eduroam
Technology and Service Overview

African eduroam Roadshow
February 12, 2021
Miroslav Milinović, CARNET/SRCE

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856728 (GN4-3).

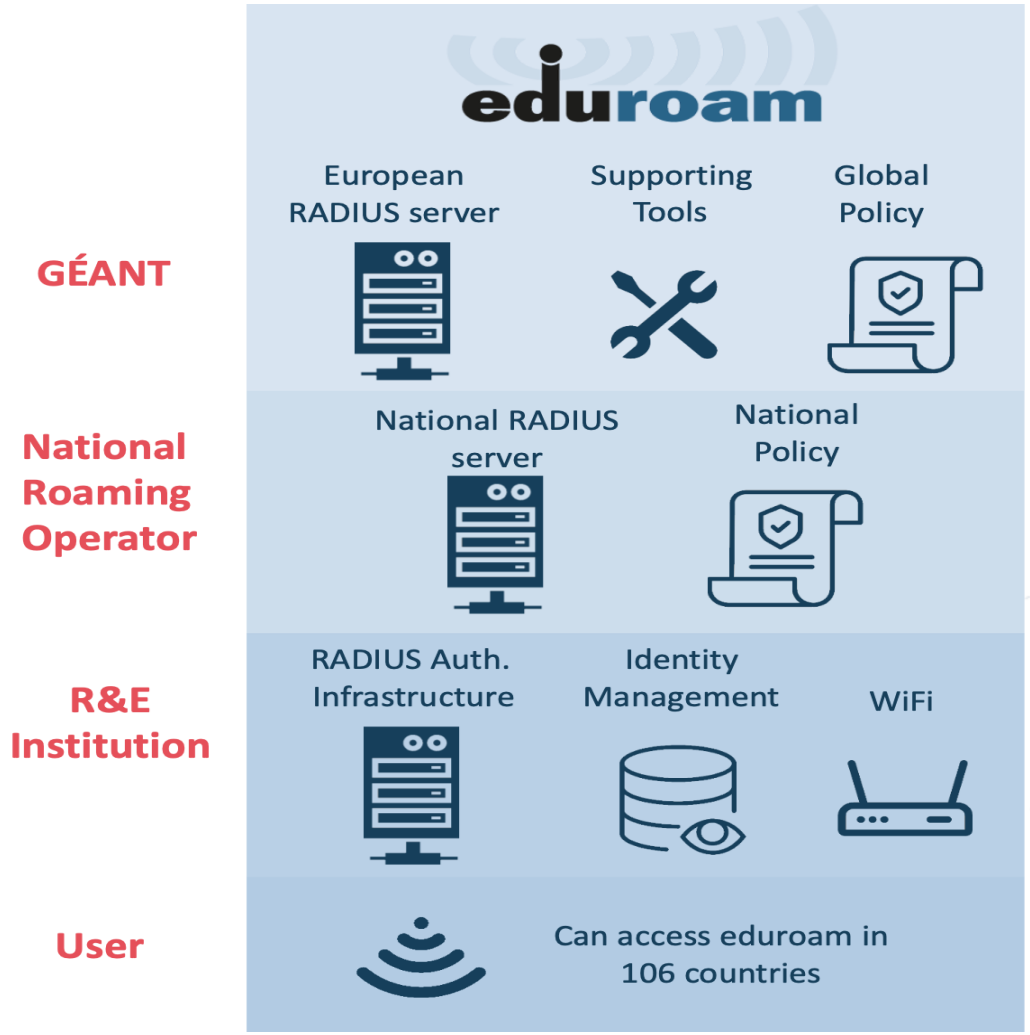
Contents

- eduroam in a nutshell
- Technology overview
- Service organisation
- Supporting services
- Future work

eduroam service in a nutshell (1)

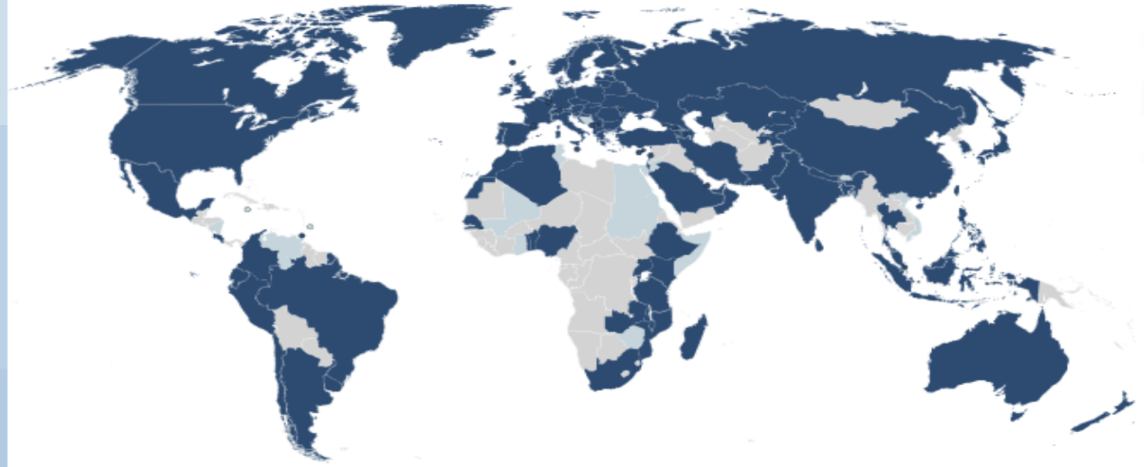
- **objectives:** build and maintain **edu**cation **roam**ing service
  - provide secure, consistent and uniform network access service (inside the boundaries of the confederation)
- motto: "**open your laptop and be online**"
- **eduroam infrastructure:**
  - **technology infrastructure**:
    - **(E)TLRSs**, FLRSs, IdPs and SP RADIUS servers, network access elements (APs/switches)
  - **supporting infrastructure → supporting services suite**
    - eduroam web (www.eduroam.org) & wiki site (wiki.eduroam.org)
    - eduroam database
    - monitoring, diagnostics, metering service (F-Ticks)
    - configuration assistance (CAT)
    - managed IdP service (MIdP)
    - ...

eduroam service in a nutshell (2)



#love2eduroam

Access to thousands of eduroam WiFi locations worldwide, with R&E institutional identity



Why eduroam?

- researchers, teachers, students, … :
  - travel with WLAN-enabled devices
  - want transparent, secure network access
  - want the same experience at visited institution as home
- experience facilitated by seamless sharing of network resources
- better for roamers, easier for administrators

It all started with ...

- TERENA TF-mobility (inter-NREN) roaming requirements (http://www.terena.org/activities/tf-mobility/deliverables/delC/DelC1-4.pdf)
  - identify users uniquely at the edge of the network
    - guarantees reasonable security and data integrity
  - enable guest usage
  - scalable
    - local user administration and authentication
  - easy to install and use
    - at the most one-time installation by the user
  - open
  - complies with privacy regulations

Technology overview

eduroam: authentication and authorisation

- Authentication:
  - Is the user who they say they are?
  - Carried out by user's home institution (IdP)
- Authorisation:
  - What network access should the user be granted?
  - Determined by visited institution (SP)

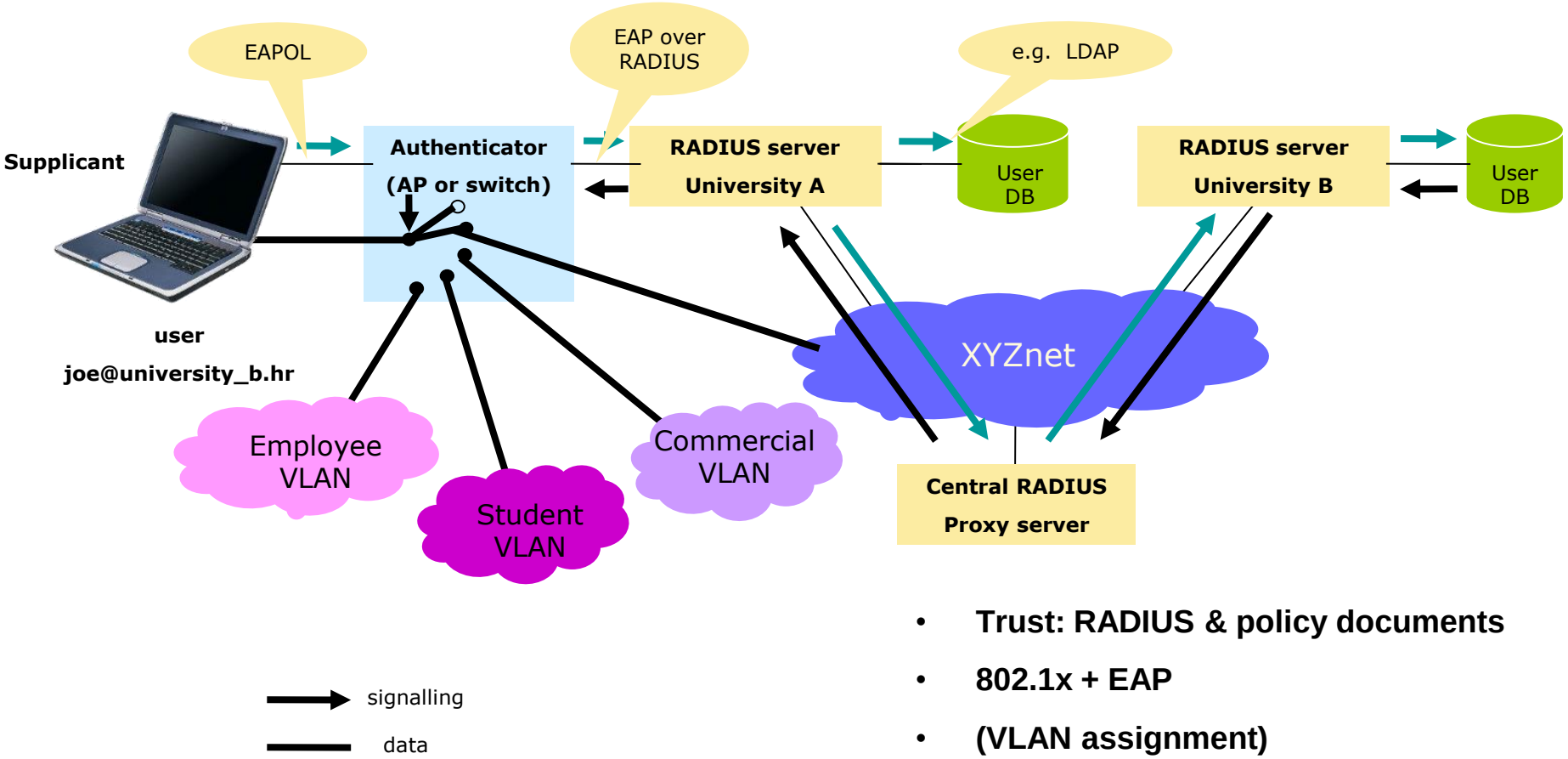
Terminology and concepts

- Home institution = **Identity Provider**.
  - Provides identity management database.
  - Responsible for user authentication.
  - Interface to eduroam: RADIUS server.
- Visited institution = **Service Provider**.
  - Provides network infrastructure (e.g. Access points, VLANs, internet access, optionally own RADIUS server).
  - Responsible for user authorisation.

Key eduroam technologies

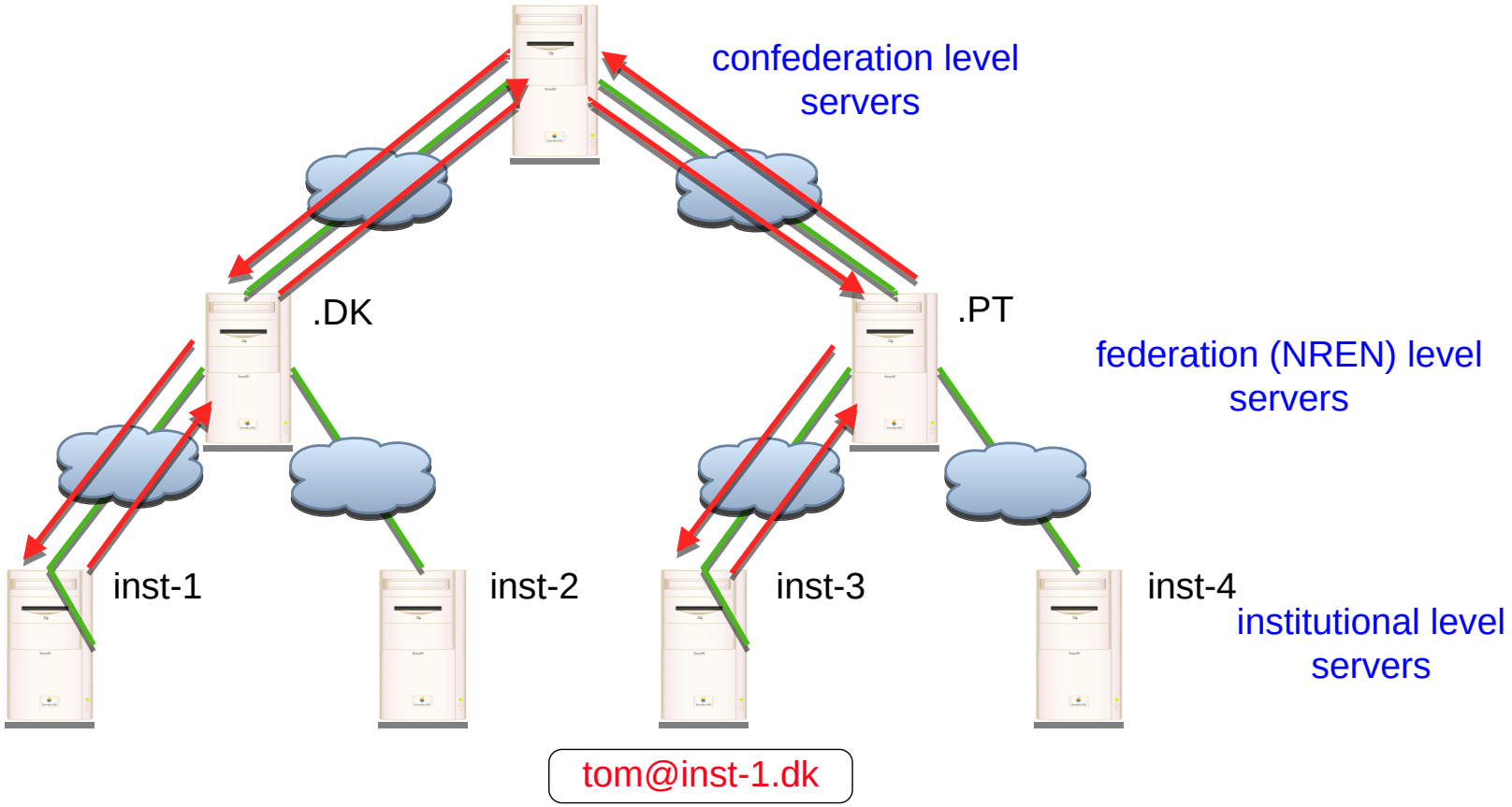
- Security based on 802.1x (standard for layer-2 port-based network access control)
  - integration with VLAN assignment (IEEE 802.1q)
  - detects user at network's edge (NAS = AP or wired switch)
  - protection of credentials (encrypts all data using dynamic keys)
  - until identity is proven allows only Extensible Authentication Protocol (EAP) traffic
  - 802.1x clients (enduser devices) reasonably easy to configure (with tools like CAT)
- Authentication based on EAP
  - different authentication mechanisms possible by using EAP (TLS, TTLS, PEAP, …)
- Roaming based on RADIUS proxying
  - Remote Authentication Dial In User Service
  - transport-protocol for authentication information
  - scalable
- Trust fabric based on:
  - technical: RADIUS hierarchy
  - policy: documents/contracts that define the responsibilities of user, institution, (N)RO

The eduroam™



- **Trust: RADIUS & policy documents**
- **802.1x + EAP**
- **(VLAN assignment)**

Forwarding the user's credentials via RADIUS hierarchy



Forwarding the user's credentials

- Realm-based proxying:
  - User names in format: "user@realm's DNS-like domain name".
  - Used to forward request to next hop in hierarchy.
- Institution's RADIUS server only communicates with:
  - Its federation's RADIUS server.
  - Its institution's NASs.
- Shared secrets authenticate other servers in hierarchy.

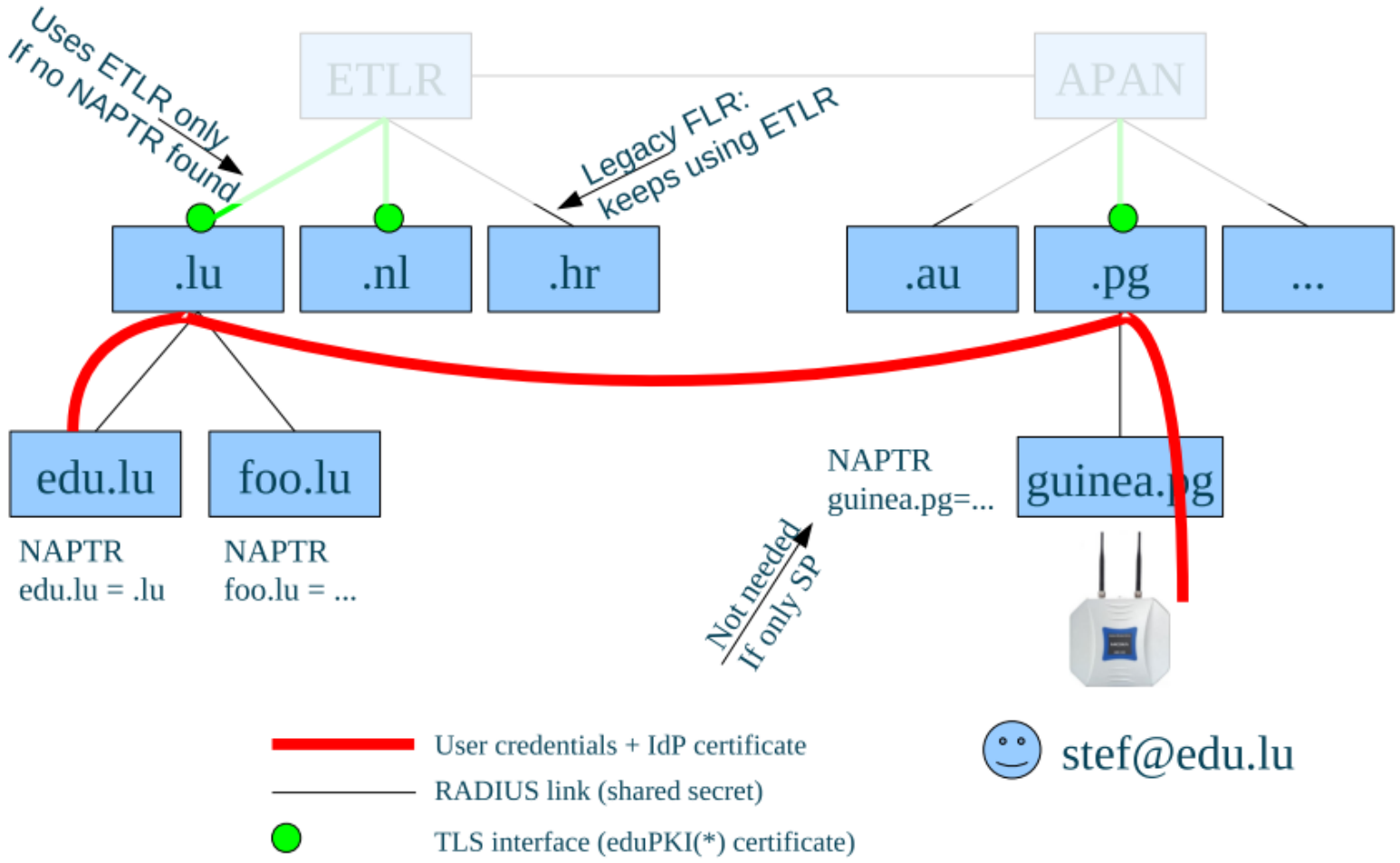
Forwarding the user's credentials (European example)

- European confederation has Top-Level RADIUS servers (ETLRs):
  - In the Netherlands, and
  - In Denmark.
- Each has a list of connected country domains.
  - .nl, .dk, .hr, .de etc.
- Each ETLR:
  - Accepts requests for its connected countries.
  - Forwards them to appropriate Federation Level RADIUS server.
  - Forwards requests for other countries to other TLRs (e.g. Asia-Pacific).

Forwarding the user's credentials - RadSec

- RADIUS/TLS (radsec) instead of RADIUS
  - IP address and shared secrets of RADIUS are obsolete
  - Replaced by TLS certificates
  - Better encryption than (plain) RADIUS
  - More flexibility for *dynamic discovery*, which will eventually replace the hierarchy
- Old RADIUS uplinks will remain in place for a (long) while
- How to:
  - eduroam wiki
  - radsecproxy SW
  - note: ongoing development

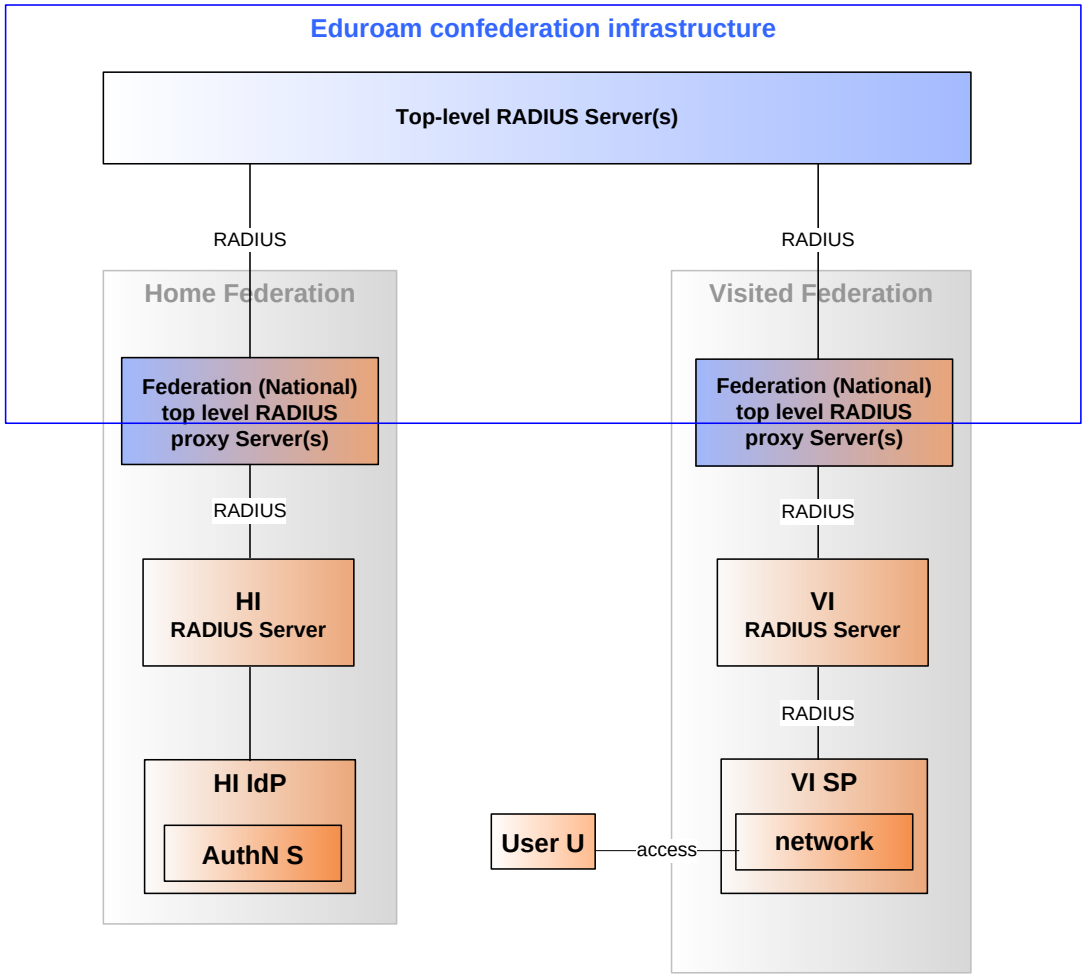
Radsec & dynamic discovery



Ensuring user credential security

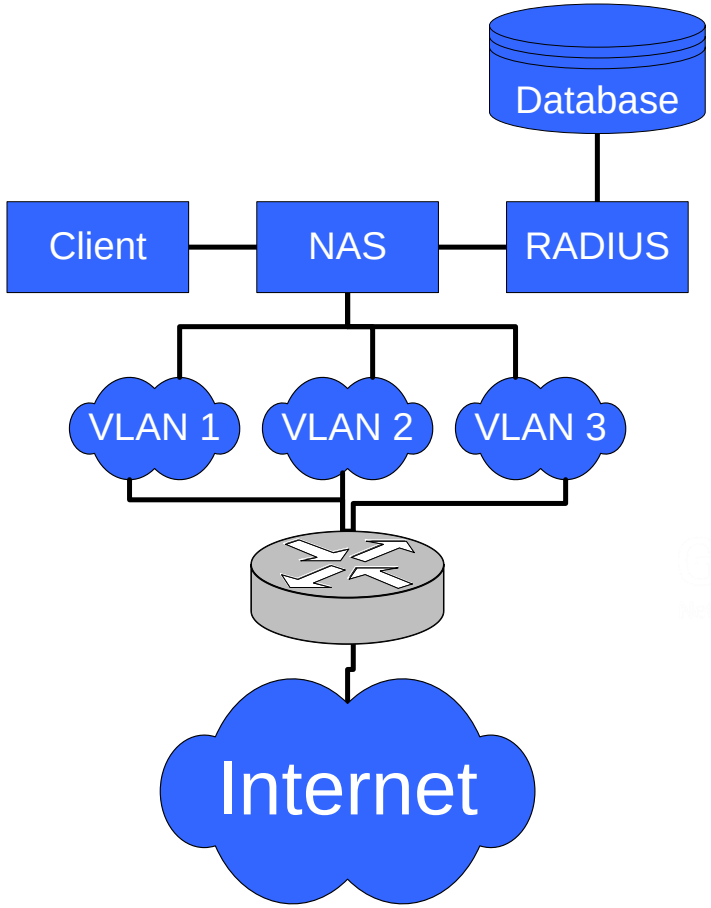
- Users' credentials are tunnelled through the RADIUS hierarchy.
- User credential security is a necessity in eduroam.
- Recommended approach:
  - EAP combined with TLS-type protocol.
  - Mutual user-server authentication.
  - Encrypted user credentials.
- Sending unencrypted credentials is prohibited.

eduroam infrastructure



The authorisation process

- VLANs in SP each have different permissions.
- Each VLAN connected to different parts of campus.
- When authentication is successful:
  - SP's RADIUS server sends configuration options to NAS.
  - NAS assigns client to a VLAN.



Service organisation

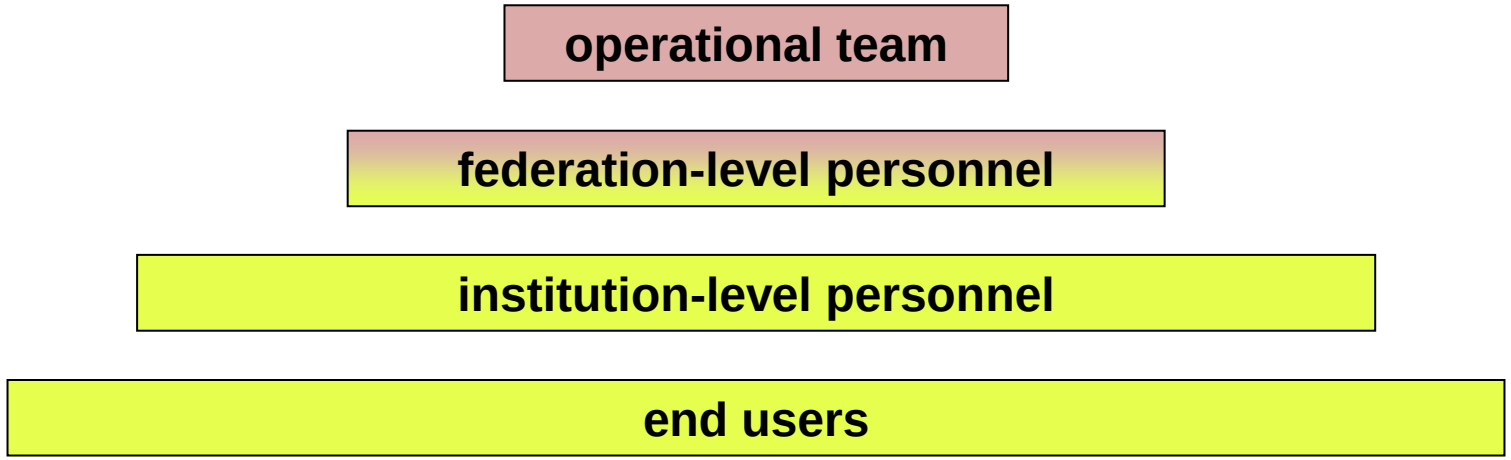
From a pilot to a service

- TF-Mobility started work on eduroam in 2002
- GN2: JRA5 (2004) → SA5 (2007)
  - European eduroam Policy v .1.0 (January 2008)
  - supporting services
  - service officially started on September 1, 2008
  - http://www.eduroam.org
- GN3 (2009-2013) / GN3plus (2013-2015) → GN4 (2015 - …)
  - European eduroam Policy v .2.0 (July 2012) https://www.eduroam.org/support/eduroam-documentation/
  - further development of infrastructure and supporting services
- GeGC (Global eduroam Governance Committee) (2011 - …)
  - global governance
  - eduroam Compliance Statement (October 2011) https://www.eduroam.org/wp-content/uploads/2016/05/eduroam_Compliance_Statement_v1_0.pdf

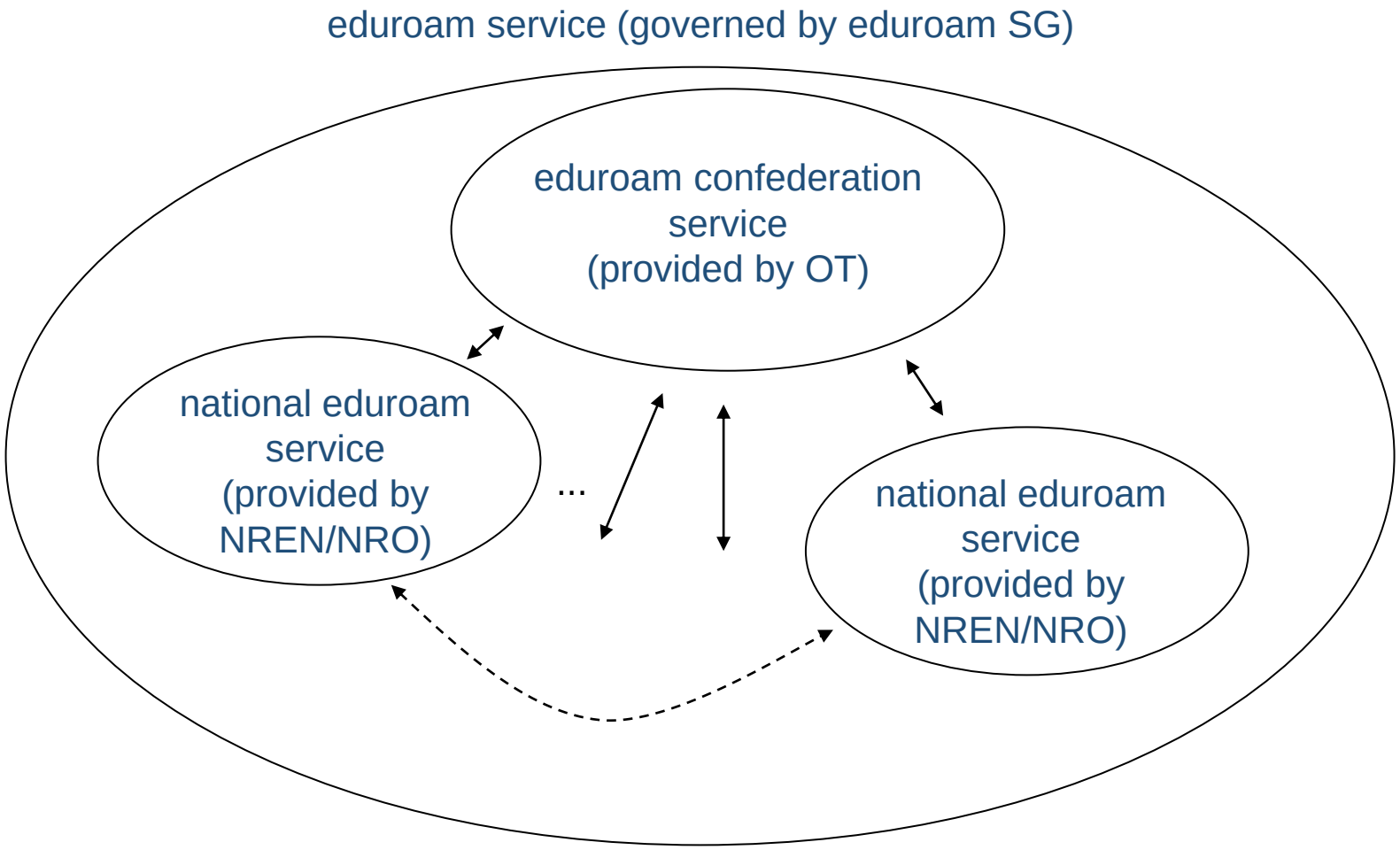
eduroam policy documents

- Policies define the rights and responsibilities of:
  - (national) roaming operators – (N)ROs
  - Institutions (IdPs and SPs)
  - Users
- Global and confederation policies
  - (global) eduroam Compliance Statement
  - European eduroam service policy
  - see: https://www.eduroam.org/support/eduroam-documentation/
  - for list of members (ROs) see: www.eduroam.org / monitor.eduroam.org
- National (local) policies
  - (N)ROs should have their own policy
  - allows for regional variations (that should not contradict global rules)

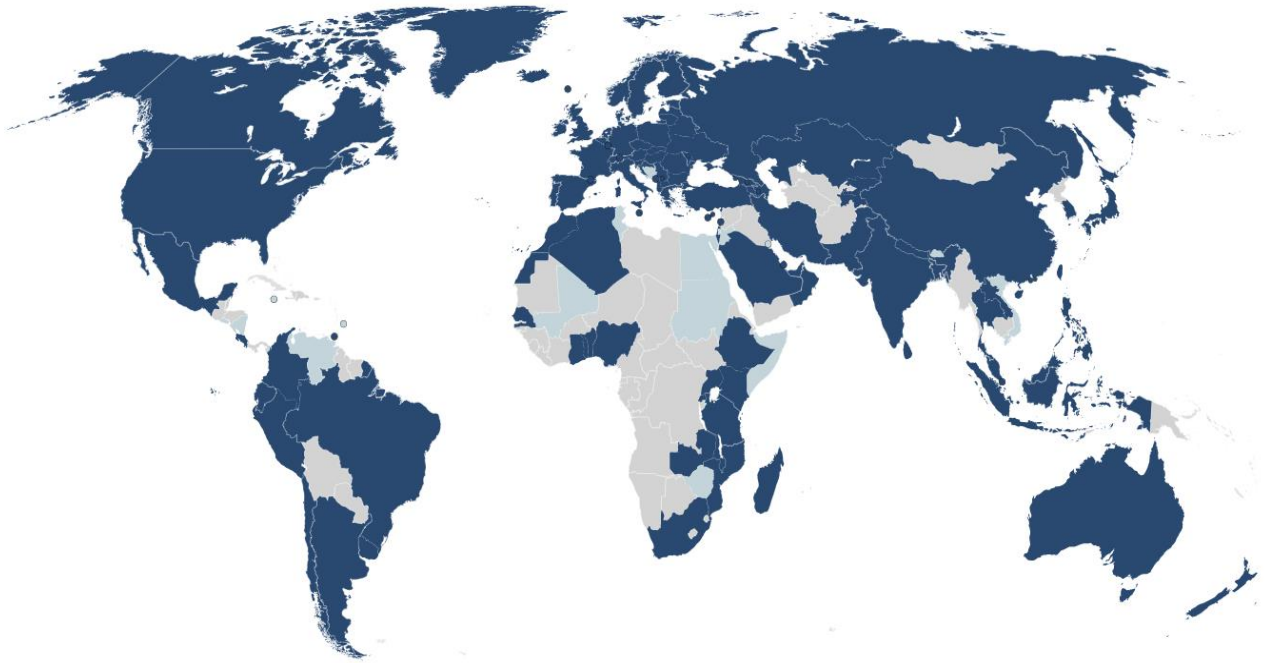
eduroam service “stack”



(European) eduroam service model

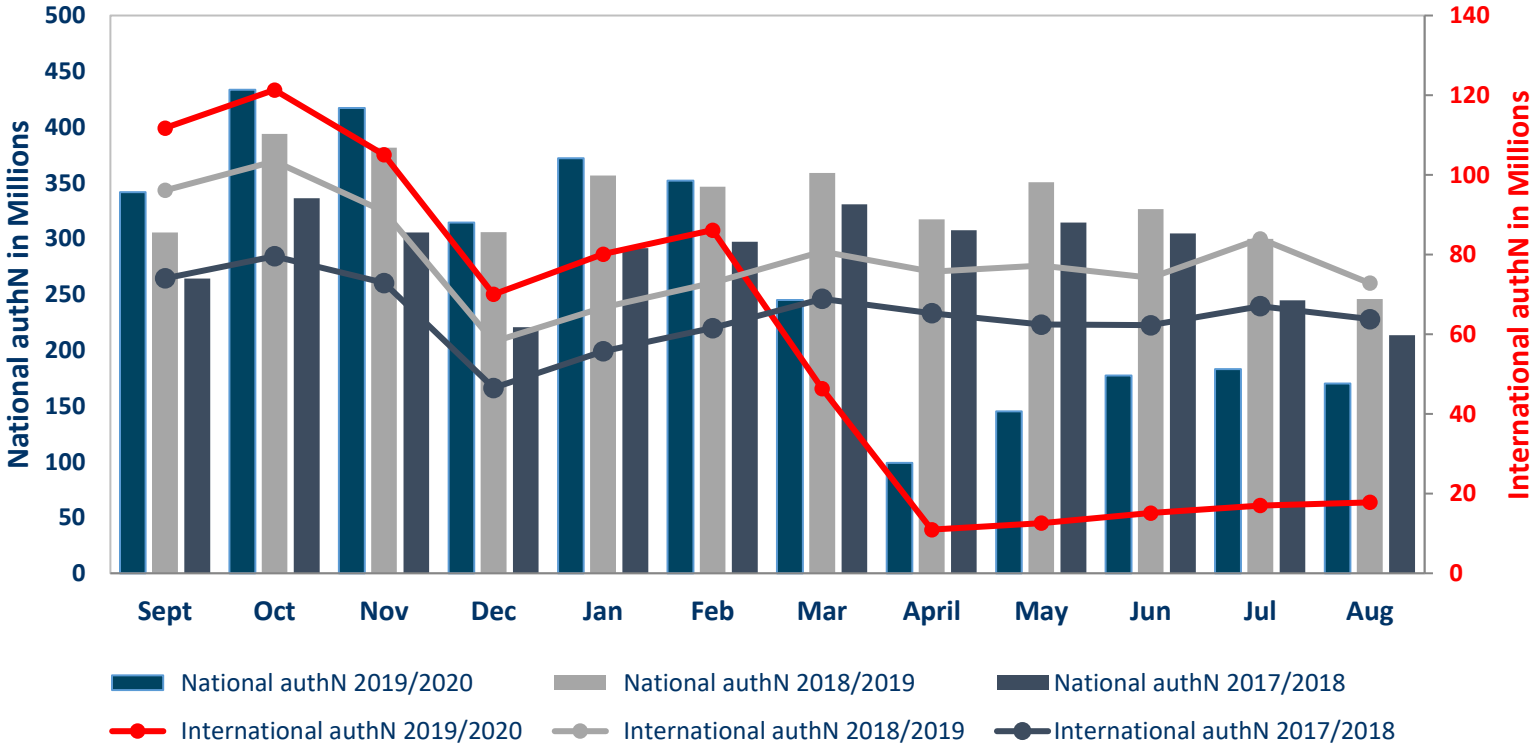


eduroam uptake



What is eduroam (video):
https://www.youtube.com/watch?v=qk9aljqu20A

eduroam in numbers



>1 billion international authN in 2019

Visible impact of COVID-19 in 2020

National traffic based on F-ticks

International traffic based on etlr logs

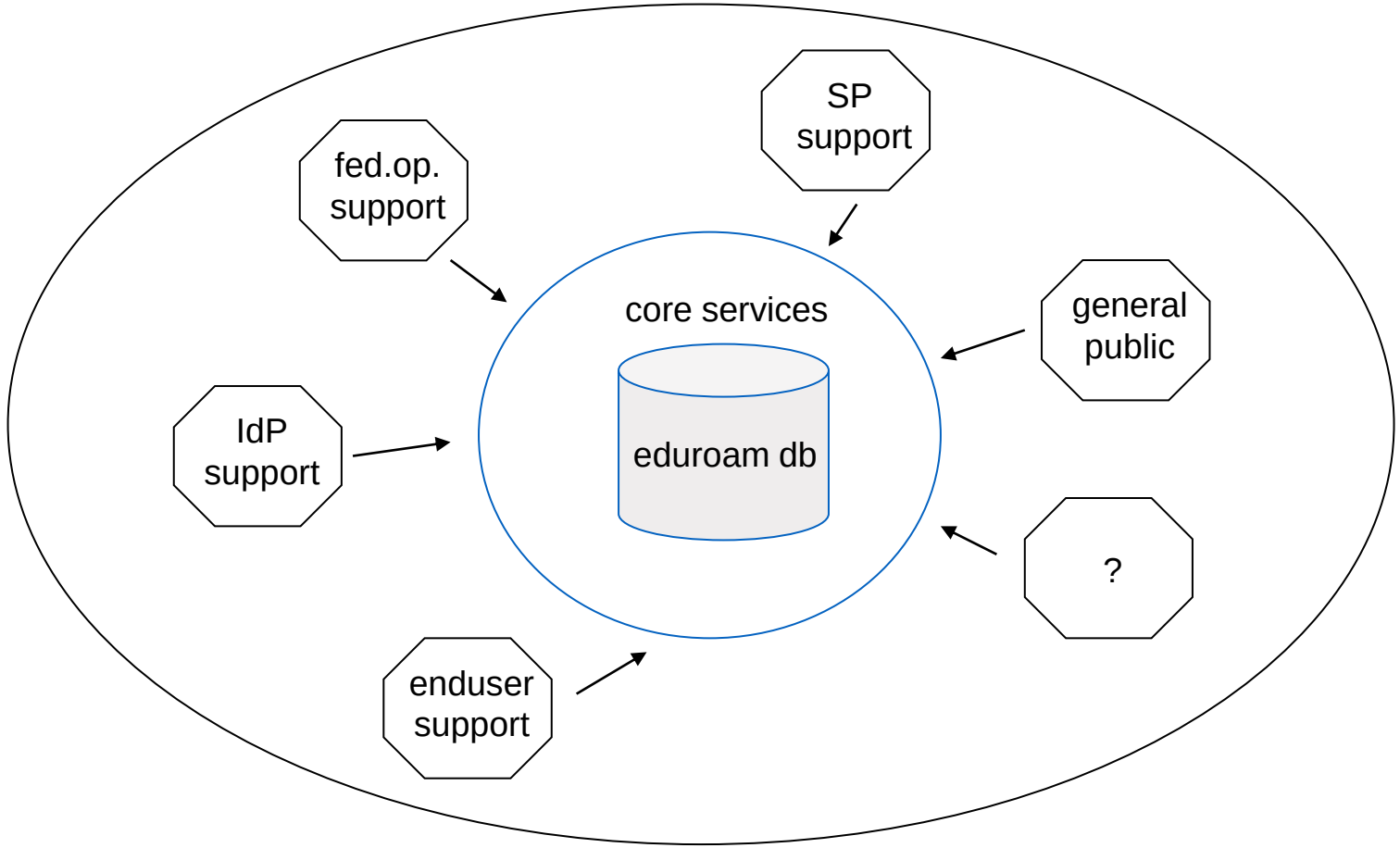
- 106 countries (51 European)
- + 19 pilots
- eduroam db facts
  - 6500+ institutions
  - 29.000+ service locations
  - data provided by 90 countries
  - data in v.2 format provided by 77 countries

Supporting services

eduroam supporting services

- supporting infrastructure → supporting services suite
  - eduroam web (www.eduroam.org) & wiki site (wiki.eduroam.org)
  - supporting services portal: monitor.eduroam.org
  - contacts:
    - first level support via GEANT OC (help@eduroam.org)
    - supporting services (monitor@eduroam.org)
    - eduroam OT - support for (N)ROs (eduroam-ot@lists.geant.org)
    - eduroam development (development@lists.eduroam.org)
  - eduroam database
  - monitoring and metering service (F-ticks: monitor.eduroam.org)
  - diagnostics, configuration assistance (CAT tool: cat.eduroam.org)
  - managed IdP service (hosted.eduroam.org)
  - …

Supporting services suite (1)



Supporting services suite (2)

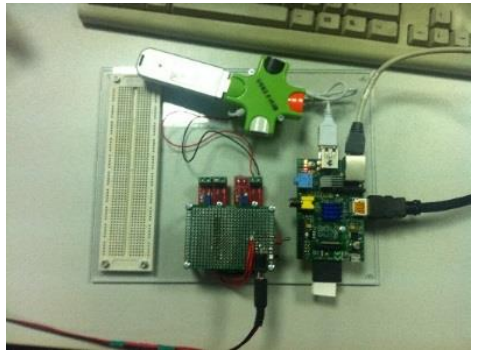
- based on the concept known as OSS (operations support system)
- supporting apps. portfolio to meet the needs of all user groups
  - end-users, IdP-admins, SP-admins, fed-admins, OT
  - general public
- eduroam db is a core data source
  - data provided by NROs
  - completeness & open data (?)

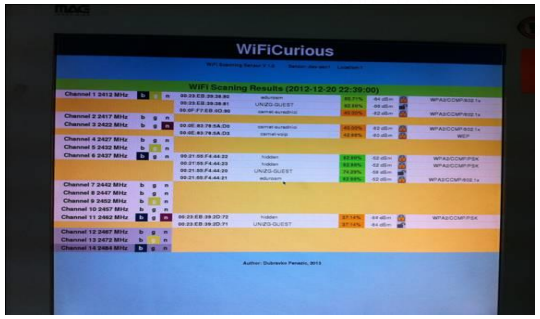
The eduroam database

- Database includes:
  - National Roaming Operator (NRO) representatives and contact details.
  - Local institutions official contacts.
    - Both Service Provider (SP) and Identity Provider (IdP).
  - Information about eduroam hot spots.
    - SP location, technical information.
  - Monitoring information.
  - Information about the usage of the service.
- NROs:
  - Should provide the necessary data (general and usage data).
    - Data must be provided in the agreed XML (or JSON) format. (https://monitor.eduroam.org/fact_eduroam_db.php)
    - Data will only be accessible from the eduroam database server.
  - Should use DB specification (ver 2.0)

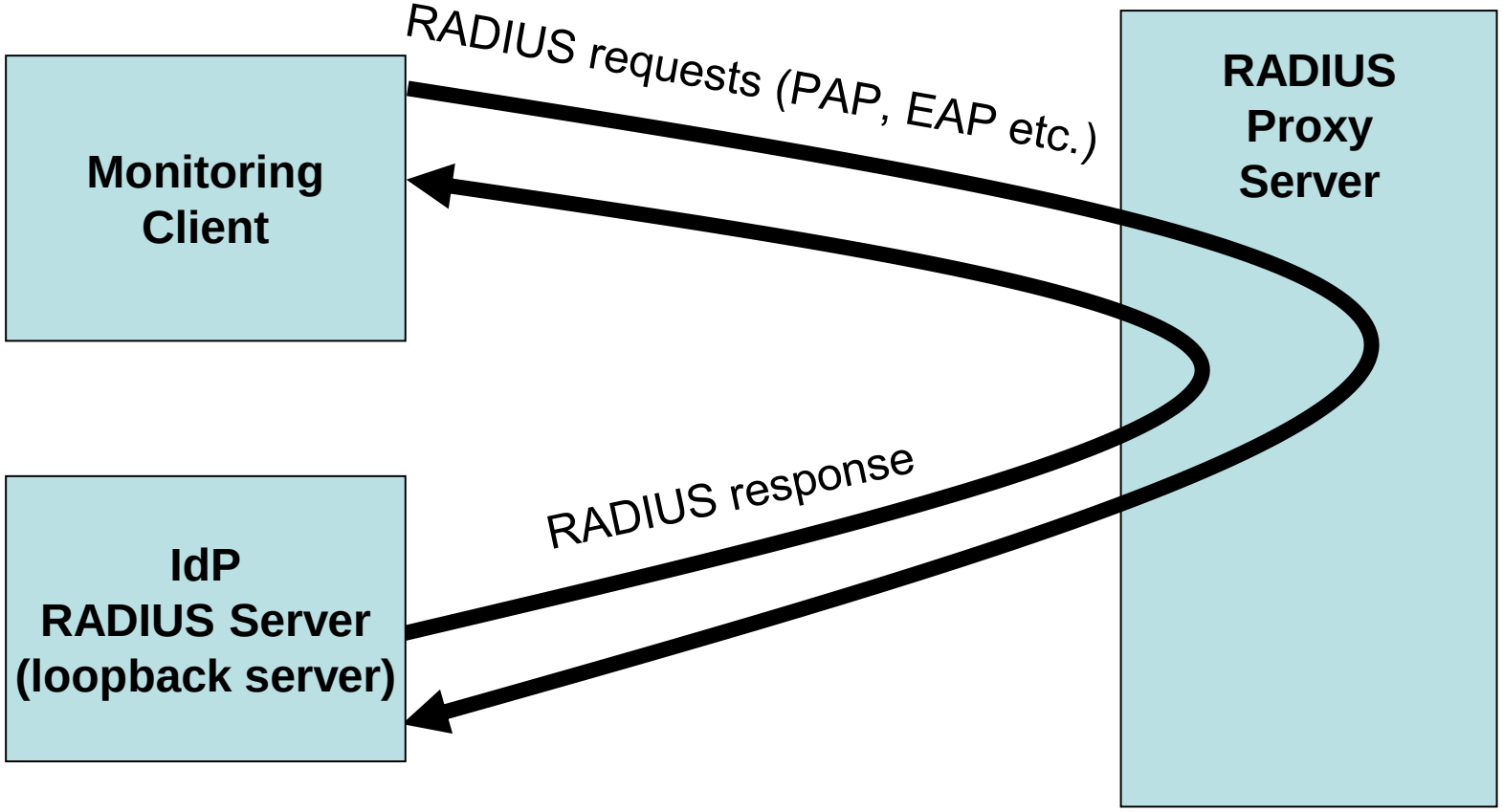
Monitoring

- monitor functionality of the eduroam infrastructure:
  - servers, infrastructure, user experience
- perform both accept and reject logic tests
- ultimate goal is to test real user experience
- challenge: diagnostics tools for end users
- current status:
  - https://monitor.eduroam.org
  - monitoring (E)TLRs and NRO Servers (FLRSs)
  - 3 monitoring scenarios (monitoring servers, monitoring infrastructure, testing on demand)
  - **ongoing development**

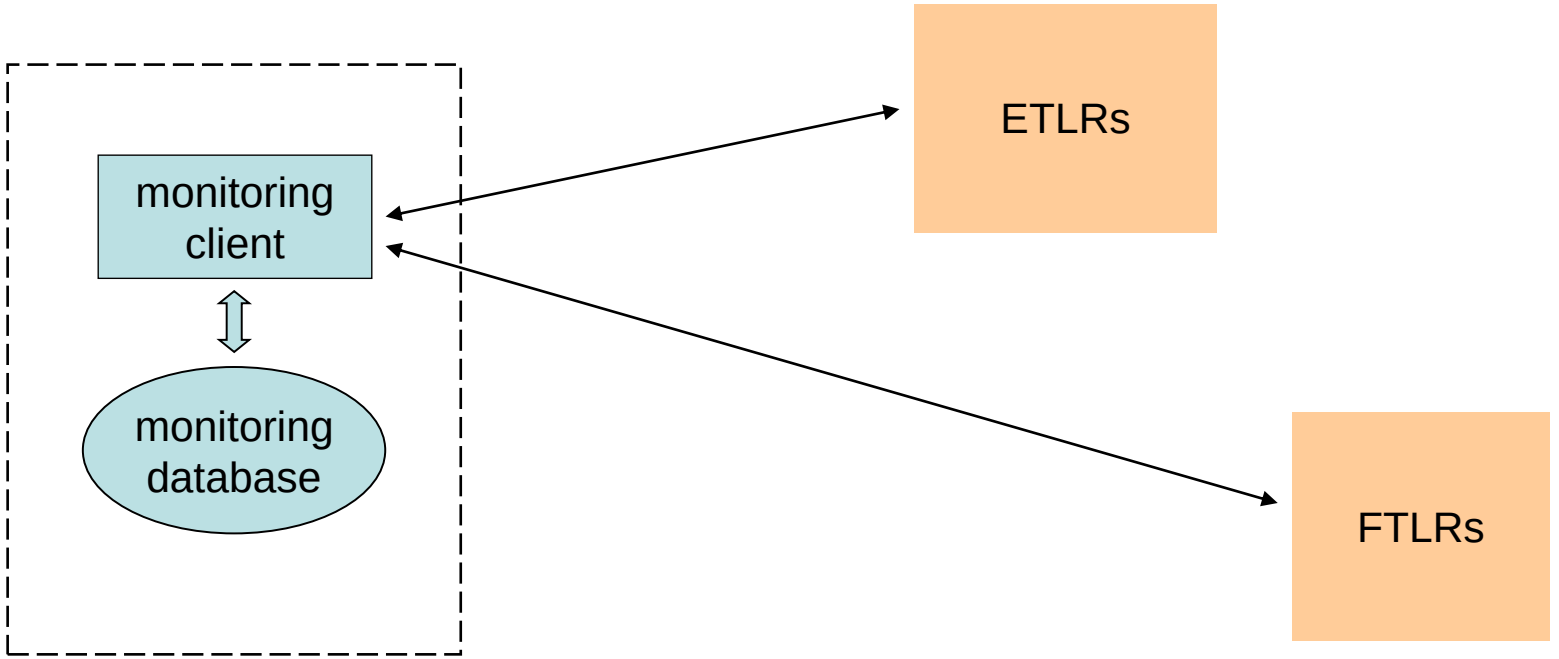




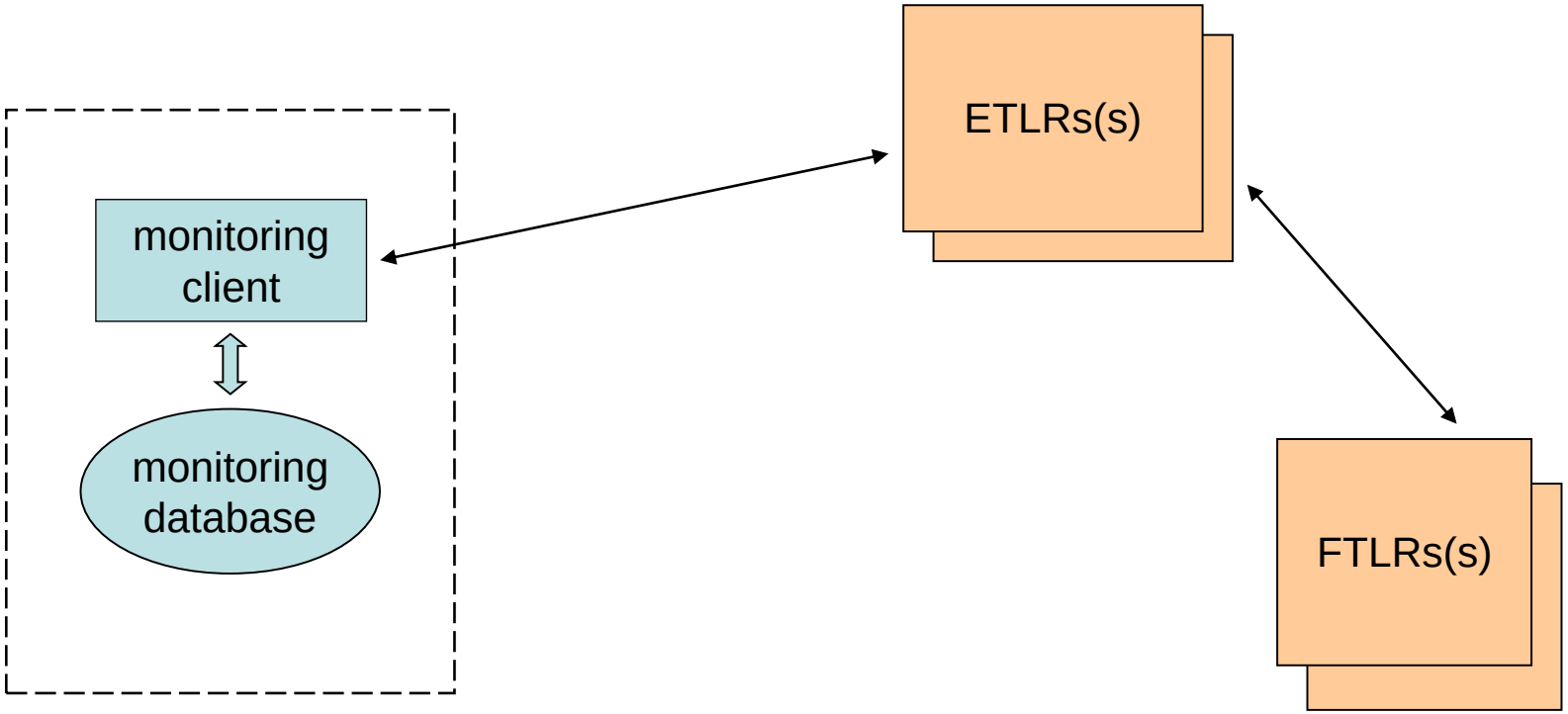
Monitoring concept



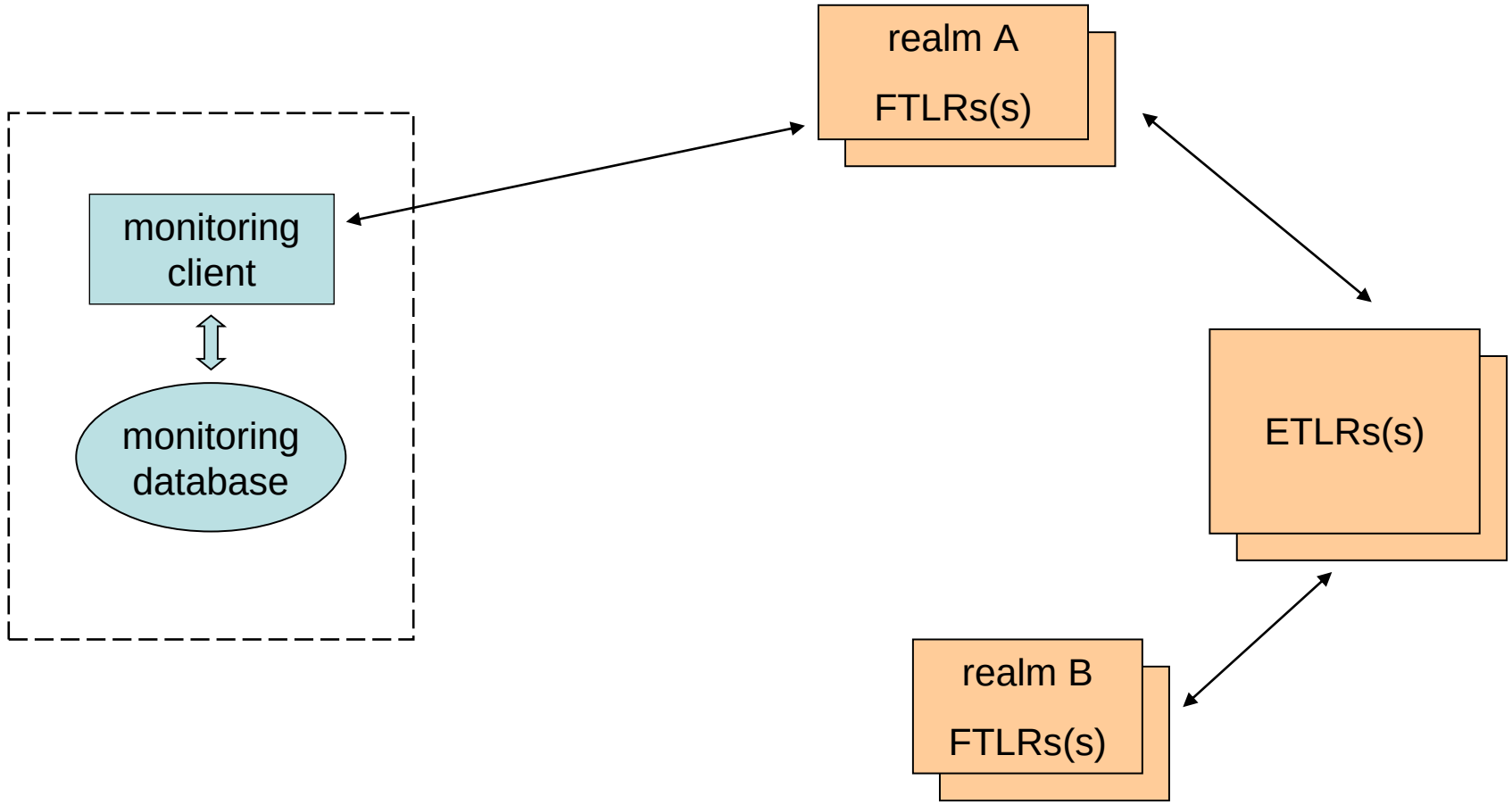
Monitoring scenarios (servers)



Monitoring scenarios (infrastructure)



Monitoring scenarios (testing on demand)



Metering: F-Ticks

- solution for collecting AuthN traffic stats
- simple, based on syslog
- http://monitor.eduroam.org

- message formats:
  - basic:
    `F-TICKS/eduroam/1.0#REALM=%R#VISCOUNTRY=HR#CSI=%{Calling-Station-Id}#RESULT=OK#`
  - extended:
    `F-TICKS/eduroam/1.0#REALM=%R#VISCOUNTRY=HR#VISINST=SP-Name#CSI=%{Calling-Station-Id}#RESULT=OK#`

- http://www.ietf.org/archive/id/draft-johansson-fticks-00.txt

eduroam CAT

- Configuration Assistant Tool
- http://cat.eduroam.org (in production since March 2013)
- build to help users and IdP admins
- generate “installers” to ease the client device configuration process
- provides diagnostics functions for IdPs
- software development homepage: https://github.com/GEANT/CAT
- https://cat-test.eduroam.org – test version
- current version 2.0 (2.0.4. ETA end of February 2021)
- documentation at https://wiki.eduroam.org
- mailing list cat-users@lists.geant.org

Why eduroam CAT?

- eduroam is a secure roaming service
  - 29.000+ hotspots
  - 4116 supported IdPs on February 1, 2021
  - 4.960.000+ profile downloads in period January 1, 2020 – December 31, 2020 (over 32.400.000 dowloads since start in 2013)
- credentials will only be disclosed to the user's "home" server (IdP)
- no hotspot (eduroam SP) or any unauthorised rogue AP/server can grab credentials …
- … IF the user cares enough to verify that he is actually connecting to his own eduroam IdP!
- software on typical end-user devices makes it too easy to neglect security – automation of the setup process is required.

How does eduroam CAT help?

- collects required setup parameters from the eduroam IdP
  - simple web interface
  - expert system verifies that information is complete and correct
- transforms parameters into automated installation programs for the eduroam Identity Provider's end users:
  - "just click" and eduroam will be installed
    - with all complexity hidden from the user
    - with full security enabled
    - digitally signed
  - for most of operating systems:
    - MS Windows 7, 8, 8.1, 10
    - Mac OS, iOS
    - Android, Linux, Chrome OS
  - setup instructions in many languages

How does eduroam CAT work?

1. end user Interface
   - selection of Identity Provider
   - download and execution of Installer

2. administrator Interface
   - overview of settings
   - deep-link to own download area
   - expert system: setup verification

- sign-up for IdPs – by invitation only:
  - eduroam Identity Providers should contact their eduroam National Roaming Operator (NRO) and request access
  - they will receive a one-time authorisation token with a login link

eduroam Managed IdP service

- Target groups:
  - institution administrators who do not have the skills or capacity to run their own RADIUS IdP infrastructure
  - end-users in such institutions who want to benefit from eduroam despite the institution's incapacity
  - NROs wishing to add more value to their national eduroam offering; and/or who wish to widen their institution-level coverage
- Product offers:
  - technical outsourcing of all aspects of user management
    - create, change users
    - provision, revoke, expire credentials for users
    - provide status information about user credentials
    - provide interface to identify user in case of abuse
- Product does NOT offer:
  - liability for end user accounts created with this system

eduroam Managed IdP service: eligibility

- eduroam Managed IdP is using work flows and technological foundation of eduroam CAT
- Eligibility and governance follow exactly the eduroam CAT way
  - Anchor point: NRO administrators
  - All NROs world-wide can enable or disable the functionality for their NRO
  - NROs invite instititutions to eduroam Managed IdP via the established process
- Institutions create exactly one Managed IdP profile where they can manage a user base, but do not have to care about EAP technical details

eduroam Managed IdP service: technology

- Credential issuance/revocation
  - System uses EAP type EAP-TLS (client certificates) for end-user credentials
  - Usernames in the certificates do not reveal usernames as configured by admin
  - Common root CA for all client certificates (run by eduroam Operations Team, OT)
- Authentication
  - eduroam Managed IdP comprises a RADIUS IdP server
    - Realm: …@...TLD.hosted.eduroam.org, reachable via RADIUS/TLS NAPTRs exclusively
  - Redundancy in two dimensions
    - Can be load-balanced and replicated (but remaining one logical entity)
    - Can be partitioned in per-NRO fashion (EAP-TLS termination point per country)
  - OCSP Responders for the client certificate root CA and central intermediate CA are in responsibility of eduroam OT
- More info & documentation:
  - https://www.eduroam.org/eduroam-managed-idp/
  - Access for admins: https://hosted.eduroam.org

Future work (2021+)

- Development:
  - Managed SP
  - OpenRoaming
  - Certificate provisioning redesign
  - Diagnostics
  - Radsecproxy development
- Maintenance & deployment:
  - eduroam db ver 2.0+ & related tools
  - (RO) Audit
  - Policy update

Thank you

As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856728 (GN4-3).