Community services that are built for global scale

What works and what doesn't with eduroam and eduGAIN

Ann Harding @hardingar

Activity Lead, Trust & Identity Development, GÉANT
Person who Asks Uncomfortable Questions, SWITCH

Above the Net Workshop
20 October 2016

GÉANT
Networks · Services · People

Finding the magic

```
function ScaleGlobalService () {
 global $UseCases;
 global $TechGlue;


//TODO – Magic Goes Here


  echo $DeclareVictory;
}


$DeclareVictory = true;
```

Two Globally Scaled Services, Two Paths to Success
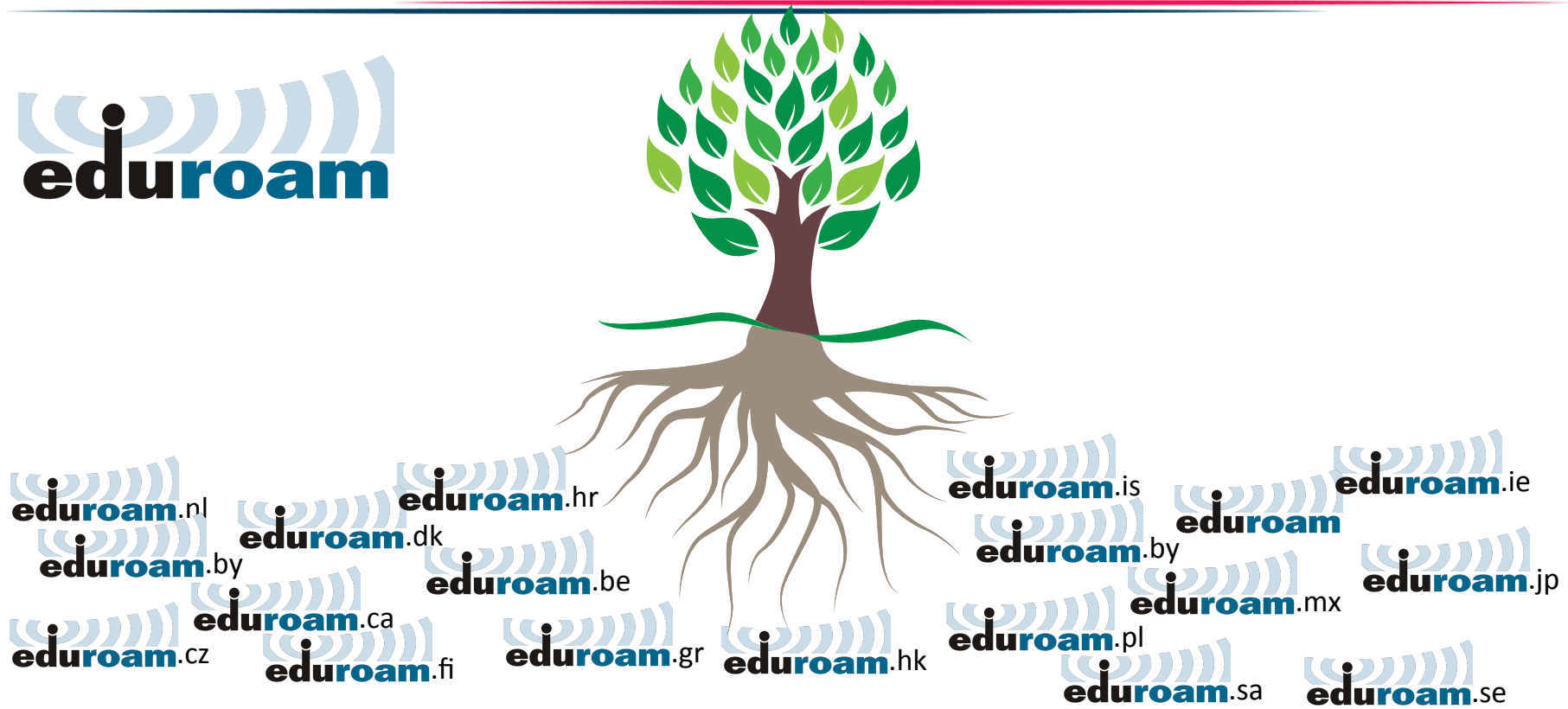
eduroam

- 10+ Years old,
- 70+ countries, tens of thousands of sites
- One service – network access
    - WIFI dominated, fix tech possible
    - Service visible to users
- Global eduroam Governance Committee (GeGC)
    - Nominated by confederations
    - Sets technical and organisational standards for the service

eduGAIN

- 5+ Years old
- 43 countries, 38 'active' members, 2k+ IdPs, nearly 1.5k services
- Service is metadata exchange
    - Not visible to users
    - User visible service is Web SSO
- eduGAIN SG and eduGAIN Executive
    - Each member has 2x SG reps
    - GÉANT Board 100% funds and is the Executive
    - SG sets technical and operational standards

From local service to global service – eduGAIN evolution

I has a question...

Who delivers these services?

Why does that matter?

Scaling Globally is Obeying the Invisible Rules of Irrationality

"There are many examples to show that people will work more for a cause than for cash."

"If you're a company, my advice is to remember that you can't have it both ways. You can't treat your customers like family one moment and then treat them impersonally—or, even worse, as a nuisance or a competitor—a moment later when this becomes more convenient or profitable."

"MONEY, AS IT turns out, is very often the most expensive way to motivate people. Social norms are not only cheaper, but often more effective as well."
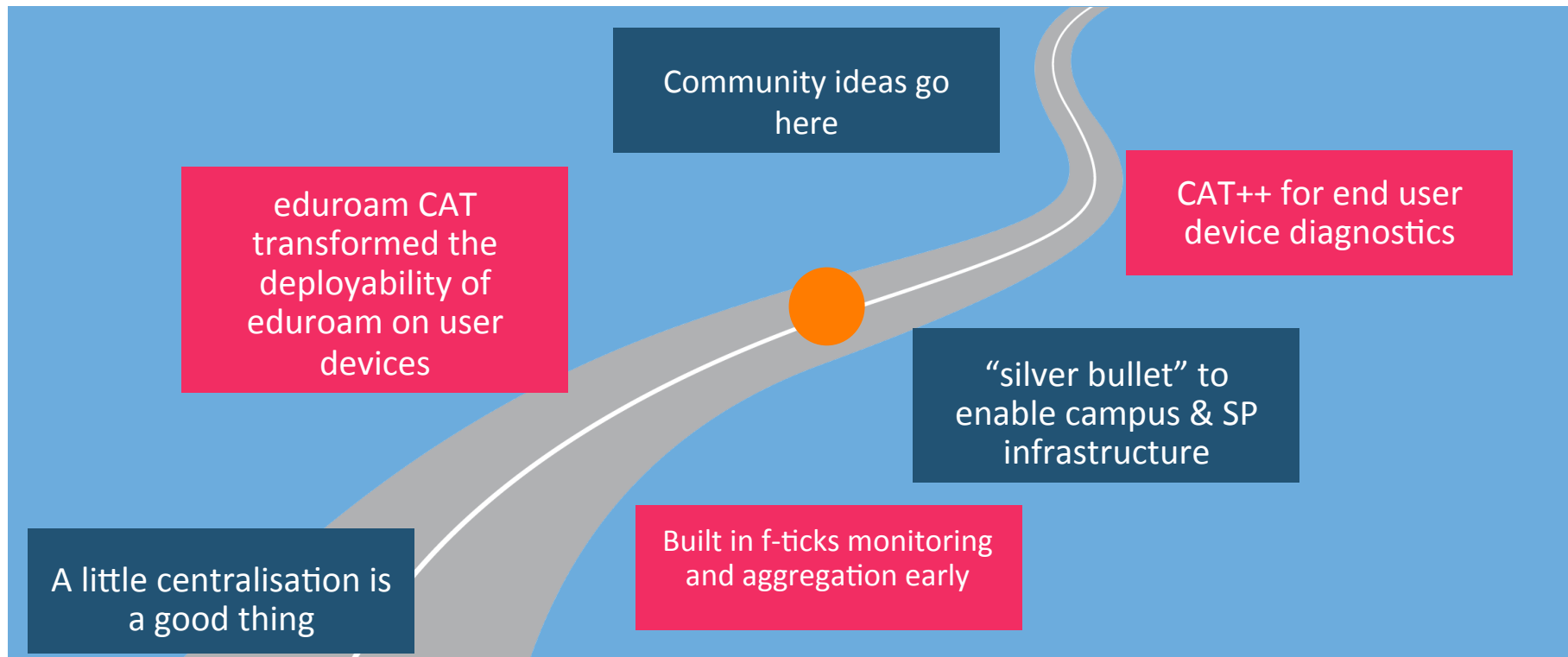
Dan Ariely, Predictably Irrational: The Hidden Forces That Shape Our Decisions

Enlightened self interest

Beating The Limitations of Success – eduroam's roadmap

Community ideas go here

eduroam CAT transformed the deployability of eduroam on user devices

CAT++ for end user device diagnostics

"silver bullet" to enable campus & SP infrastructure

Built in f-ticks monitoring and aggregation early

A little centralisation is a good thing

Beating The Limitations of Success – eduGAIN's roadmap

Support Federations to Support Campus

Next Generation Architectures and Protocols

Beyond the baseline: CoCo & R&S

Beyond the baseline: SIRTFI & MFA

Robustness of Operations

Support for Federations: FaaS

Federation coverage

Entity coverage
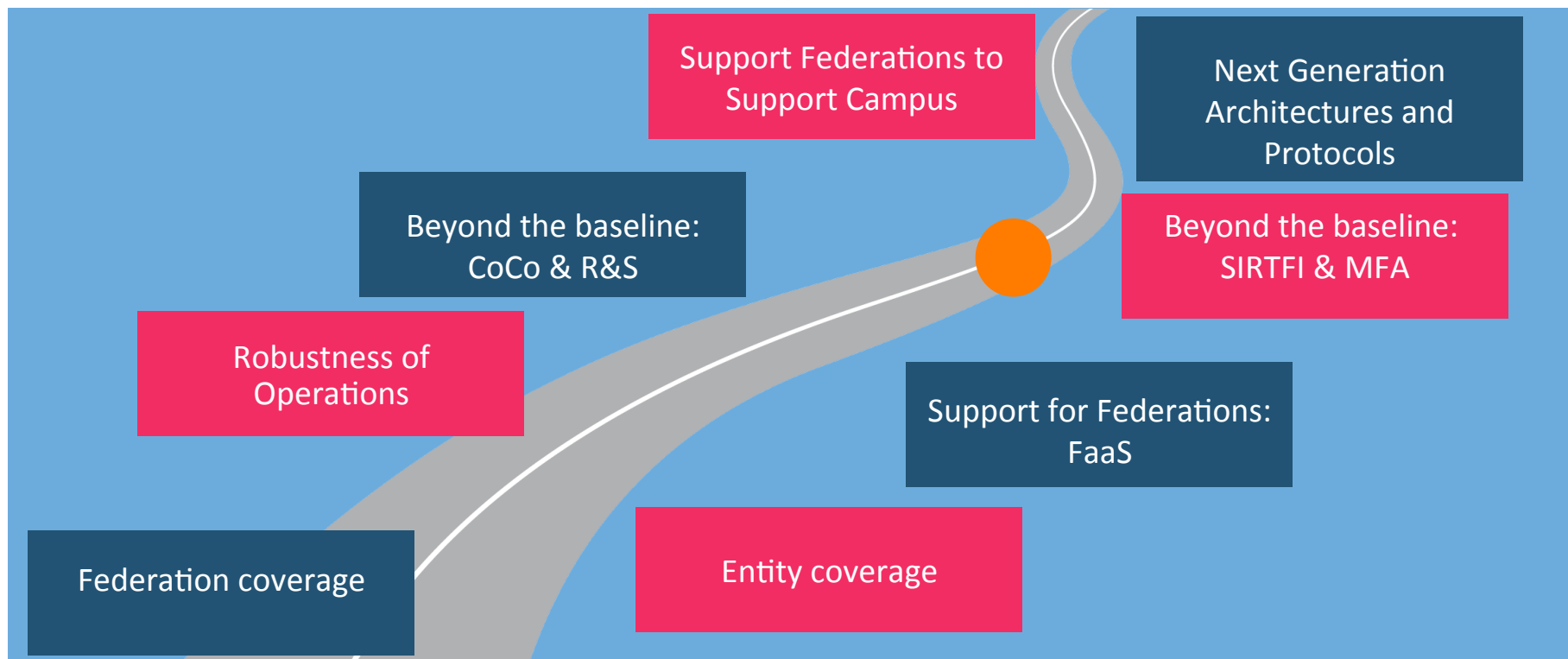
The challenges that remain

Predictability of experience is not guaranteed

- "Release the attributes"
- "eduroam is broken"

When you go above the net, it isn't all just bits, it's personally identifiable information

- With many legal jurisdictions

Strategic focus and funding differs wildly from country to country

- Affects what campus and federations can and will do

Centralisation still viewed with suspicion

- First step – monitoring and stats
- Trust MUST be earned, not demanded

New frontiers for eduGAIN
When acting locally is not enough

- **eduTEAMS - AAI as a Service for Collaborative organisations**
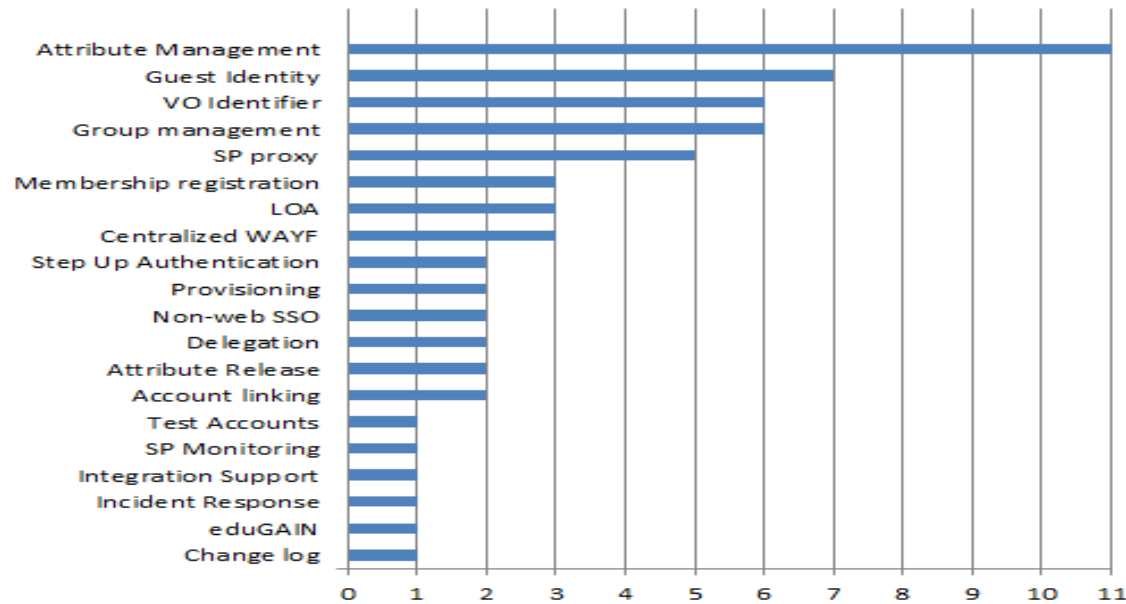 - Investigate Requirements
  - Discuss deployment model
  - Discuss challenges

- **InAcademia – Simple affiliation validation as a Service**
  - Describe usecases
  - Describe setup
  - Discuss Business model and Cost Benefit Analysis

eduTEAMS market analysis

http://www.geant.org/Projects/GEANT_Project_GN4-1/deliverables/D9-2_Market-Analysis-for-Virtual-Organisation-Platform-as-a-Service.pdf

eduTEAMS deployment model

- **eduTEAMS: a *suite* of services that supports AAI for Virtual Organisations**

- **Basic Services**
  - For Collaborative Organisations with generic AAI requirements
  - Operated by GÉANT as a multi tenant service
  - Also for Collaborations that are not legal entities
    - **eduTEAMS Identity Hub**
    - **eduTEAMS Membership Management**

- **Advanced Services**
  - Aimed to support 'larger' Collaborative Organisations with advanced/bespoke AAI requirements
  - Single tenant service, operated by GÉANT *on behalf of* a *VO*
  - A legal entity is responsibility for the data and pays a fee

eduTEAMS sustainability challenges

- **Virtual Organisations**
    - (Many) small groups of end users in institutions,
      how to interact with them and support them?
    - VOs have very little interaction with central IT, let alone with
      federation operators and NRENs
        - How do VOs find us?
        - What should be the role of the Institution and NREN?
        - How do we include Institutions and NRENs?

- **Pay per service?**
    - VOs many are not legal entities, how to charge them?
    - AAI is needed, but often not budgeted by Vos
    - What happens if the VOs project dies?

- **Global**
    - eScience is global, how to be inclusive beyond GEANT project?

InAcademia - *a Simple validation Service*

GÉANT

How to make affiliation validation much easier?

- Services get **most attributes from user** (self asserted)
- Only **affiliation** must come from the Home Organisation
- Query a **single, centralised service** to **confirm** affiliation (yes or no)
- A user 'proves' affiliation by **authentication** with home IdP
- A **simple protocol** is used by the Services (OpenID Connect)
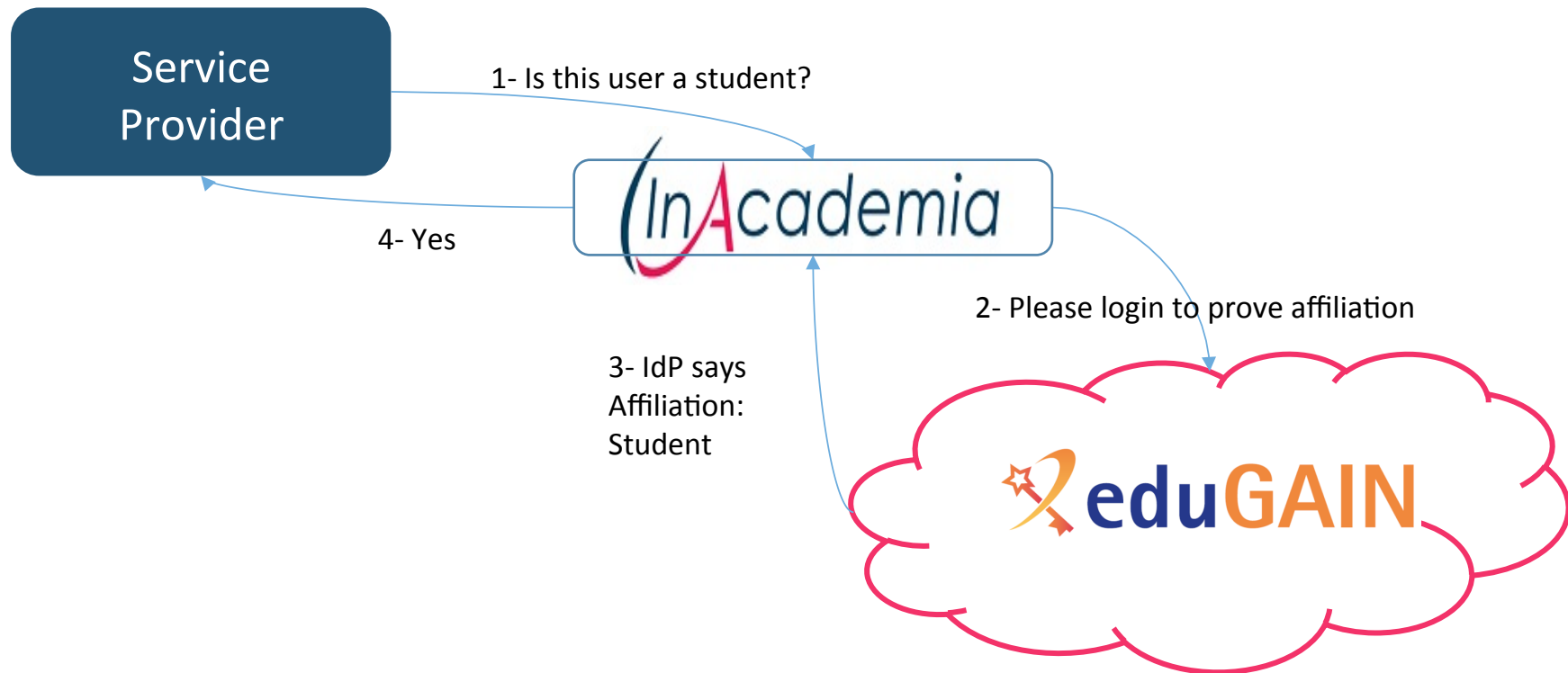- The **policy barrier** for using should be **low** (a single contract)

Why not directly use eduGAIN?

- Trust framework of eduGAIN and federations is much broader than just affiliation
- Joining a federation has several obstacles (policies and contracts)
- Implementing SAML and doing federation is not easy
- Inter-federation is even harder
- What defines an Academic institution?
- Upfront cost, but no customers

Different Business Model

- Service pays a **small transaction fee** (pay per use)
- Academic services get 100% discount
- Aim - Validation service interacts with all **eduGAIN IdPs**
- Income used for strategic investments for sustainability
- Additional fees shared back to participating organisations

InAcademia - *Flow*

Service Provider

1- Is this user a student?

InAcademia

4- Yes

2- Please login to prove affiliation

3- IdP says Affiliation: Student

eduGAIN

InAcademia – *Building a sustainable business*

COST

- Manpower:
  - Product management
  - Technical Product management
  - PR and marketing
  - Helpdesk
  - Development

- Upfront work to engage with commercial entities:
  - Proposition ready
  - Contract ready
  - Financial Handling ready

- Infrastructure
  - VMs
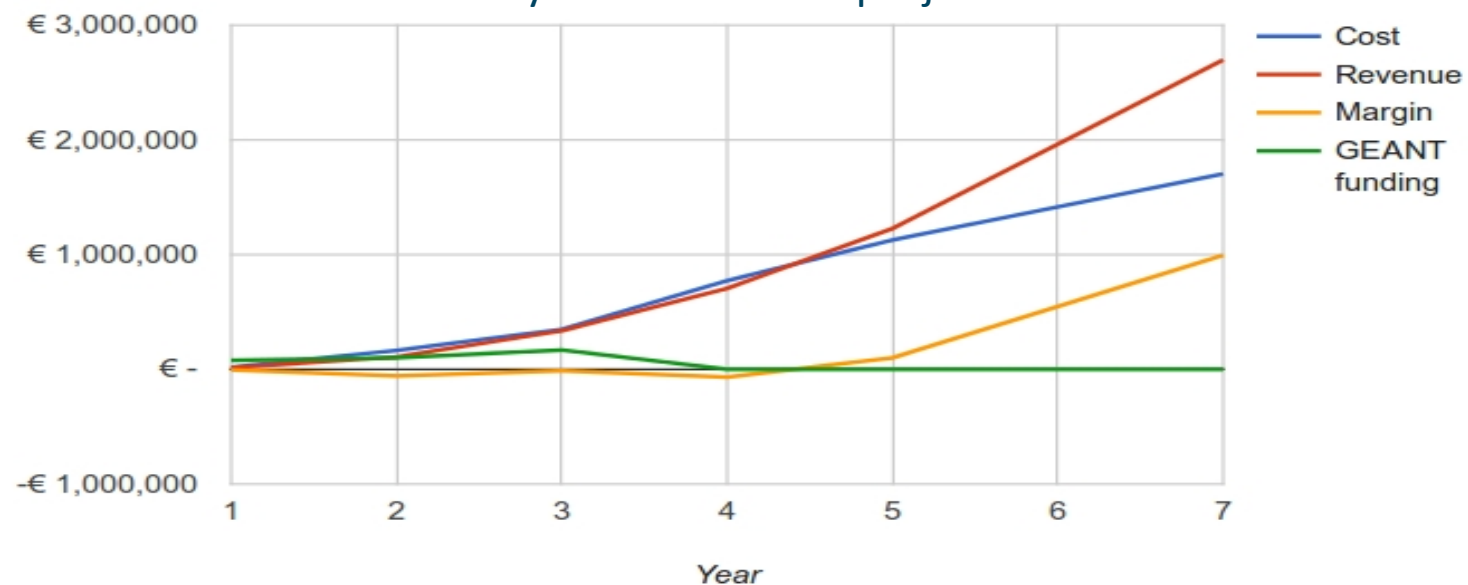 - Website and Support
  - Accounting and Statistics

BENEFITS

- One time setup fee

- Transaction fee

- GEANT project funding

InAcademia – *Cost benefit analysis*

InAcademia will be charging services a pay-per-use transaction fee, with a 100% discount for academic services. This helps NRENs to sustain the service during and beyond the GÉANT project

InAcademia sustainability challenges

Indirect benefit for Institutions and federations is hard to quantify

What is the definition of an Academic institution?

Legal support is hard to get

Business development people are hard to get

Engaging with commercials while we are not the customer

Who / How to handle payments?

What is the magic?

| Unify genuine use cases	Scale 'cheaply' by bringing in infrastructure from many parties	Design fairness	Build trust to help you overcome your limitations
Not so abstract that you will need 38 ways to implement, even if you leave it free as a theoretical possibility	Respect the advantages of social contract and understand where they outweigh the certainty of financial contract	Balance the pain points within the different stakeholders of the infrastructure	We as NRENS are proud and fiercely protective of our reputations
		You want more stats from the system? Make it easier to get them.	No amount of technical trust or governance tweaking will make you be able to go further than you are trusted
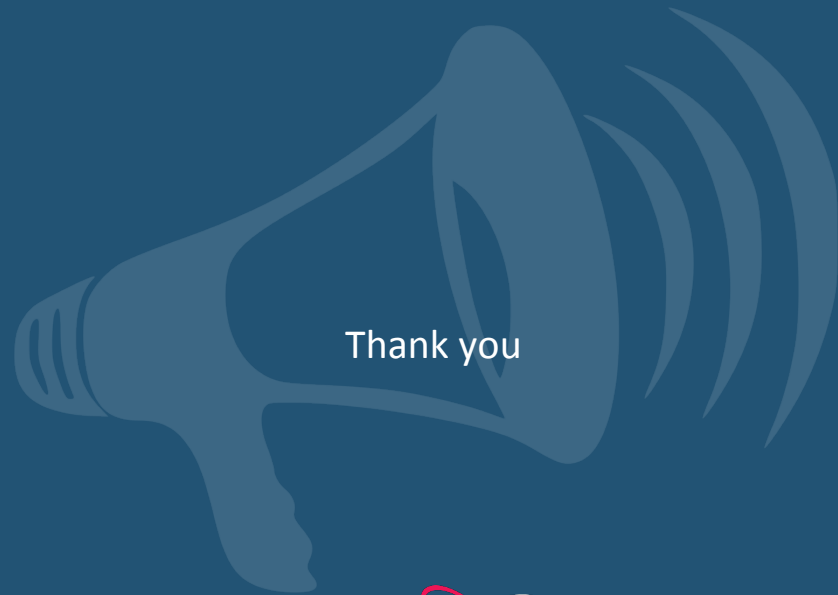
Thank you

GÉANT

Networks · Services · People
www.geant.org