

# Federated Identity

## and access to (library) resources

**Klaas Wierenga**  
*Chief Community Support Officer*

**20. DINI-Jahrestagung**  
**Osnabrück, 09. Oktober 2019**

[www.geant.org](http://www.geant.org)



# Membership Association

**GÉANT Association supports and represents over 40 NRENs across Europe.**

Together they support over 10,000 institutions and 50 million academic users.





**To support collaboration and development amongst researchers, the dissemination of information & knowledge, and provide access to a portfolio of services and infrastructure resources:**



**Runs a membership association for Europe's National Research & Education Networks (NRENs)**  
GÉANT Association



**Coordinates and participates in EC-funded projects**

Under Horizon 2020 the financial instrument for implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness



**Operates a pan-European e-infrastructure**  
GÉANT network



**Manages a portfolio of services for research & education**  
EduX



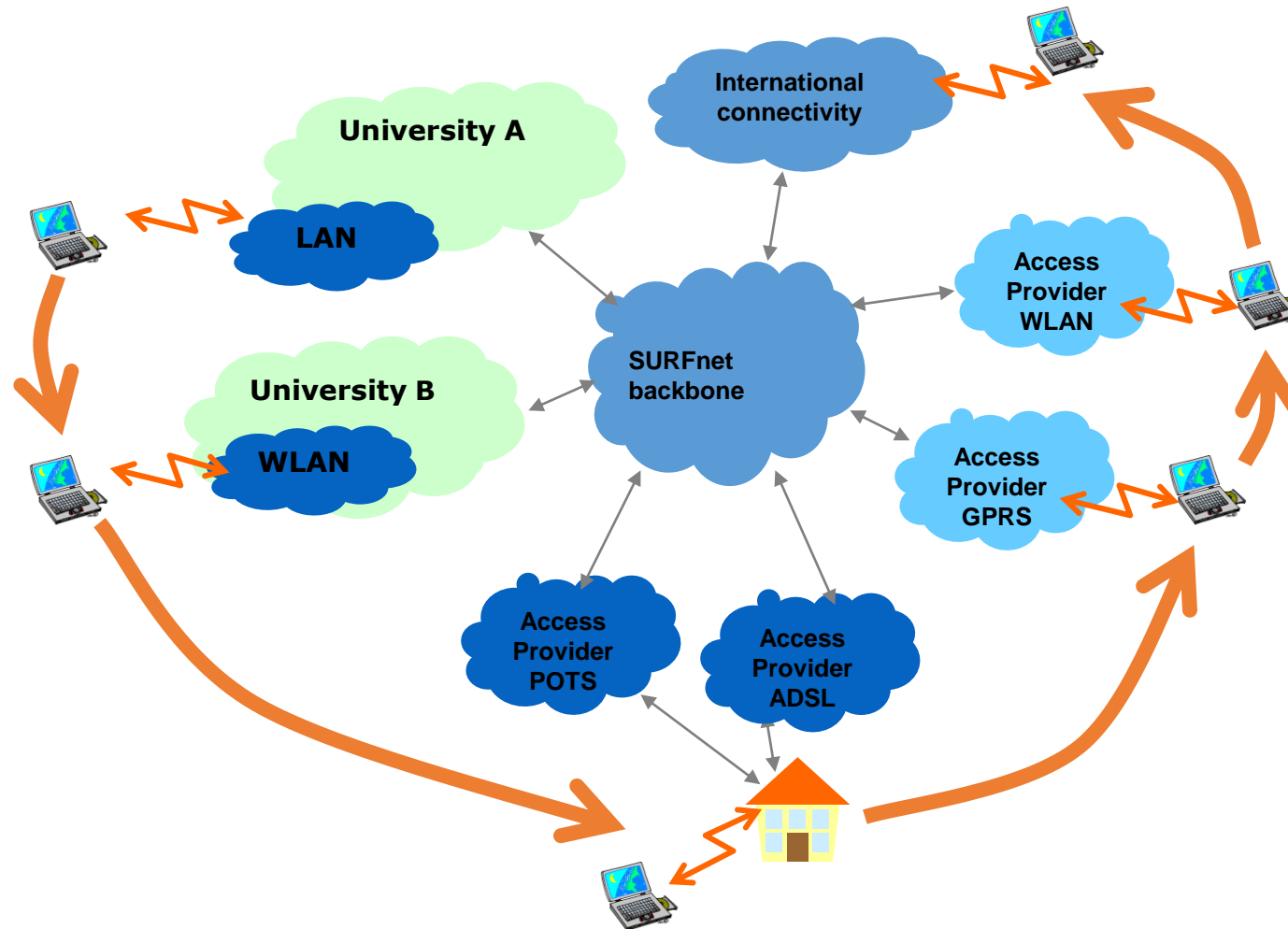
**Organises and runs community events & working groups**  
TNC, task forces & special interest groups

*“Complacency is the biggest enemy of any librarian”*

Jean Armour Polly aka Net-mom – 2019 Internet Hall of Fame acceptance speech



# Motivation





# IP recognition worked well in this environment



Until.... people began connecting  
from everywhere





# Terminology

- Authentication:
  - Is the user who they say they are?
  - Carried out by user's home institution
- Authorisation:
  - What access should the user be granted?
  - Determined by resource owner



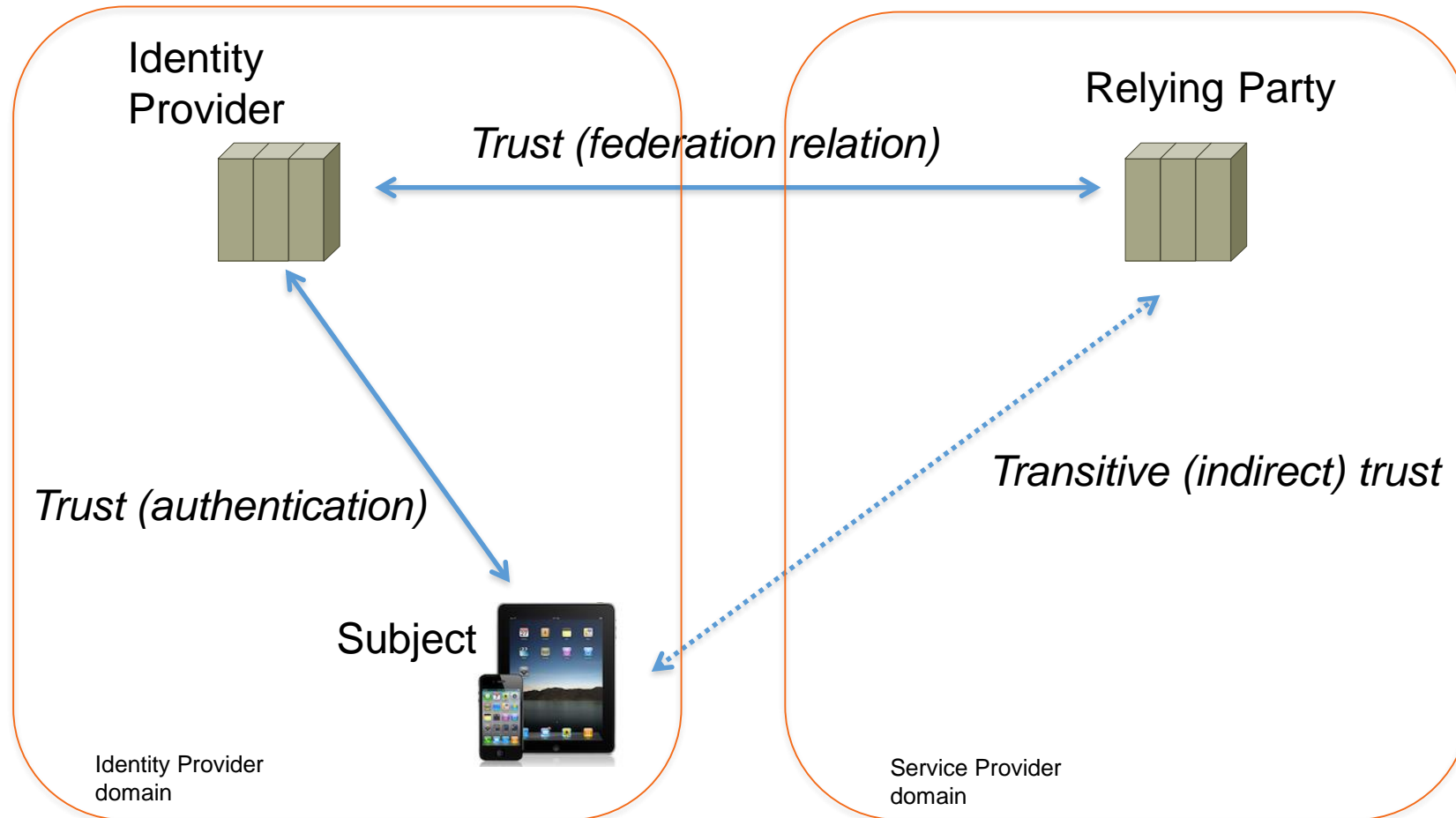
# What is **Federated Identity** and what does it buy us?

- Definition: Delegation of responsibility to authenticate and authorize individuals to a trusted party
  - This trusted party is typically the individual's organization in an enterprise environment, the involved parties agree on rules, technologies etc.
- Why?
  - No long term employee credentials necessary on partner sites
  - Automated user provisioning and removal
  - Managed access to employee information
  - Minimize sharing of attributes about a user (GDPR!)
  - Single sign-on
  - Scalable establishment of relations

“The only real problem is scaling. All others inherit from that one.”

Mike O'Dell, Chief Scientist UUNET, 2000

## What does it look like?



*"I, IdP, claim that the Subject is successfully authenticated and is authorized to access the service offered by Relying Party"*











# eduroam

Linking students to the global community

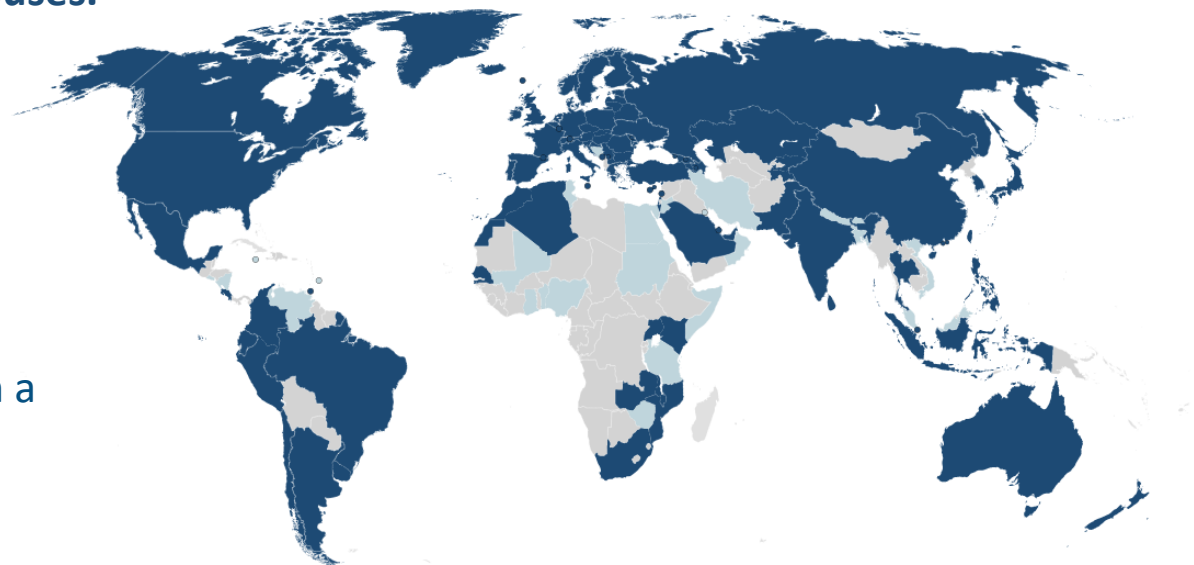


**Free secure Wifi provided by NRENs between campuses.**

**A global network of users across 101 territories.  
More than 2 billion international authentications  
and counting**

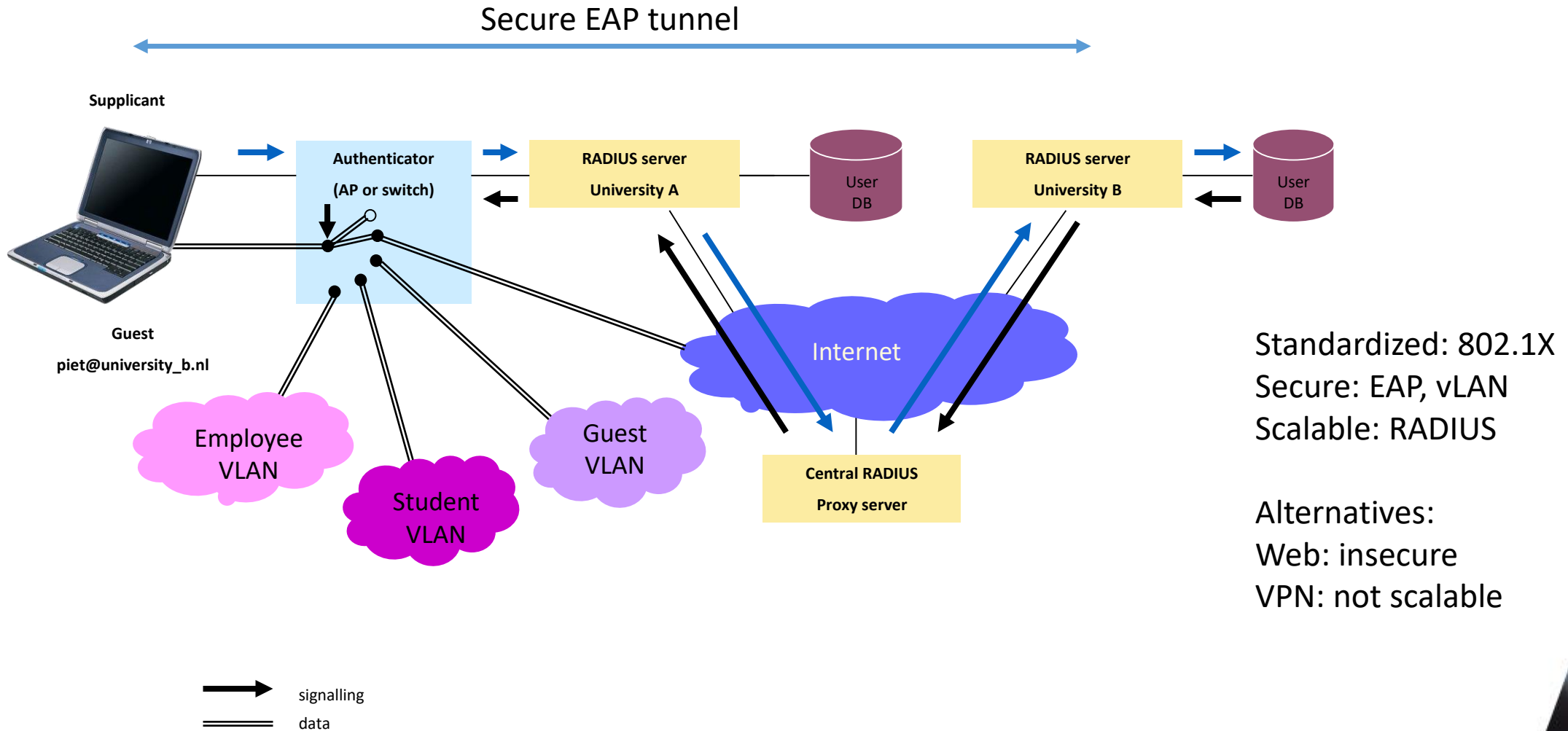
### **A worldwide success story**

From its early beginnings as a joint venture between a few European universities to today – with millions of users in more than 100 territories worldwide, eduroam has been an amazing success story and an example of research and education collaboration.



[www.eduroam.org](http://www.eduroam.org)

# Cross-domain 802.1X with VLAN assignment



Standardized: 802.1X  
Secure: EAP, vLAN  
Scalable: RADIUS

Alternatives:  
Web: insecure  
VPN: not scalable



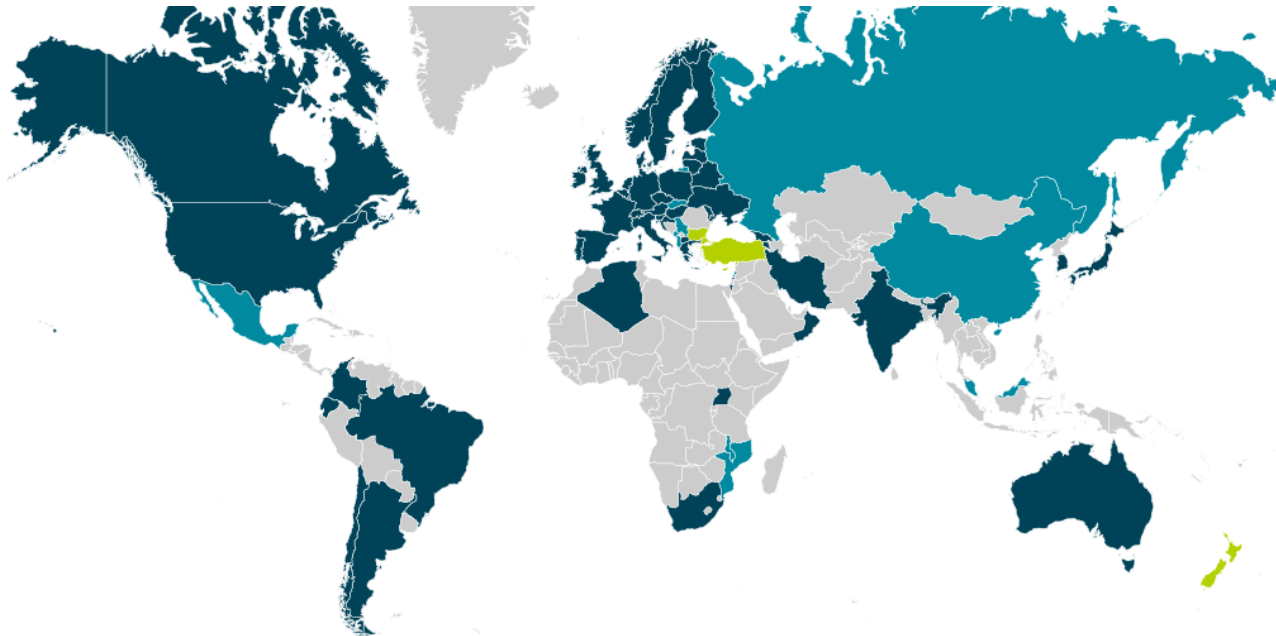
# eduGAIN

Enabling secure Single Sign On services to global research and educational resources



**Federated identities enable users to access a wide range of services using a single account sign-on managed by their 'home' institution**

- Improves access
- Improves security
- Reduces management overhead and costs.



September 2019:  
66 Federations active  
5 Federations in process of  
joining  
5666 entities

eduGAIN depends on federations



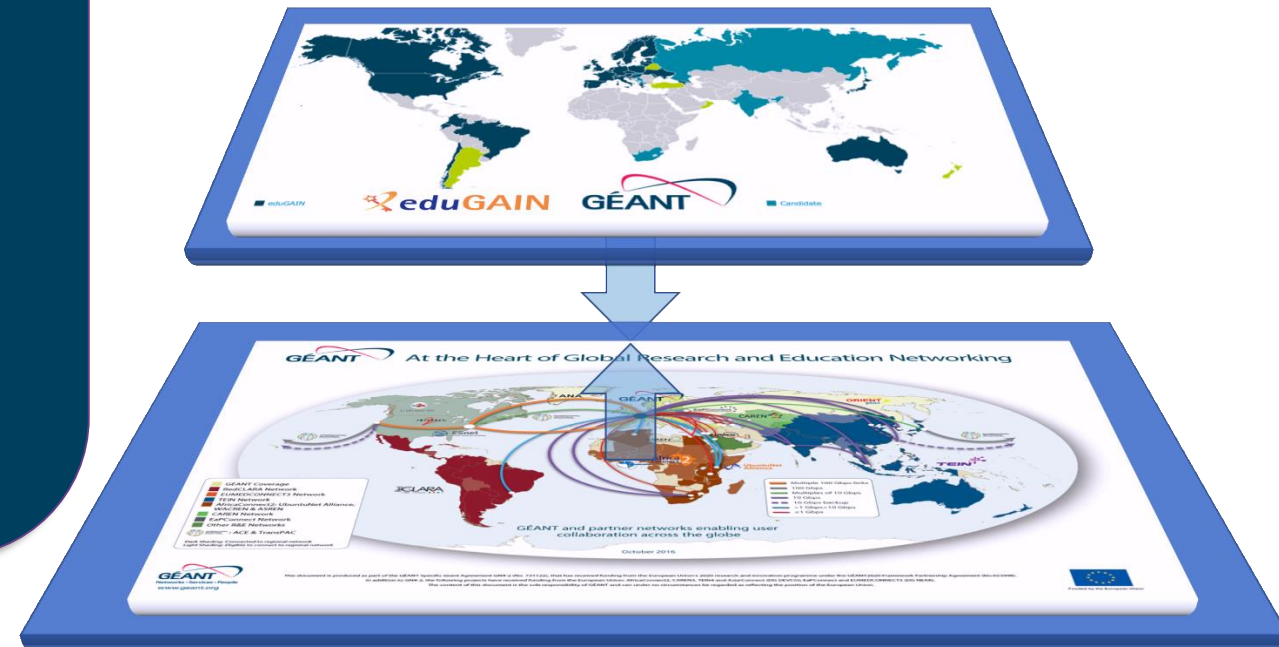
SWITCHaai





# eduGAIN – A global network of academic identities

- Allows researchers to use ONE digital identity to access MANY services and resources available in eduGAIN
- Access to resources based on the user's affiliation
  - AuthZ done by resources



# AARC Blueprint Architecture - Enabling an ecosystem of solutions on top of eduGAIN

- A Blueprint **Architecture** for authentication and authorization
  - A set of architectural and policy building blocks on top of eduGAIN
- eduGAIN and the Identity Federations
  - A solid foundation for federated access in Research and Education





A service to enable use of federated identities in research communities

Partner for any e-Infra or Research Infra inc. “long tail”, informal groups



## Components

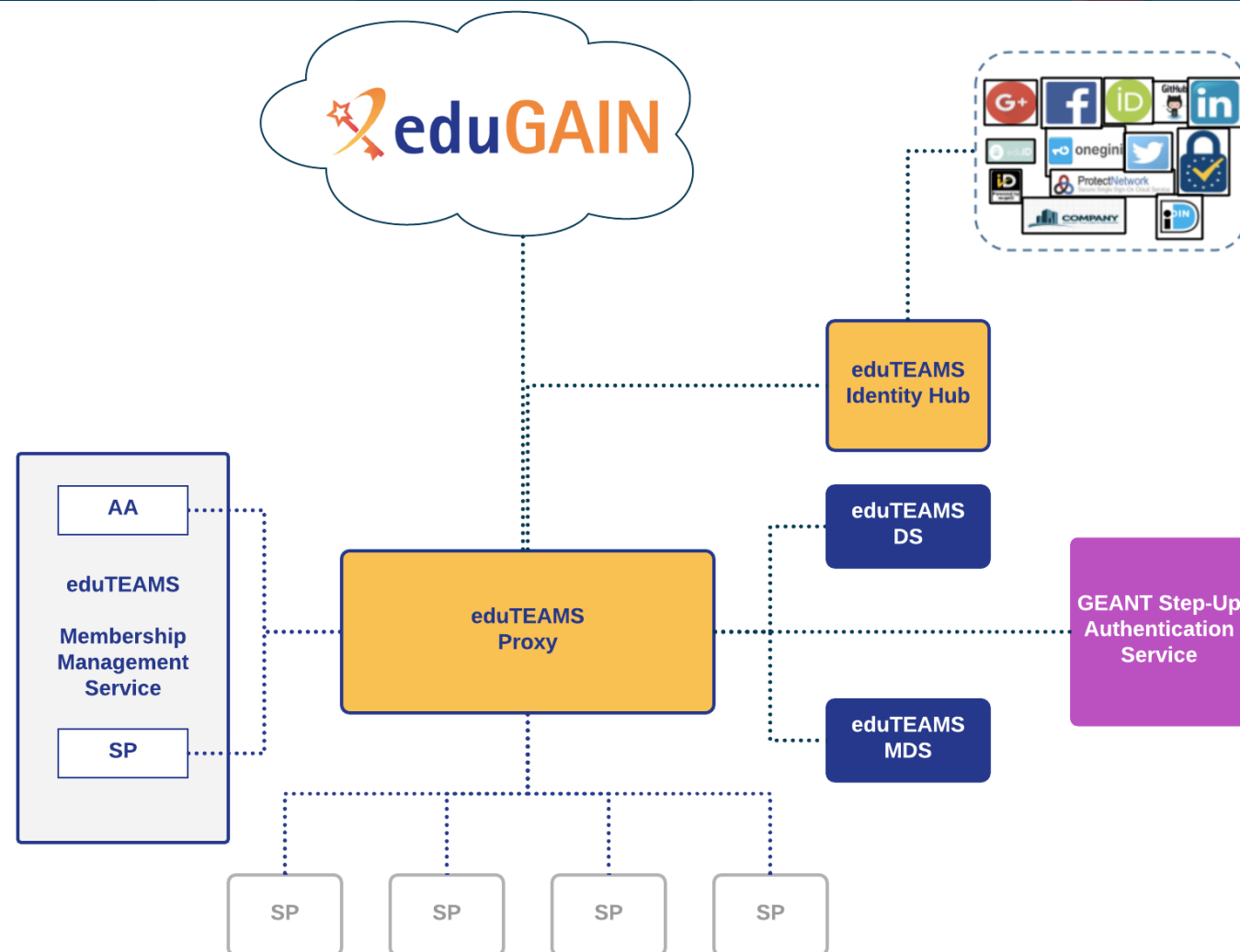
- Proxy & Identity Hub
- Membership Management service
- Discovery Service
- Metadata Service
- **Second Factor Authentication (Pilot!)**

## Characteristics

- Full implementation AARC Blueprint Architecture
- Single- and multi-tenant options
- Sustainability and strategic partnerships

# eduTEAMS for communities

- Users sign in to services with their **community identity** via eduTEAMS
- Users **register once and access any service** (available to their community)
- Reduces complexity for Service Providers by providing **one integration point for all services**
- Integration with GÉANT, EOSC(-hub) and other community and/or eduGAIN services







# InAcademia

## Online student validation

InAcademia is a service being developed that simply validates to other services that the user is a student or staff member of the academic community. Helps service providers offer academic discounts online and in real time.

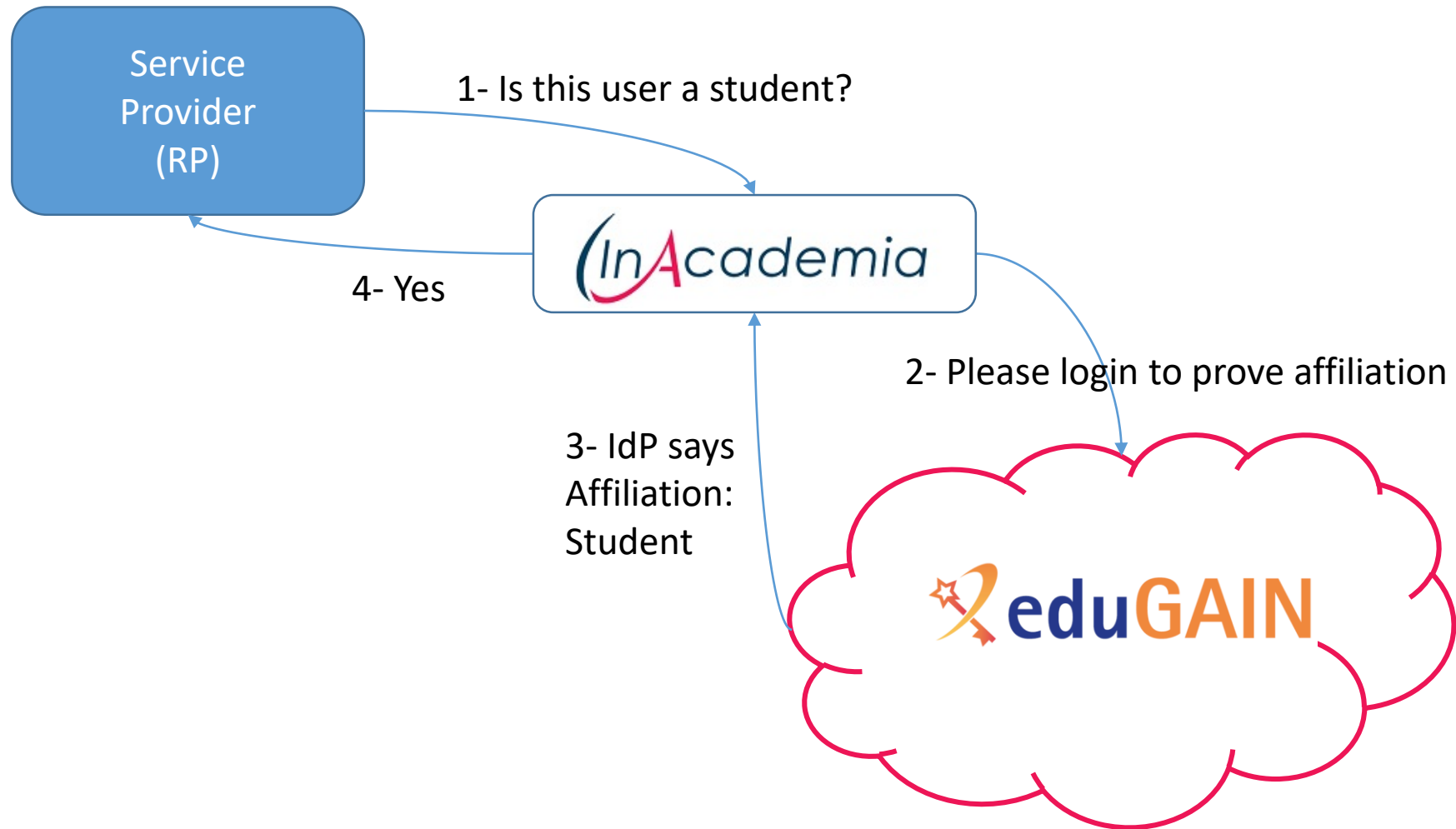
**A lightweight federated identity process with minimal attribute release (essentially a simple yes/no).**

**Easy for Service Providers to implement.**

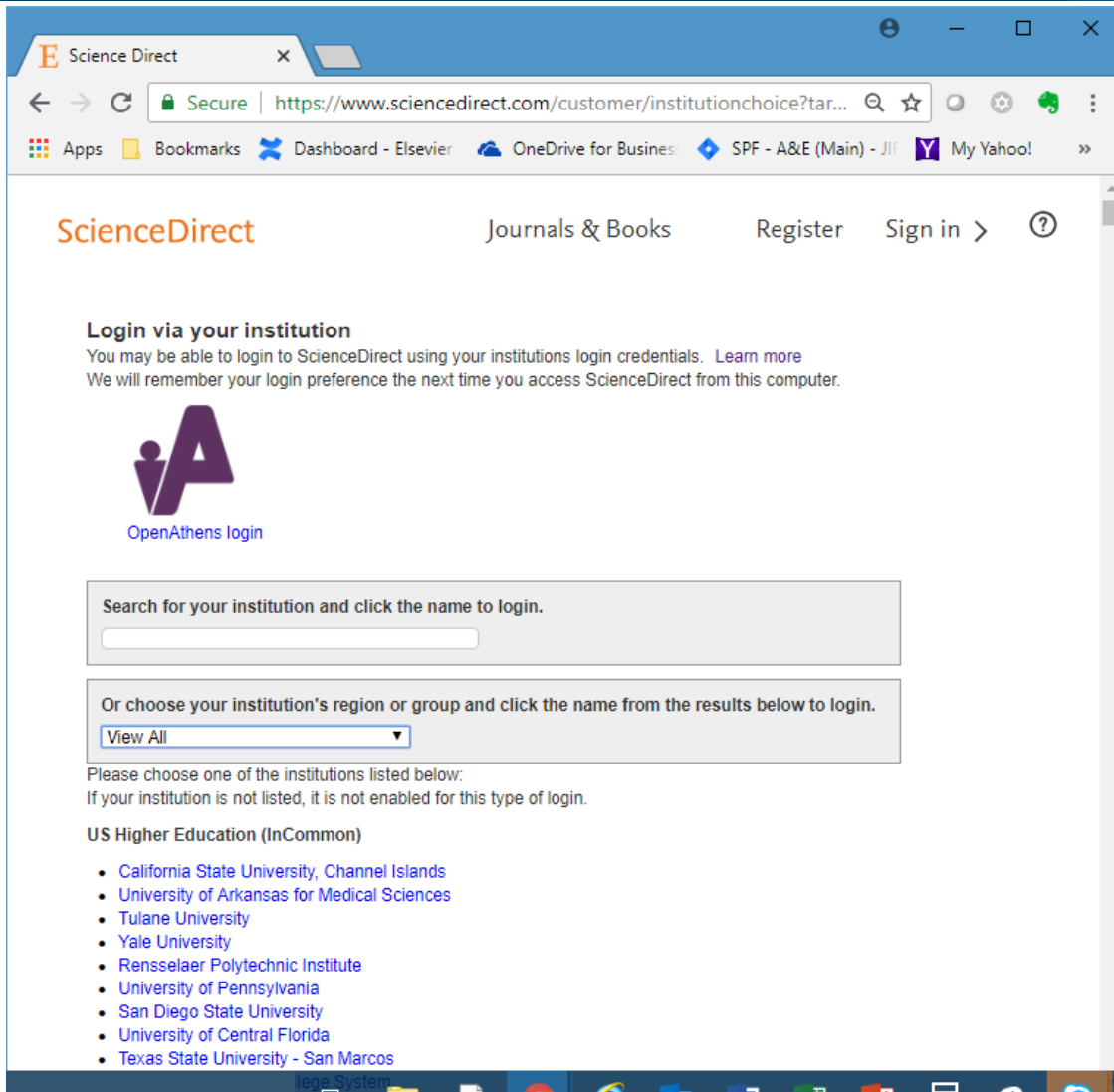
**Removes need for scans of ID cards or primitive e-mail address-based 'authentication'.**



## InAcademia – *Flow overview*



The current institutional discovery workflow is very difficult for users to navigate



# UX Building Blocks

1

Consistent visual cue  
and call to action signals  
institutional access



To get document (PDF, etc.)

1. Find your institution
2. Log in at your institution site
3. Get this document

2

Flexible and smart search

- Search by institution name, abbreviation or email
- Typeahead matching and URL

### Find Your Institution

Your university, organization or company

Examples: Science Institute, xxx@YourInstitution.edu, UCLA

**We found these institutions**

University of Minnesota  
University of Minnesota, All Campuses  
Search matched *University of Minnesota*

umn.edu

3

Remembered institution  
on next access

### Choose Your Institution

Institutions you used previously

University of Minnesota


[+ Choose another](#)



*“Complacency is the biggest enemy of any librarian”*

Jean Armour Polly aka Net-mom – 2019 Internet Hall of Fame acceptance speech





Thank you  
Any Questions?

[klaas.wierenga@geant.org](mailto:klaas.wierenga@geant.org)



Networks · Services · People  
[www.geant.org](http://www.geant.org)