eduroam Managed IdP

Product Presentation

Stefan Winter

GeGC Technical Expert, Task Leader eduroam Development @GEANT

R&D Engineer, RESTENA Foundation, Luxembourg

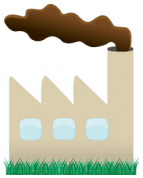
Last updated: 13 June 2017

eduroam Managed IdP


institutional eduroam IdP infrastructure


using the best technology available


run by experts from eduroam Operations Team


in professionally managed central infrastructure


controlled by you from a web browser

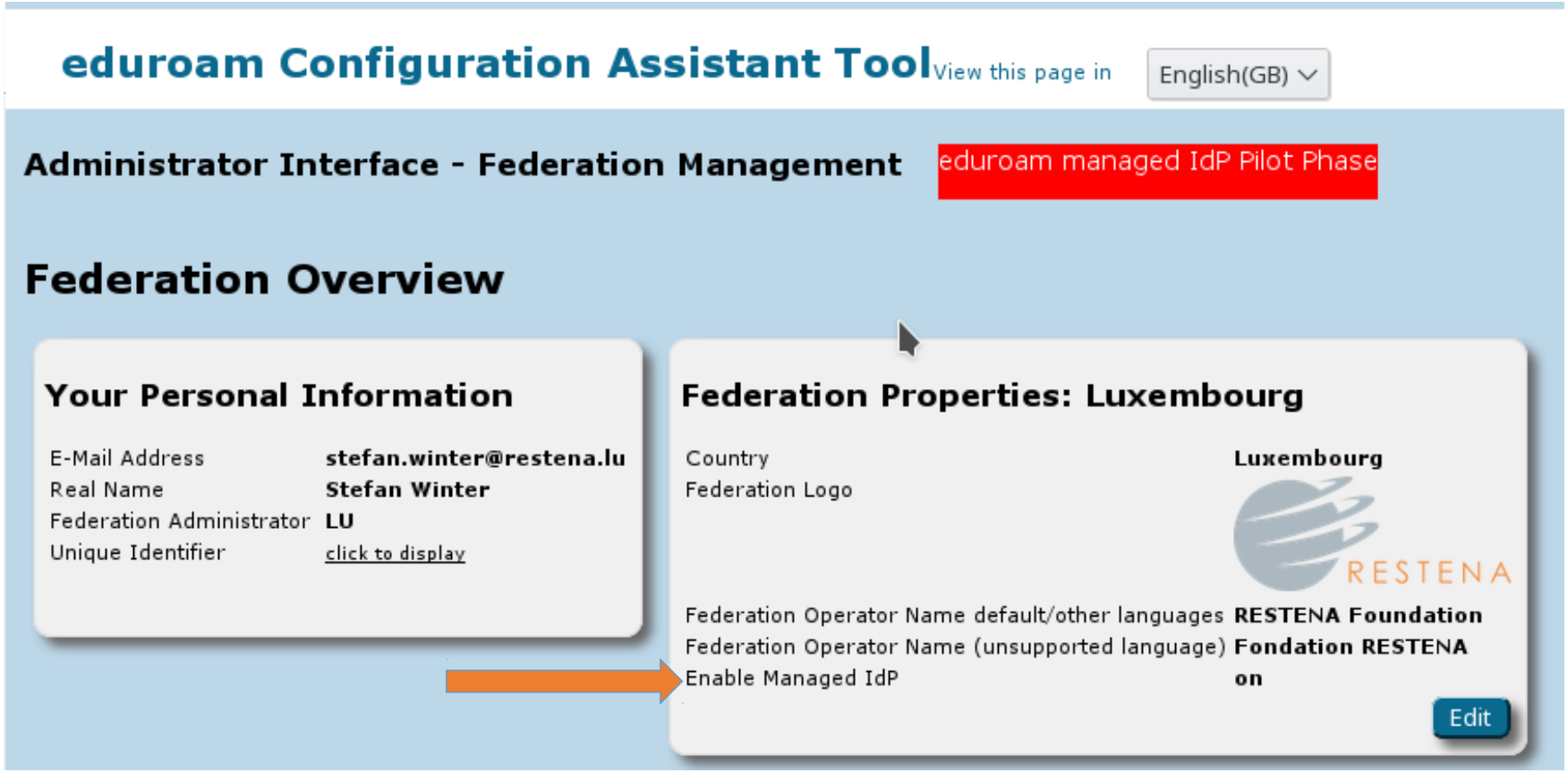
Value Proposition

- 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

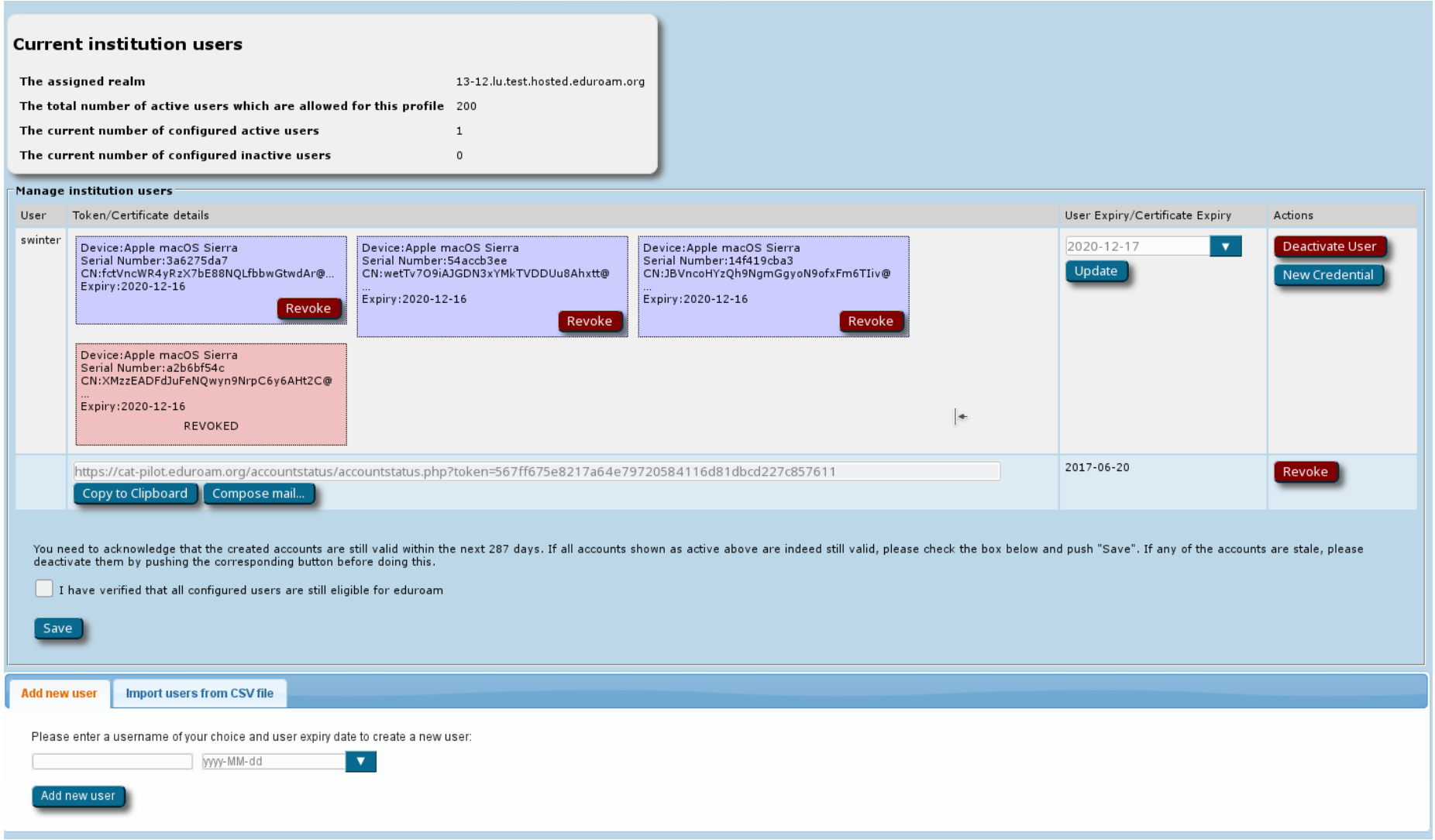
Eligibility

- 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 (invited to Operations Support Services via “realm.xml” denomination)
  - All NROs world-wide can enable or disable the functionality for their NRO (see screenshot “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 (see screenshot “IdP”)

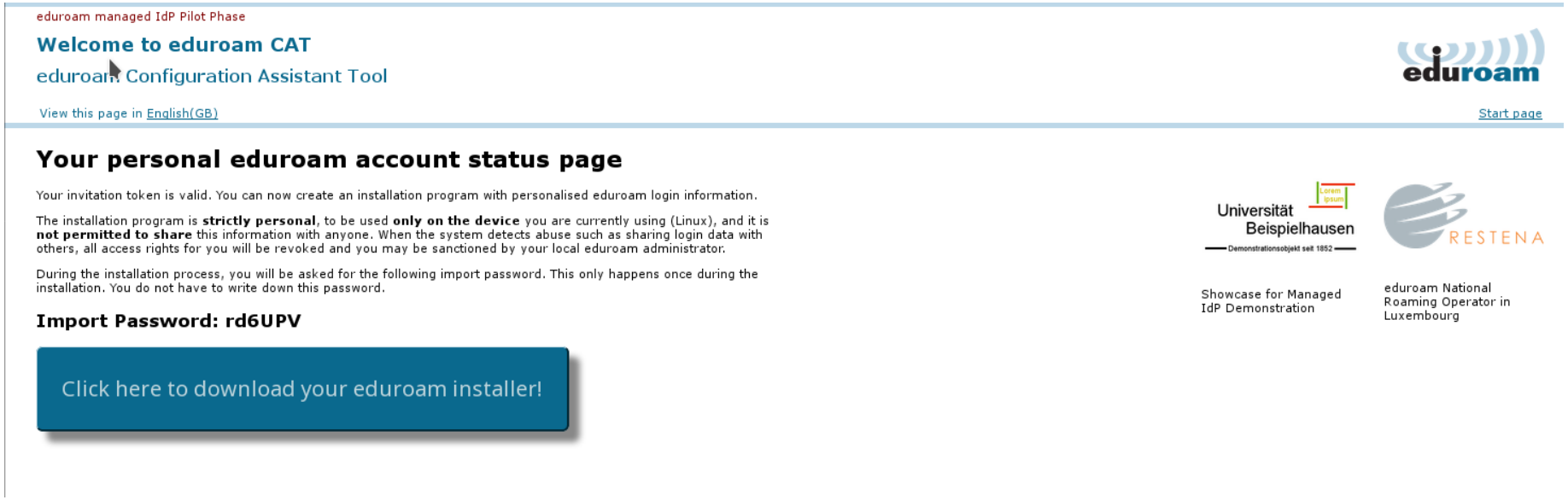
Screenshot: NRO



Screenshot: IdP



Screenshot: end-user download interface



Accountability for end-user accounts

- Individual accounts are created by institution administrator
  - Analogous to the creation of a user in a local IDM system
  - Merely the location of the user database is not local at the institution, but inside the Managed IdP infrastructure
  - The responsibility for these accounts, i.e. they
    - pertain to actual humans
    - are currently members of the institution in question
    - are considered eligible for the eduroam service
    - can be contacted and reprimanded when abusing the service

    rest with the administrator!
- eduroam Managed IdP platform provides technical means to make the link between an access credential and a user in the system
  - Institution administrators can find out which user account name is behind a (pseudonymous) access credential.
  - Anyone can find out to which institution an access credential belongs.

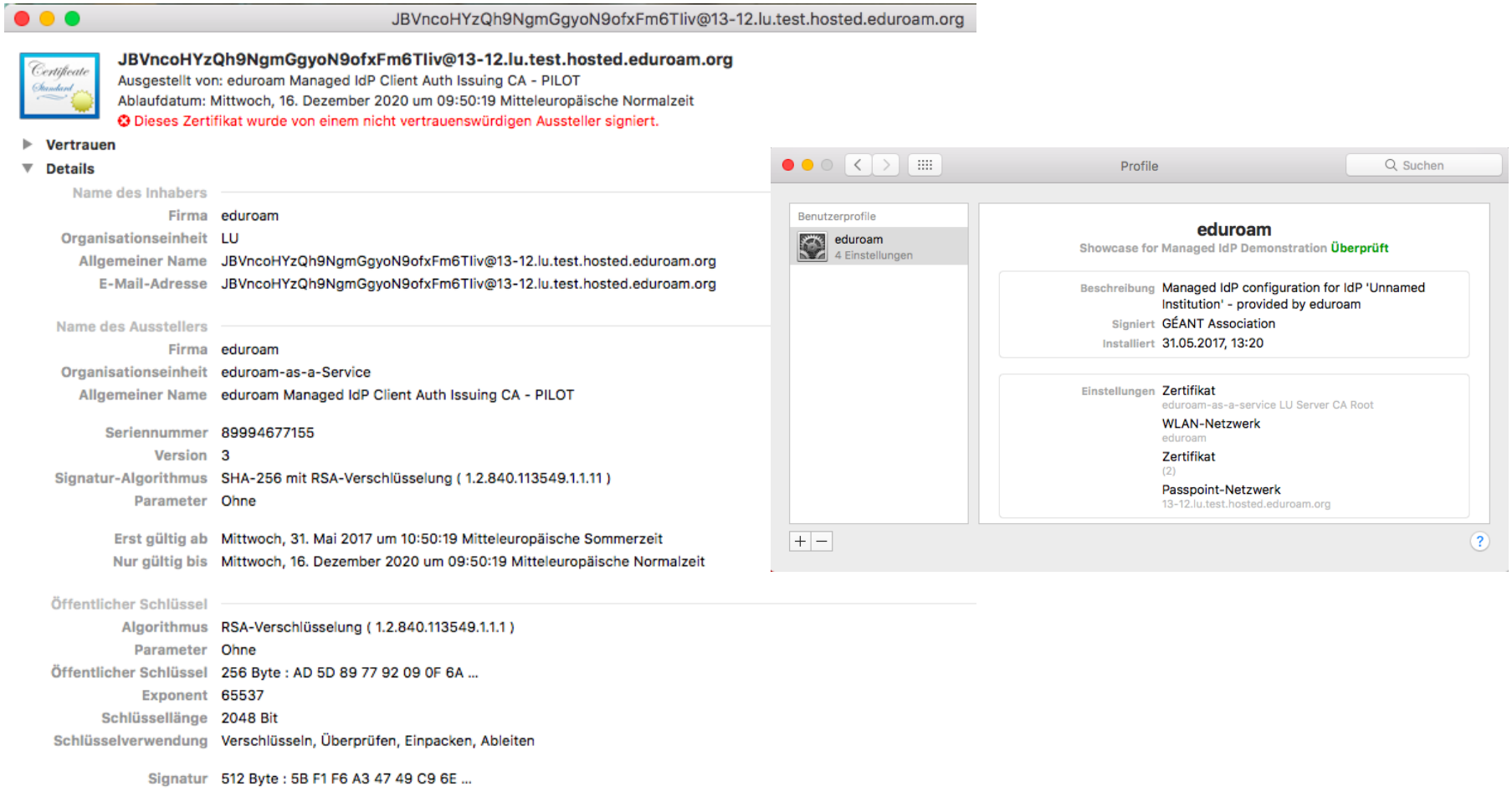
Privacy considerations for issued accounts

- **Strive towards: no data which can be considered personally identifiable should be stored at all.**
- Admin (himself known only by his ePTID or equivalent)
  - Creates accounts for end-users
  - These are simply strings
  - They do not need to be (and we don't ask for) strings that can be linked to actual humans.
  - Ex.: "localuser123" is perfectly fine as a username, and not PII
  - Only the admin himself, locally, has to be able to make a link between the usernames we see and the actual human behind it
- Credentials
  - Do not even carry that username as a property. The EAP-TLS username in the client certificates is a random hash; that's the only thing being seen during authentication.
  - Only the Managed IdP database can make a link between the hash and the username chosen in the interface (and that is not a link to the human, see above)
- Authentication
  - IdP only sees the certificates (hash…) and a MAC address.
  - A MAC address is not usually considered personally identifiable data.

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)
  - Intermediate CAs per-NRO foreseen
  - Initial deployment with one central Intermediate CA for world-wide account issuance (run by OT)
  - That one CA is going to operate as an online CA in controlled premises
  - Every NRO can transition from using the central Intermediate to its own per-NRO one at any time (“nameConstraints”) (-> NRO request via the usual channels)
  - this introduces technical complexity for the NRO (!)
    - needs to run its own copy of the issuing parts of eduroam-as-a-service
    - needs to operate an online CA incl. OCSP responders
- All CAs maintain OCSP responders
  - Administrator user interfaces allows revocation of credentials
  - Revocation status is propagated immediately and checked during authentication

Screenshot: Installed on a Mac OS Sierra



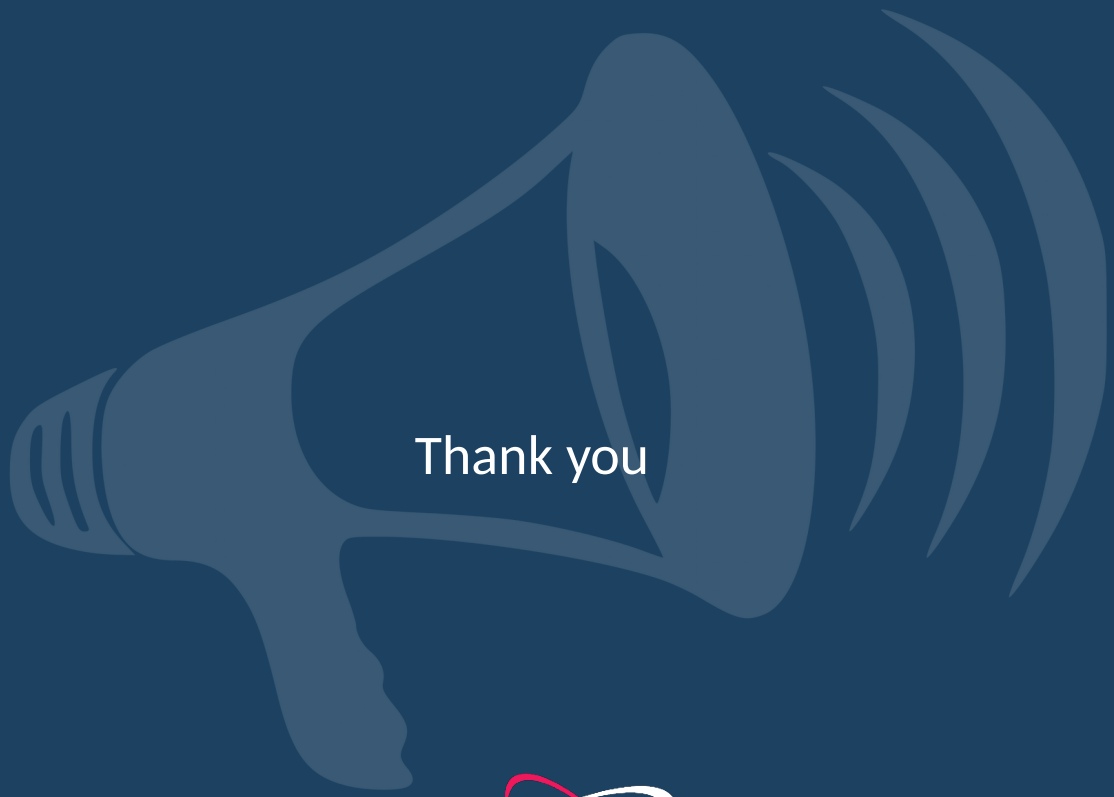
Technology: authentication

- 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)
- To facilitate partitioning, initial deployment starts with server-side CAs and server certificates per-NRO (ca. 200 NRO personalities in one server)
- As soon as NRO wishes to run its own partition (-> NRO requests via usual channels),
  - issue new server certificate, run termination point both on central and NRO-based instance
  - Or transfer CA and private key to NRO, run termination point only on NRO-based instance
- OCSP Responders for the client certificate root CA and central intermediate CA are in responsibility of eduroam OT

Implementation Status / Challenges

- Implementation Progress
  - Working system is currently in pilot phase
  - Waiting for your evaluation, feedback and feature requests
  - https://cat-pilot.eduroam.org
- Manual: https://wiki.geant.org/pages/viewpage.action?pageId=66650390
  - Chapter 5 for NROs wishing to enable the service
  - Chapters 6+7 for IdPs
- Product includes level 1 helpdesk services (provided by GEANT Service Desk)
- We are considering to make this service a charged one due to its operational complexity and associated cost
  - Probably “TCS-style”
    - NROs pay for enabling this country-wide
    - There are several levels, criteria and price point TBD

stefan.winter@restena.lu



Thank you

GÉANT

Networks · Services · People

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).