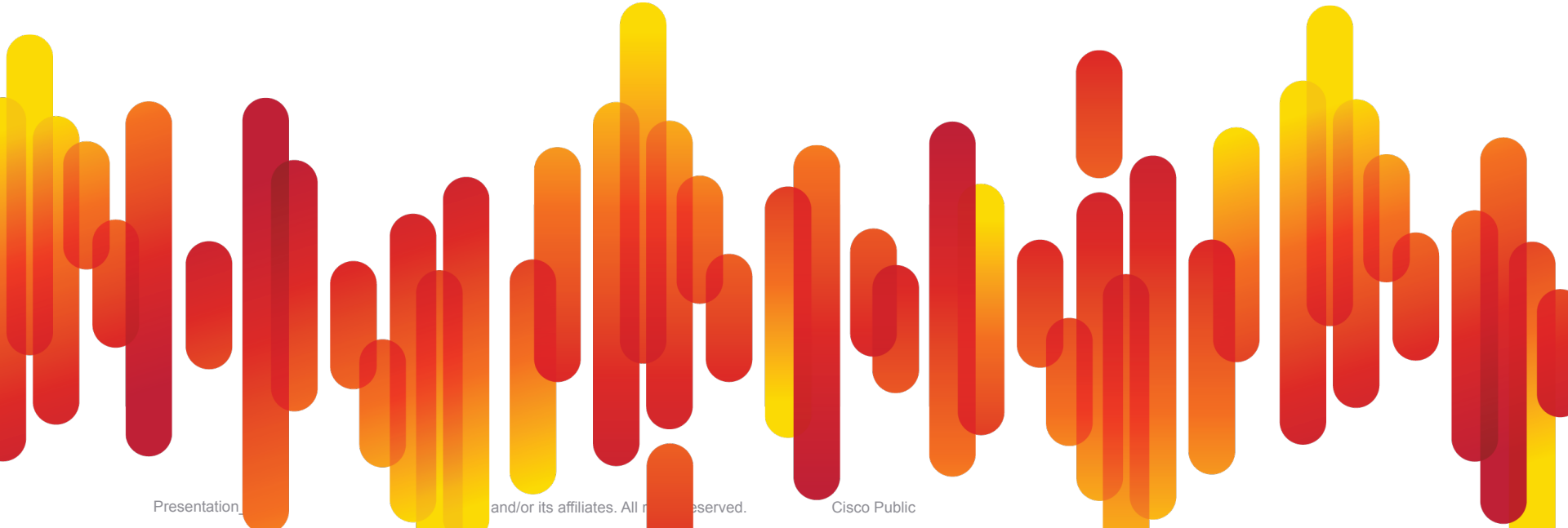
Conferenza GARR – Da 20 anni al futuro

10 Novembre, 2011

Federated Access for User Mobility

Klaas Wierenga
<klaas@cisco.com>



Agenda

- Federated access in the Higher Education today
  - Intro
  - eduroam
- Challenges in and solutions for network access
  - RadSec
  - 3/4G operators
- An excursion to the application layer
  - Project Moonshot
- Summary and Conclusions
- Questions / Domande

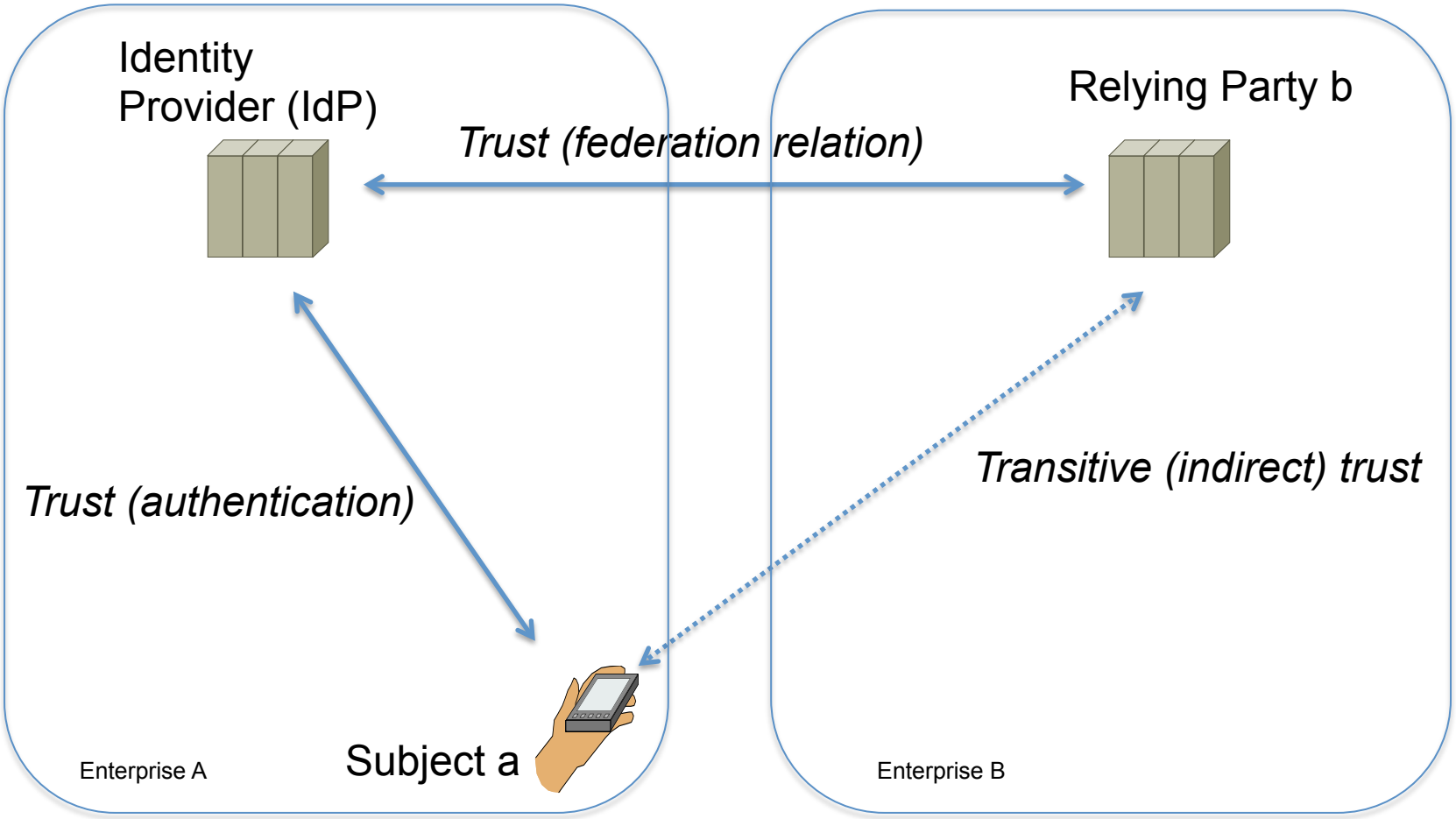
Federated access in Higher Education

"Always and everywhere access to all services"

- eduroam
  - "open your laptop and be online"
  - Truly global (Africa, Asia, Australia, Europe, North-America, South-America)
  - Growing pains
  - Network access only
  - Campus only

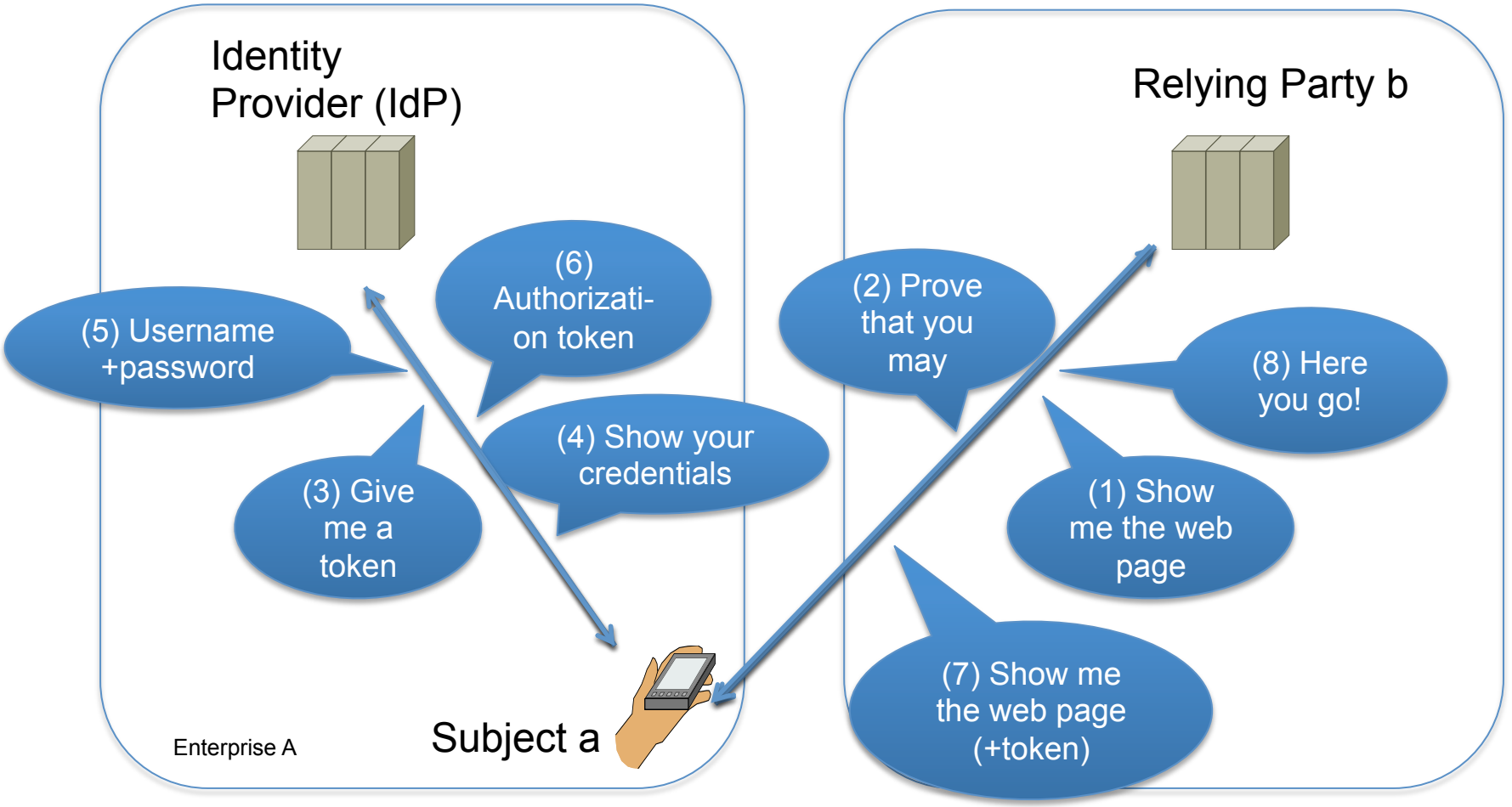
- SAML-based federations
  - Shibboleth, SimpleSAMLphp
  - Like IDEM
  - Mostly national
  - Starting European (eduGAIN)
  - Struggling with scaling
  - Web-applications only

What are the entities in a federation?



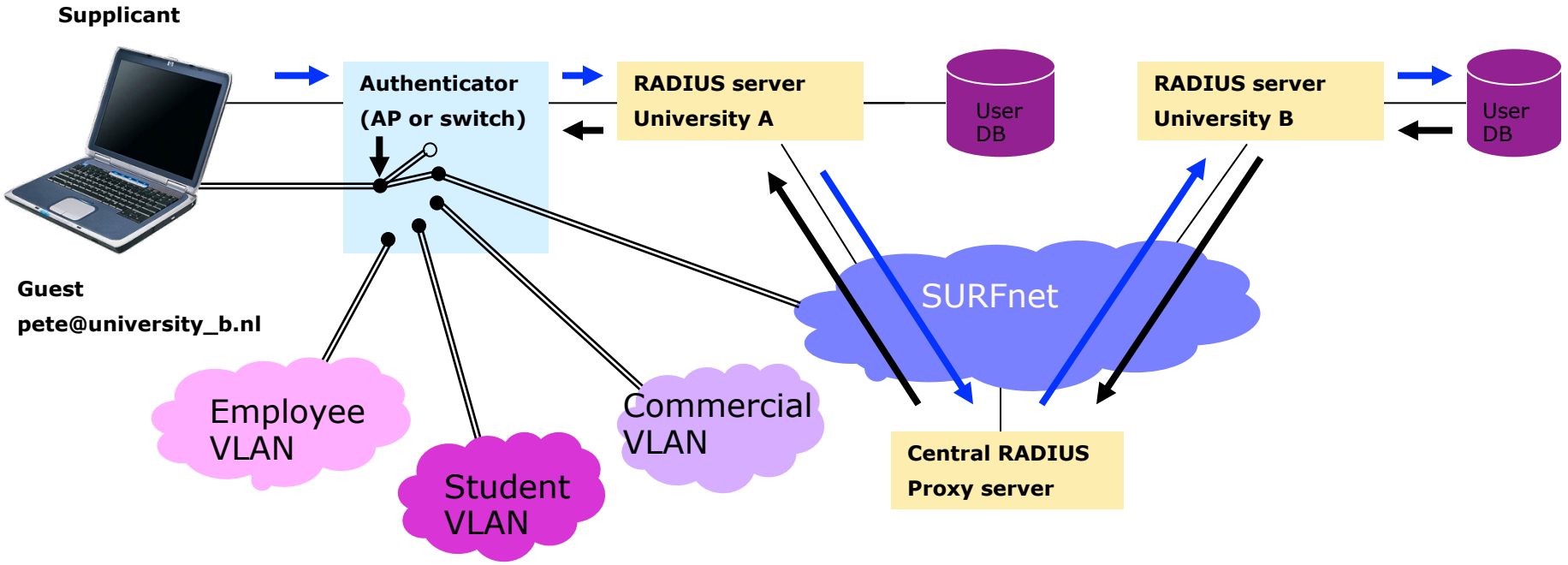
"I, IdP A, claim that Subject a is a succesfully authenticated and is authorized to access service b"

What does a federated transaction look like?



Typical SAML flow with browser redirect

eduroam architecture



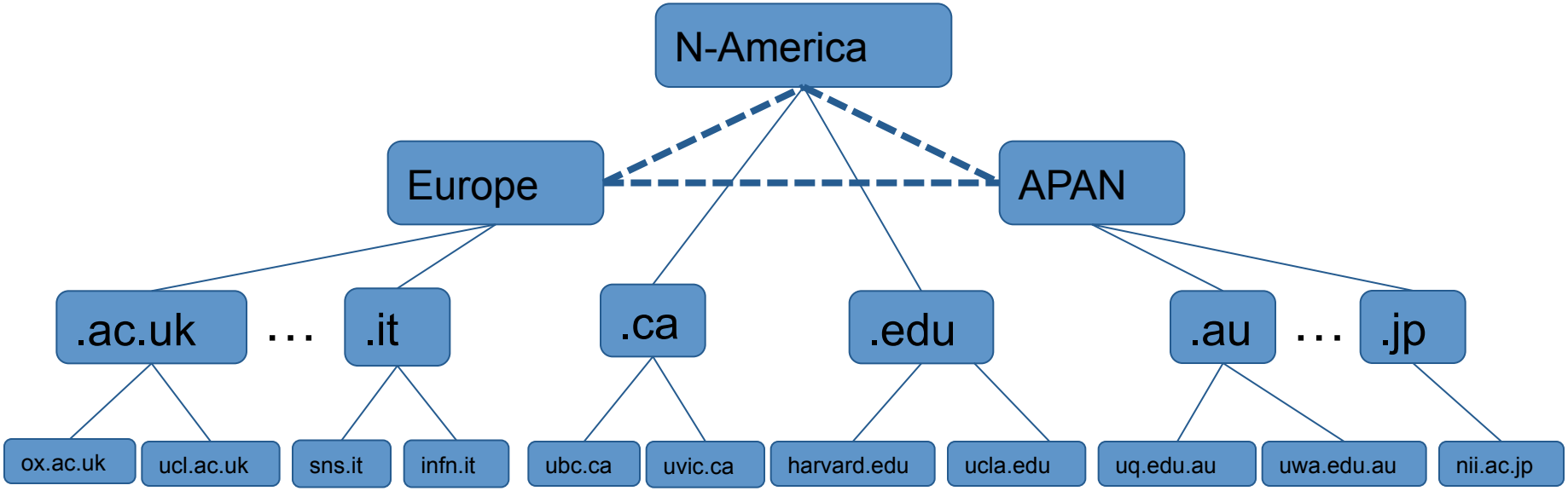
Source: SURFnet

- Trust between institutions based on RADIUS plus policy documents
- 802.1X
- VLAN assigment to separate local users and visitors
- User privacy and flexible mutual authentication through EAP

Intermezzo: federated web captive portals considered harmful

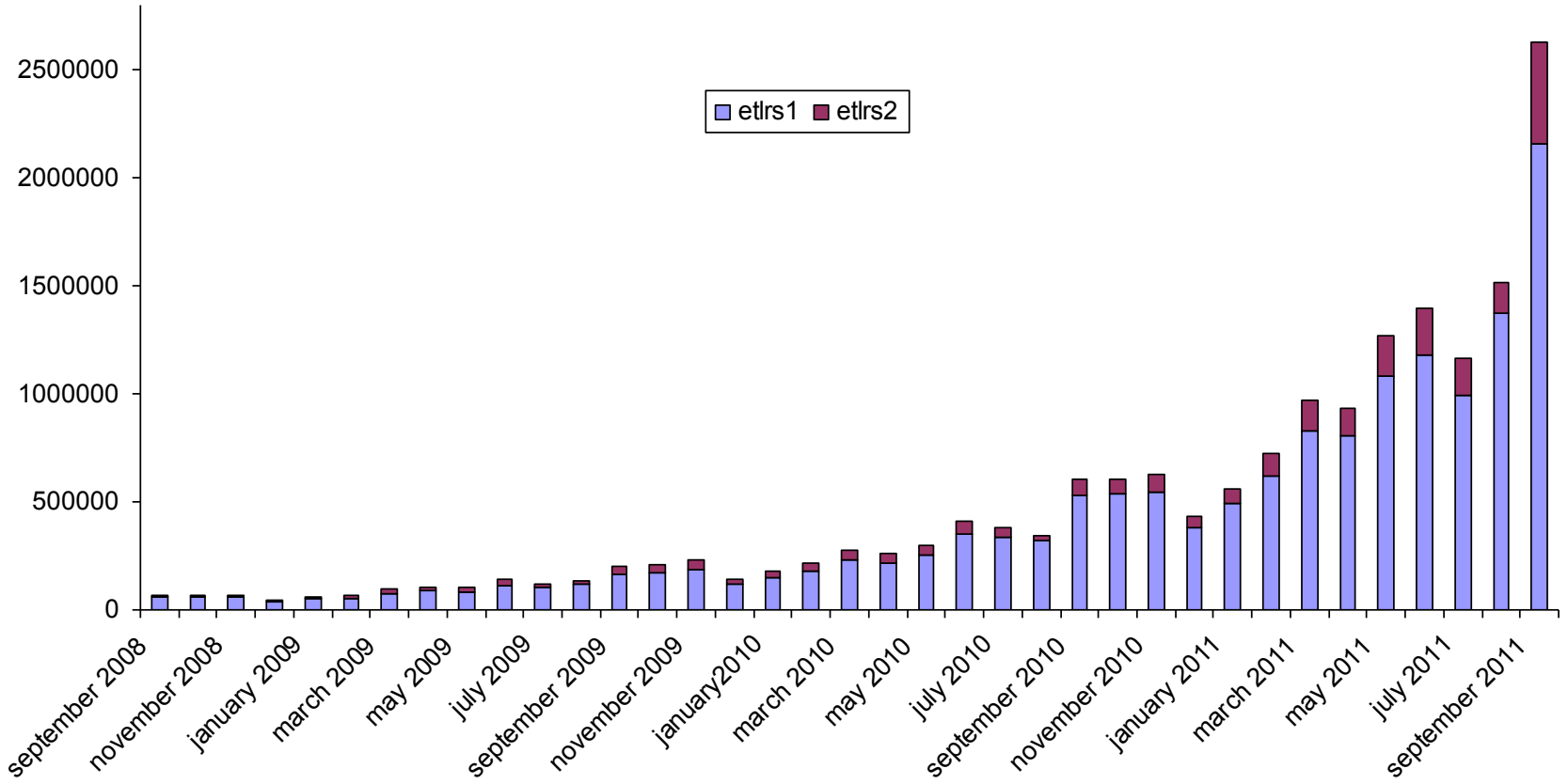
- Either enter user credentials at visited site web page
  - Verified through RADIUS backend
  - Teach your users to share their password with the world
  - Not protected en route
- Or redirect to home IdP
  - Need to open port 80/443 to ALL IdP's in the consortium
  - Maintain ACL list of all IdP's in the world
- Both share the unpleasant property that authentication may be secure, but authorization is based on IP-address and/or MAC, which can be captured easily by a malicious user
  - Unless some sort of keep-alive applet/script is running
  - But wasn't that what you got for free with 802.1X?
  - Oh, and all the traffic on "the wire" after authentication is in the clear

eduroam hiearchy



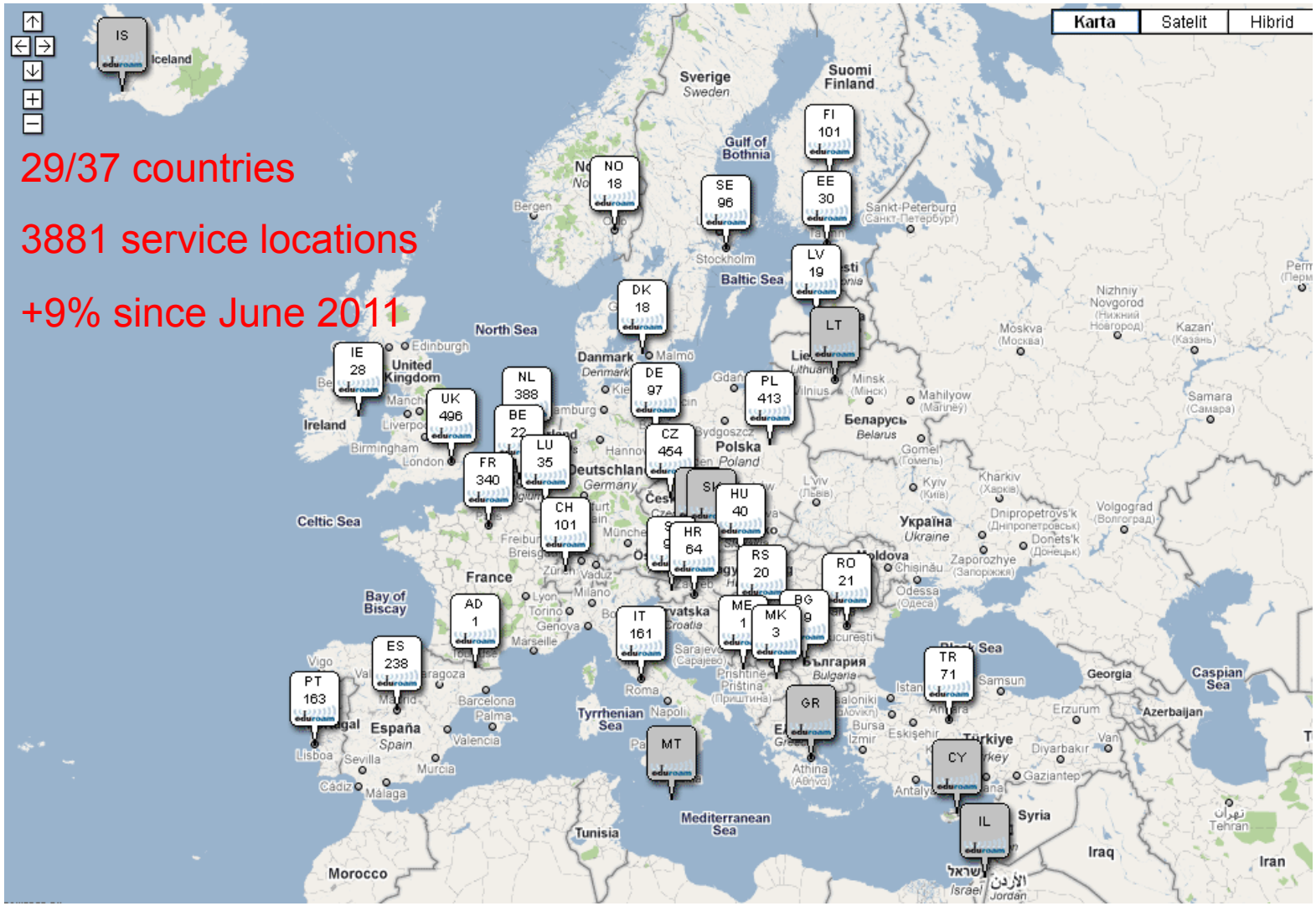
- Continental toplevel servers have static mapping cc-tld to toplevel server
- Within continent request routing based on ”DNS hierarchy”
- Trust between universities is transitive, i.e. if the access request is answered through RADIUS hierarchy there is implicit trust that home institution of the user is part of the federation

International eduroam traffic



Source: GN3 eduroam OT

Eduroam in Europe

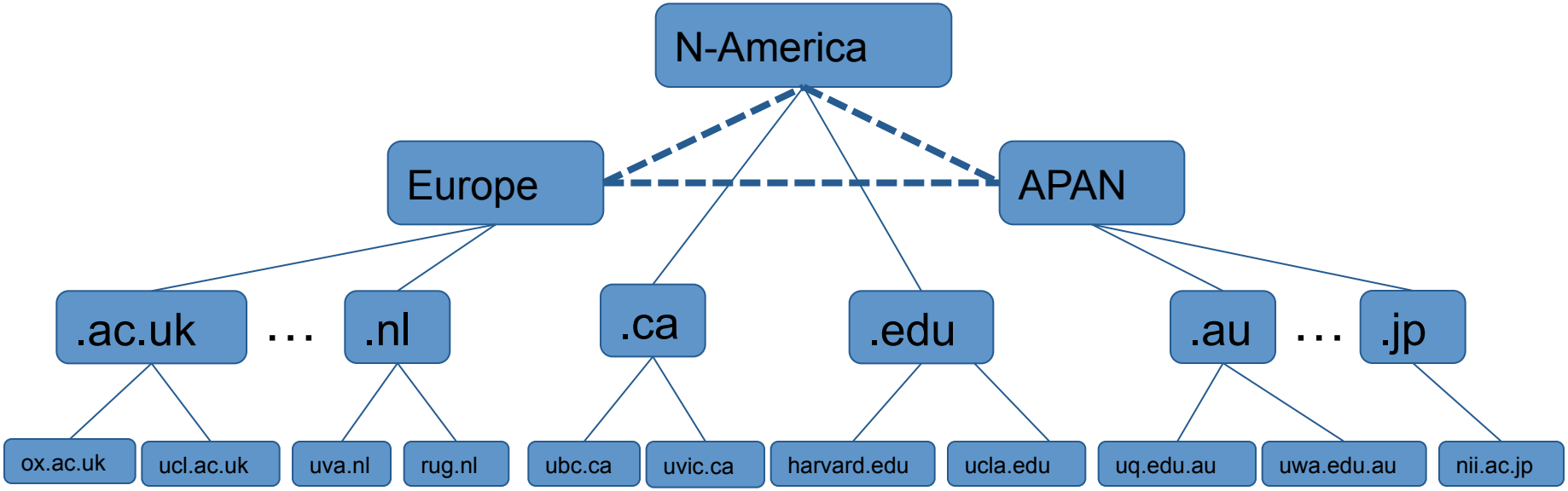


Source: GN3 eduroam OT

Agenda

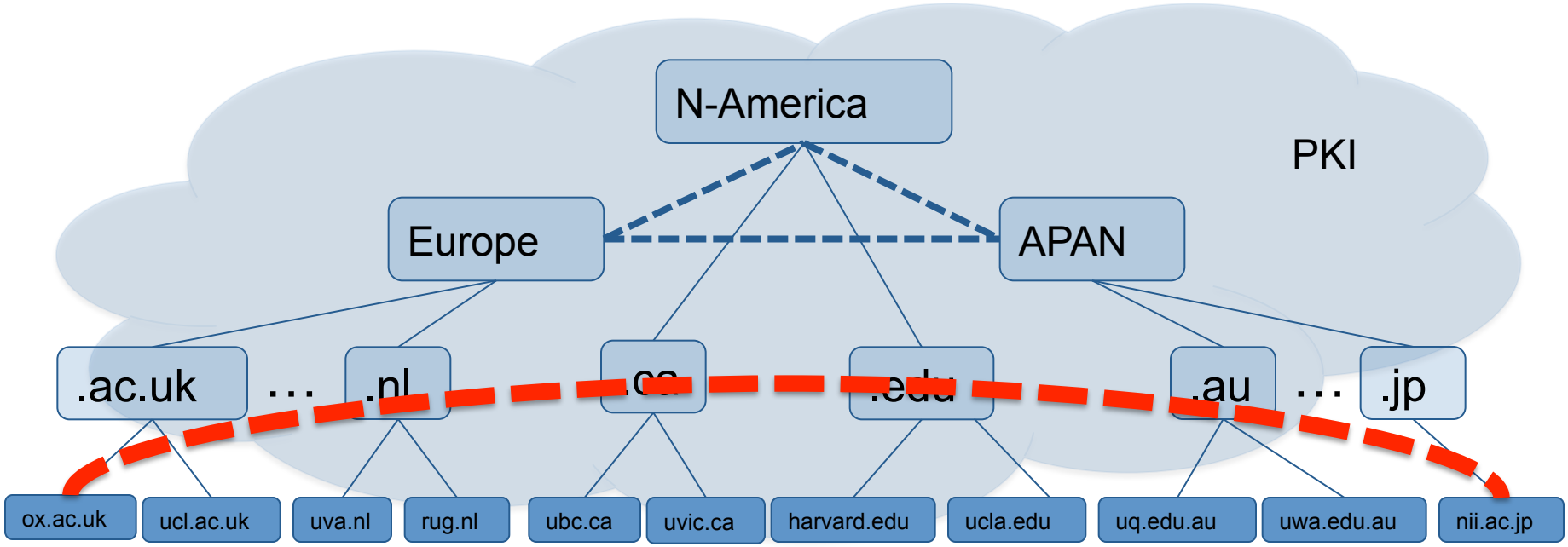
- Federated access in the Higher Education today
  - Intro
  - eduroam
- Challenges in and solutions for network access
  - RadSec
  - 3/4G operators
- An excursion to the application layer
  - Project Moonshot
- Summary and Conclusions
- Questions / Domande

eduroam hierarchy problems



- Dead peer discovery
- Peer authentication
- Fragmentation
- Managing shared secret/IP-address based trust
- Static hierarchy
- The “.edu problem”

RadSec

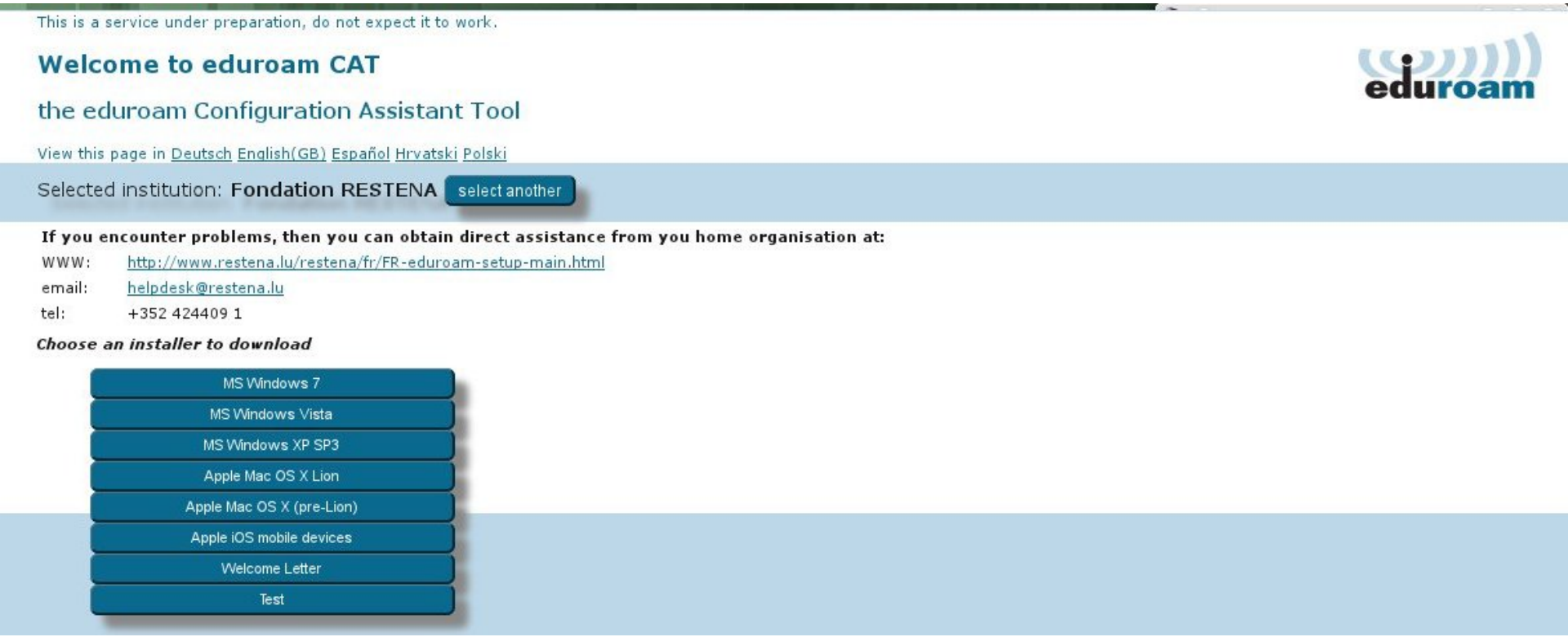


- RADIUS with:
  - TLS: RADIUS proxy hierarchy replaced by PKI)
  - TCP: Reliable transport
- draft-ietf-radext-radsec, draft-ietf-radext-tcp-transport
- Allows for dynamic peer lookup in DNS!
- Implementations in Radiator, FreeRADIUS, RadSecProxy and OpenWRT and Lancom AP's
- Standardised in IETF radext WG

Client deployment: CAT

- Configuration Assistance Tool
- Developed in Geant3 JRA3
  - beta end ‘11, production mid ‘12
- IdP (institution) provides configuration details:
  - CA, Certificate CN
  - EAP methods
  - Profiles
  - Preferred language (including Italian!)
- eduroam operational team provides:
  - Site specific installer for select devices (Windows >XP, OSX, iOS, Linux)
  - Screen shots for other devices
- User:
  - Selects home institution and device
  - Gets site specific installer

CAT for users (select institution)

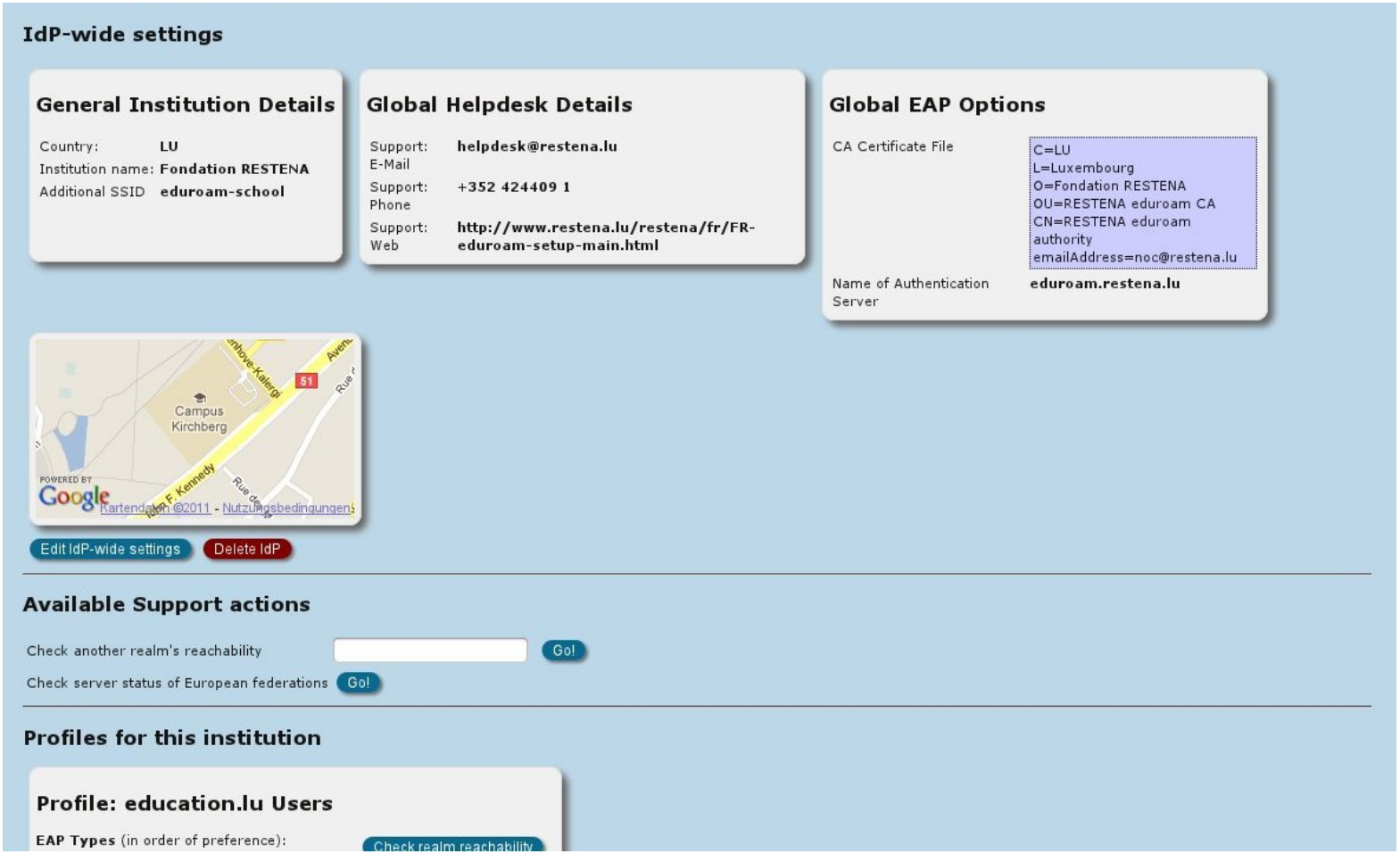


Source: GN3 JRA3

CAT for users (win7 installer)

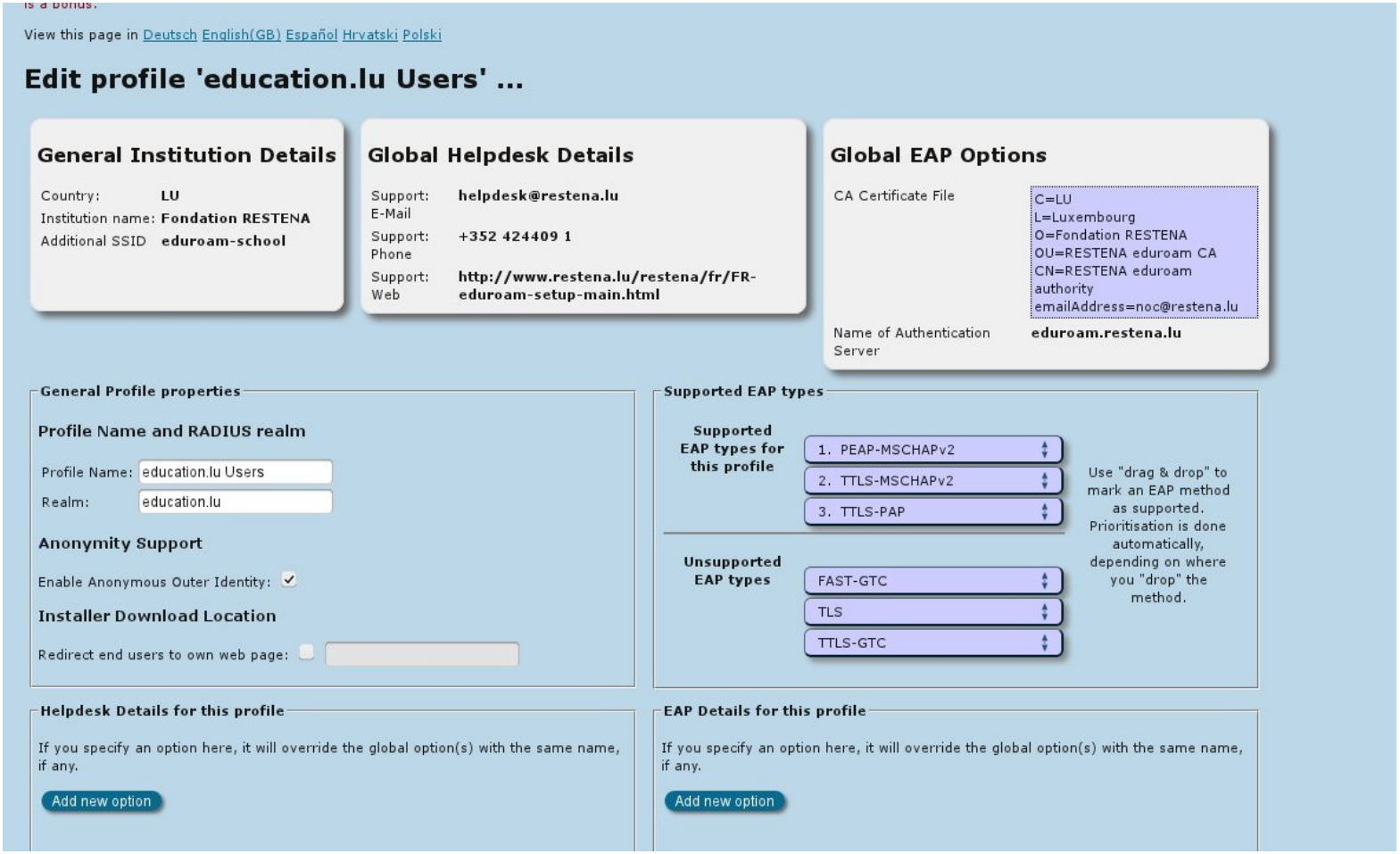
Source: GN3 JRA3

CAT for institutions (dashboard)



Source: GN3 JRA3

CAT for institutions (profiles)

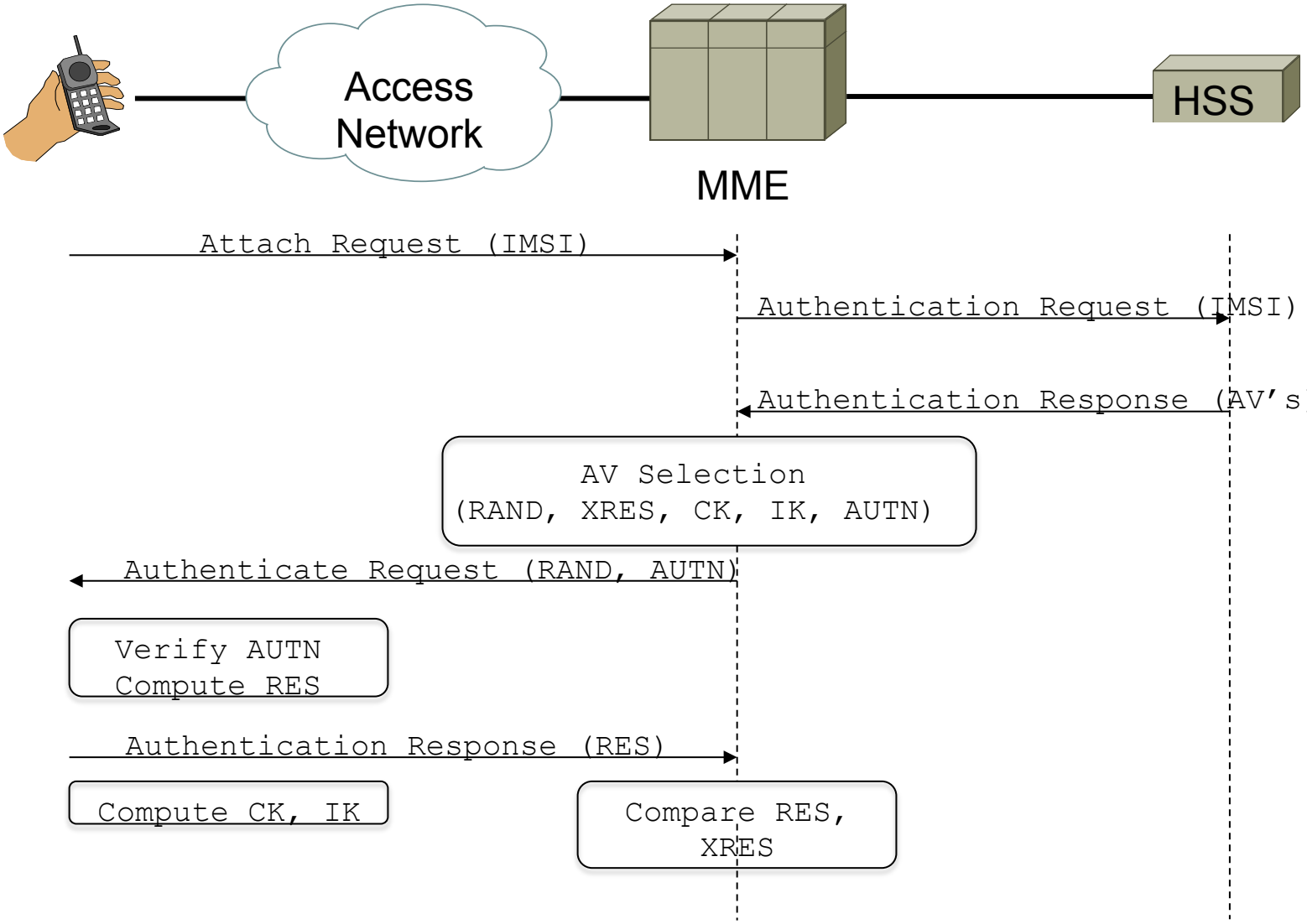


Source: GN3 JRA3

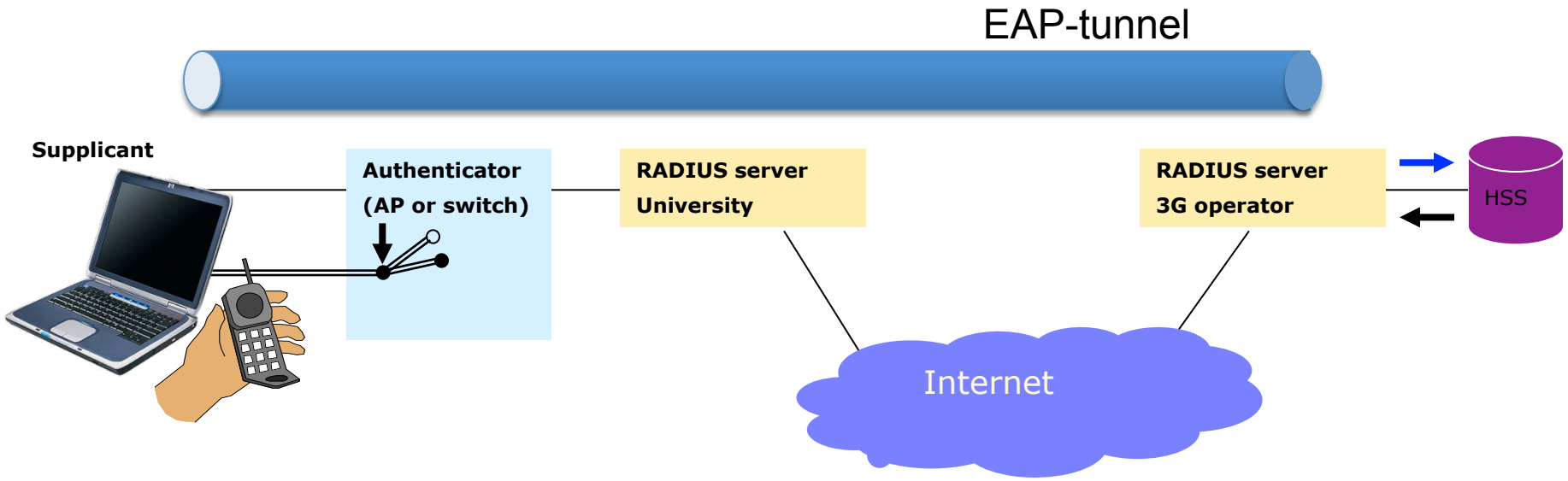
Integration with other operators

- Operator as a Service Provider
  - Using RADIUS infrastructure
  - But how to protect user credentials?
  - Integration with WiFi operators straightforward if they use 802.1X
  - Integration with 3/4G operators with EAP-SIM and EAP-AA
    - Authentication at mobile operator?
    - NREN as Mobile Virtual Network Operator (MVNO)?
- Operator as an Identity Provider
  - How about acceptable use?
  - Carrying commercial user traffic over NREN network

AKA Authentication in an LTE network



EAP-AKA’



- Similar to eduroam architecture
- Authentication at Mobile Operator

Agenda

- Federated access in the Higher Education today
  - Intro
  - eduroam
- Challenges in and solutions for network access
  - RadSec
  - 3/4G operators
- An excursion to the application layer
  - Project Moonshot
- Summary and Conclusions
- Questions / Domande

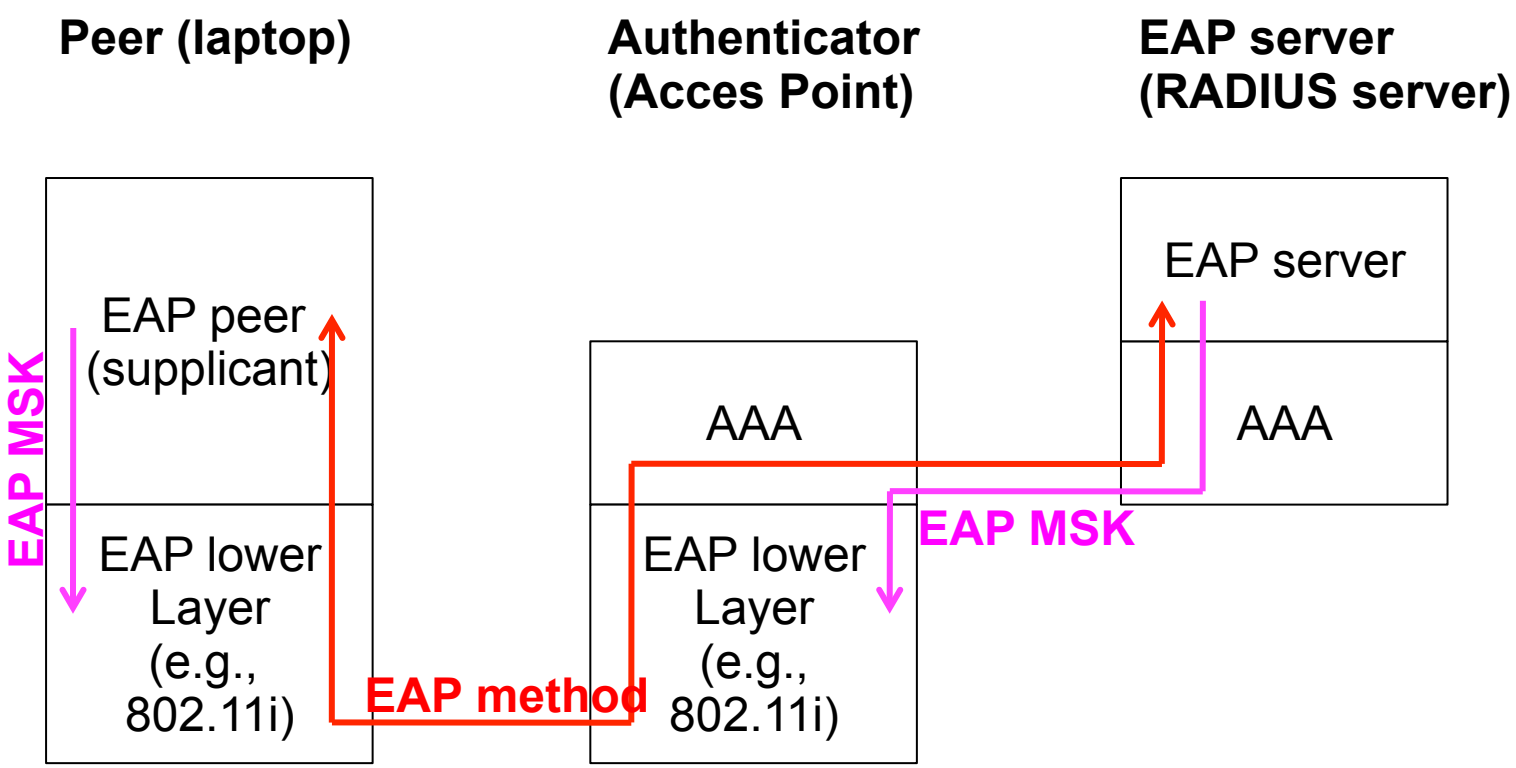
SAML federations

- Wildly succesful for enterprise identity for web-applications
- Scaling problems
  - IdP discovery
  - Multiple affiliations
  - Cross national boundaries
  - Non-web applications

Project Moonshot

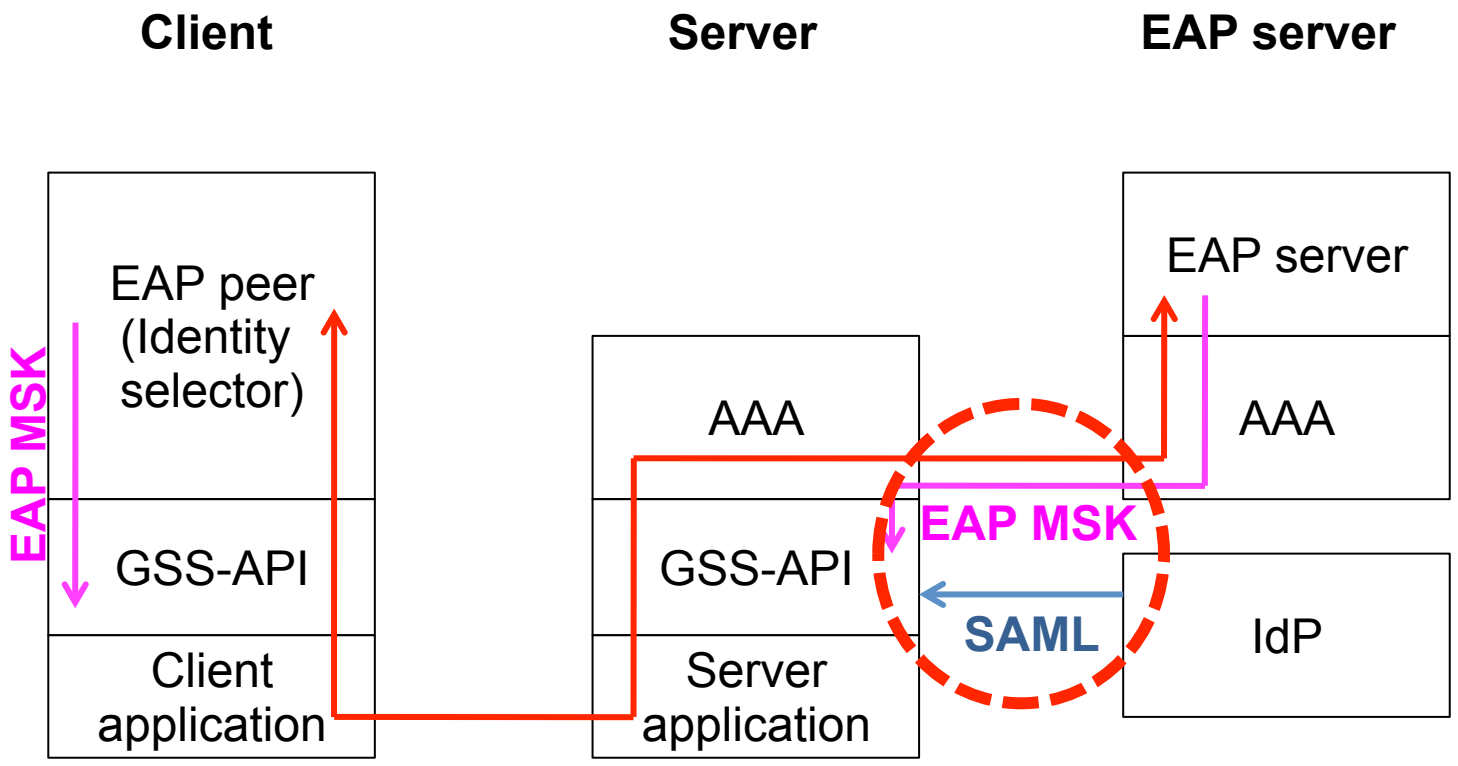
- Leverages:
  - **RADIUS hierarchy for federation**
  - **EAP for privacy protection**
  - SAML for identity assertions and attribute exchange
  - GSS-API for application interface
- Use cases:
  - IMAP
  - SSH
  - XMPP
  - …
- Standardisation in Abfab (Application Bridging for Federated Authentication beyond Web sso) working group in the IETF

EAP for network access (eduroam)



Source: Moonshot project

Moonshot



Source: Moonshot project

Agenda

- Federated access in the Higher Education today
  - Intro
  - eduroam
- Challenges in and solutions for network access
  - RadSec
  - 3/4G operators
- An excursion to the application layer
  - Project Moonshot
- Summary and Conclusions
- Questions / Domande

Summary and concusions

- The eduroam architecture is the only likely candidate for a global solution for network roaming
- New developments address some of the weaknesses of the eduroam model
- The use of EAP+RADIUS proves to be very powerful, also in other contexts
- It is early days, but Moonshot does address a number of use-cases and scaling problems that current SAML-based inter-federation doesn’t solve

Questions?

Domande?

Vragen?

<klaas@cisco.com>