TU Clausthal

eduroam: Migration von FreeRADIUS auf neue DFN CA (Global G01 → G02)

C. Strauf
Rechenzentrum TU Clausthal
67. DFN Betriebstagung

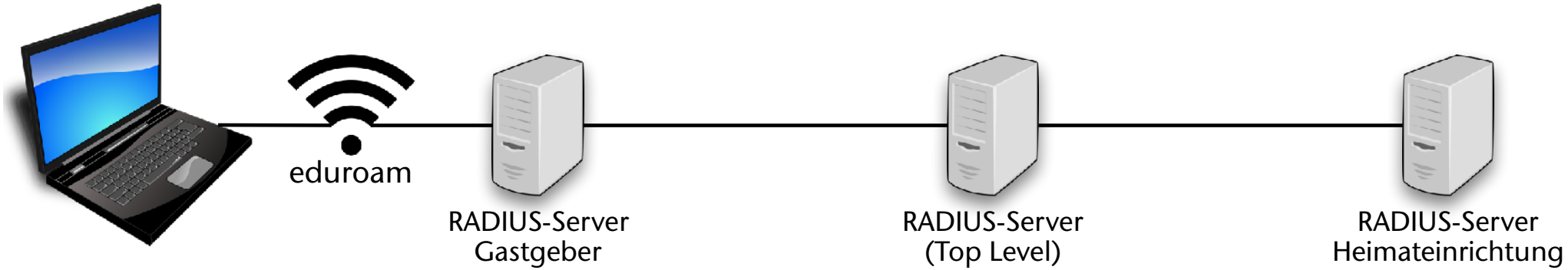
Agenda

- Wofür eine CA für eduroam?
- Wechsel von DFN PCA Global G01 zu G02
- Probleme der Migration
- Praktikables Migrationsszenario
- Umsetzung in FreeRADIUS
- Umsetzung auf Seite der Nutzer
- Fazit

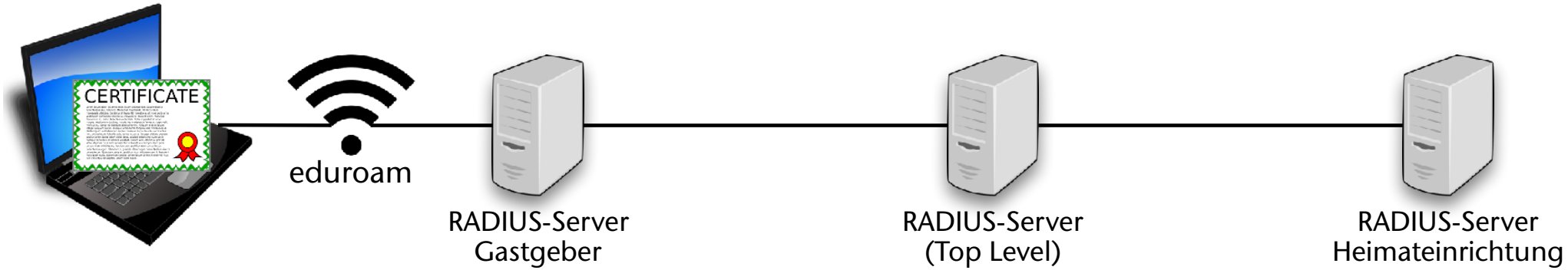
Wofür eine CA für eduroam?

- Die Autorisierungs-, Authentifizierungs- & Accounting-Infrastruktur (AAA) für eduroam basiert auf RADIUS.
- Für die Authentifizierung werden bestimmte, für eduroam geeignete Verfahren des Extensible Authentication Protocol (EAP) verwendet.
- Folgende Verfahren basieren auf X.509-Zertifikaten:
  - EAP-TTLS,
  - PEAP,
  - EAP-TLS.
- Die Server- & Client-Zertifikate (letztere wo zutreffend) werden von einer CA signiert, um Vertrauenswürdigkeit herzustellen.
- Die meisten Einrichtungen nutzen hierfür Zertifikate der DFN PKI.

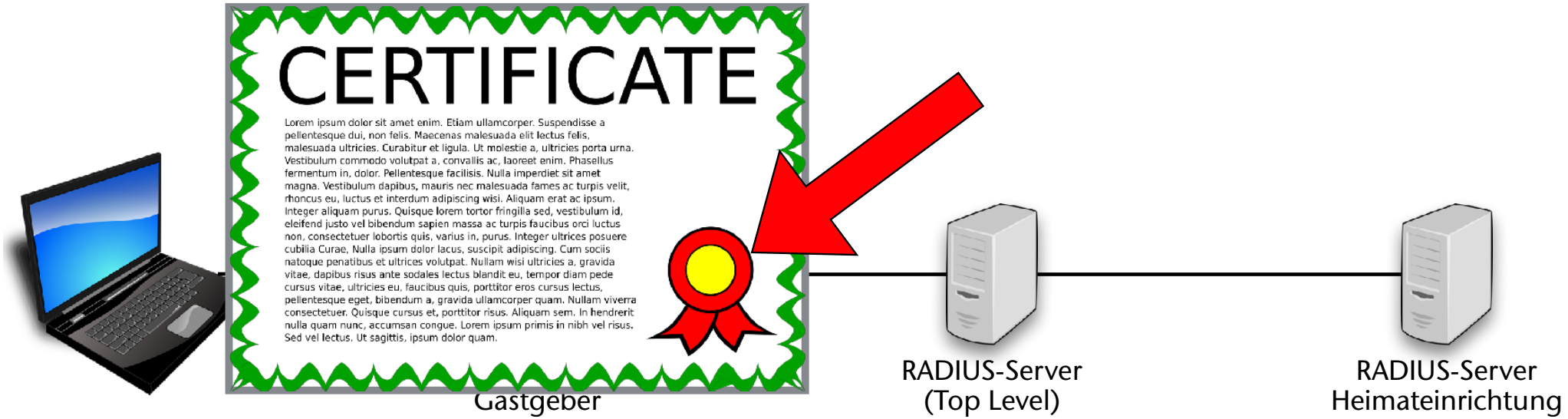
Wofür eine CA für eduroam?



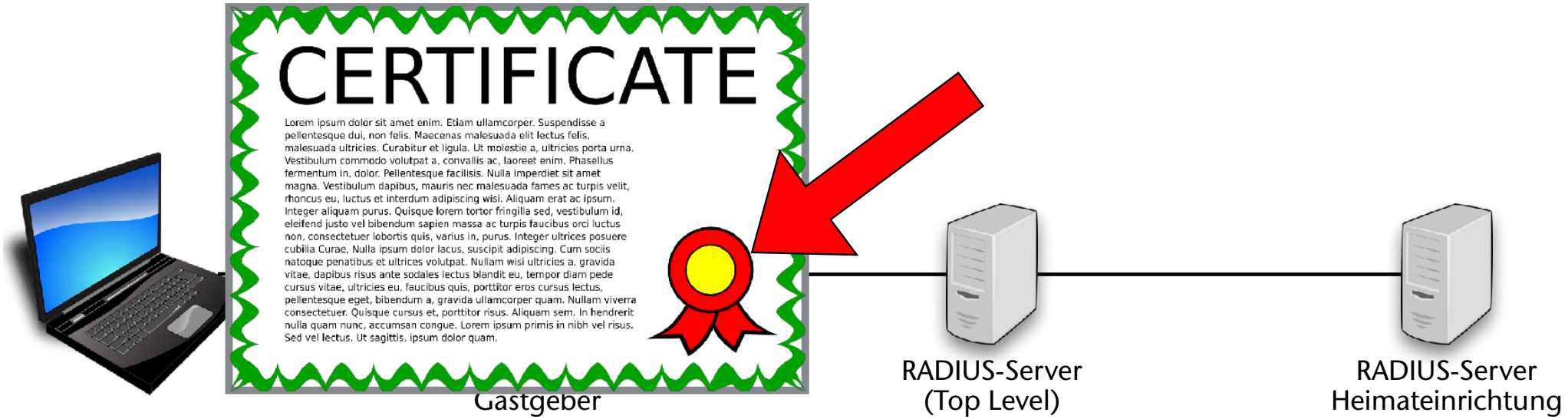
Wofür eine CA für eduroam?



Wofür eine CA für eduroam?

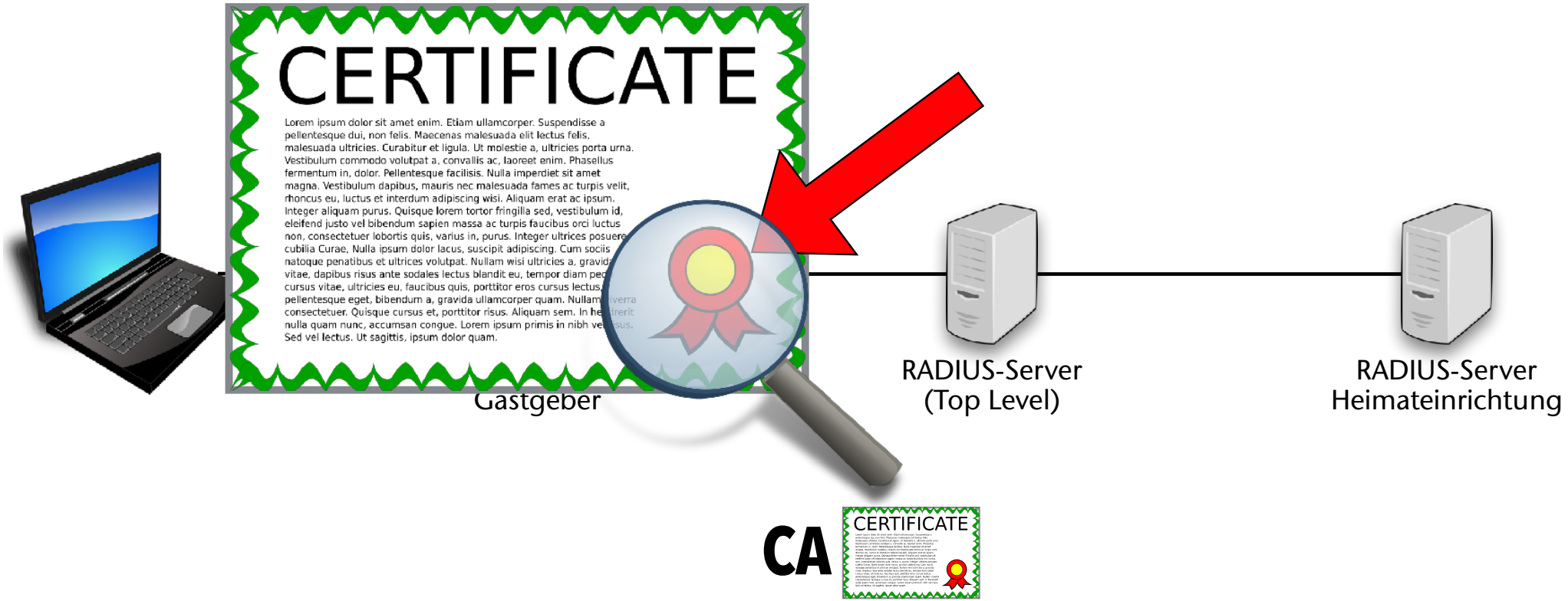


Wofür eine CA für eduroam?

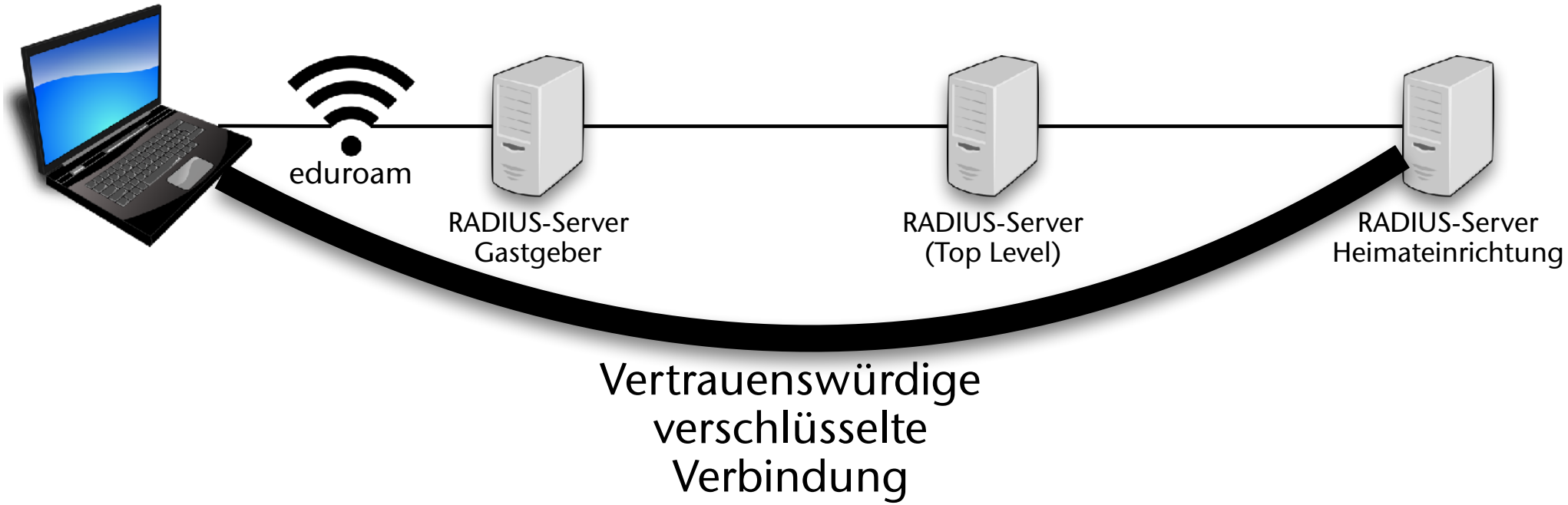


CA 

Wofür eine CA für eduroam?



Wofür eine CA für eduroam?



Dipl.-Math. Christian Strauf
Rechenzentrum TU Clausthal

Wechsel von DFN PCA Global G01 zu G02

- Das Root-Zertifikat, mit dem das „DFN PCA Global G01“-Zertifikat unterschrieben wurde, läuft im **Juli 2019** ab.
- Neue CA mit DFN PCA Global G02 ist seit längerem verfügbar.
- Da bei der Mehrheit der Einrichtungen RADIUS-Server-Zertifikate verwendet werden, die von der DFN PCA Global G01 signiert wurden, verlieren diese mit Ablauf des Root-Zertifikats ihre Gültigkeit. → Ab Ablaufdatum verbinden sich eduroam-Clients **nicht mehr** mit dem RADIUS-Server!

Probleme der Migration

- Neukonfiguration der Clients (Suplikanten) auf jeden Fall notwendig.
- Fast alle Clients unterstützen keine zwei CAs für die Zertifikatsprüfung.
- Eine „harte“ Umstellung des Zertifikats auf dem/den RADIUS-Server(n) hat folgende Auswirkungen:
  - Clients mit alten CA-Zertifikaten können sich nicht mehr anmelden.
  - Ein „Flag Day“ erfordert Umstellung von RADIUS-Server(n) und allen (!) Clients.
  - Flag Day ist eine große logistische Herausforderung für den 1st-Level-Support.

Praktikables Migrationsszenario

- Vorübergehender Betrieb der RADIUS-Server mit zwei gültigen Zertifikaten: 1x von G01 unterschrieben (altes Zertifikat) und 1x mit G02 unterschrieben (neues Zertifikat).
- Problem:

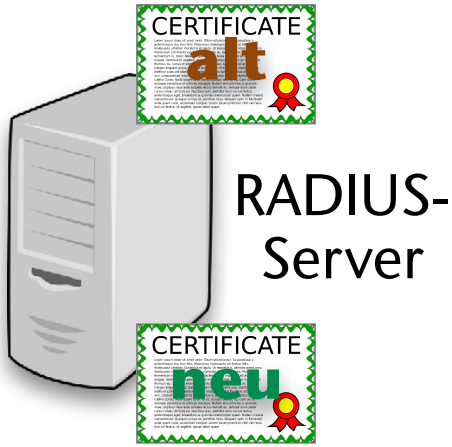
  Keine server-seitige Erkennung möglich, welche CA ein Client installiert hat (sprich: es ist nicht klar, welches von welcher CA unterschriebene Zertifikat der Client akzeptieren wird).

- Lösung:

  Fallunterscheidung an Hand der äußeren anonymen Identität.

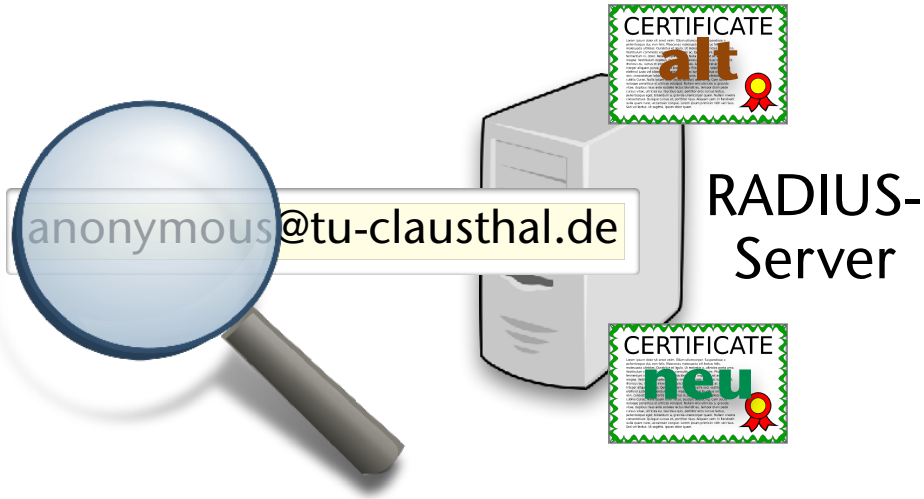
Praktikables Migrationsszenario

Client 



Praktikables Migrationsszenario

Client



Praktikables Migrationsszenario

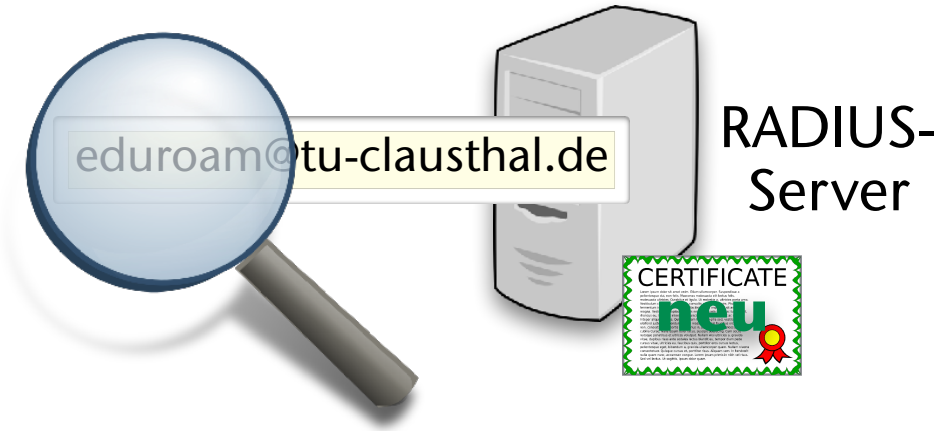
Client

anonymous@tu-clausthal.de

RADIUS-Server

Praktikables Migrationsszenario

Client 



Dipl.-Math. Christian Strauf
Rechenzentrum TU Clausthal

Praktikables Migrationsszenario

Client

eduroam@tu-clausthal.de

RADIUS-Server

Dipl.-Math. Christian Strauf
Rechenzentrum TU Clausthal

Umsetzung in FreeRADIUS

- Folgende Schritte sind erforderlich:
  - Neues Zertifikat generieren und durch G02 signieren lassen.
  - Zertifikate auf den RADIUS-Server bringen und Fallunterscheidung konfigurieren:
    - Anpassung des relevanten Servers in `sites-available/xxxx`.
    - Anpassung der verfügbaren EAP-Konfigurationen in `mods-available/eap`.
  - Client-Konfigurationen und -Dokumentationen anpassen.

Umsetzung in FreeRADIUS

- Anpassung von `sites-available/xxxx`:

```
authorize {
        ...
        eap {
                ok = return
        }
        ...
}
```

Umsetzung in FreeRADIUS

- Anpassung von `sites-available/xxxx`:

```
authorize {
        ...
        if ( &User-Name == "eduroam@einrichtung.de" ) {
                eap {
                        ok = return
                }
        } else {
                eapoldca {
                        ok = return }
        }
        ...
}
```

Umsetzung in FreeRADIUS

- Anpassung von `sites-available/xxxx`:

```
authenticate {
        ...
        eap
        ...
}
```

Umsetzung in FreeRADIUS

- Anpassung von `sites-available/xxxx`:

```
authenticate {
        ...
        Auth-Type eap {
                eap
        }
        Auth-Type eapoldca {
                eapoldca
        }
        ...
}
```

Umsetzung in FreeRADIUS

- Arbeiten in `mods-available/eap`:
  - Alten Abschnitt eap {} nach eap eapoldca {} kopieren.
  - Im Abschnitt eap {} alle Sektionen, in denen die alten Zertifikate referenziert werden, editieren und die neuen Zertifikate referenzieren.
- Arbeiten an den Client-Konfigurationen:
  - CA-Zertifikate der G01 durch die der G02 ersetzen.
  - Wo zutreffend: Namen der RADIUS-Server (wo CNs geprüft werden) aktualisieren.
  - Äußere Identität auf „eduroam@einrichtung.de“ ändern.

Umsetzung auf Seiten der Nutzer

- Nach erfolgter RADIUS-Konfiguration kann der RADIUS-Server zwei Zertifikate anbieten:
  - signiert mit G01,
  - signiert mit G02.
- Nutzer steuert über die äußere anonyme Identität, welches Zertifikat er vom Server angeboten bekommen möchte:
  - „anonymous@einrichtung.de“: „Biete mir altes Zertifikat an“.
  - „eduroam@einrichtung.de“: „Biete mir neues Zertifikat an“.
- Durch die parallele Verfügbarkeit von Zertifikaten, die durch alte und neue CA signiert sind, kann ein sanfter Übergang von mehreren Monaten gewährleistet werden.

Fazit

- Steuerung des angebotenen RADIUS-Server-Zertifikats über äußere Identität ist eine elegante Lösung, um eine sanfte Migration zu ermöglichen (kein „Flag Day“).
- Keine Änderungen bei Bestandsnutzern vor der Migrationsphase nötig.
- Entlastung 1st-Level-Support durch ggf. mehrmonatige Migrationsphase.
- Nach erfolgter Client-Migration kann ohne Eingreifen auf Nutzerseite altes Zertifikat auf RADIUS-Server-Seite deaktiviert werden.
- Aber: Zertifikate für RADIUS-Authentisierung machen keinen Spaß. Sinnvoller: EAP-Mechanismen, die ohne Zertifikate auskommen (EAP-pwd, EAP-EKE etc.).

Vielen Dank für Ihre Aufmerksamkeit!