

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

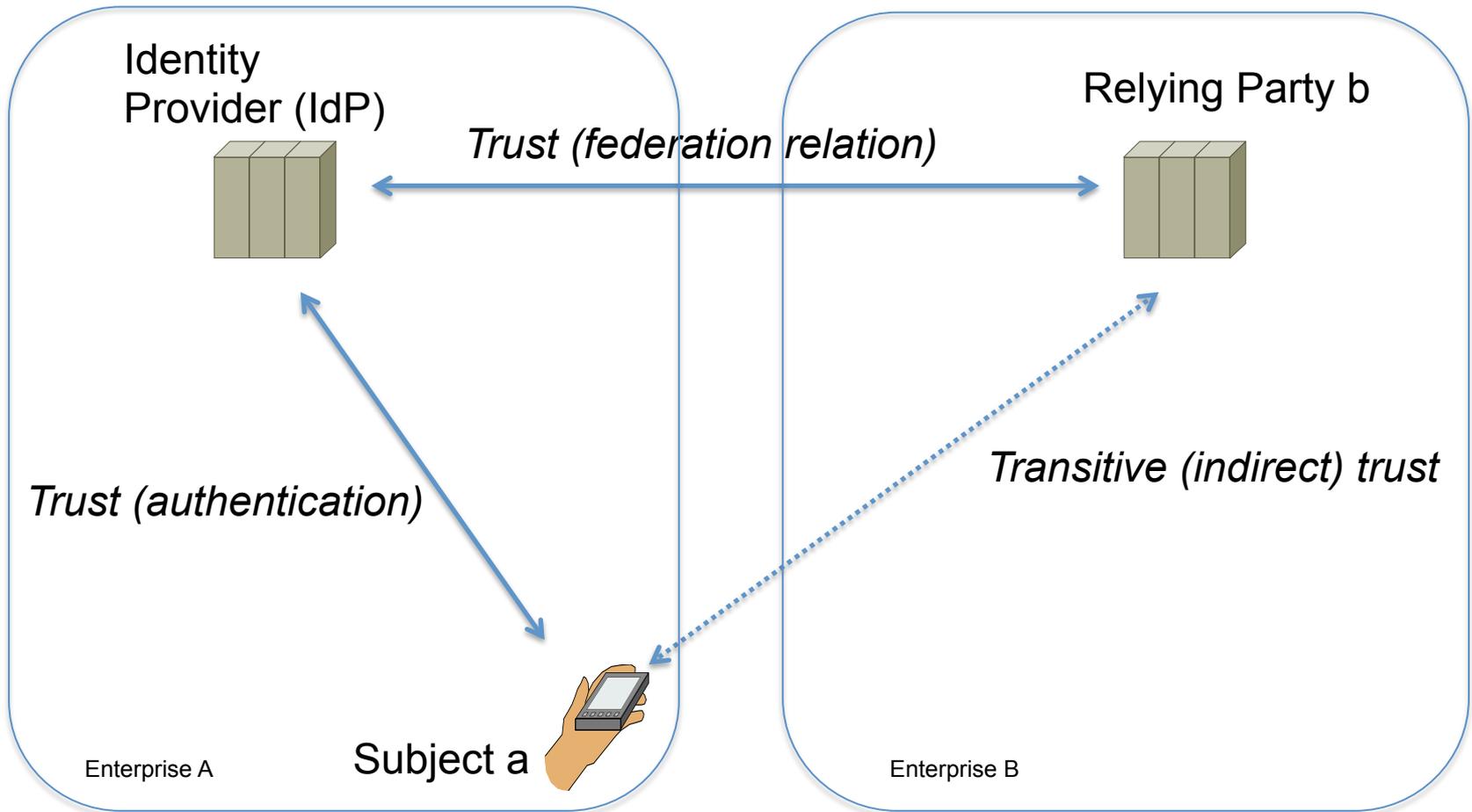
Starting European (eduGAIN)

Struggling with scaling

Web-applications only

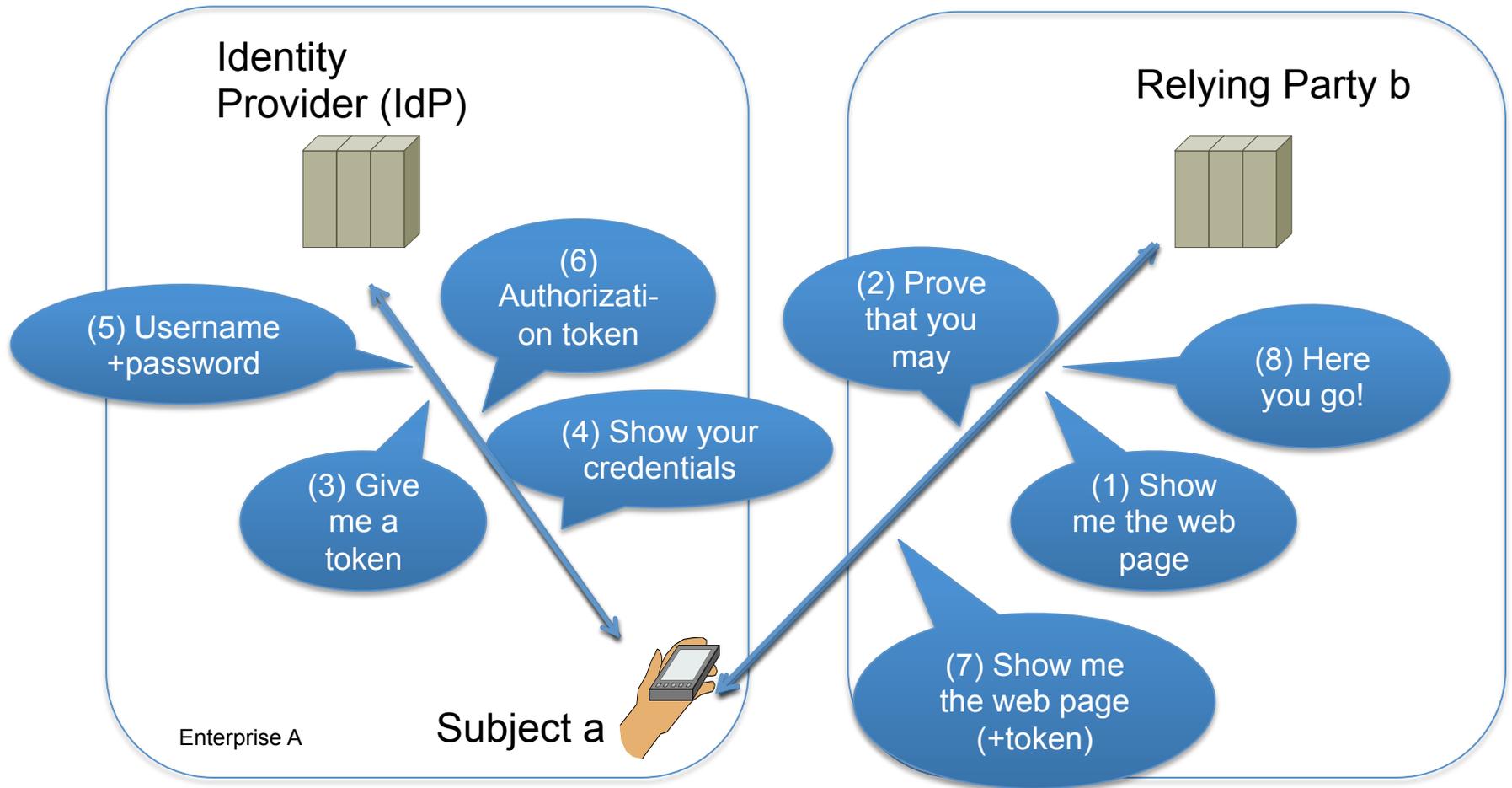


# What are the entities in a federation?



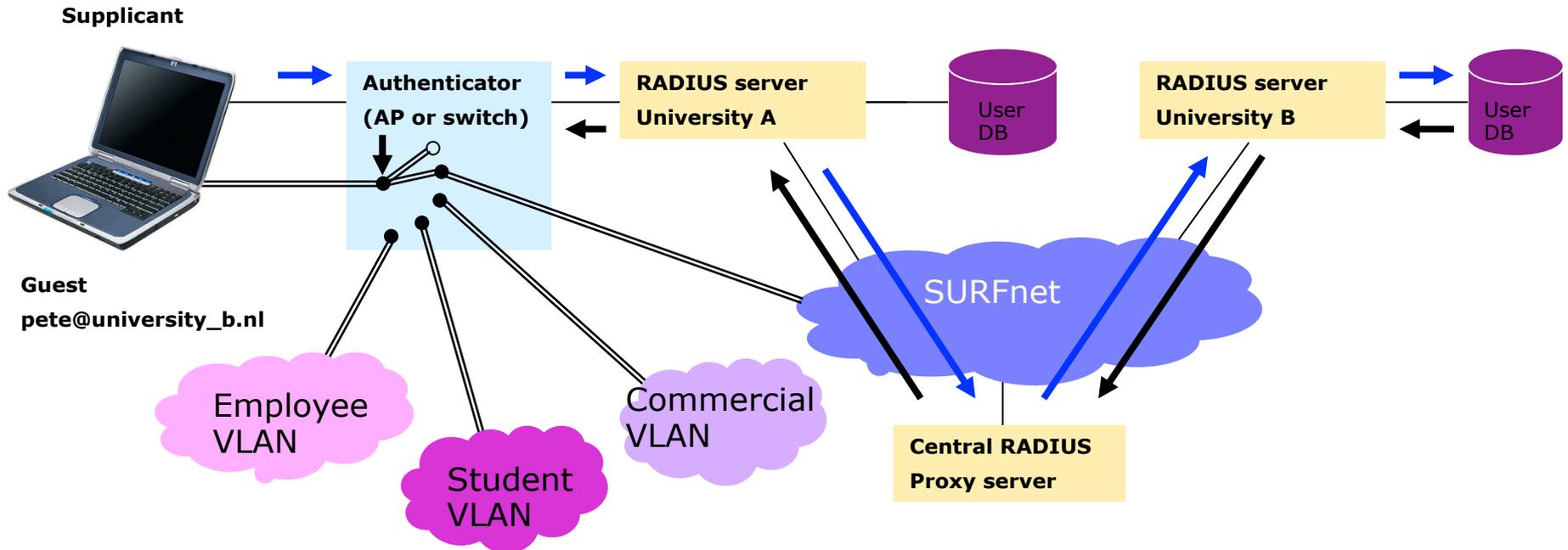
“I, IdP A, claim that Subject a is a successfully authenticated and is authorized to access service b”

# What does a federated transaction look like?

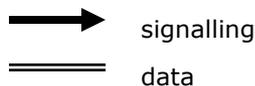


Typical SAML flow with browser redirect

# eduroam architecture



Source: SURFnet

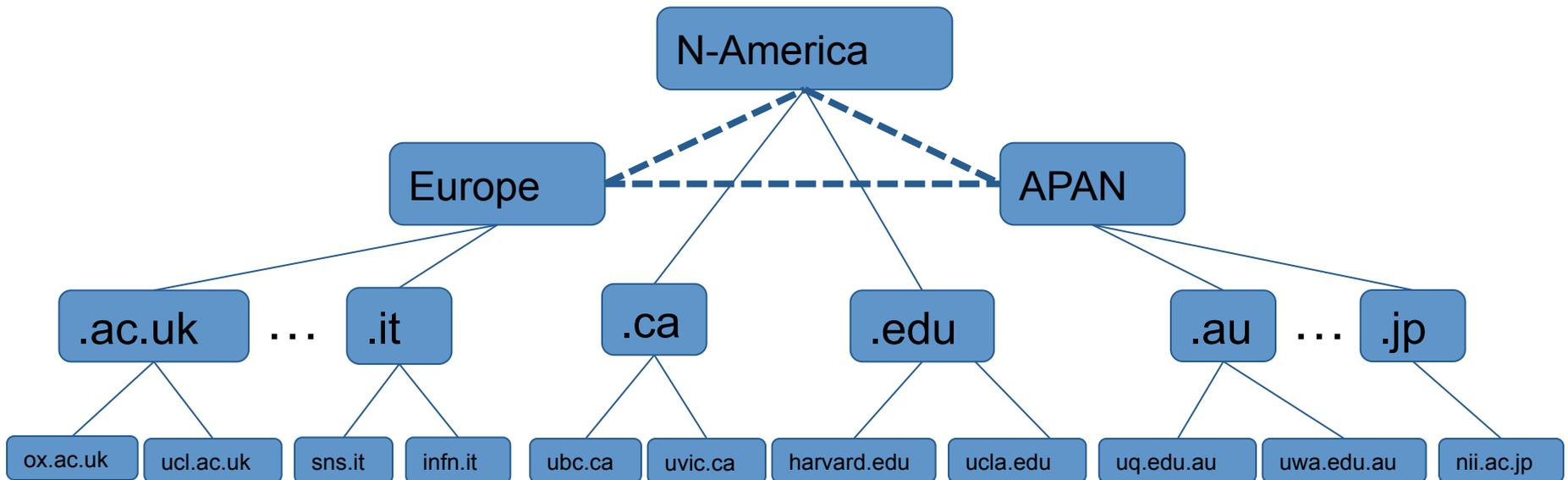


- Trust between institutions based on RADIUS plus policy documents
- 802.1X
- VLAN assignment to separate local users and visitors
- User privacy and flexible mutual authentication through EAP

# Intermezzo: federated web captive portals considered harmful

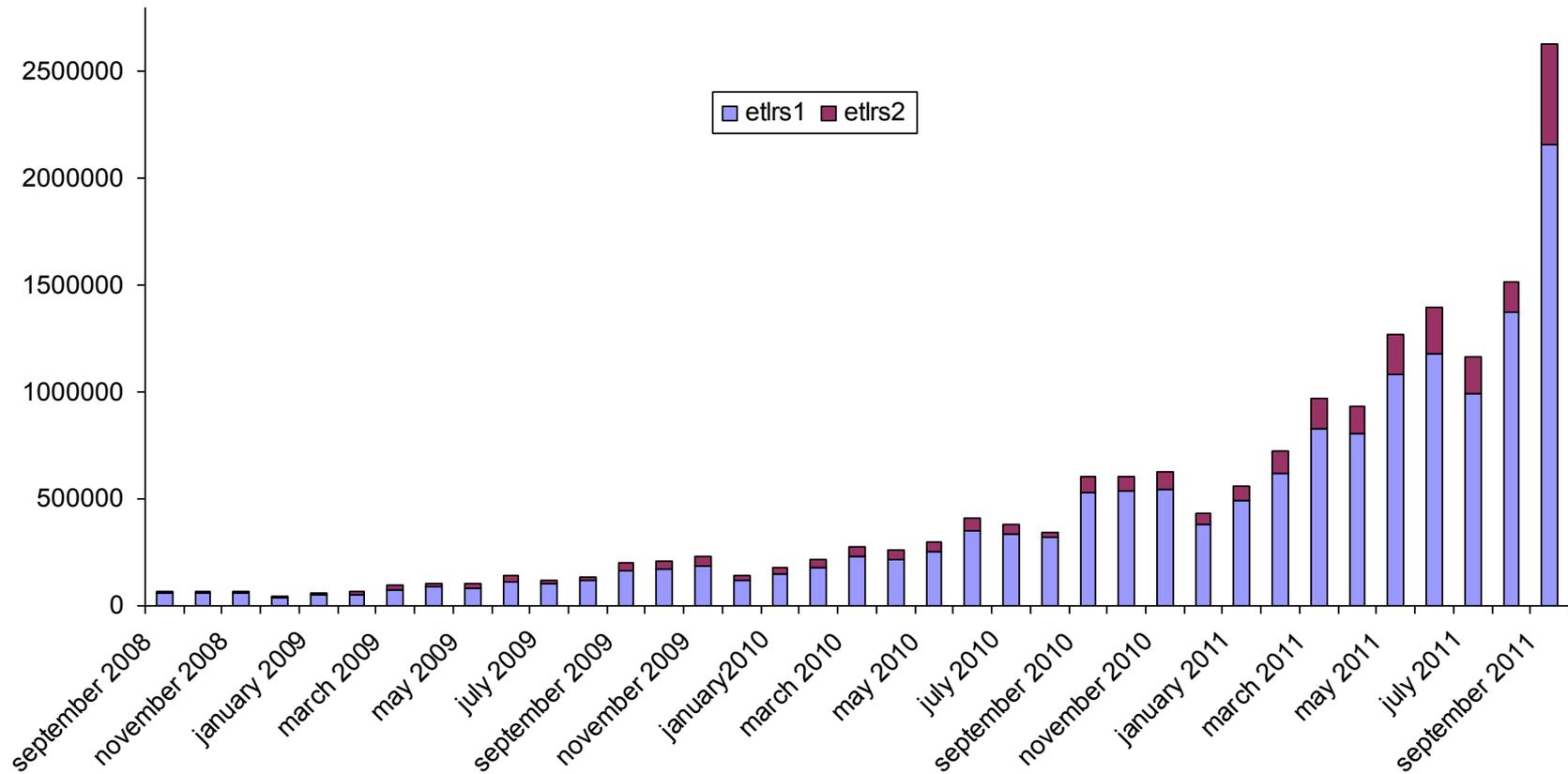
- Either enter user credentials at visited site web page
  - Verified through RADIUS backend
  - Teach your users to share their password with the world
  - Not protected en route
- Or redirect to home IdP
  - Need to open port 80/443 to ALL IdP's in the consortium
  - Maintain ACL list of all IdP's 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 hierarchy

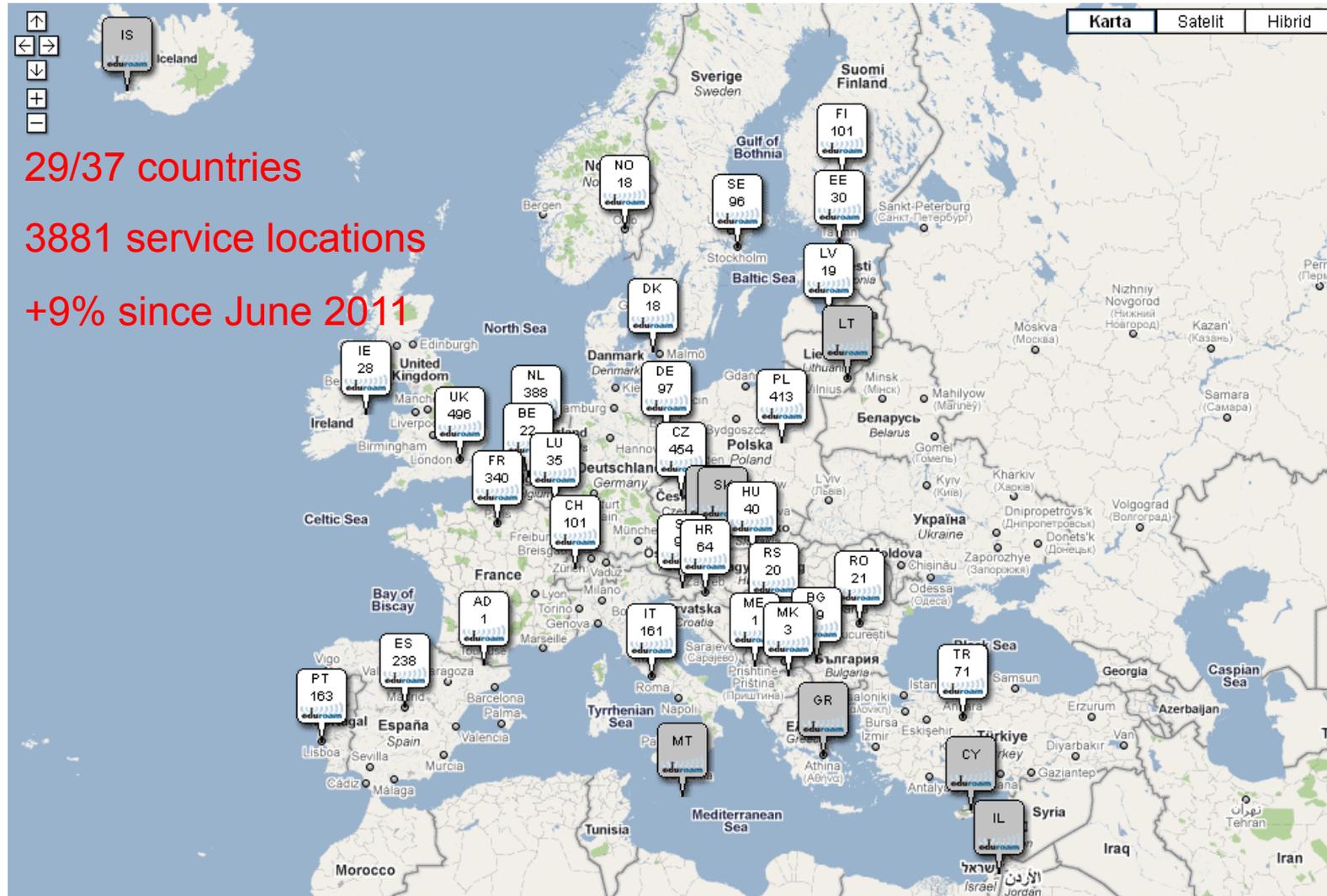


- Continental toplevel servers have static mapping cc-tld to toplevel server
- Within continent request routing based on "DNS hierarchy"
- Trust between universities is transitive, i.e. if the access request is answered through RADIUS hierarchy there is implicit trust that home institution of the user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

# International eduroam traffic



# Eduroam in Europe



29/37 countries

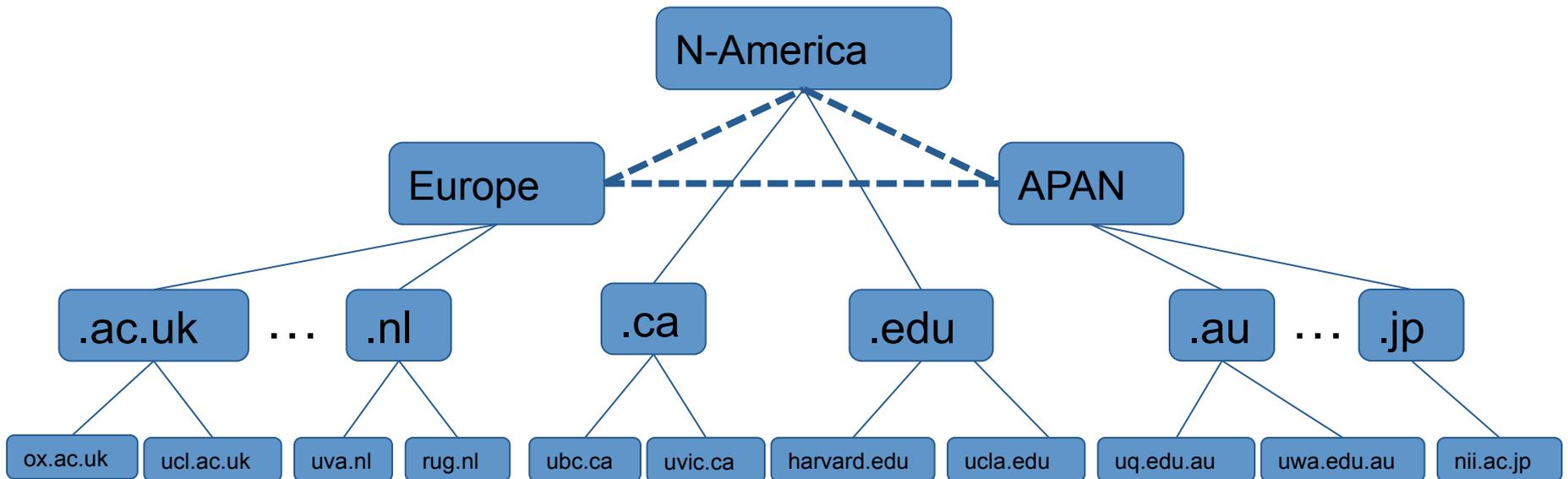
3881 service locations

+9% since June 2011

# Agenda

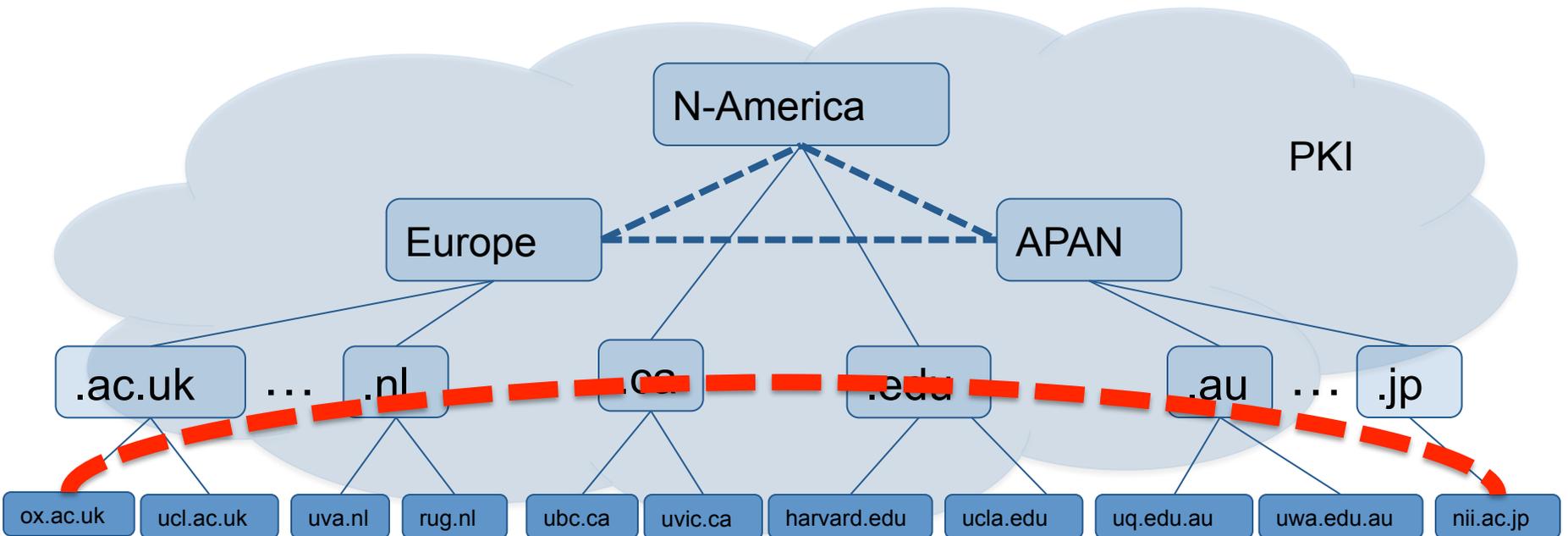
- Federated access in the Higher Education today
  - Intro
  - eduroam
- Challenges in and solutions for network access
  - RadSec
  - 3/4G operators
- An excursion to the application layer
  - Project Moonshot
- Summary and Conclusions
- Questions / Domande

# 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)

This is a service under preparation, do not expect it to work.

## Welcome to eduroam CAT

the eduroam Configuration Assistant Tool



View this page in [Deutsch](#) [English\(GB\)](#) [Español](#) [Hrvatski](#) [Polski](#)

Selected institution: **Fondation RESTENA** [select another](#)

**If you encounter problems, then you can obtain direct assistance from your home organisation at:**

WWW: <http://www.restena.lu/restena/fr/FR-eduroam-setup-main.html>

email: [helpdesk@restena.lu](mailto:helpdesk@restena.lu)

tel: +352 424409 1

**Choose an installer to download**

MS Windows 7

MS Windows Vista

MS Windows XP SP3

Apple Mac OS X Lion

Apple Mac OS X (pre-Lion)

Apple iOS mobile devices

Welcome Letter

Test

# CAT for users (win7 installer)



# CAT for institutions (dashboard)

## IdP-wide settings

### General Institution Details

Country: **LU**  
Institution name: **Fondation RESTENA**  
Additional SSID: **eduroam-school**

### Global Helpdesk Details

Support: **helpdesk@restena.lu**  
E-Mail  
Support: **+352 424409 1**  
Phone  
Support: **http://www.restena.lu/restena/fr/FR-eduroam-setup-main.html**  
Web

### Global EAP Options

CA Certificate File  

```
C=LU
L=Luxembourg
O=Fondation RESTENA
OU=RESTENA eduroam CA
CN=RESTENA eduroam
authority
emailAddress=noc@restena.lu
```

  
Name of Authentication Server: **eduroam.restena.lu**



[Edit IdP-wide settings](#)

[Delete IdP](#)

## Available Support actions

Check another realm's reachability  [Go!](#)

Check server status of European federations [Go!](#)

## Profiles for this institution

### Profile: education.lu Users

EAP Types (in order of preference):

[Check realm reachability](#)

# CAT for institutions (profiles)

is a bonus.

View this page in [Deutsch](#) [English\(GB\)](#) [Español](#) [Hrvatski](#) [Polski](#)

## Edit profile 'education.lu Users' ...

### General Institution Details

Country: **LU**  
Institution name: **Fondation RESTENA**  
Additional SSID: **eduroam-school**

### Global Helpdesk Details

Support: **helpdesk@restena.lu**  
E-Mail  
Support: **+352 424409 1**  
Phone  
Support: **http://www.restena.lu/restena/fr/FR-eduroam-setup-main.html**  
Web

### Global EAP Options

CA Certificate File  
Name of Authentication Server

```
C=LU
L=Luxembourg
O=Fondation RESTENA
OU=RESTENA eduroam CA
CN=RESTENA eduroam
authority
emailAddress=noc@restena.lu
```

**eduroam.restena.lu**

### General Profile properties

#### Profile Name and RADIUS realm

Profile Name:   
Realm:

#### Anonymity Support

Enable Anonymous Outer Identity:

#### Installer Download Location

Redirect end users to own web page:

### Supported EAP types

**Supported EAP types for this profile**

1. PEAP-MSCHAPv2
2. TTLS-MSCHAPv2
3. TTLS-PAP

**Unsupported EAP types**

- FAST-GTC
- TLS
- TTLS-GTC

Use "drag & drop" to mark an EAP method as supported. Prioritisation is done automatically, depending on where you "drop" the method.

### Helpdesk Details for this profile

If you specify an option here, it will override the global option(s) with the same name, if any.

[Add new option](#)

### EAP Details for this profile

If you specify an option here, it will override the global option(s) with the same name, if any.

[Add new option](#)

# 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?

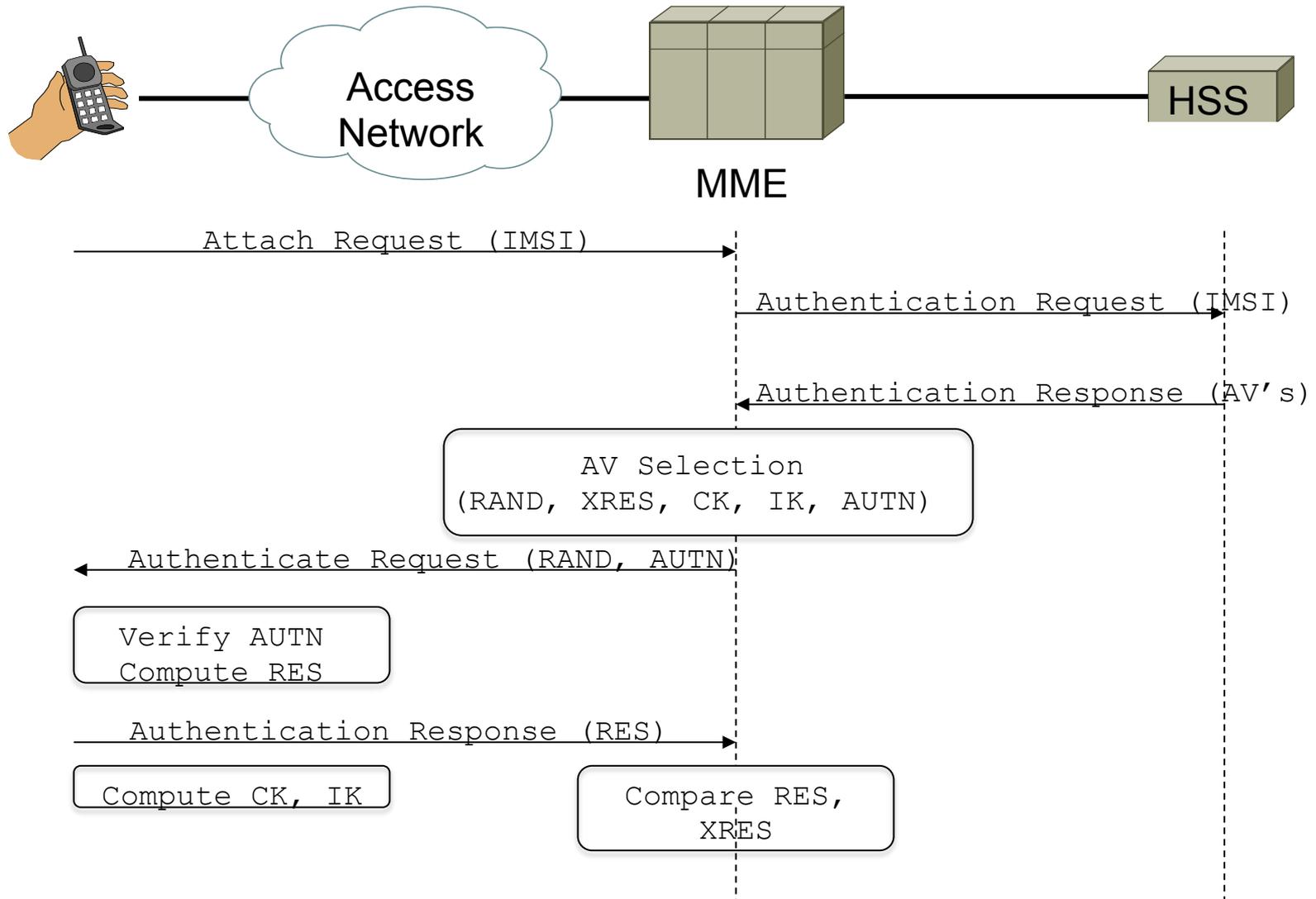
    - NREN as Mobile Virtual Network Operator (MVNO)?

- Operator as an Identity Provider

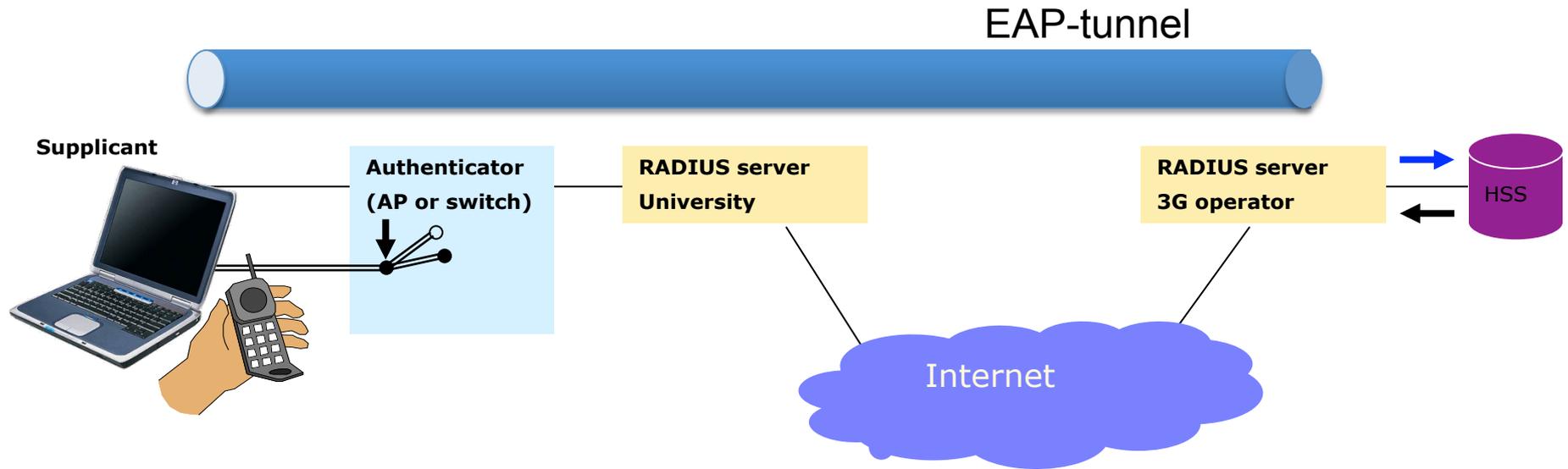
  - How about acceptable use?

  - 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

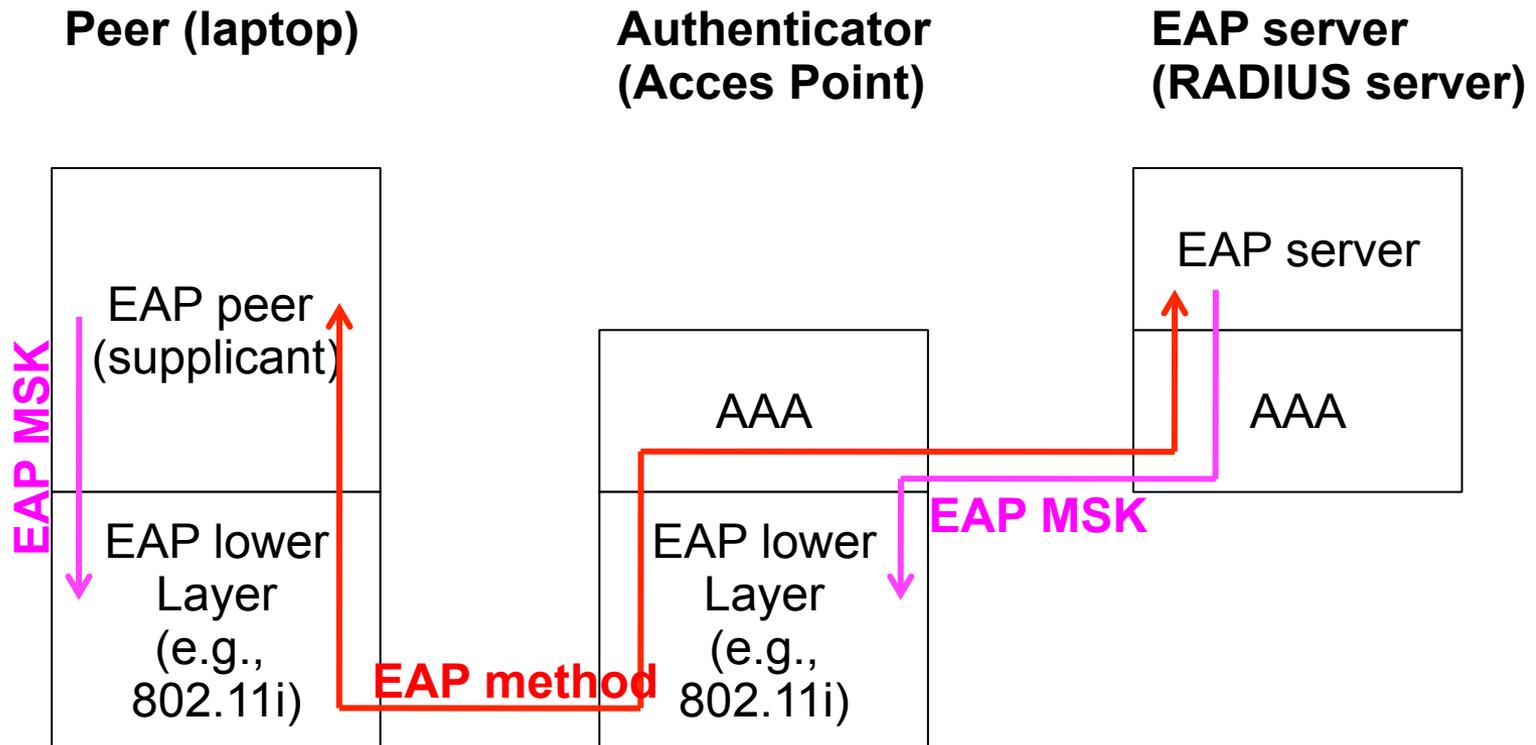
# SAML federations

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

# Project Moonshot

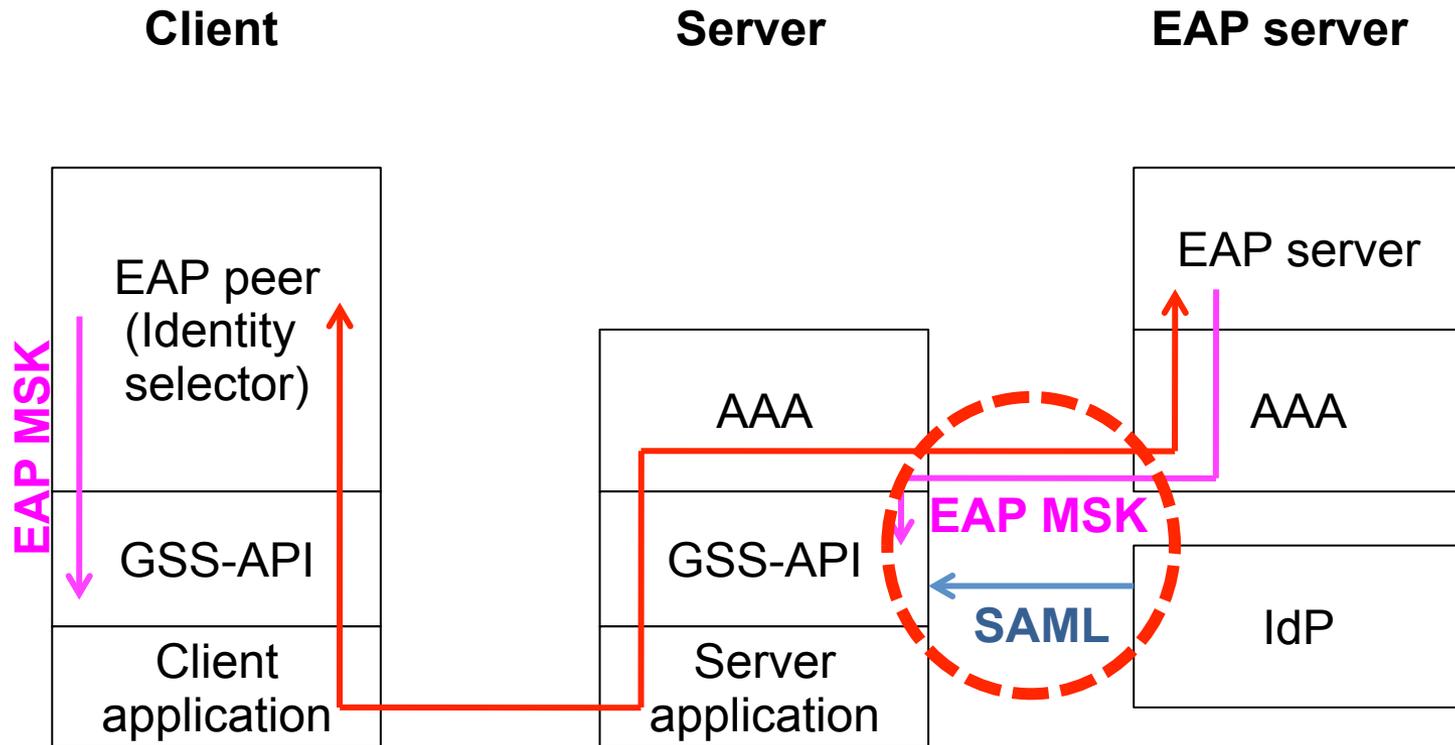
- Leverages:
  - RADIUS hierarchy for federation**
  - EAP for privacy protection**
  - SAML for identity assertions and attribute exchange
  - GSS-API for application interface
- Use cases:
  - IMAP
  - SSH
  - XMPP
  - ...
- Standardisation in Abfab (Application Bridging for Federated Authentication 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 conclusions

- 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>