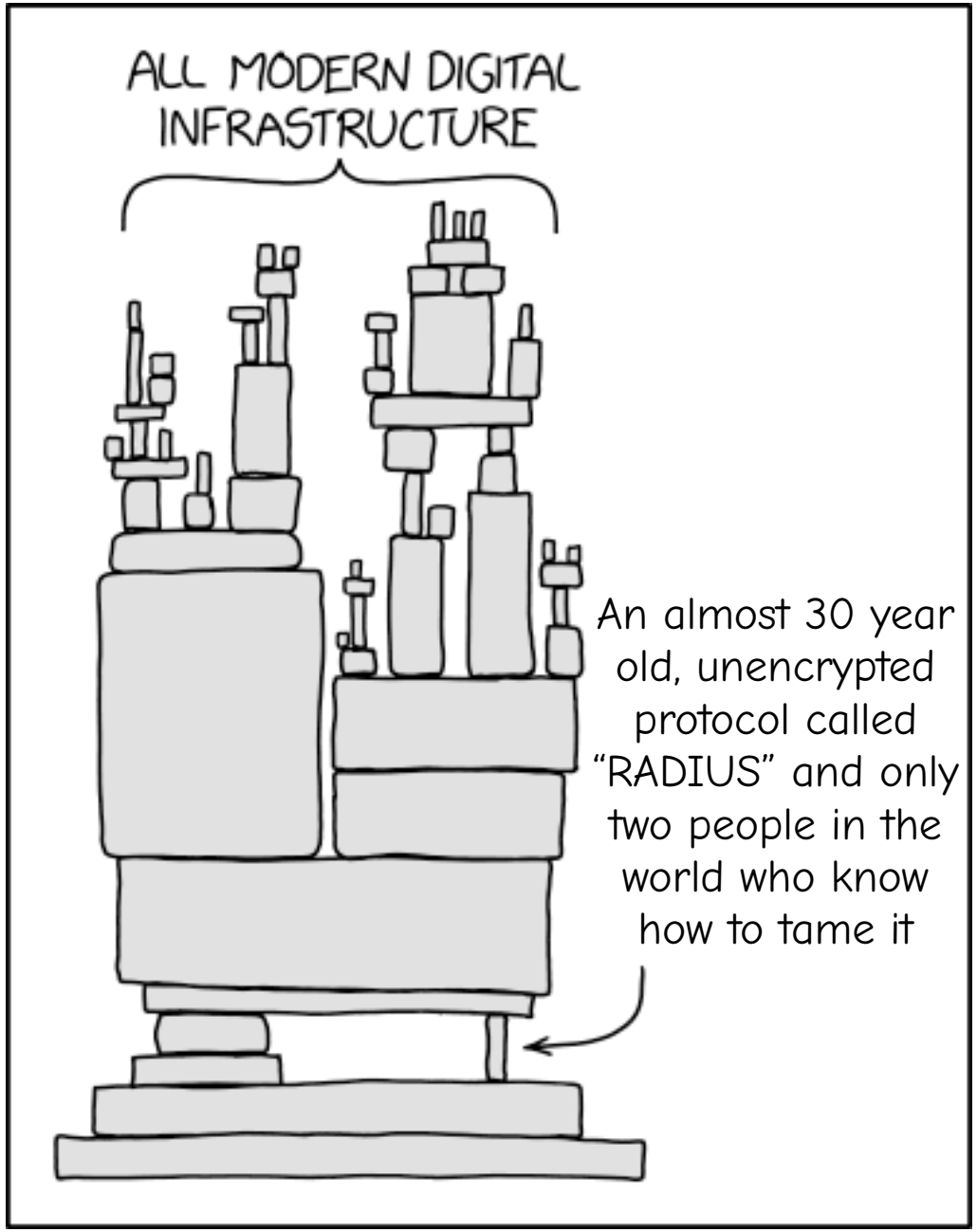
The good thing about standards...
Aktuelles aus der IETF

82. DFN-Betriebstagung | 26. März 2025

Jan-Frederik “Janfred” Rieckers



https://xkcd.com/2347/

Die RADIUS-Standards

- RFC 2865 bis RFC 2869 – Remote Authentication Dial In User Service – Juni 2000 – „Traditionelles“ RADIUS/UDP
  - Ursprünglich RFC 2058 – Januar 1997
- RFC 6614 – RADIUS/TLS (Experimental) – Mai 2012
- RFC 7360 – RADIUS/DTLS (Experimental) – September 2014

IETF Working Group radext

- RADIUS EXTensions
- Bis 2015 aktiv, danach fast keine Aktivität, im März 2022 offiziell geschlossen
- zur IETF 115 (November 2022) Birds-of-Feather (BoF) Session zur Wiedereröffnung der Working Group (radextra – RADIUS EXTensions ReAnimated)
- Bei der IETF 116 (März 2023) erste Session der neuen radext Working Group
  - Aktive Teilnehmende:
    - eduroam, FreeRADIUS, Radiator

IETF Working Group radext - Charter

- „... will focus on extensions to the RADIUS protocol.“
  - Deprecating the use of insecure transports outside of secure networks
  - Bring RFC 6614 (RADIUS/TLS), and RFC 7360 (RADIUS/DTLS) to standards track
  - Define best practices for using TLS-PSK with TLS-based transport.
  - Define best practices for RADIUS roaming
  - Improve operations for multi-hop RADIUS networks

radext@ietf.org Mailingliste - (Archiv)

https://datatracker.ietf.org/group/radext/about/

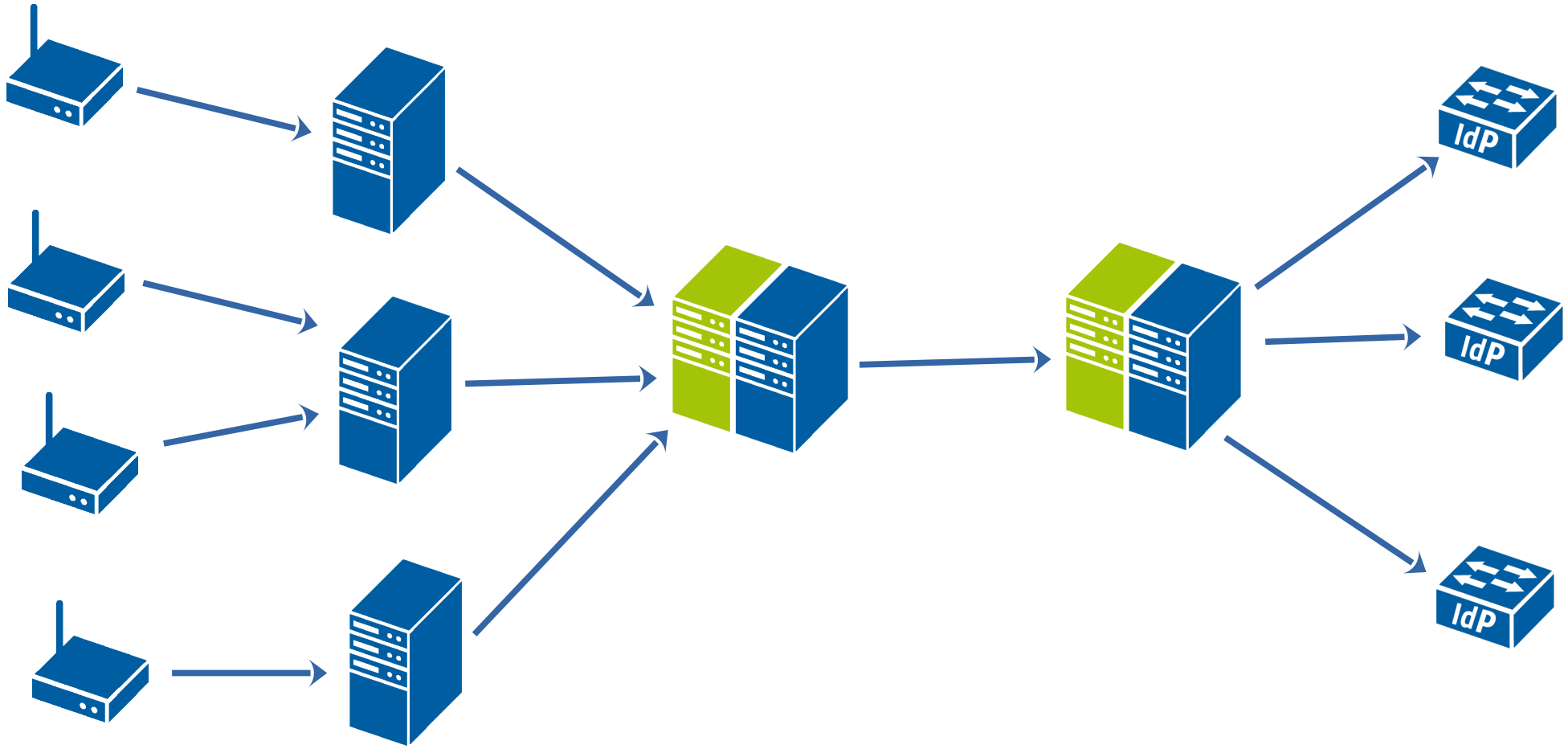
Deprecating insecure practices

- https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/
- Wichtigster Punkt: RADIUS/UDP wird offiziell als „veraltet“ designiert
  - Ausnahme: Innerhalb von geschützten, internen Netzen (z.B. vom Wireless Controller zum ersten RADIUS-Server über das interne NOC-Netz)
- Weitere Punkte zu aktuellen unsicheren RADIUS-Use-Cases
  - MS-CHAP/MS-CHAPv2 als veraltet markiert
    - Wichtig: Zunächst nur für natives RADIUS mit MS-CHAP(v2), nicht PEAP/MSCHAPV2 oder TTLS/MSCHAPV2
- Kurz vor Working Group Last Call
  - Gerne lesen und Feedback geben!

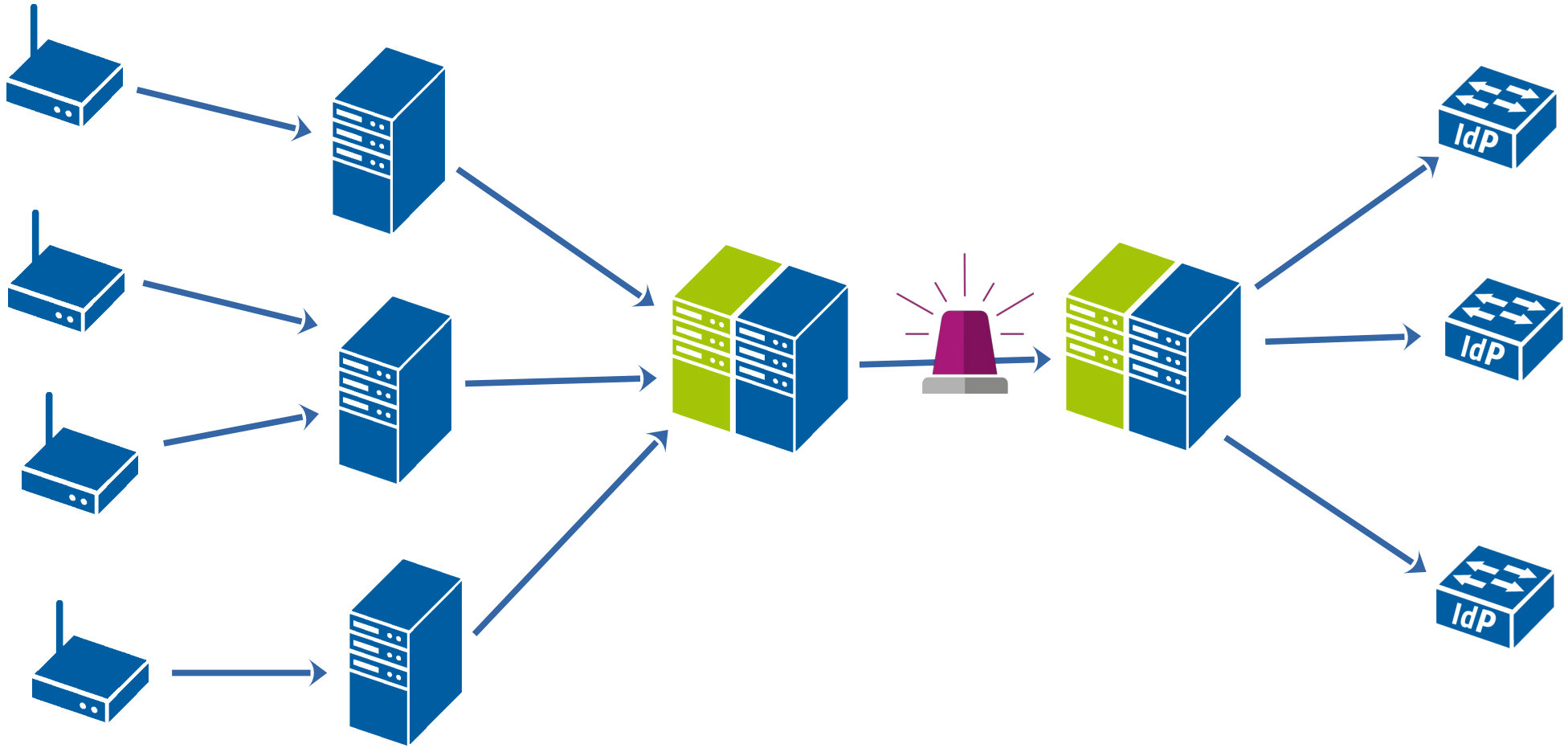
Make RADIUS/(D)TLS a proposed standard

- https://datatracker.ietf.org/doc/draft-ietf-radext-radiusdtls-bis/
- Update von RFC6614 und RFC7360
  - Keine großen funktionalen Änderungen
  - RADIUS/TLS und RADIUS/DTLS zusammen in ein Dokument
  - Änderung: Antwort auf ungewollte Accounting-Pakete
    - Bisher: Accounting-Reject mit Error-Cause Attribute
    - Neu: Protocol-Error
- Kurz vor Working Group Last Call
  - Gerne lesen und Feedback geben!

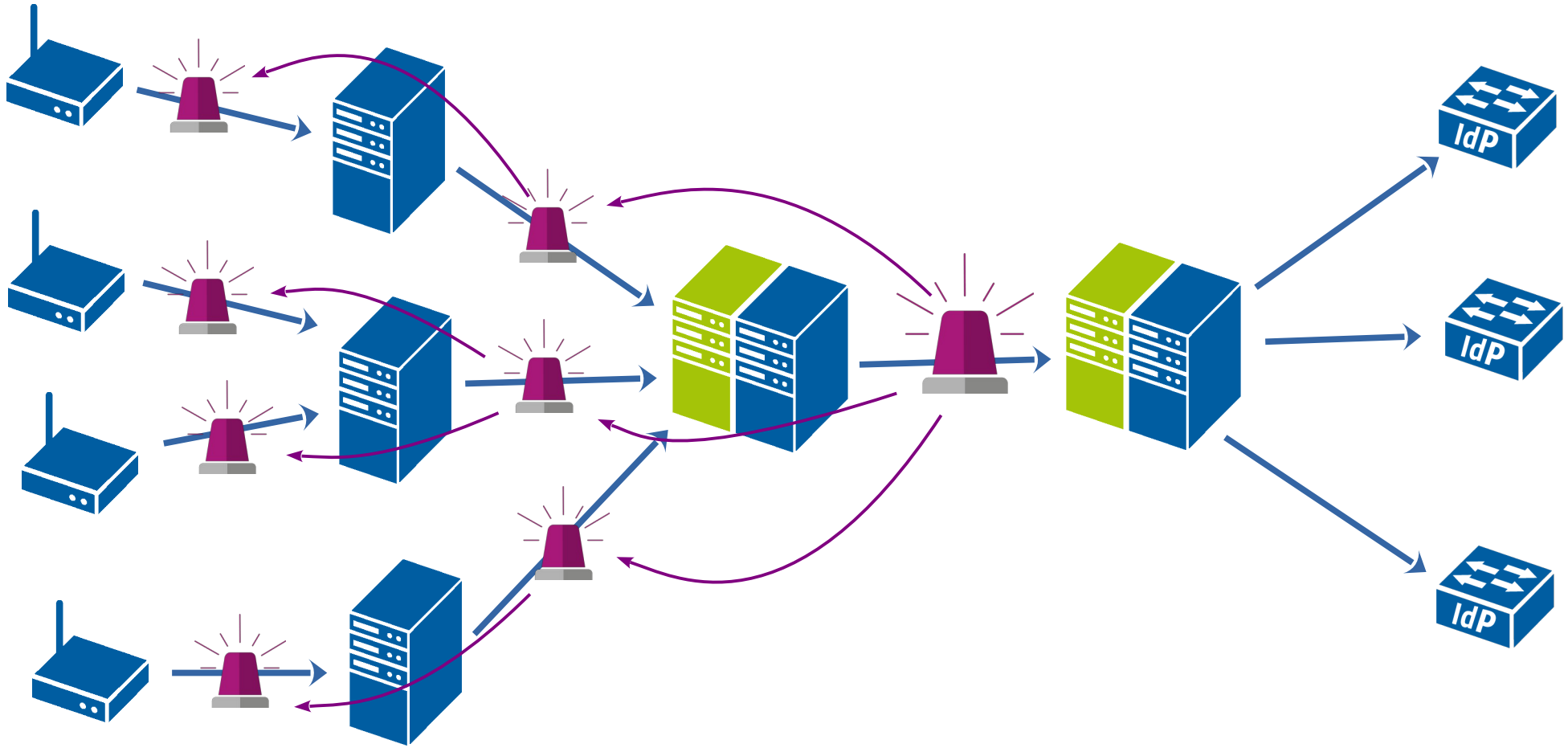
RADIUS Proxy-Chains



RADIUS Proxy-Chains



RADIUS Proxy-Chains



Die RADIUS-Proxy-Chain robuster machen

- Missing Responses sind ein Problem in eduroam
  - Blockieren die Paket-ID bis zum Timeout
    - Bei RADIUS nur 256 IDs pro Verbindung
    - radsecproxy macht nur eine Verbindung pro Server
  - Können für falsche Dead-Peer-Detection sorgen
    - Side note: Status-Server aktivieren!
- Vorschlag: Protocol-Error mehr benutzen
  - wird nicht weitergeleitet, strikt auf einen RADIUS Hop beschränkt
  - Enthält Error-Cause (z.B. „Route zum Home-IdP down“)
  - Gibt dem Proxy die Möglichkeit, den Request woanders hin zu routen
  - Ist aktuell ein Experimental RFC und nur für Teile von RADIUS definiert

RADIUS Load balancing

- Betrieb mehrerer RADIUS-Server
- RADIUS ist Request-Response-basiert, reine RADIUS-Authentifizierungen können Round-Robin verteilt werden (Bsp.: 2FA)
- EAP ist Session-basiert, Round-Robin Load-Balancing macht die EAP-Sessions kaputt
  - Hosts müssten den EAP Session State (inkl TLS-Keys) synchronisieren, ist zu aufwendig.
  - Daher: Aktuell meist nur Hot Standby / Failover statt Load balancing
- Load-Balancing muss auf Basis von bestimmten RADIUS-Attributen passieren
  - Username, Calling-Station-ID (MAC-Adresse) -> Consistent Hashing

Neues Sub-Protkoll: Status-Realm
Ist der Home-Server überhaupt da?

- RADIUS ist Hop-by-Hop => Sämtliche Komplexität wird vom Proxy verschleiert
- Status-Server kann einzelnen Hop überprüfen, aber keine Überprüfung der ganzen Proxy-Chain
- Neuer Vorschlag: Status-Realm
  - Ping/Traceroute-ähnliche Funktionalität für RADIUS
  - Time-To-Live-Attribut mit TTL-Exceeded-Antworten (Traceroute)
  - Test, ob Home-Server antwortet
  - Ggf. auch Test, wo in der Proxy-Chain das Problem liegt
  - Zusätzlich: Loop-Erkennung möglich

Neue Idee: Response-Delay und Request-Block

- Hoher Anteil an Last durch Authentifizierungsanfragen alter Geräte
  - z.B. Alumni mit alter eduroam-Config
- Reject-Delay belastet ganze Proxy-Chain
- Vorschlag: Gegenmaßnahmen die Proxy-Chain herunter schicken
  - Proxy-Server fügen Attribut in Request hinzu, um Fähigkeit zu signalisieren
  - Home-Server fragt die Gegenmaßnahme in Attribut in der Antwort an
  - Proxy-Server setzt die Gegenmaßnahmen um
    - Reduziert Last auf allen Proxies in der Kette

Beyond RADIUS: EAP mit FIDO-Keys

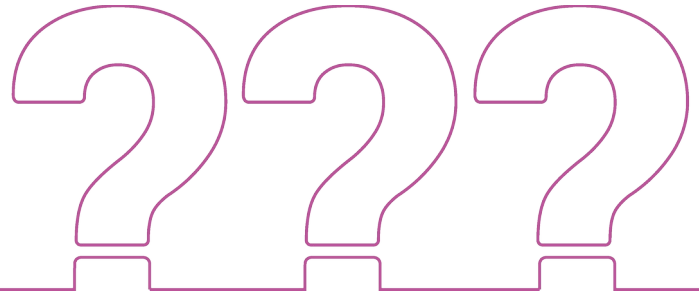
- Neuer Forschlag als Alternative für EAP-{TTLS|PEAP|TLS|PWD|...}: Einfach FIDO-Keys benutzen!
- Aktiver Internet-Draft: https://datatracker.ietf.org/doc/draft-ietf-emu-eap-fido/
- Die meisten Geräte haben einen Platform Authenticator, den können wir einfach auch für WLAN benutzen
  - Registrierung des Platform Authenticators über WebAuthn
  - Einfache Konfiguration auf dem Gerät
    - Keine Zertifikatskonfiguration notwendig, alles implizit
- Proof-of-Concept mit wpa_supplicant und hostapd
  - Leider noch ohne Platform Authenticator, nur YubiKey/NitroKey
- Funktioniert hier im eduroam
- Bei Interesse gerne auf mich zukommen

Fragen?

- Kontakt
  - Jan-Frederik Rieckers

    Mail: rieckers@dfn.de
    Phone: 0049 30 884299-339
    Fax: 0049 30 884299-370

    Address:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz1
    10178 Berlin



Bonus: RADIUS/1.1 mit ALPN

- RADIUS/(D)TLS, aber über ALPN wird neue Protokollversion ausgehandelt
- Alle MD5-basierten „Sicherheitsmechanismen“ werden entfernt
  - Request/Response Authenticator
  - MessageAuthenticator Attribut
  - „Verschlüsselung“ des MS-MPPE-Key (Key für WPA2/3-Handshake)
- Vergrößerung des RADIUS ID-Raums von 1 Byte auf 4 Byte
  - Kein Problem von ID-Exhaustion wenn nur eine Verbindung aufgemacht werden kann
- Rückwärtskompatibel
  - Wenn RADIUS/1.1 nicht per ALPN augehandelt wird wird auf traditionelles RADIUS/(D)TLS ausgewichen.

Bonus: RADIUS/TLS mit TLS-PSK

- Zertifikatsverwaltung ist schwer. Daher: Pre-Shared Keys
- Ähnlicher Prozess wie mit RADIUS Shared Secret
- Internet-Draft mit Best-Practices zum Umgang mit TLS-PSK in RADIUS/TLS
  - Kurz vor Veröffentlichung als RFC