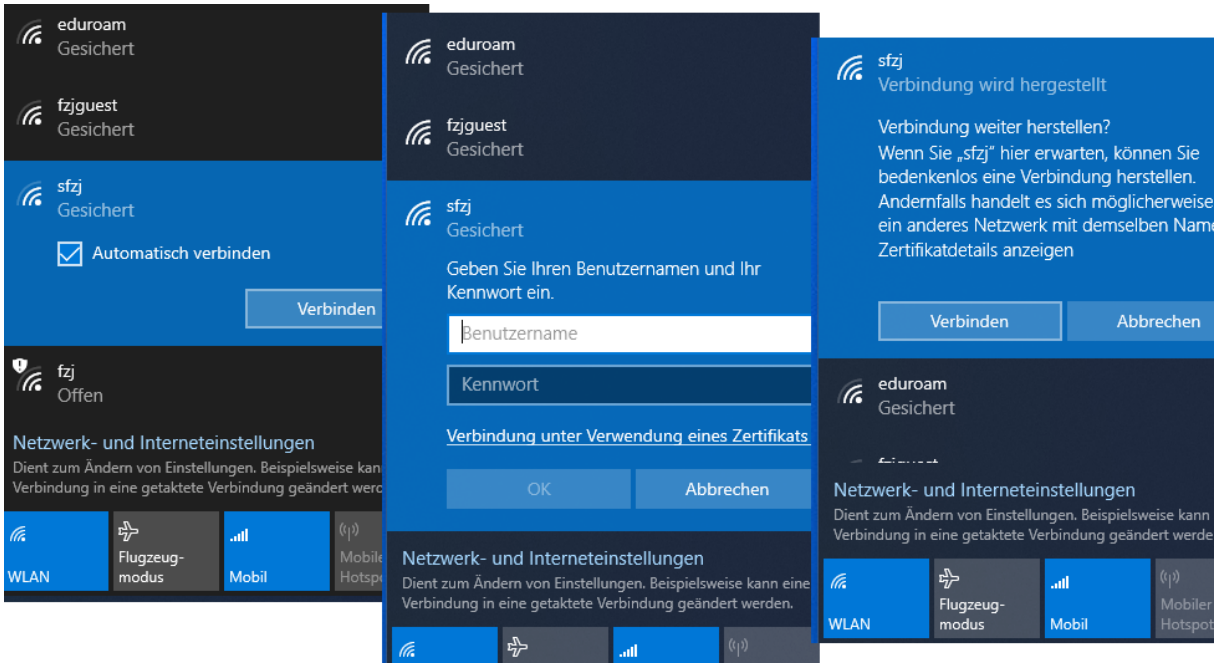
2.1.2. sfzj

Um das Mitarbeiter-WLAN unter Windows 10 nutzen zu können, müssen zunächst die unter Kapitel 3.2 beschriebenen Voraussetzungen erfüllt sein.

Die WLAN-Software unter Windows 10 nutzt zum Authentifizieren mit dem persönlichen Zertifikat den Zertifikatsspeicher des Systems. Falls das persönliche Zertifikat mitsamt Schlüssel dort noch nicht hinterlegt ist, importieren Sie es indem Sie auf die Schlüsselkontainer-Datei mit der Endung `p12` doppelklicken. Damit wird der Zertifikatimport-Assistent gestartet. Dabei sollen die default-Parameter nicht verändert werden. Im Zertifikat-Manager-Tool (ausführen: certmgr.msc) für den aktuellen Benutzer werden persönliche Zertifikate mit Schlüssel durch einen Schlüssel vor dem Namen angezeigt:

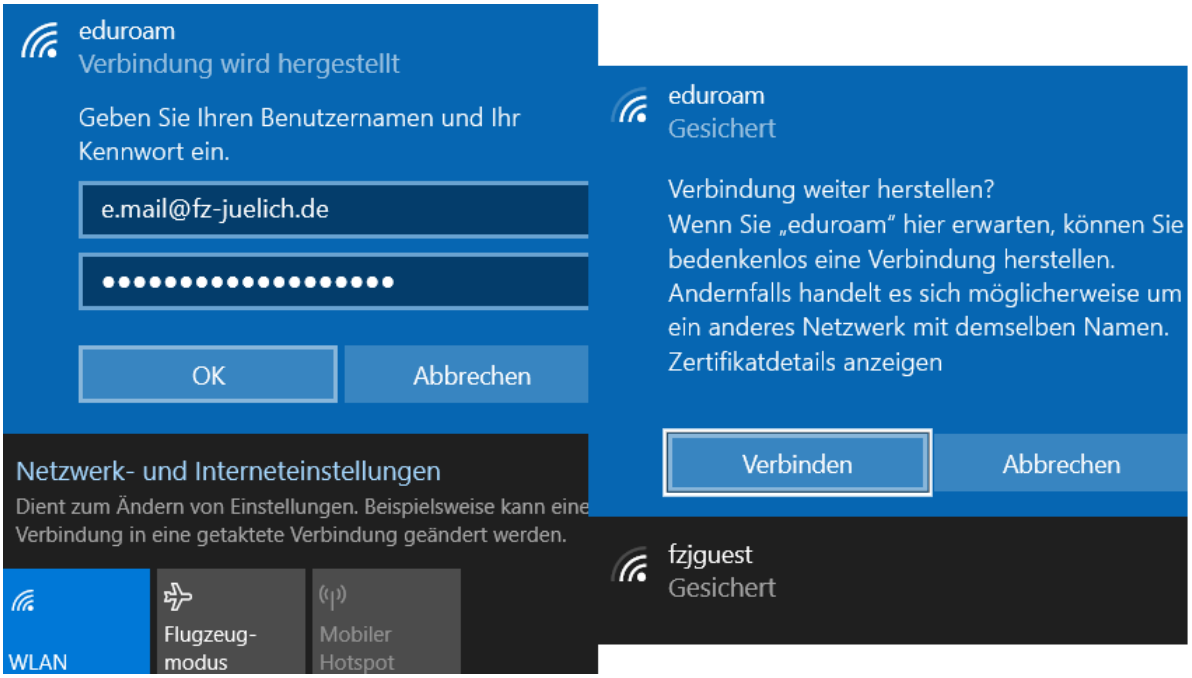


Damit die Verbindung mit sfzj hergestellt wird, wählen Sie bei sfzj `Verbinden` aus. Wenn ein persönliches Zertifikat vorliegt, bietet das System die Möglichkeit neben Benutzername und Kennwort die `Verbindung unter Verwendung eines Zertifikats herstellen` an. Windows 10 verwendet nach dessen Auswahl automatisch das zuletzt importierte gültige Zertifikat für die Authentifizierung und die Verbindung wird hergestellt.



2.1.3. eduroam

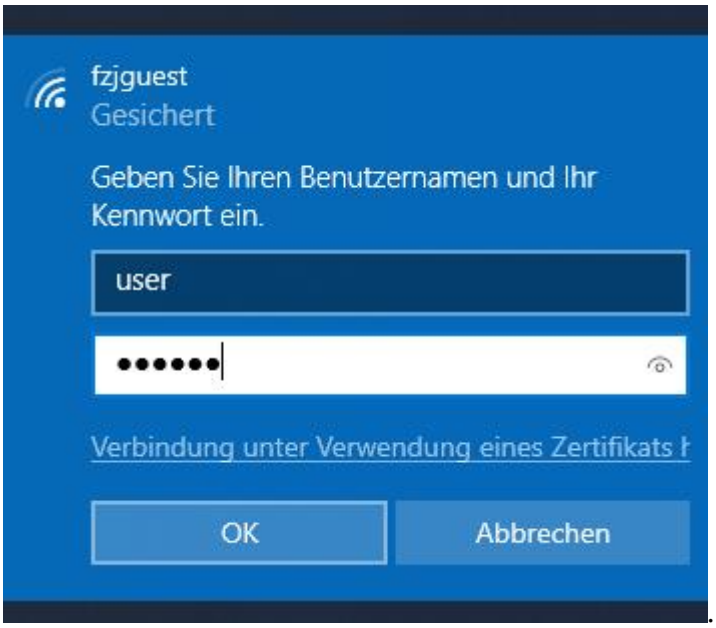
Nach Auswählen des WLANs *eduroam* müssen Benutzername (vollständige Mail-Adresse) und Kennwort (Passwort des Mailkontos auf dem zentralen Mailserver) entsprechend dem Screenshot angegeben werden. Windows 10 nutzt standardmäßig die passende Authentifizierungsmethode und stellt die Verbindung zum WLAN `eduroam` her.



Mit dieser Konfiguration ist der Zugriff auf das eduroam-WLAN bei allen teilnehmenden Einrichtungen möglich.

2.1.4. fzjguest

Nach Auswählen des WLANs *fzjguest* müssen Benutzername und Kennwort (aus dem Voucher) entsprechend dem Screenshot angegeben werden. Windows 10 stellt nach Bestätigung der Angabe die Verbindung mit der passenden Authentifizierungsmethode her.



2.2. Linux, GUI, am Beispiel von Ubuntu 18.04

2.2.1. fzj

Für eine Teilnahme am Gästenetz des FZJ ist es erforderlich, dass die Hardware-Adresse des Drahtlosnetzwerkadapters registriert ist. Auslesen kann man die Hardware-Adresse `addr` im Terminal mit dem Kommando `iw dev`

Ist die Adresse wie in Kapitel 3.1 beschrieben registriert, wird nach Auswahl des WLAN-Netzes fzj die Verbindung automatisch hergestellt. Die IP-Adressvergabe geschieht automatisch per DHCP.

```
user@hostname:~$ iw dev
phy#0
        Interface wlp4s0
                ifindex 3
                wdev 0x1
                addr aa:bb:cc:12:34:56
                type managed
                txpower 8.00 dBm
user@hostname:~$
```

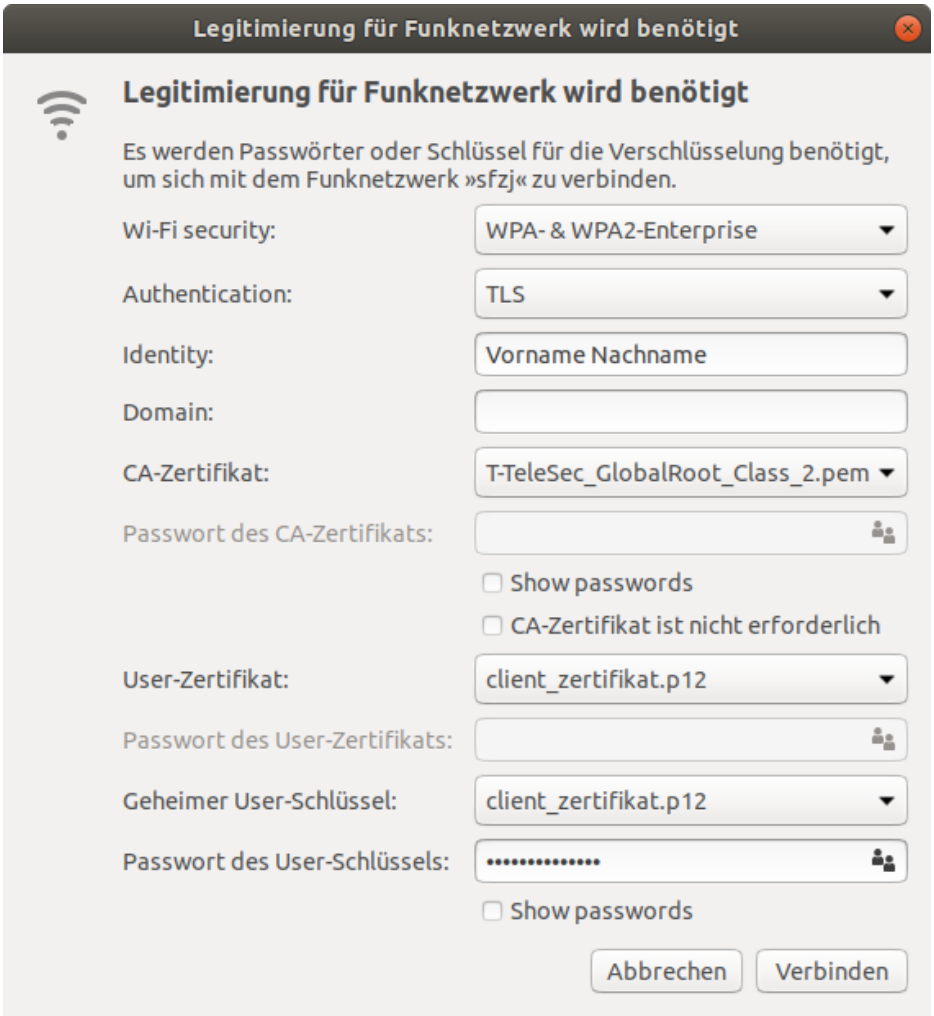
2.2.2. sfzj

Für die Teilnahme am sfzj-WLAN müssen zunächst die in Kapitel 3.2 beschriebenen Vorrausetzungen erfüllt sein.

Das Zertifikat muss als Zertifikatskontainer-Datei (hier client_zertifikat.p12) vorliegen. Des Weiteren muss das Wurzelzertifikat auf dem System hinterlegt werden:

https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.pem

Danach ist die Verbindung gemäß folgender Abbildung möglich. Als Identity ist zwingend der CN aus dem Zertifikat zu nehmen, der in der Regel aus Vor- und Nachname besteht.



2.2.3. eduroam

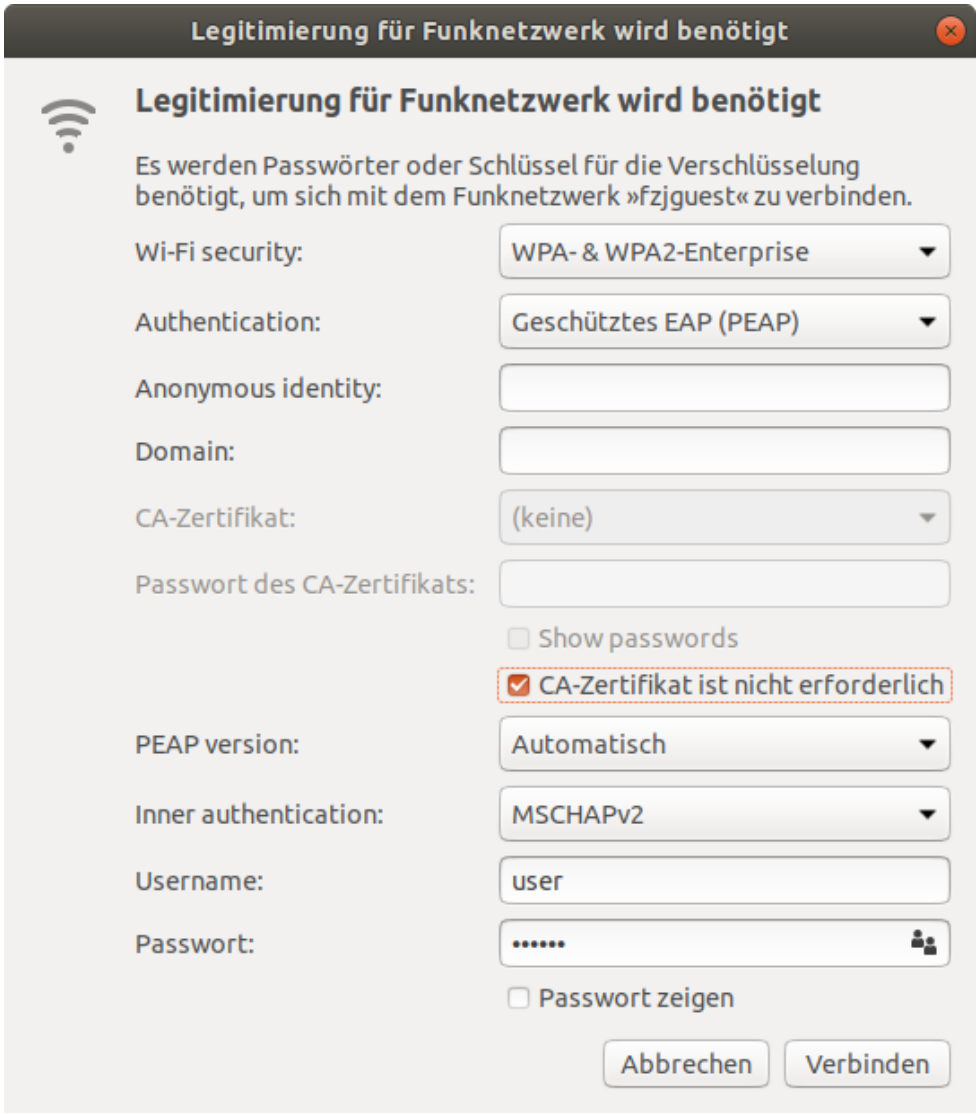
Zugang zum eduroam-WLAN bekommt jeder Mitarbeiter mit gültiger FZJ-Mailadresse ohne vorherige Anmeldung. Um die Vertraulichkeit zu gewährleisten muss zunächst das Wurzelzertifikat der DFN-PKI Global2 heruntergeladen werden:

https://go.fzj.de/wlan-eduroam-root-zertifikat

Danach kann die Verbindung gemäß den Einstellungen der folgenden Abbildung hergestellt werden. Der Username ist die Mail-Adresse inklusive `@fz-juelich.de`. Das Passwort ist das auf dem zentralen Mail-Server konfigurierte Passwort.

2.2.4. fzjguest

Für den Zugriff zum WLAN fzjguest werden Berechtigungen (Coupons) benötigt, siehe Kapitel 3.3. Anschließend ist der Zugriff analog zum folgenden Screenshot möglich.



2.3. Linux, CLI (wpa_supplicant)

Im folgenden Kapitel wird der Zugriff zum WLAN-Netzwerk des Forschungszentrums mit Linux im Allgemeinen beschrieben. Die Authentifizierung und Verschlüsselung der Kommunikation übernimmt der `wpa_supplicant`, die Adressvergabe erfolgt mittels `dhclient`. Das WLAN-Interface wird im Folgenden mit `wlan0` bezeichnet, der genutzte Treiber ist `wext` (müssen ggfs. angepasst werden).

1. Authentifizierung und Verschlüsselung

   ```
   sudo /usr/sbin/wpa_supplicant -c <conf-datei> -i wlan0 -D wext
   ```

2. Adressvergabe:

   ```
   sudo /sbin/dhclient wlan0
   ```

Die Konfigurationen für die einzelnen WLAN-Netze sind in den folgenden Unterkapiteln beschrieben.

2.3.1. fzj

Voraussetzung für den Zugriff zum Gäste-Netz ist die wie in Kapitel 3.1 beschriebene Registrierung der Hardware-Adresse des Funkadapters.

wlan_fzj.conf:

```
ctrl_interface=/var/log/wpa_supplicant
ap_scan=1

network={
      ssid="fzj"
      mode=0
      key_mgmt=NONE
}
```

2.3.2. sfzj

Für die Teilnahme am Mitarbeiter-WLAN müssen zunächst die unter Kapitel 3.2 beschriebenen Voraussetzungen erfüllt sein.

Liegt das persönliche Zertifikat als PKCS12-Datei vor (Endung .p12), muss man zunächst den Zertifikatsanteil `client.crt` und den privaten Schlüssel `client.key` extrahieren. Dies erfolgt mit zwei openssl Befehlen:

```
openssl pkcs12 -in zertifikat.p12 -clcerts -nokeys -out client.crt
openssl pkcs12 -in zertifikat.p12 -nocerts -out client.key
```

Die Parameter `identity`, `ca_cert` `client.cert`, `private_key` und `private_key_passwd` sind anzupassen. Das Feld `identity` muss dabei dem DN (distinguished name) des Zertifikates entsprechen.

Ab dem 9.7.2019 wird ein Zertifikat aus der Global-2 Hierarchie verwendet. Das passende Wurzelzertifikat kann unter folgendem Link heruntergeladen werden:

https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.pem

wlan_sfzj.conf:

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
        ssid=”sfzj”
        mode=0
        proto=WPA2
        key_mgmt=WPA-EAP
        eap=TLS
        identity=”Markus Meier”
        ca_cert=”/home/m.meier/wlan/global_ca_cert_telekom.pem”
        client_cert=”/home/m.meier/wlan/client.crt”
        private_key=”/home/m.meier/wlan/client.key”
        private_key_passwd=“xyz“
}
```

2.3.3. eduroam

Die Einträge `identity`, `password` und `ca_cert` in der Konfigurationsdatei müssen angepasst werden. Ab dem 09.02.2023 ist das das Wurzelzertifikat „AAAServices“. Dies kann unter https://go.fzj.de/wlan-eduroam-root-zertifikat runtergeladen werden.

Wlan_eduroam.conf:

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1
network={
        ssid="eduroam"
        proto=WPA2
        key_mgmt=WPA-EAP
        eap=PEAP
        identity="e.mail@fz-juelich.de"
        password="secret"
        ca_cert="AAAServices"
       phase2="auth=MSCHAPV2"
 }
```

2.4. Apple Mac OS X

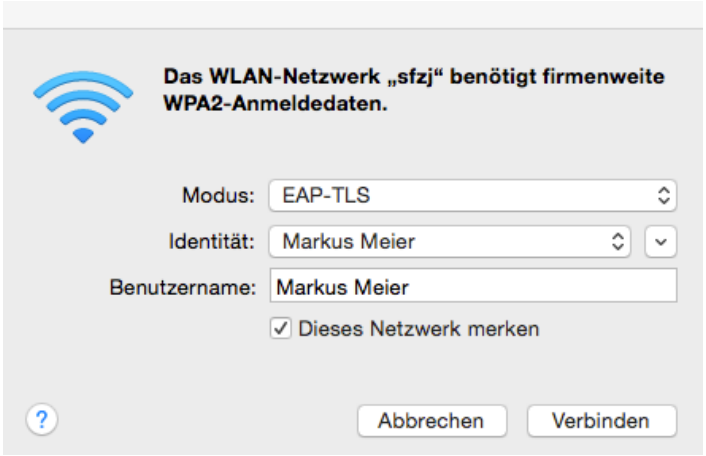
Die hier vorgestellte Anleitung bezieht sich auf OS X 10.10 (Yosemite) bzw 10.12 (Sierra).

2.4.1. fzj

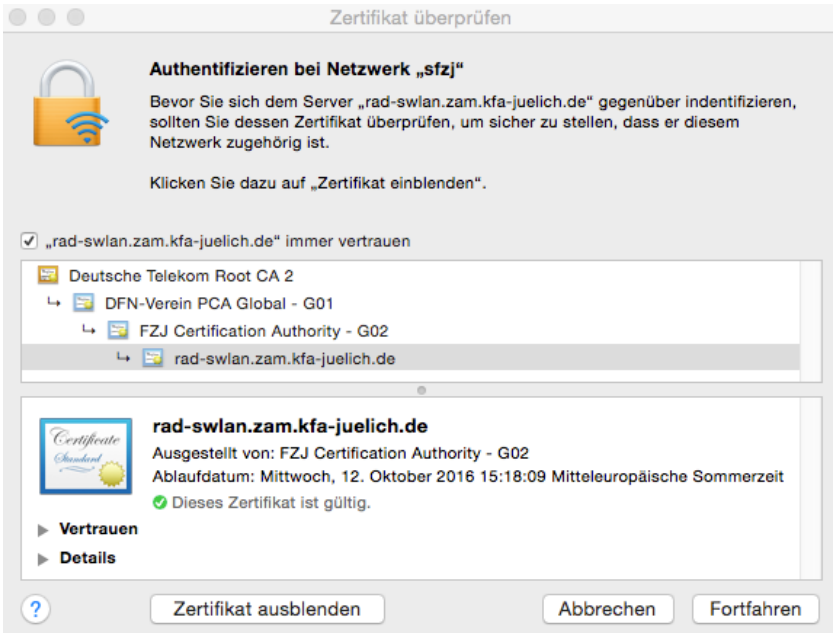
Für den Zugang zum Gäste-WLAN muss zunächst die Hardware-Adresse des Funkadapters, wie in Abschnitt 3.1 beschrieben, registriert werden. Diese kann in der *Systemeinstellung Netzwerk* unter *Weitere Optionen* abgelesen werden. Nach erfolgreicher Registrierung ist der Zugriff durch Auswahl der entsprechenden SSID, `fzj`, möglich. Die entsprechenden Verbindungsparameter für das Gäste-WLAN werden vom MacOS automatisch erkannt.

2.4.2. sfzj

Für die Teilnahme am Mitarbeiter-WLAN müssen zunächst die unter Kapitel 3.2 beschriebenen Voraussetzungen erfüllt sein. Als nächstes muss das persönliche Zertifikat mit dem zugehörigen privaten Schlüssel im *Schlüsselbund Anmeldung* auf dem System hinterlegt werden. Danach ist der Zugang, wie auf den folgenden Screenshots zu sehen ist, durch Auswahl des *sfzj*-WLANs und Angabe des Zertifikatnamens möglich.



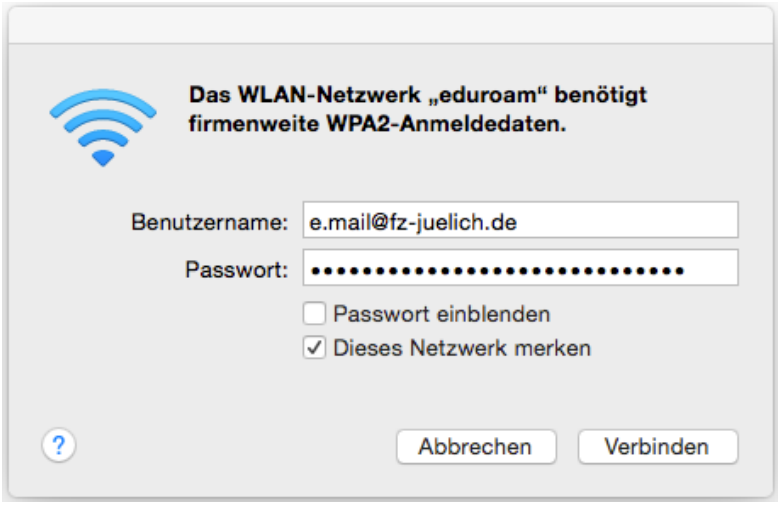
Im Authentifizierungsprozess muss einzig dem Server „rad-swlan.zam.kfa-juelich.de“ vertraut werden. Sollte zu einem späteren Zeitpunkt ein abweichender Server angezeigt werden, ist der Anmeldevorgang unmittelbar abzubrechen.



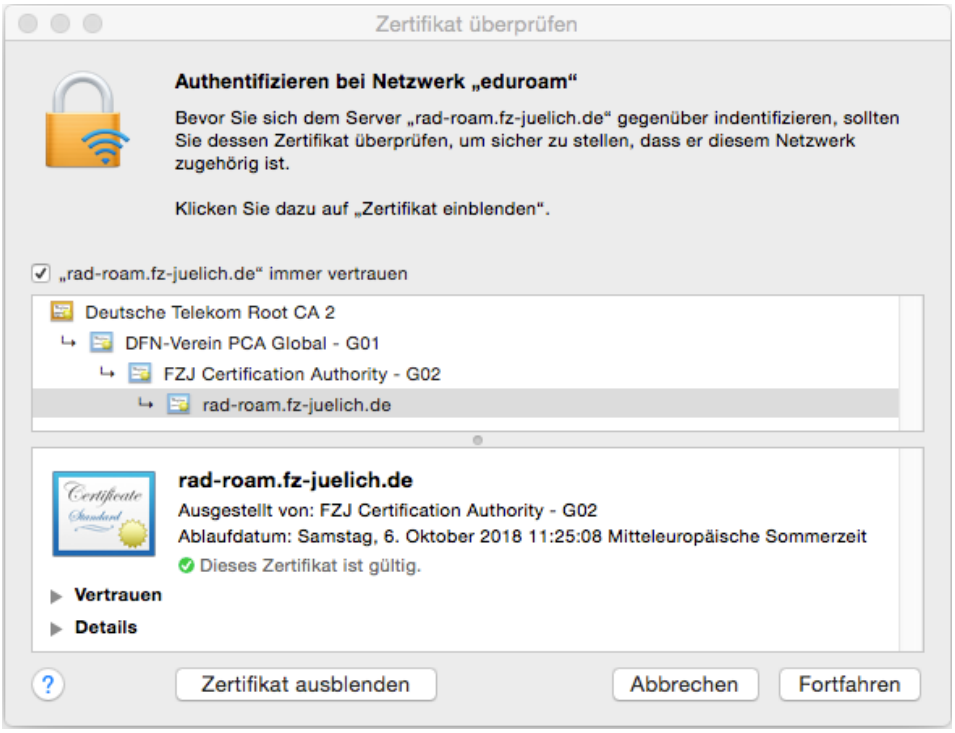
Am 9.7.2019 wird das Serverzertifikat getauscht, welches unter der Global-2 Hierarchie geführt (Wurzelzertifikat: T-Telesec Global Root Class 2)

2.4.3. eduroam

Der Zugriff zum *eduroam*-WLAN ist durch Eingabe der vollständigen Mail-Adresse und des auf dem zentralen Mail-Server gespeicherten Passwortes direkt möglich (siehe Fenster):



Um die **Vertraulichkeit** zu gewähren **MUSS** darauf geachtet werden, dass einzig dem Server „rad-roam.fz-juelich.de“ das Passwort übermittelt werden darf. Ab dem 09.02.2023 ist das das Wurzelzertifikat "AAAServices". . Beim ersten Verbindungsversuch wird das entsprechende Zertifikat angezeigt: (Screenshot noch nicht aktuell)



Sollte zu einem späteren Zeitpunkt ein abweichendes Zertifikat zum Authentifizieren angezeigt werden, ist der Vorgang unmittelbar abzubrechen, um keinem Dritten das Mail-Passwort zu übermitteln.

2.4.4. fzjguest

Nach Auswahl des WLANs fzjguest ist der Zugriff durch Eingabe der Parameter gemäß fogendem Screenshot direkt möglich:

Gegebenenfalls muss noch die Vertrauenswürdigkeit des Authentifizierungsservers „rad-guestwlan.fz-juelich.de“ bestätigt werden.

2.5. Apple iOS

Die Konfiguration und Screenshots beziehen sich auf die iOS Version 8.1.2.

2.5.1. fzj

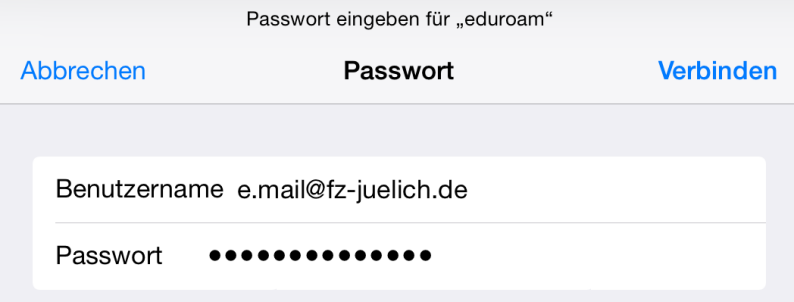
Um Zugang zum Gäste-Netz des FZJ zu bekommen ist es notwendig, die Hardware-Adresse des Gerätes zu registrieren (Kapitel 3.1). Die Hardware-Adresse kann in den *Einstellungen -> Allgemein -> Info* unter *WLAN-Adresse* ausgelesen werden. Nach erfolgreicher Registrierung ist der Zugang durch Auswahl des Netzes `fzj` ohne weitere Einstellungen möglich.

2.5.2. sfzj

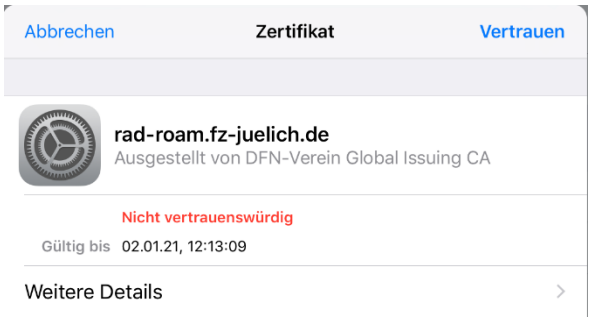
Der Zugang zum Mitarbeiter-WLAN *sfzj* ist für Apple iOS-Geräte nicht vorgesehen!

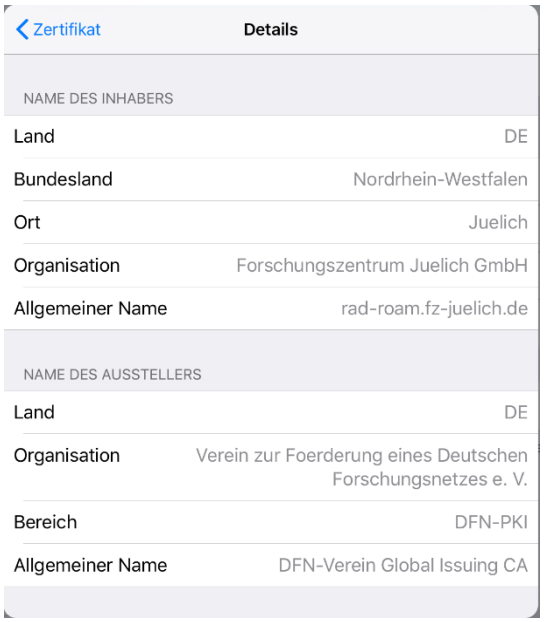
2.5.3. eduroam

Zugang zum *eduroam*-WLAN erhält man nach Auswahl des entsprechenden WLANs durch Eingabe der vollständigen Mail-Adresse mit dem auf dem zentralen Mail-Server gespeicherten Passwortes. Alle notwendigen Verbindungsparamater werden automatisch erkannt.



Es ist zwingend darauf zu achten, dass **NUR** der Server **rad-roam.fz-juelich.de** (Ab dem 09.02.2023 ist das das Wurzelzertifikat "AAAServices") als Authentifizierungsserver auftreten darf: (Screenshot nicht aktuell)





Sollte zu einem späteren Zeitpunkt ein alternativer Server Authentifizierungsanfragen entgegennehmen **MUSS** der Vorgang unmittelbar abgebrochen werden, um keinem Externen das Mailpasswort zu senden.

2.5.4. fzjguest

Der Zugang zum fzjguest-WLAN kann nach Auswahl des entsprechenden WLANs gemäß folgendem Screenshot hergestellt werden:

Im Folgendem muss nur noch die Vertrauenswürdigkeit des Authentifizierungsservers bestätigt werden.

2.6. Android

Konfiguration und Screenshots beziehen sich auf Android Firmware Version 9.

2.6.1. fzj

Zunächst muss die Hardware-Adresse des WLAN-Chipsatzes, wie in Kapitel 3.1 beschrieben, registriert werden. Die Hardware-Adresse findet man im Menü <Über das Telefon> unter dem Punkt <WLAN-MAC-Adresse>. Danach ist eine Verbindung durch Auswahl des WLANs sofort möglich.

2.6.2. sfzj

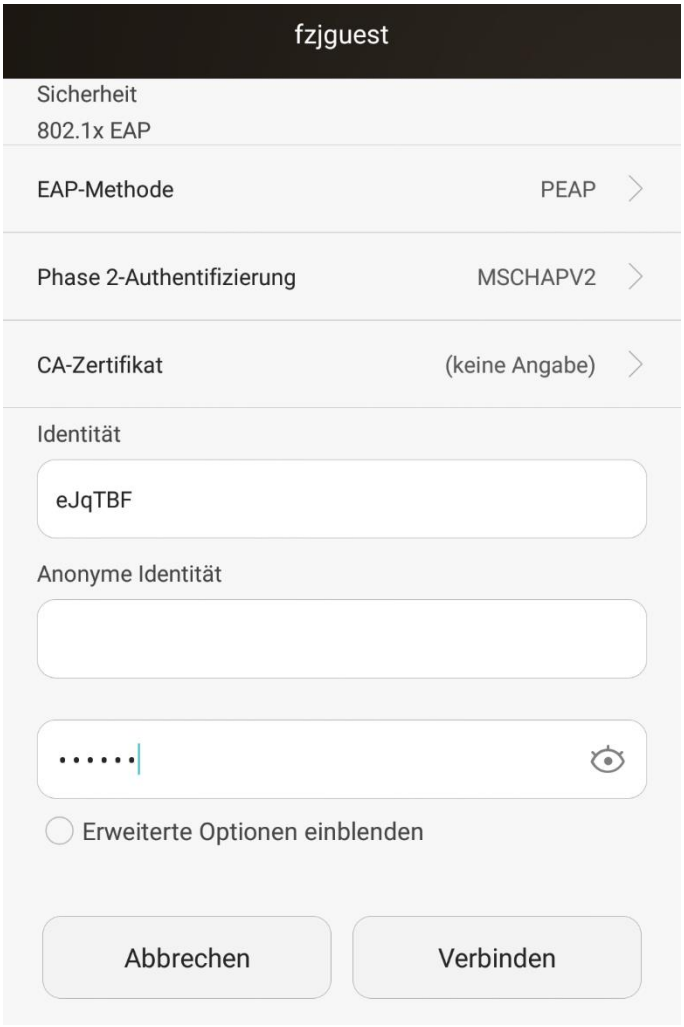
Der Zugang zum Mitarbeiter-WLAN *sfzj* ist für Android-Geräte nicht vorgesehen!

2.6.3. eduroam

Um eine Verbindung mit dem eduroam-WLAN herzustellen konfigurieren Sie ihr Smartphone gemäß unten abgebildeten Screenshot:

2.6.4. fzjguest

Folgender Screenshot zeigt den Zugriff zum WLAN fzjguest mit einem Android Betriebssystem:



Es sind die drei Parameter „Phase-2-Authentifizierung“ Identität und Passwort entsprechend anzupassen.

2.7. Allgemein

WLAN-SSID	fzj	sfzj	eduroam	fzjguest
Authentifizierung	Hardware-Adresse	TLS persönliches Zertifikat	PEAP	PEAP
Authentifizierung Phase2	-	-	MSCHAPv2 User: Mail-Adresse Password: Mail-Passwort	MSCHAPv2
Roaming-Identität:	-	-	anonymous@fz-juelich.de	-
Verschlüsselungs-Methode	Keine	WPA2 (oder WPA)	WPA2	WPA2
Verschlüsselung-Algorithmus	Keine	AES	AES	AES
Vertrauenswürdige CA		T-Telesec Global Root Class 2	T-Telesec Global Root Class 2	AAAServices
Servername:		rad-swlan@fz-juelich.de	rad-roam.fz-juelich.de	rad-guestwlan.fz-juelich.de

3. Anhang

3.1. Registrierung der Hardware-Adresse für das WLAN fzj

Für die Teilnahme am Gäste-Netz des Forschungszentrums muss die Hardware-Adresse des Clients registriert werden. Über die Seite

https://junet-portal.fz-juelich.de/cgi-bin/public/wlan_fzj.cgi

können unbefristete Zugänge für Mitarbeiter, befristete Gastzugänge oder Zugänge für Tagungsteilnehmer eingerichtet werden. Die Autorisierung erfolgt über einen Einmal-Link, welcher zu einer frei wählbaren offiziellen FZJ-Mail-Adresse geschickt wird. Dieser Einmal-Link ist nur eine begrenzte Zeit gültig und wird benutzt, um die Anmeldung abzuschließen. Nach erfolgreicher Registrierung ist der Zugriff spätestens nach 15 Minuten möglich.

Für eine unbefristete Nutzung muss ein Formular, welches bei der Anmeldung angezeigt wird, ausgedruckt und unterschrieben an das Dispatch des JSC geschickt werden.

Sollen für Workshops oder Tagungen diverse Hardware-Adressen registriert werden, so bietet es sich an, einen Zugang für Tagungsteilnehmer einzurichten. Man erspart sich hierbei das Bestätigen jeder einzelnen Hardware-Adresse per Mail. Stattdessen definiert man ein frei wählbares Passwort mit dem dann beliebig viele Hardware-Adressen für einen fest definierten Zeitraum freigeschaltet werden können.

3.2. Voraussetzung für die Teilnahme am Mitarbeiter-WLAN

Für die Nutzung des Mitarbeiter-WLAN müssen die folgenden Eigenschaften erfüllt sein.

I. Für die Authentifizierung des Teilnehmers muss ein gültiges Client-Zertifikat aus der Global-Hierarchie des Forschungszentrums vorliegen. Sollte noch kein gültiges oder nutzbares[1] Nutzerzertifikat vorliegen kann dies auf der folgenden Seite beantraget werden:

   https://pki.pca.dfn.de/dfn-pki/dfn-ca-global-g2/2100

II. Um nur autorisierten Personen Zugang zum Mitarbeiter-WLAN zu ermöglichen, muss das Zertifikat über eine Web-Schnittstelle registriert werden:

   https://junet-portal.fz-juelich.de/cgi-bin/public/auth/junet_reg_zert.cgi

III. Um eine feste IP-Adresszuordnung zu gewährleisten, muss der WLAN-Adapter in der JuNet-Datenbank registriert sein.

   Befindet sich das Gerät schon in der JuNet-Datenbank, steht folgendes Formular zur Verfügung:

   https://junet-portal.fz-juelich.de/junet-aenderung/

   Unter „sonstige Fragen, Wünsche, Bemerkungen“ einen kurzen Begleittext einfügen, wie z.B. „Diese Maschine bitte für das Mitarbeiter-WLAN anmelden: Die Mac-Adresse des WLAN-Adapters lautet: XX-XX…“

   Für eine Neu-Anmeldung des Gerätes das JuNet-Anmeldungsformular benutzen:

   https://junet-portal.fz-juelich.de/junet-anmeldung/

3.3. Erstellen von Zugangsberechtigungen / Coupons für das WLAN fzjguest

Auf folgender Web-Seite können alle Mitarbeiter des Forschungszentrums einen oder mehrere Zugangsberechtigungen (Coupons) für das WLAN fzjguest anlegen.

[1] Unter Windows (XP, Vista, 7) ist ein Zertifikat mit dem Verwendungszweck „Smartcard-Anmeldung“ nicht nutzbar.

https://junet-portal.fz-juelich.de/wlan-fzjguest

Die Gültigkeit der Coupons ist wählbar zwischen 3 und 45 Tagen. Spätestens 10 Minuten nach Erstellen sind die Coupons aktiv. Ein Coupon bietet Zugang für genau ein Device. Wir sind dazu verpflichtet am Netz befindliche Geräte bei Bedarf einer Person zuordnen zu können. Die Zuordnung eines Coupons zu einem Gast muss mindestens noch eine Woche nach Ablauf zurückverfolgt werden können. Dazu muss der Name des Gastes auf dem Mitarbeiter-Teil des Coupons notiert werden. Den Gäste-Teil können Sie abtrennen und dem Gast aushändigen.

4. Problembehandlung

4.1. Zertifikatsimportierung unter Windows

Bei der Importierung eines Zertifikates unter Windows darf die Option „Hohe Sicherheit für den privaten Schlüssel aktivieren. …“ nicht gewählt werden. Der WLAN-Supplicant bietet keine Möglichkeit zur Eingabe des Passworts des privaten Schlüssels an. Somit könnte dann keine Authentifizierung stattfinden.