Neue Radius-Umgebung für eduroam

Dr.-Ing. Andreas Bischoff
Zentrum für Informations- und Mediendienste
Universität Duisburg-Essen

WLAN –Sicherheit eduroam

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- Das Root-Zertifikat „Deutsche Telekom Root CA2“ läuft im Juli 2019 ab. Das damit unterschriebe Radius-Zertifikat der UDE läuft am 31.5.2019 ab. Korrekt konfigurierte eduroam-Klienten werden sich dann nicht mehr über die Radius-Server authentifizieren können.
- Um einen harten Termin zu vermeiden, an dem sämtliche eduroam Klienten zwingend umkonfiguriert werden müssen, ist ein Parallelbetrieb neuer und alter Zertifikate realisiert worden.

WLAN –Sicherheit eduroam

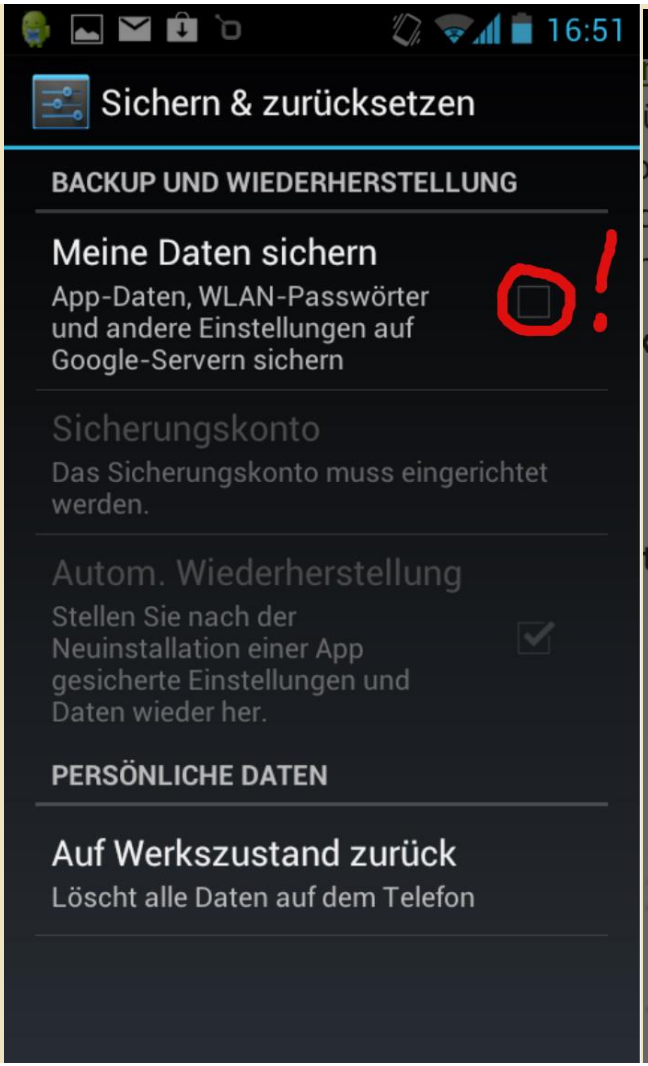
UNIVERSITÄT DUISBURG ESSEN

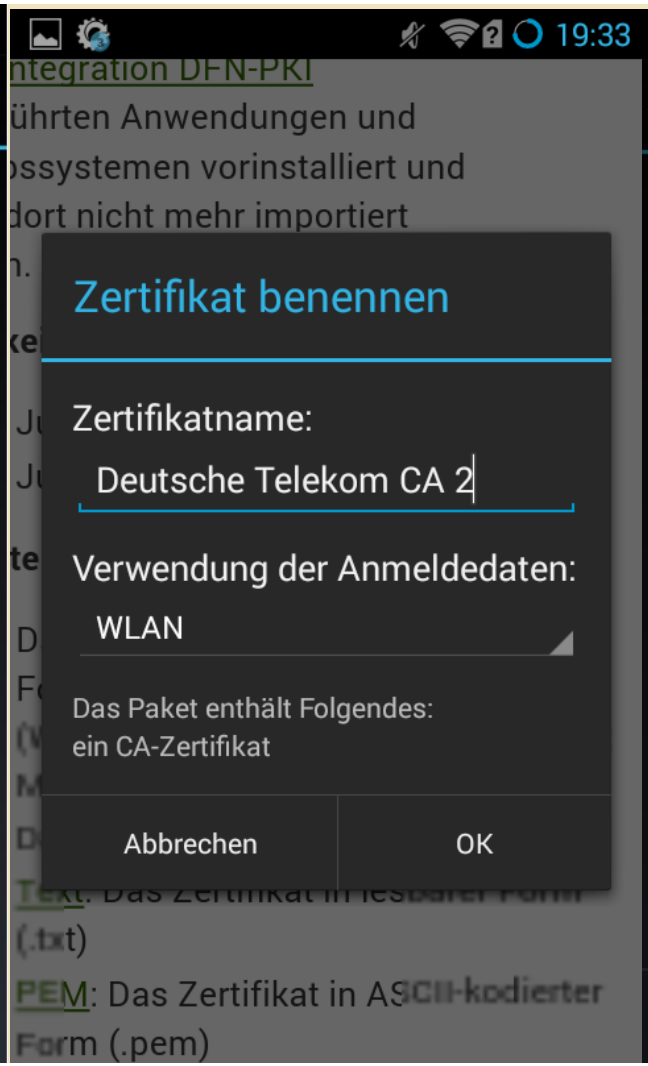
Offen im Denken

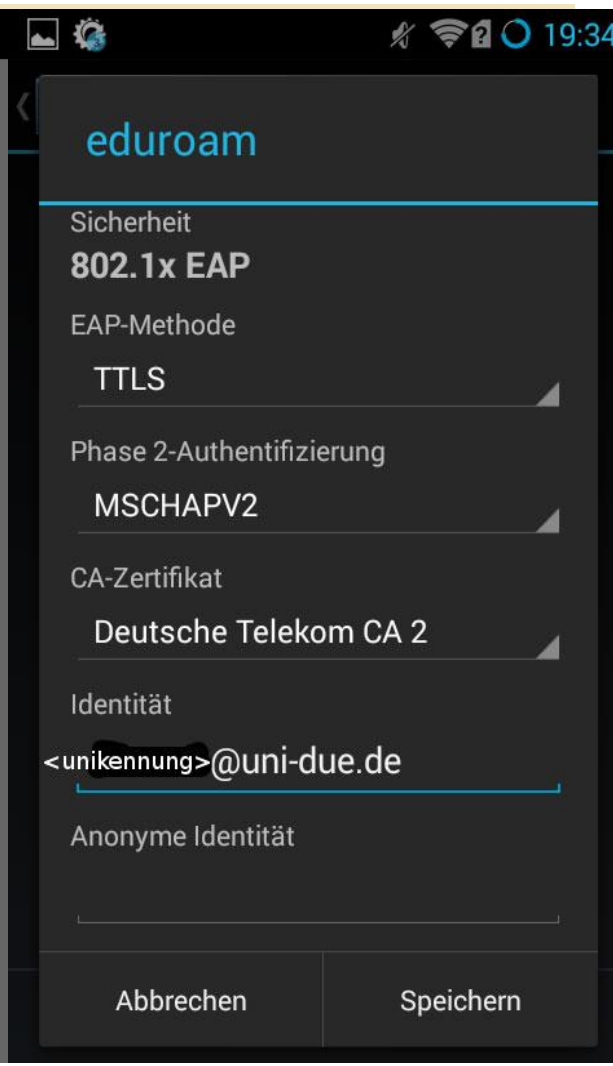
- Alle neuen Endgeräte werden ab jetzt nur noch für das neue Zertifikat konfiguriert.
- Das eduroam-CAT-Tool ist entsprechend angepasst worden.
- Nur noch cat.eduroam.org verwenden!

eduroam bisherige Konfiguration:

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken







Aber: Das Telekom-Root-Zertifikat läuft am 9.Juli 2019 ab:

If you want to decode certificates on your own computer, run this OpenSSL command:

```
openssl x509 -in certificate.crt -text -noout
```

Paste Certificate Text

rFDa1sPeg5TKqAyZMg4ISFZbavva4VhYAUIfckE8FQYBjI2tqriTtM2e66foai1S
NNs671x1Udrb8zH57nGYMsRUFUQM+ZtV7a3fGAigo4aKSe5TBY8ZTNXeWHmb0moc
QqvF1afPaA+W5OFhmHZhyJF81j4A4pFQh+GdCuatI9ldxjp9y7zaAzTVjlsB9WoH
txa2bkp/AgMBAAGjQjBAMB0GA1UdDgQWBBQxw3kbuvVT1xfgiXotF2wKsyudMzAP
BgNVHRMECDAGAQH/AgEFMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQUFAAOC
AQEAlGRZrTIk5ynrE/5aw4sTV8gEJPB0d8Bg42f76Ymmg7+Wgnxu1MM9756Abrsp
tJh6sTtU6zkXR34ajgv8HzFZMQSyzhfzLMdiNiXiltjJVbSYSKpk+tYcNthEeFpa
lzpXl/V6ME+un2pMSyuOoAPjPuCp1NJ70rOo4nI8rZ7/gFnkm0W09juwzTkZmDLI
6iFhkOQxlY40sfcvNUqFENrnijchvllj4PKFiDFT1FQUhXB59C4Gdyd1Lx+4ivn+
xbrYNuSD7Odlt79jWvNGr4GUN9RBjNYj1h7P9WgbRGOiWrqnNVmh5XAFmw4jV5mU
Cm26OWMohpLzGITY+9HPBVZkVw==
-----END CERTIFICATE-----

Certificate Information:

- **Common Name:** Deutsche Telekom Root CA 2
- **Organization:** Deutsche Telekom AG
- **Organization Unit:** T-TeleSec Trust Center
- **Country:** DE
- **Valid From:** July 9, 1999
- **Valid To:** July 9, 2019
- **Issuer:** Deutsche Telekom Root CA 2, Deutsche Telekom AG
- **Serial Number:** 38 (0x26)

Siehe auch https://www.sslshopper.com/certificate-decoder.html

WLAN –Sicherheit eduroam

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- Unser damit unterschriebenes Radius-Zertifikat läuft schon am 31.5. 2019 (um 14:28 Uhr) ab.
- Neue Zertifikate stellt der DFN-Verein ausschließlich mit dem neuen Root-Zertifikat aus.
- d.h. am 31.5.2019 ab 14:28 Uhr streiken alle Radius-Klienten, die die Zertifikatsüberprüfung (richtig) konfiguriert haben.
- Möglicherweise verzichten viele Android-Klienten auf die Zertifikatsüberprüfung.

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Das ist bisher im eduroam noch nie passiert!

Was tun wir:

Zwei parallele Konfigurationen

Abhängig von der äußeren Identität

anonymous@uni-due.de → altes Zertifikat

kennung@uni-due.de → altes Zertifikat

eduroam@uni-due.de → neues Zertifikat

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Was tun?

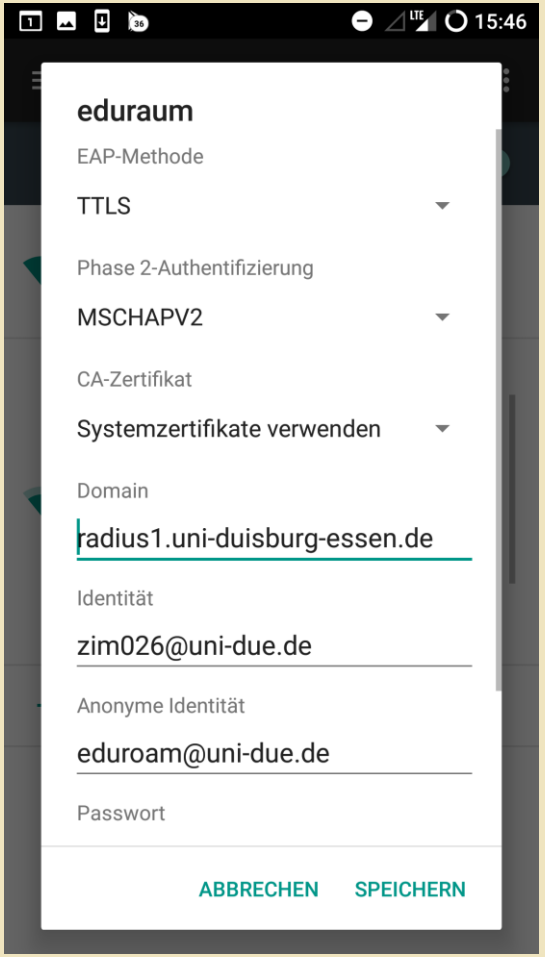
- Nicht bis zum 31.5.2019 warten, sondern zeitnah neu konfigurieren!
- EMPFEHLUNG: eduroam-CAT nutzen: cat.eduroam.org
- Manuelle Konfiguration → Anleitungen für viele Betriebssysteme und generische Anleitung unter :
- https://www.uni-due.de/zim/services/wlan/eduroam-konfiguration.shtml

Neue eduroam Konfiguration Android 7:

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Hier beispielhaft für Android:

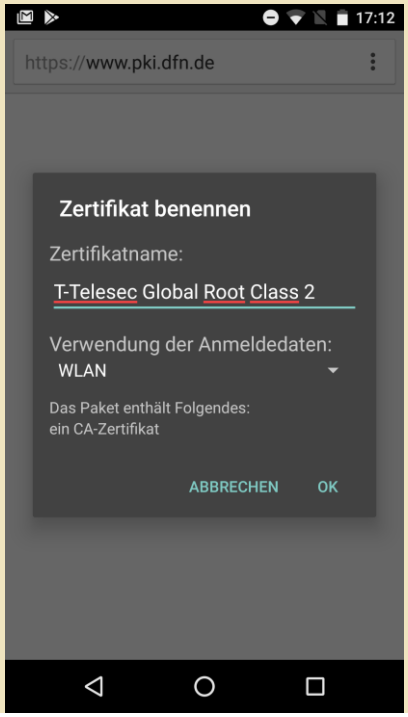
- eduram-CAT für Android unnötig kompliziert
- manuelle Konfiguration ist m.E. einfacher
- wenn der Menuepunkt „Systemzertifikate verwenden“ bei CA-Zertifikat existiert:

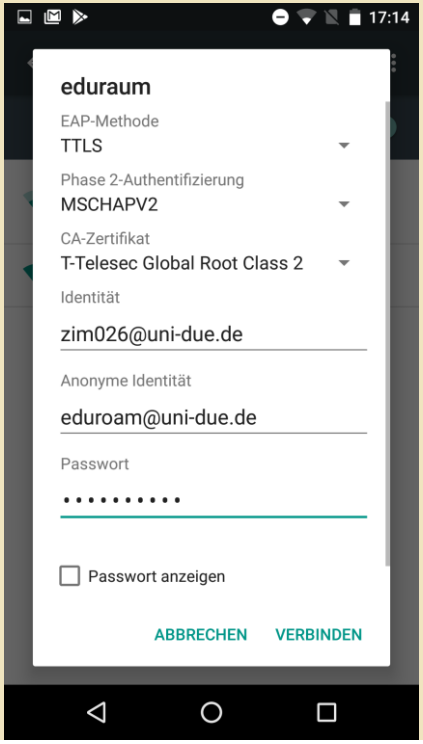


Neue eduroam Konfiguration Android 6,5,4 2.4:

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Alternativ, wenn kein Menuepunkt „Systemzertifikate verwenden“ existiert : *NEUES* DFN-CA Global G2 Zertifikat nachinstallieren (bei Android 6, 5, 4, 2,4):
https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.crt





Wofür diese „äußere“ Identität?

- Der Betreiber eines eduroam-Netzes soll die innere Identität, also bei uns: kennung@uni-due.de nicht sehen! Bei uns ist die Kennung nicht öffentlich.
- Datenschutz: Auch die Administratoren der WLAN-Infrastruktur bzw. die WLAN-Monitoring-Softwaresollen die innere Identität nicht sehen!
- Der DFN-Verein/eduroam.org drängen auf die Verwendung der äußeren Identität!

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Der REALM „@uni-due.de“ bzw. „@uni-duisburg-essen.de“ ist wichtig!

- Nur so kann das Roaming mit den Partnerhochschulen deutschlandweit/weltweit überhaupt funktionieren!
- Bitte niemals ohne REAM konfigurieren!
- Es gibt bim Radius *niemals* den Realm @stud.uni-due.de
- Wie kommt eine Konfiguration ohne äußere Identität in die Welt/ auf das Gerät?
- IOS, MacOS und Windows 10 erlauben die Konfiguration „bequem“ nur mit Username/Passwort und handeln alles weitere „zufällig“, d.h. nach Präferenzen des Herstellers aus → keine äußere Identität

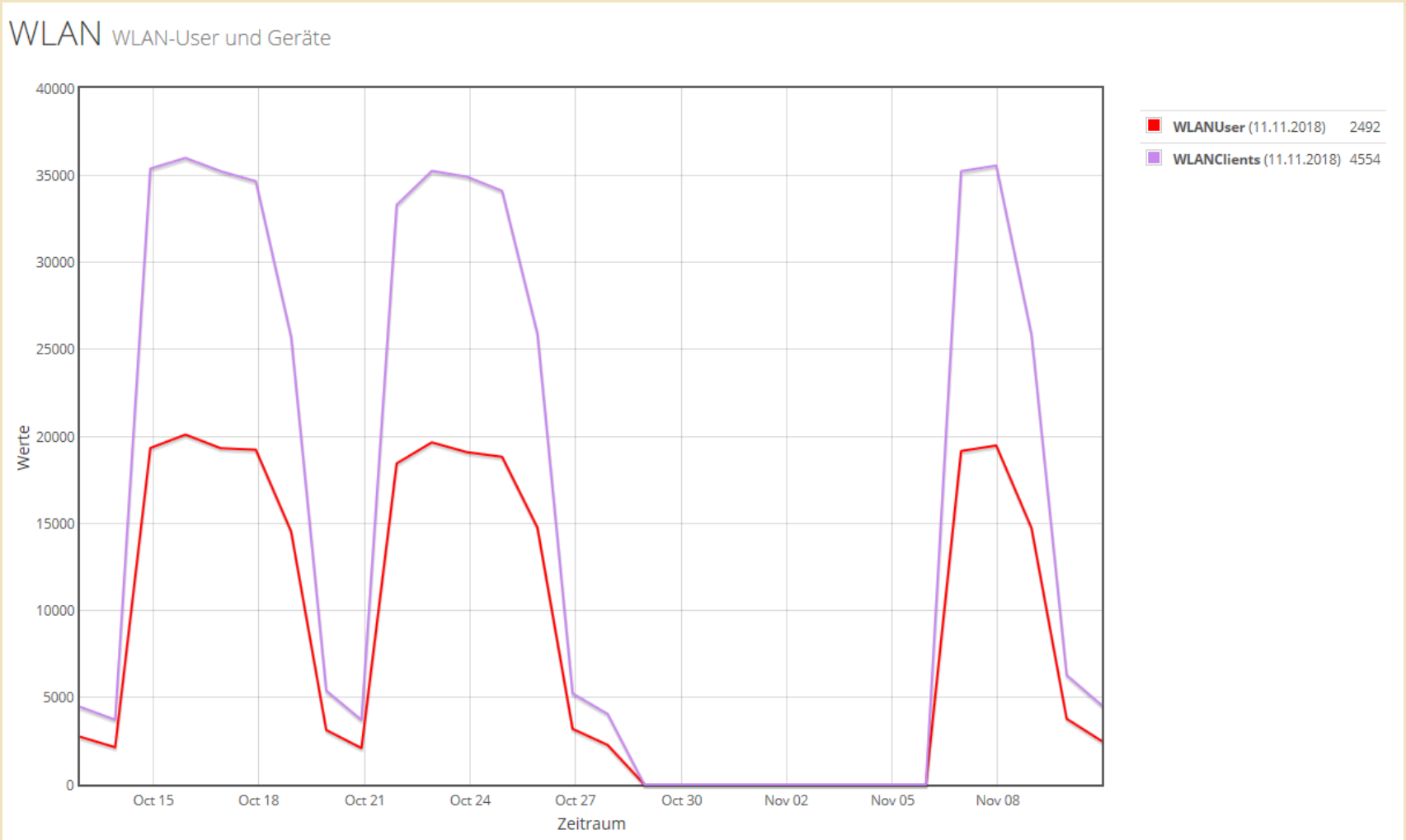
Die WPA2-Zertifikate sind wichtig!

- Nur so kann man sicher sein, mit dem richtigen Radiusserver zu sprechen. Sonst sind Rogue-Acesss-Points möglich!
- Wir haben keine Möglichkeit die Zertifikatsüberprüfung zu erzwingen. Das wird am Klienten konfiguriert.
- Mit Ablauf des eduroam-Root-Zertifikates plane ich den alten Server mit abgelaufenem Zertifikat weiterlaufen zu lassen → Wer sich dort erfolgreich authentifiziert hat keine Zertifikatsüberprüfung aktiviert → wird vom ZIM angeschrieben!
- Wer, wie von uns empfohlen, das eduroam CAT-Tool verwendet, bekommt immer die richtige sichere und datenschutzkonforme Konfiguration mit Zertifikaten und äußerer anonymer Identität!

WLAN Statistik eduroam

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken



Zusammenfassung

- Alle bisher konfigurierten Klienten laufen ohne Probleme bis zum 31.5.2019 weiter.
- Es wird aber empfohlen vorher eduroam-CAT zu nutzen, um die neue zukunftssichere Konfiguration zu bekommen.
- Insbesondere versuchen wir einen RUN auf den e-Point am 31.5.2019 zu verhindern.
- Wissenschaftler die häufig unterwegs sind, sollten zeitnah umkonfigurieren!
- Es muss an alle Geräte gedachtet werden (auch selten genutzte Notebooks für Konferenzen)
- Nicht vergessen: Wenn ein separates WLAN-Passwort konfiguriert war, muss dieses auch verwendet werden!

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Zusammenfassung

- Weiterführende Informationen:
- http://blogs.uni-due.de/zim/2018/10/31/das-eduroam-wurzelzertifikat-der-deutschen-telekom-laeuft-am-9-juni-2019-ab-und-ploetzlich-funktioniert-eduroam-nicht-mehr/
- Kontakt: andreas.bischoff@uni-due.de