eduroam

evoluzione a livello globale

Paul Dekkers
eduroam, SURF
Global eduroam

• eduroam, a service we all build together

You!
- Campuses, IdPs, SPs
- National roaming operators
- Regions
- Global eduroam
Global developments, highlight today

• Operations, development
  • International proxies
  • Supporting services, like eduroam CAT
  • Monitoring, data exchange
• Liaison different organizations
  • Wi-Fi-Alliance
  • WBA
  • …

• OpenRoaming
• geteduroam
eduroam is WBA member (so you benefit)

Participation, similarities, what does it mean…

“eduroam has been doing federated Wi-Fi roaming since over a decade with many of the building blocks that meanwhile underpin Passpoint®. Now that Passpoint® and OpenRoaming™ provide a coherent vision and technology to enable inter-federation roaming in a scalable way, it is only natural for eduroam to join forces and take this exciting next step as a first-to-market pioneer participant.”

Paul Dekkers
Chair of the Global eduroam Governance Committee in GÉANT
eduroam, (inter fed) roaming, ...

- **eduroam is the biggest federated roaming-infrastructure**
  - 7200 IdPs
  - 30000 locations
  - 106 countries

- Roaming by standardizing on SSID (1x, RADIUS, transparent EAP)
- Blueprint, authorisation, use-case, rules are simple (reused largely in eg. govroam)
- Global governance (GeGC), regions, NROs

- Hotspot 2.0/Passpoint,
  We have an eduroam RCOI for venues that have no SSID available
  Participated in NGH trials
  WiFi4EU
- Dynamic peer discovery
Hotspot 2.0, HS20, Passpoint®, 802.11u

- More than just SSIDs:
  - **RCOI** (Roaming Consortium Organization Identifier),
  - NAIrealm, domain, 3GPP (MNC/MCC, offloading)
- **ANQP** (Access Network Query Protocol) for discovery of networks (home, roaming, EAP-types)
- Afterwards: WPA(2)-Enterprise, EAP
- Multiple releases, limited support
  - R1: Basics, 802.11u
  - R2: Online Sign-Up (OSU)
  - R3: safe “AUP/T&C portal”, details in RADIUS req.’d for routing
RadSec, dynamic peer discovery (1)

- eduroam test RadSec since 2004
- RADIUS (UDP) trust is IP, shared secret
- RadSec (TCP, TLS) trust is PKI
direct connections possible
Passpoint, dynamic peer discovery, ... OpenRoaming™

• Previous slides showed technology behind Passpoint and dynamic peer discovery
• We do this (in part) in eduroam

Insert: OpenRoaming™
• More roaming hubs, between mobile operators, vendors, providers, NGH trials
• Is not just secure Wi-Fi, but like eduroam accepts many (different) IdPs, SPs
• Complex matrix asks for complex technology
OpenRoaming™

• Developed by Cisco, transferred to WBA
• WBA’s Wireless Roaming Intermediary eXchange (WRIX) Framework Interconnect, reporting/rating/data clearing, settlement
• Policies (what SPs, IdPs, privacy modes)
• Roaming based on different RCOIs
  • OpenRoaming education RCOI
  • OpenRoaming ALL (compatible T&C)
  • Settlement or settlement free
  • Privacy: true identity or anonymous, CUI
  • Type: Vendor, Service Provider, Hospitality, Enterprise, Government, …
• WBAID (ours is “eduroam”, some suffixed by country ID)
In eduroam we require an App for (proper) (Passpoint) onboarding
Also, for: security, privacy

- Mutual authentication easiest attack-vector (EAPHammer)
  - -PAP < -MSCHAPv2 < EAP-TLS
- User is the weakest link
  - Trust-on-first-use (TOFU)
- https://eduroam.org/eduroam-advisory-mutualauth/
- Privacy wrt data “in the air”

- To configure everything right: use a profile
  - Outer username for privacy
  - Server mutual authentications (CAs (rollover!) and Common Names)
  - And why not: client-certificate (no passwords to steal)
Certificate validation Android, WPA3 R3 / Wi-Fi certification

• The Android December update removed the “Do not validate server certificate” option (complies with Wi-Fi alliance certification)

• Good, this was never a good idea! (But maybe users accidentally misconfigured.)

Still not OK? Options:
• Offer CA download
• “System certificates”
• Different EAP-type

Easier and better:
• Installer, eduroam CAT / geteduroam
eduroam CAT

👍
• Single place for profiles
• All settings correctly!

👎
• Android app
• No built-in credentials
• Certificate provisioning for users is hard
• HS20/Pp profiles hard
• Hosted IdP is not for a big userbase
geteduroam

👍

• Good client for all platforms
• Contains CAT profiles: works for all organizations!
• Passpoint, Hotspot 2.0 settings (OpenRoaming!)
• Alternative workflow to provision TLS pseudo-credentials using federated authentication (OAUTH, SAML)
• With that flow: also a Hosted IdP
• Initiative from NORDUnet and SURF

🤔

• Chicken-Egg: need connectivity for the app
geteduroam scenarios

- Use organization profile
- Hosted geteduroam, pseudo accounts via SAML
geteduroam, OpenRoaming

- User-friendly Apps to properly onboard devices
  - Replaces old eduroam CAT app for Android
- Increased security and flexibility with certificates and (Cloud) IdPs
- Comes at the right time for onboarding Passpoint/OpenRoaming, and WPA3 R3
- eduroam users may benefit from future OpenRoaming sites