

Änderung WLAN-Authentifizierung



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Free Roaming



[Quelle] geant

- Um was geht es?
- Wie ist es entstanden?
- Was ist das Problem?
- Was wird geändert?



once upon a time ...

Ursprünglich was das WLAN der TU auf den Campus beschränkt. Der Login geschah deshalb über die NDS-Accounts, später mit der TU-ID.

- .user.hrz.tu
- Stud_tud
- TU-ID

Dann kam eduroam an die TU und damit der Login

TU-ID@tu-darmstadt.de bzw. anonymous@tu-darmstadt.de

was ist das Problem?

eduroam kam zusätzlich zu dem vorhandenen WLAN. Also gingen die alten Wege auch noch

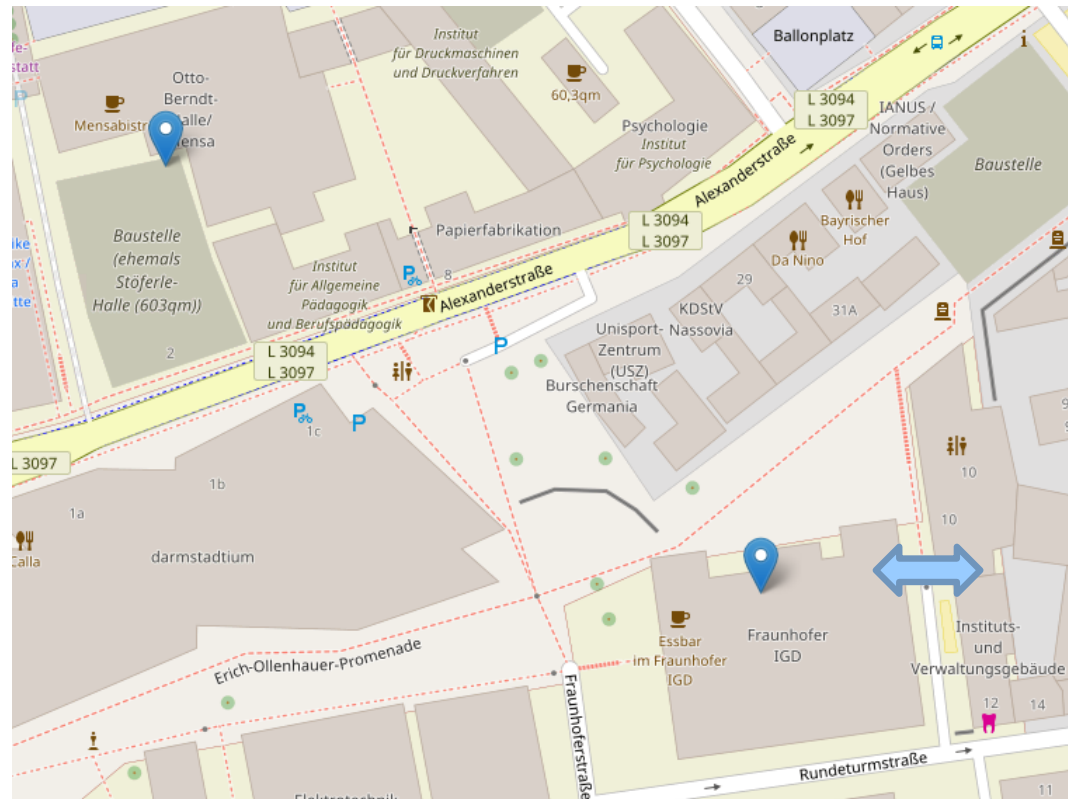
Erst nur ein Problem Weniger: Reisende hatten Probleme, wenn sie an eine Gastuni kamen: bei mir geht es doch mit TU-ID im eduroam der TU. Warum nicht hier?

@tu-darmstadt.de fehlt....

Inzwischen ist es schlimmer – eduroam ist gewachsen, so dass man auch auf dem Campus andere Einrichtungen sehen kann, Kooperation mit anderen Unis hat stark zugenommen

eduroam in Darmstadt

- TU im gesamten Stadtgebiet mit Darmstadtium, Anmietungen, Wohnheime, ...
 - h_da
 - FhG/IGD
- Alle haben die gleiche SSID



Ist das alles?

Nein – Die Authentifizierungsserver weisen sich mit einem Zertifikat aus. Das tragen aber nur paranoide Zeitgenossen freiwillig ein.

Daher:

eduroam configuration assistent tool

<https://cat.eduroam.de/>

Das macht alles automatisch, auch das Zertifikat und die CA.

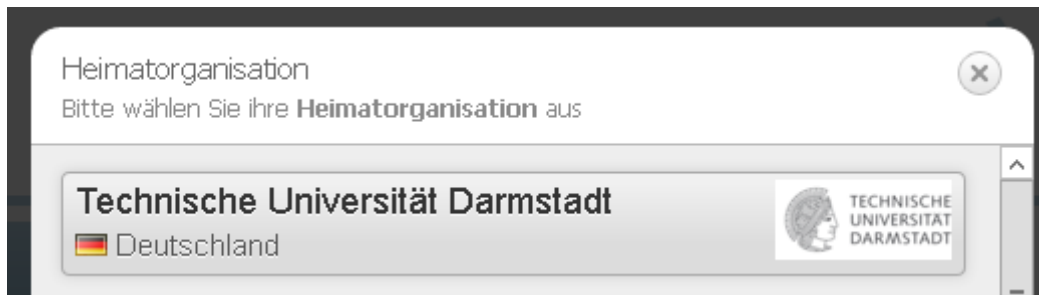
Änderungen ab dem Wintersemester

Authentifizierung ohne Realm (@tu-darmstadt.de) soll zum Wintersemester abgeschaltet werden.

Authentifizierung ohne TU-ID wird mit der Umstellung des eDirectories wegfallen.

was ist zu tun?

<https://cat.eduroam.de/>



Wählen Sie einen Installer zum Herunterladen



Fragen?



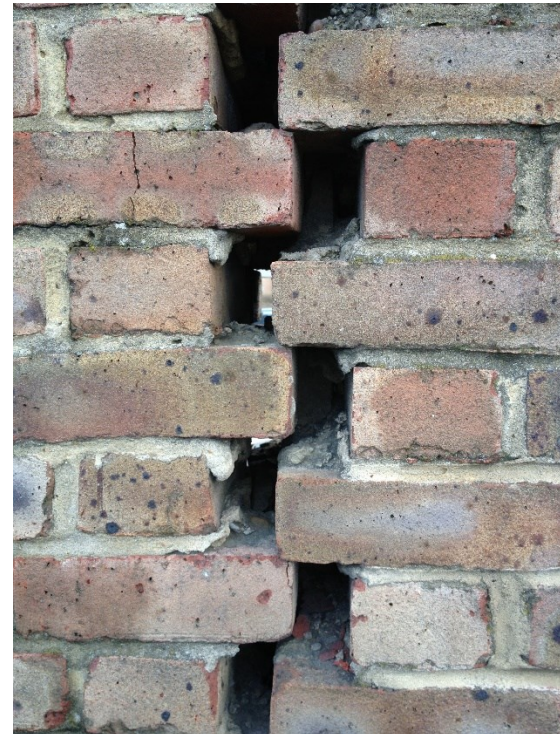
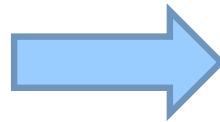
TECHNISCHE
UNIVERSITÄT
DARMSTADT



Firewall-Änderungen



TECHNISCHE
UNIVERSITÄT
DARMSTADT



- Um was geht es?
- Wie war es bisher?
- Was ist das Problem?
- Was wird geändert?

Wie war es bisher?

Über die Rechneranmeldung wurden IPv4 und IPv6-Adressen angemeldet.

Für alle gibt es einen „Grundschutz“^[1]

Bei IPv4 wurden nur bekannte Adressen für eingehenden und ausgehenden Verkehr freigegeben.

Bei IPv6 konnte das wegen der Privacy-Extension nicht umgesetzt werden, IPv6 war daher bislang ungeschützt

[1] <https://www.hrz.tu-darmstadt.de/itsicherheit/regelwerke/filterregelnfirrewall.de.jsp>

Das Problem:

Bei **IPv4** ging nur frei oder gesperrt.

Manche Rechner sollen nur Updates holen können oder im Internet surfen (Pools). Abhilfe bisher: kein Internetzugang und Nutzung des WWW-Proxy. Der Proxy ist veraltet.

Bei **IPv6** war mit diesem Modell kein Schutz möglich, da sich die Absende-Adressen durch die Privacy-Extension ändern können.

Was wird geändert?

Lösung: alles geht, nichts muss:

Es wird eine Berechtigung „O“ geben, in der nur ausgehender Verkehr zugelassen wird.

Dies sollte die künftige Standardeinstellung sein, nur Server benötigen ein „J“
Aktivierung voraussichtlich am 9.10.2017

Achtung: Nicht angemeldete IPs in v4: „N“, in v6: „O“

Internetzugang	N	O	J
IPv4 in	block	block	pass
IPv4 out	block	pass	pass
IPv6 in	block	block	pass
IPv6 out	block	pass	pass

Was muss ich tun?

- Bei der Rechneranmeldung sollte künftig bei IPv6 und IPv4 „O“ beim Internetzugang für Clients gewählt werden.
- Server sollten mit einer festen IP versehen werden und den Internetzugang „J“ erhalten
- Alle anderen sollten mit „N“ angemeldet werden
- **Stichtag im Auge behalten!**

Internetzugang	N	O	J
IPv4 in	block	block	pass
IPv4 out	block	pass	pass
IPv6 in	block	block	pass
IPv6 out	block	pass	pass

Vielen Dank

Fragen?

