Federated Roaming: Design and Results

Mark O'Leary, Jisc.

About Jisc

Digital solutions for UK education and research

Our vision is for the UK to be the most digitally-advanced higher education, further education and research nation in the world.

The Janet network:

- 9,000km of fibre connecting ~600 organisations to a backbone running at up to 600 Gbits/s;
- 3 Tbits/s peering capacity with 600+ providers;
- Carries 3 PetaBytes traffic per day / 1 ExaByte per year;
- “Busiest NREN in Europe” – Géant.

The visitor requirement

You ideally need to know:

- Who they are;
- What organization they are affiliated to;
- Current status with that organization;
- Will they meet local acceptable use policies;
- Is their device appropriately configured.

You might also need to know:

- Who they are visiting / who will vouch for them;
- How long they plan to stay.

Jisc

Overheads

This might entail:

- Checking ID documents;
- Telephoning their employer;
- Getting a signature on an AUP agreement;
- Helping configure their device;
- Having a colleague sign them in;
- Securely issuing a temporary credential;
- Ensuring credentials are revoked promptly;
- Incurring GDPR responsibilities.

But someone already holds this info…

Their employer:

- Has robust identity verification;
- Can give real-time feedback on their status;
- Has a contractual relationship that can help enforce any agreement;
- Manages issued devices.

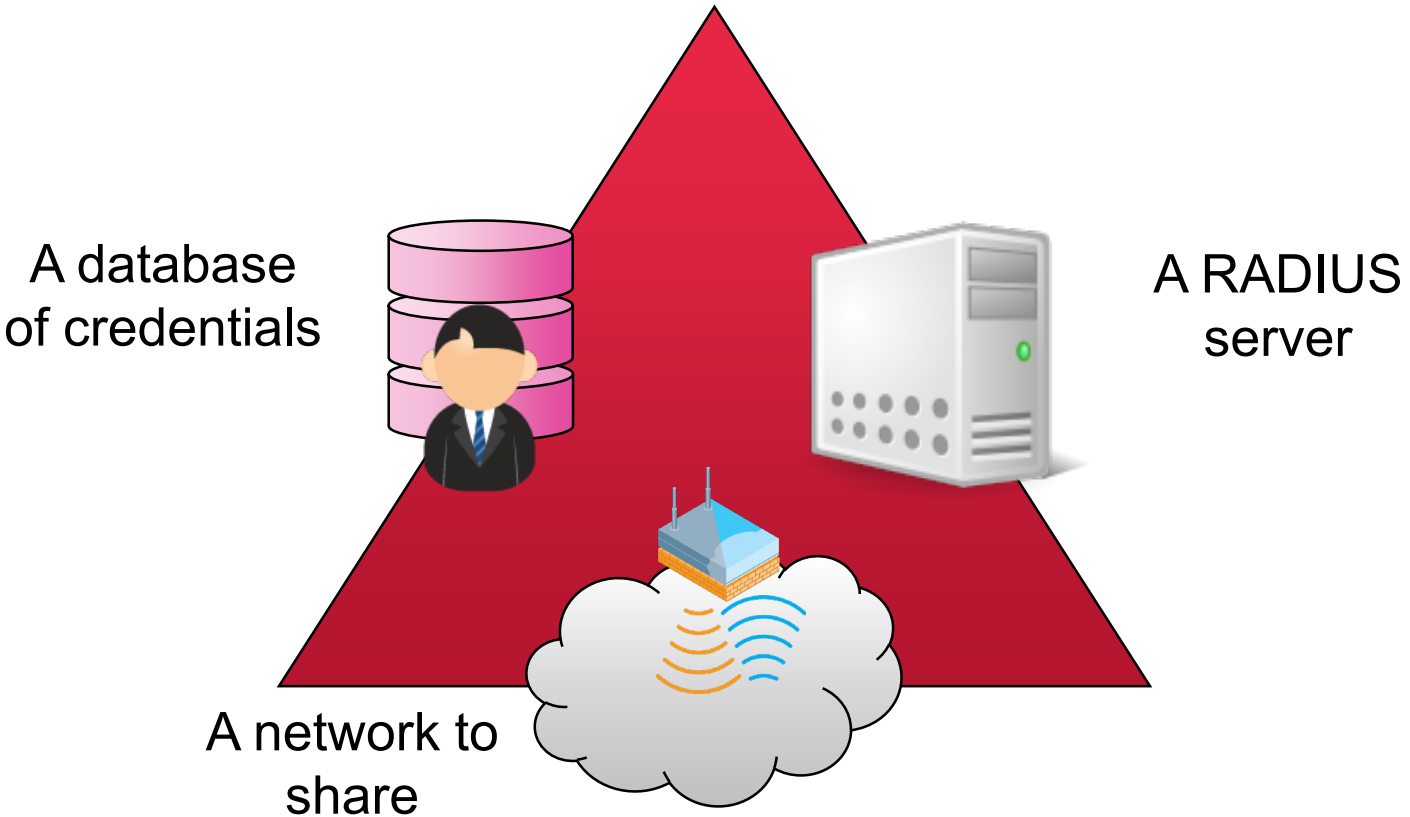
Federated roaming

Decouple grant of access from authentication, pushing responsibility for authentication back to the employer, who is best placed to make an informed decision.

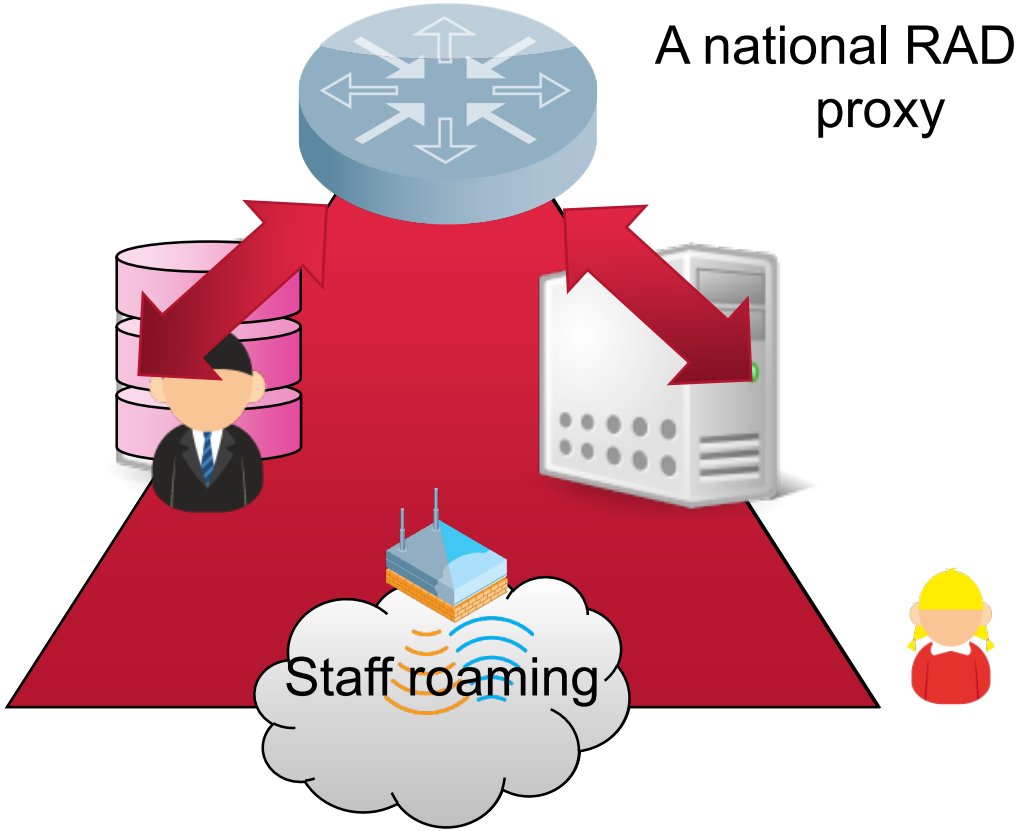
Support this mechanism with policy that binds both ‘visited’ and ‘home’ organisations into a fabric of trust.

Jisc

How does it work?

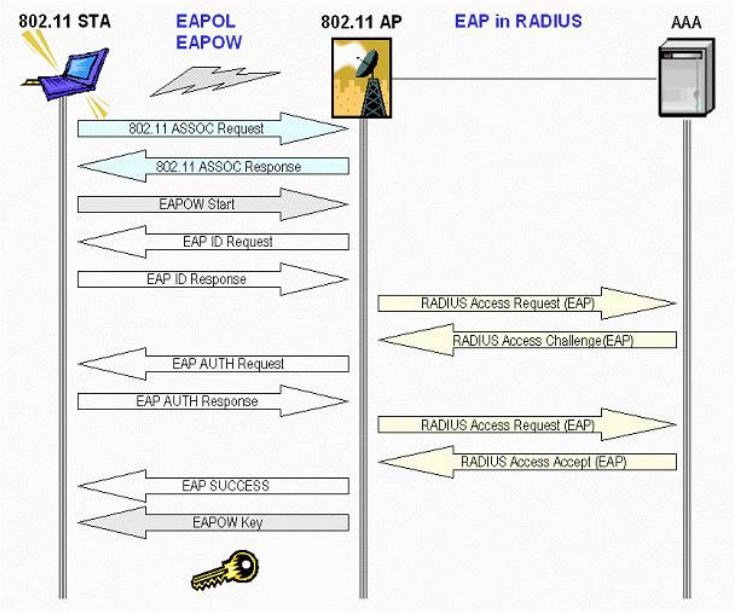


How does it work?



A little more detail

- Supplicant software on the end user's device manages an 802.1X authentication against a certificate-verified home RADIUS server using any authentication mechanism that can be EAP encapsulated.
  - Provides strong cryptographic protection of credential payload
  - Mutual authentication through certificate exchange (network validates client and client validates network)
  - Uses dynamic keys



What problems does this solve?

For the visitor:

- Your devices are already configured to connect before you arrive at participating venues;
- You don’t have to prove your identity/status or find hosting staff to sign off your access;
- You don’t have to reconfigure your device, or read and sign any local terms and conditions;
- If you experience a problem, you don’t have to hunt for a help desk in the visited location, you just phone back to your familiar home support team, and they will investigate on your behalf;
- You’ll often encounter connectivity in places you weren’t expecting.

What problems does this solve?

For the home organisation:

- Your mobile workers gain access to high quality connectivity with guaranteed productivity features (email, web and VPN) available;
- Every time your staff member logs on, you get a record of the authentication – and the option to permit or deny it as required, in real time;
- You save on purchasing mobile data sim-based products, as the federated alternative is free at point of use, and not metered by bandwidth consumed or number of users per organisation.

What problems does this solve?

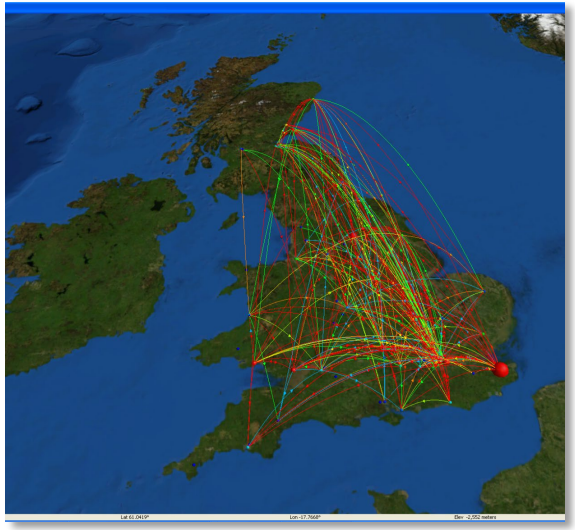
For the visited organisation:

- You don’t need to provide a visitor helpdesk;
- You don’t need to manage a temporary account mechanism, with its associated increase in attack surface;
- By contributing a guest LAN to the federated commons, you gain the right for your staff to securely access guest networks at other participating venues;
- You get the benefit of a minimal GDPR overhead guest facility, but with the capability to recover full visitor identity by reconciling logs with their home organization.

Examples of federated roaming - 1

eduroam is the global federated roaming solution for education.

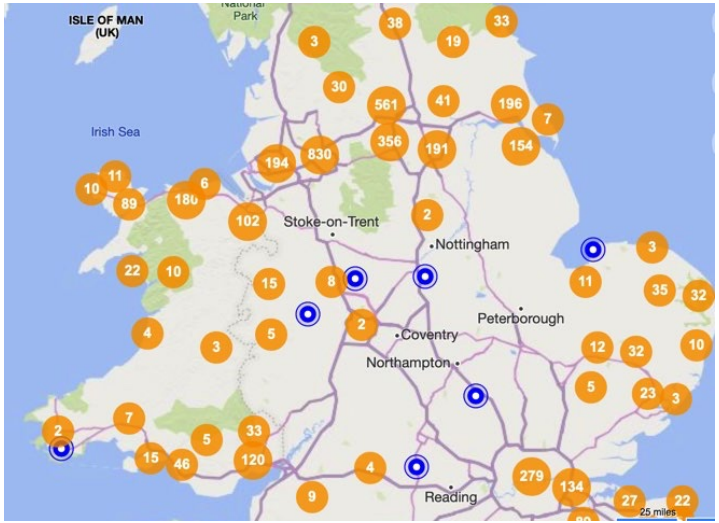
- Ubiquitous roaming connectivity across 119 countries;
- ‘zero touch’ user experience;
- GDPR-compliant solution;
- Builds on existing infrastructure.



- **In March 2019 in the UK alone:**
  - **11,158,192** roaming-days* (50k+ person-years!) facilitated;
    - Assuming 5 minutes boarding time saved, this equates to the work of ~1k extra full time staff for a year
  - **1,599,258** unique devices seen on the network.

* *Roaming day = a day on which we saw a unique device connected to eduroam away from its home site at least once.*

Examples of federated roaming - 2



govroam is the federated roaming solution for the wider public sector.

- UK-only at present (future inter-federation likely);
- ‘zero touch’ user experience;
- GDPR-compliant solution;
- Builds on existing infrastructure.

- Launched October 2016
- Now available at 4,571 public venues across the UK
- 42% NHS, 40% government by organisation

building better healthcare awards 2019
WINNER

Example use case: KentPSN

Govroam deployed at:

100+ council buildings, 100+ university buildings, 87 libraries, 63 fire stations, 49 children's centres, 8 youth centres, 6 hospitals, 5 adult education centres, 4 leisure centres, 3 family centres, 1 theatre and 1 castle.

~6,500 user sessions per week in 2018

Co-deployed with eduroam at many of these venues.

Key applications:

- BREXIT
- Supporting safeguarding of adults service transition to paperless working;
- Kent Resilience Forum – Fire and Rescue staff embedded in KCC council offices during emergency conditions;
- Joining up health and social care, e.g. for Medway Community Health, East Kent Hospitals;
- Closer collaboration with education (offering eduroam alongside govroam at 208 sites);
- Enhanced engagement with the Kent Interdisciplinary Research Centre for Cyber Security;
- Supported auditors assessing KCC readiness for 2018 web accessibility legislation;
- Recruitment and student placements.

Take home message

- A federated approach offers a number of advantages for supporting roaming across a defined community;
- The required infrastructure builds from proven, simple components and reuses what is already deployed in local solutions;
- The *-roam services are delivering savings and efficiencies across the public estate.

Jisc

Thanks for your attention