

**eduTEAMS**

## **GEANT Trust & Identity Development**

**Niels van Dijk, SURFnet**

eduTEAMS Hands-On, TNC2018

June 11, 2018

Trondheim, NO

[support@eduTEAMS.org](mailto:support@eduTEAMS.org)  
<https://www.eduTEAMS.org>  
<https://wiki.geant.org/display/ED>



- **Introduction into eduTEAMS (Niels)**
  - eduTEAMS in the GEANT project
  - High-level design and components
  - Recent developments
- **eduTEAMS showcases (Christos)**
  - GEANT eduTEAMS Stand Alone service demo
  - LifeScience AAI pilot
- **eduTEAMS Demo (Christos, Mihaly)**
  - GEANT eduTEAMS Stand Alone service
- **eduTEAMS 'OpenSpace' (Christos, Mihaly, Niels)**
  - How do I.. ? , What is .. ? Why is.. ? What if I... ?

# About GÉANT

GÉANT supports and represents over 40 NRENs across Europe.

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



## Supporting users and enabling secure access to services



**eduroam** - secure global roaming access service *250+ million authentications per month* in 89 territories



**eduGAIN** - interconnects identity federations around the world, simplifying access to content, services and resources ~ 3500 identity providers accessing services



**AARC project** – collaborating with e-infrastructures, research collaborations, libraries & federations to share policies, architectures, training materials & pilots that avoid re-inventing the authentication & authorisation wheel



**REFEDs** – supporting identity federations worldwide



**Trusted Introducer** – services for security and incident response teams

**Certificate Service** – delivering cost-effective digital certificates.  
In partnership with 

- **Challenges in Authentication space**
  - International Collaboration
  - Collaborative organizations work with people outside scope of R&E communities as well
  - Requires Collaborative organizations to peer with other non R&E Identity providers or maintain an additional Identity provider
- **Challenges in Authorization space**
  - Services run by Collaborative Organizations often need attribute or group related information in the context of their collaboration, which are not issued by Institutions
  - Requires Collaborative Organizations to manage and provide additional attributes and groups towards their services, independently from the Institutions



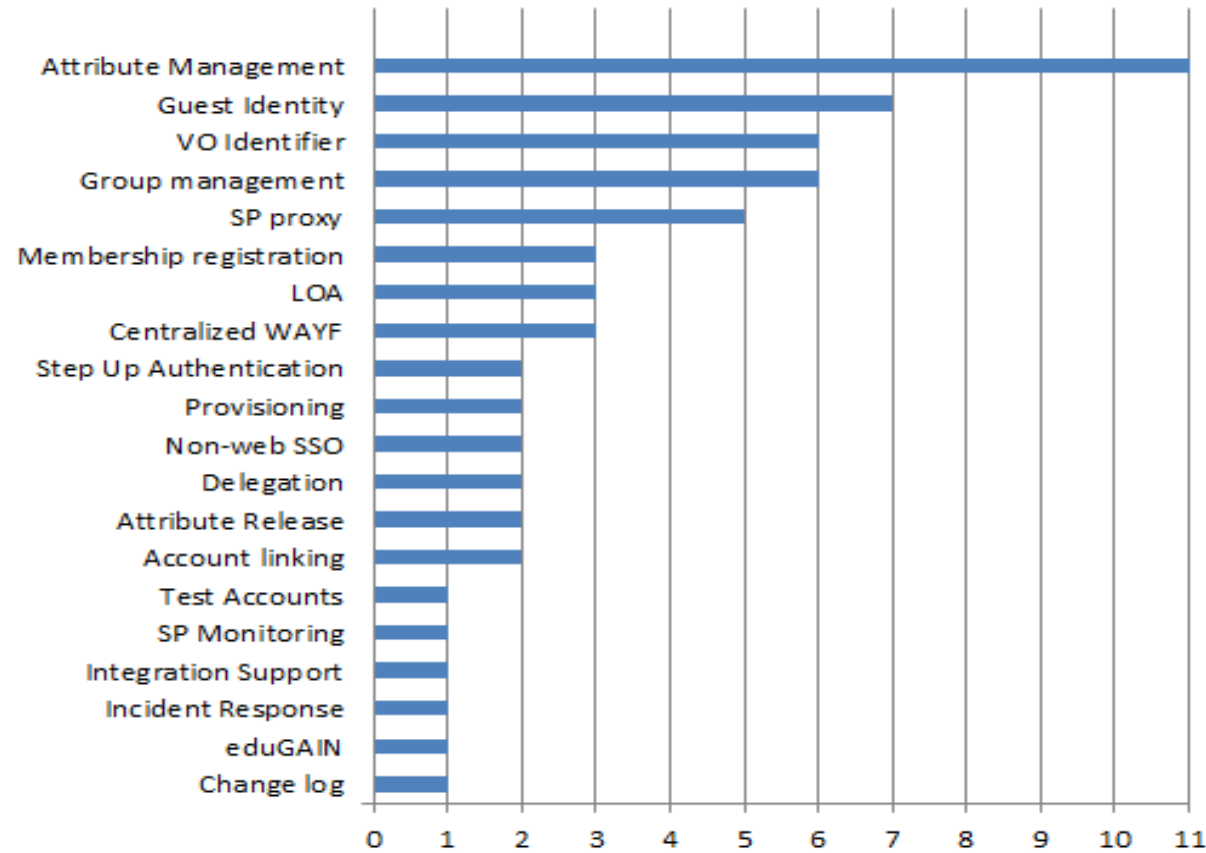
- **Goal**
  - Investigate the conditions that would allow GÉANT to provide **services** to support Collaborative organizations
  - Focus on delivery of technical services
  - Out of scope:
    - Technical development
    - Policy & LOA development
- **Activities**
  - Gather requirements and priorities with/from communities
  - Look at *existing* tools and technologies
  - Look into delivery model
  - Investigate business case & sustainability
  - Pilot with communities
  - Operations and Market



- The FIM4R paper (April 2012) was one of the first to articulate collective requirements for using Federated AAI for VOs.
- performed a survey among several small and large Pan-European VOs to (re-)validate the requirements.



# Market Analysis Results



[http://www.geant.org/Projects/GEANT\\_Project\\_GN4-1/deliverables/D9-2\\_Market-Analysis-for-Virtual-Organisation-Platform-as-a-Service.pdf](http://www.geant.org/Projects/GEANT_Project_GN4-1/deliverables/D9-2_Market-Analysis-for-Virtual-Organisation-Platform-as-a-Service.pdf)



Collaboration suite to enable use of federated identity in research communities

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



## Components

- Membership Management service
- Discovery Service
- Identity Hub
- **Second Factor Auth (Pilot!)**

## Characteristics

- 2 monthly release cycle
- Supports AARC architecture
- Single- and multi-tenant options

Documentation, Cookbooks, Privacy Policy etc available

<https://wiki.geant.org/display/ED>

### Research communities and e-Infrastructures

- AARC2-as-VO (Pilot committed)
- Life Science AAI (Pilot)
- Umbrella (Pilot committed)
- HPC-Europe (Pilot interest)
- EUDAT (Pilot committed)\*
- EGI \*

\* as part of AARC2 interoperability activity

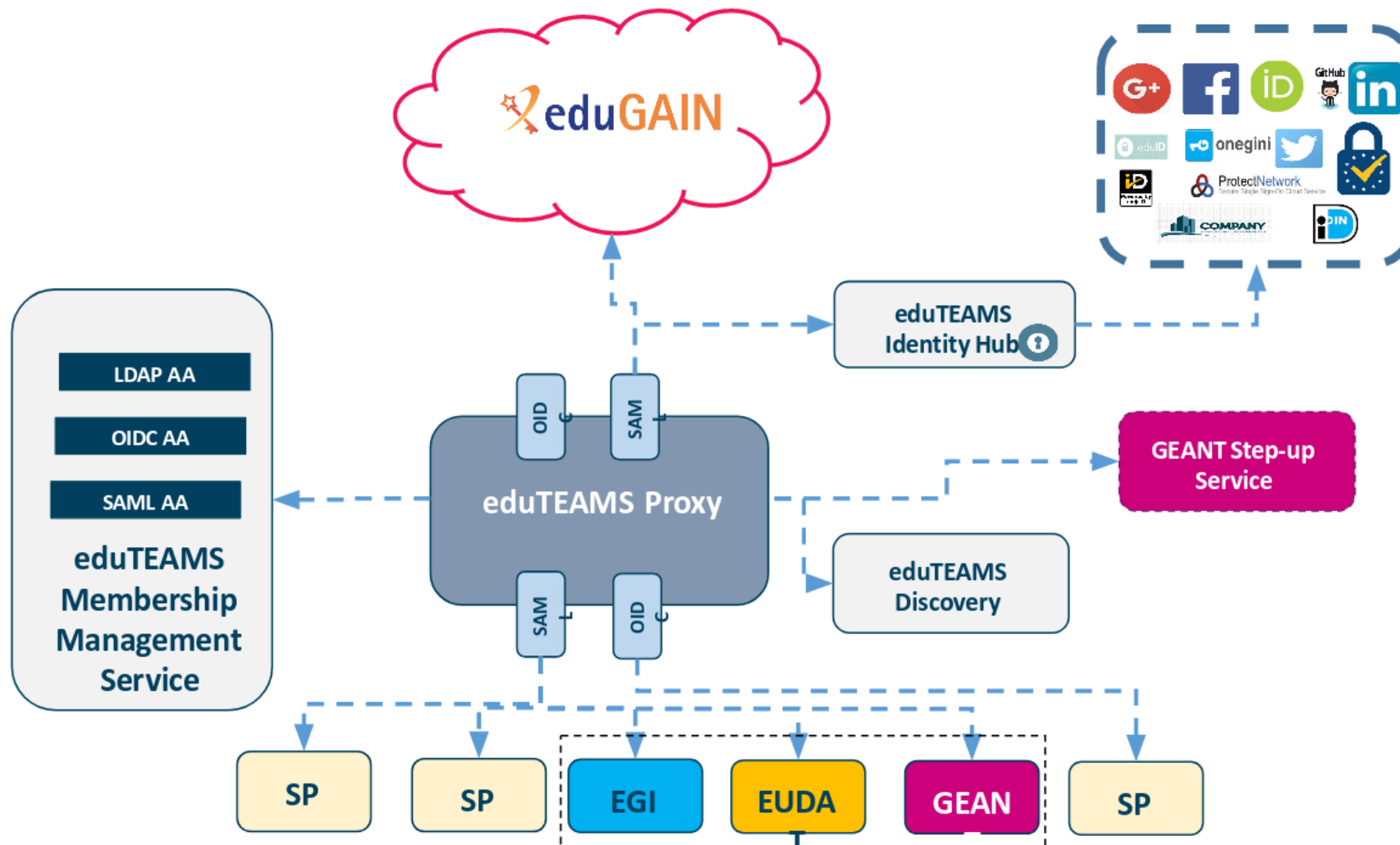


### NRENS

- JISC (UK)  
Moonshot Pathfinder project
- SURFnet (NL)  
Science Collaboration Zone project
- WAYF (DK)  
eduVPN  
Collaboration usecases



- **eduTEAMS Membership Management service**
  - CO specific workflows for onboarding members
  - Registry for CO persistent Identifier
  - Limited set of attributes to maximize interoperability
    - Use of eduPerson entitlement to carry richer info
  - Available through eduGAIN
- **eduTEAMS Identity Hub**
  - One persistent (SAML) IdP for many 'Guest' Identity Providers
  - Available and accessible through eduGAIN
  - Supports Research and Scholarship Entity Category
- **eduTEAMS Service proxy**
  - Single integration point for SP identity
  - SAML and OIDC support
  - Attribute aggregation from MMS
- **Discovery Service**
  - Service based or embedded discovery for eduGAIN SPs
  - Allows per SP filtering of IdPs
  - Allows per entity category filtering, e.g. R&S, CoCo, Sirtfi



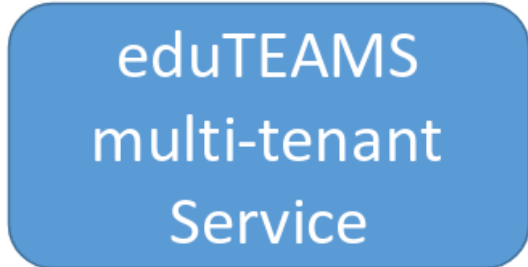
- **eduTEAMS multi-tenant service**  
A shared service that can be used by small and medium communities/long tail collaborations and is connected to EOSC
- **eduTEAMS standalone service**  
A standalone service offering, specific to a community or NREN national use, and is connected to EOSC
- **eduTEAMS bespoke** – a bespoke solution, typically involving individual components for a specific community

eduTEAMS  
multi-tenant  
Service

eduTEAMS  
standalone  
Service

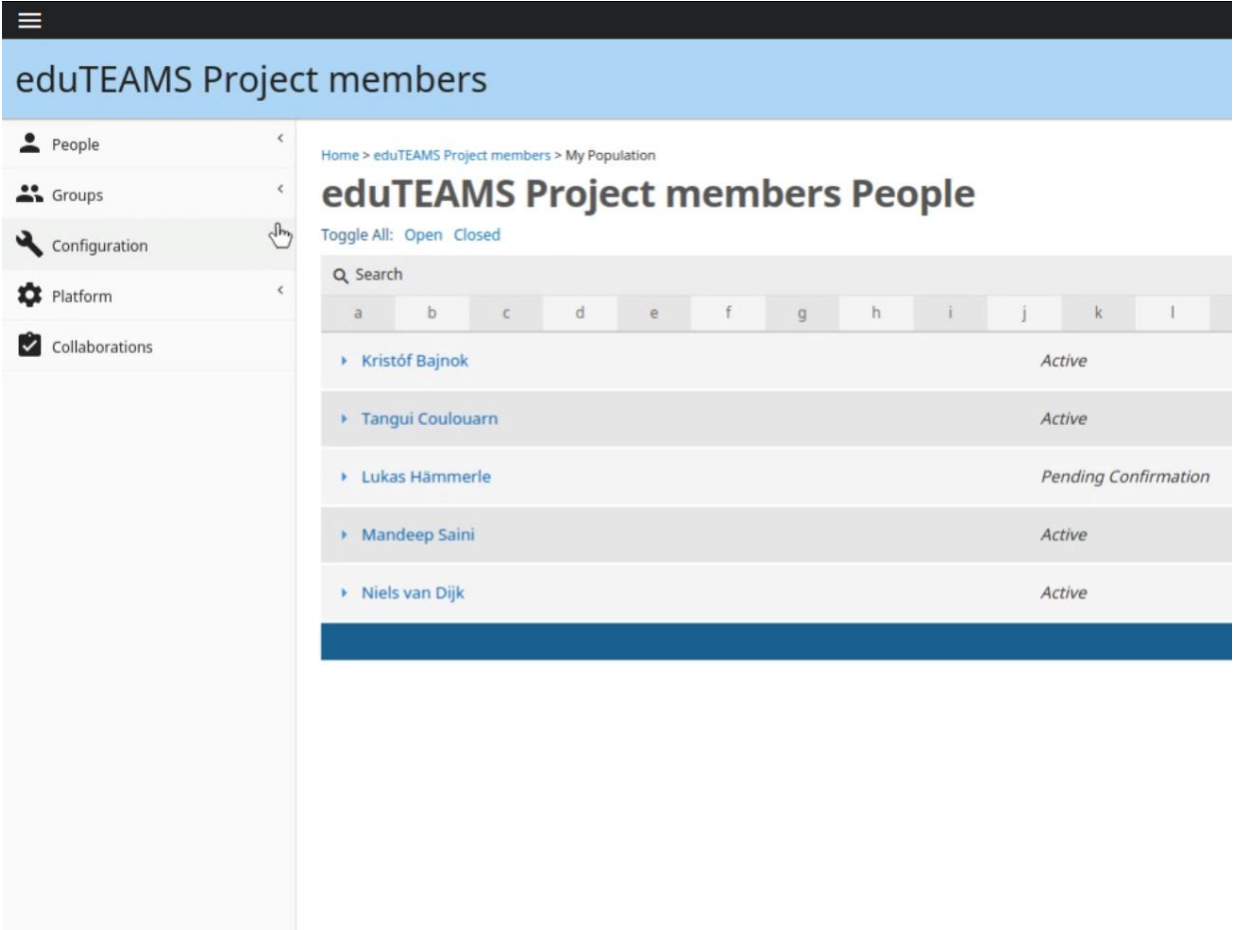
eduTEAMS  
bespoke Service

- Shared services that can be used by small and medium collaborations, “long tail” communities
- Available through eduGAIN
- Connects to eduGAIN based SP and EOSC services
- Owned by GEANT and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- GDPR & Data protection taken into consideration
- Community has to follow the eduTEAMS service policies
- Some components can also be used for generic Service providers in eduGAIN



### Manage Roles and Rights

- Available through eduGAIN
- CoCo and R&S supported
- Strong focus on privacy and GDPR
- part of AARC2 interop activity
- Technical and cookbooks:  
<https://wiki.geant.org/display/ED/Membership+Management+Service>
- Service available at:  
<https://registry.eduTEAMS.org>

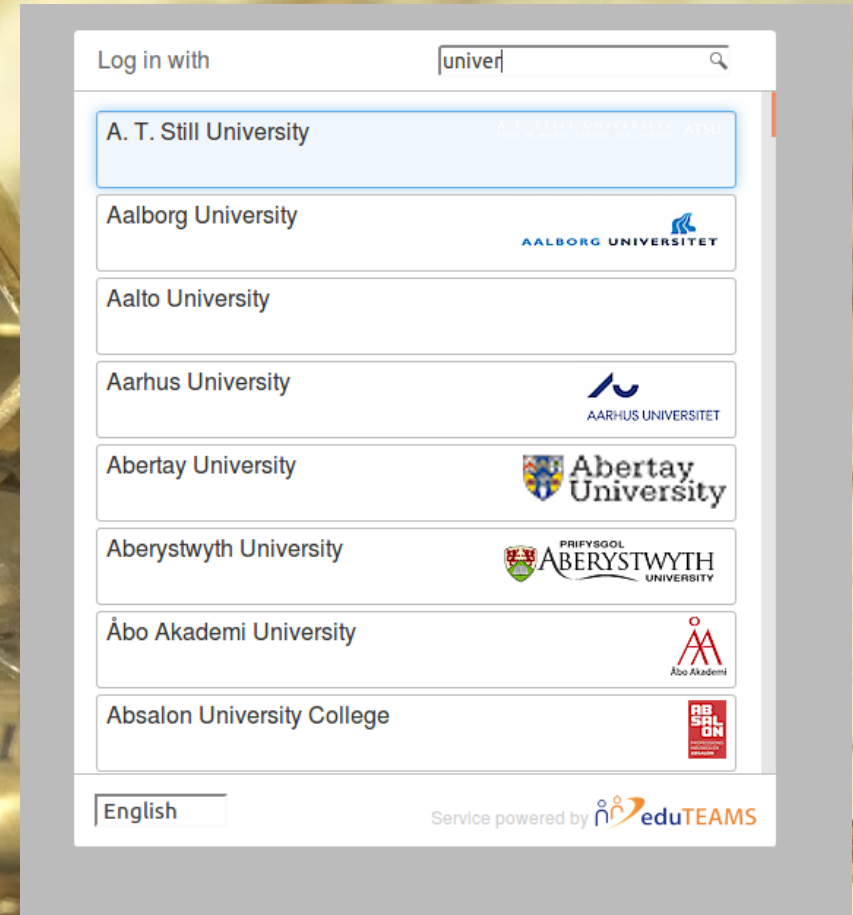


The screenshot shows the 'eduTEAMS Project members' interface. On the left is a navigation menu with options: People, Groups, Configuration, Platform, and Collaborations. The main content area displays the title 'eduTEAMS Project members People' and a breadcrumb trail 'Home > eduTEAMS Project members > My Population'. Below the title, there is a 'Toggle All: Open Closed' link and a search bar. A table lists members with columns for name and status:

Q Search											
a	b	c	d	e	f	g	h	i	j	k	l
▶	Kristóf Bajnok										Active
▶	Tangui Coulouarn										Active
▶	Lukas Hämmerle										Pending Confirmation
▶	Mandeep Saini										Active
▶	Niels van Dijk										Active

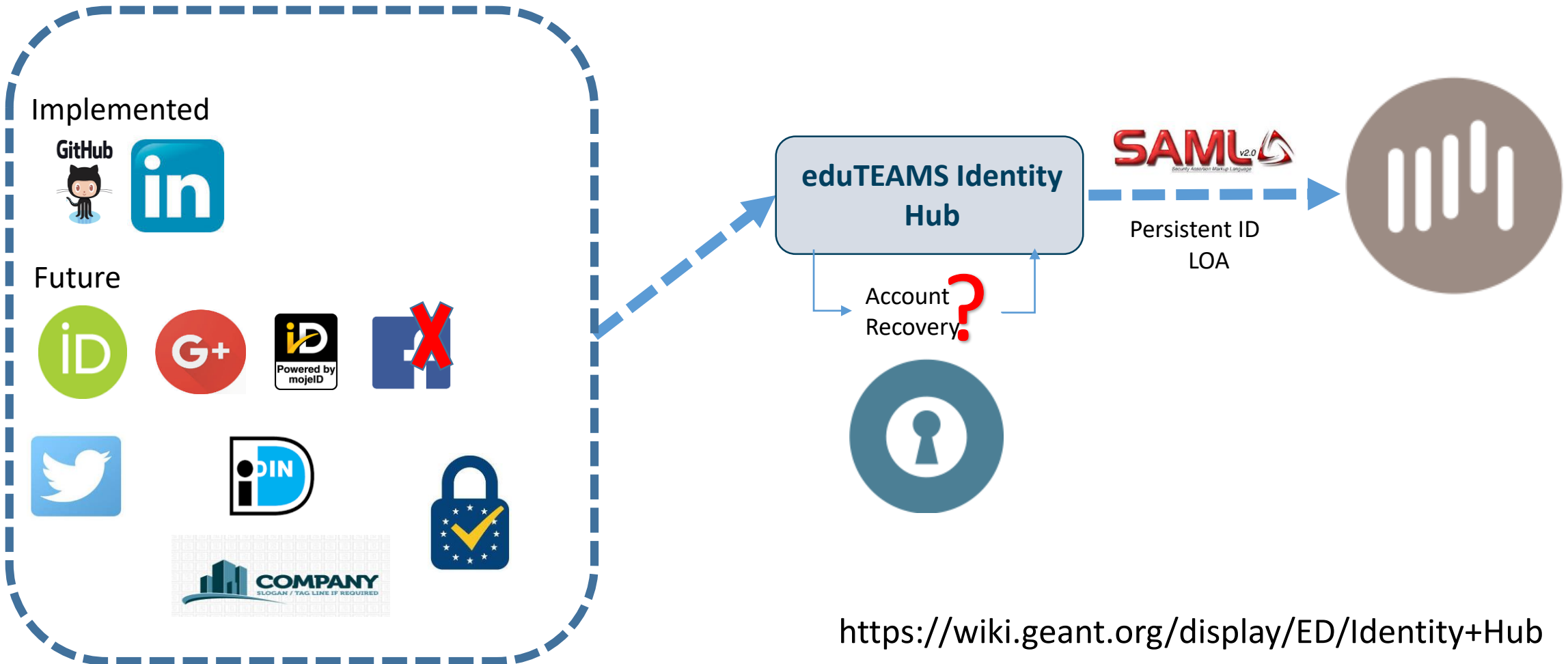
- Component of eduTEAMS, but generically usable for eduGAIN SPs
- Based on proven service from CESNET
- Engaged in RA21 Pilot – Resource Access for the 21<sup>st</sup> Century (<https://ra21.org>)

<https://wiki.geant.org/display/ED/Discovery+Service>

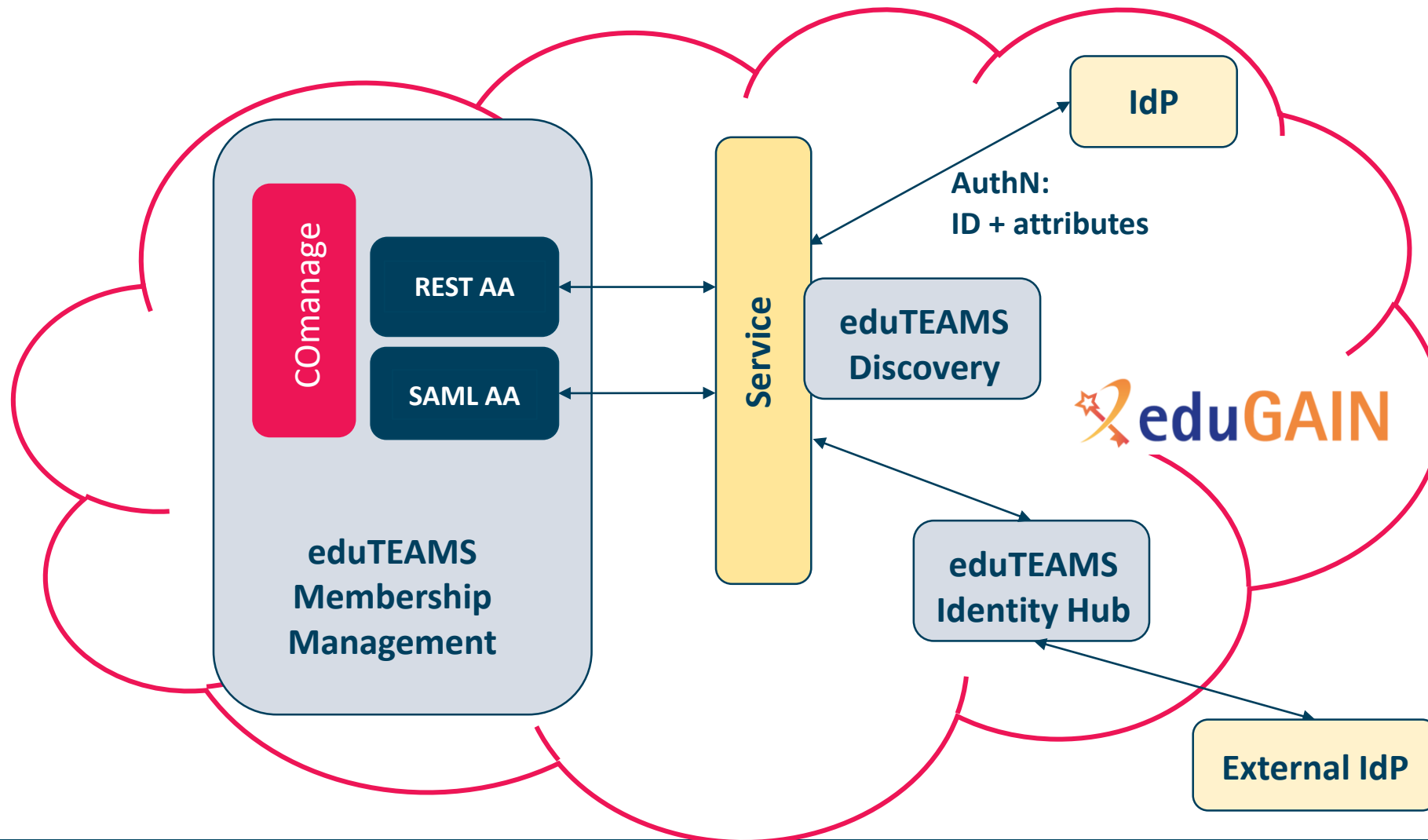


The screenshot shows the login interface of the eduTEAMS Discovery Service. At the top, there is a search bar labeled "Log in with" containing the text "univer". Below the search bar is a list of university entries, each with the university name and its logo. The entries are: A. T. Still University, Aalborg University, Aalto University, Aarhus University, Abertay University, Aberystwyth University, Åbo Akademi University, and Absalon University College. At the bottom of the interface, there is a language selector set to "English" and a footer that reads "Service powered by eduTEAMS".





<https://wiki.geant.org/display/ED/Identity+Hub>



## eduTEAMS multi-tenant Service

- All services have been available in pilot for some time now
- Tweaking and tinkering based on pilots and other input
- Further improving documentation
- Moving the services into production before the end of Q1 2019
- Not only technical services, but also delivering service policy, GDPR compliance

<https://wiki.geant.org/display/ED>

- Standalone service offering, specific to a community or NREN
- Owned by the community or NREN, operated by GEANT
- Community branding & community specific identifier
- Community managed policies
- Connected to eduGAIN services and/or EOSC (GEANT, EGI and EUDAT)
- Connected to community specific services
  
- More details in presentation Christos

eduTEAMS  
standalone  
Service

- Bespoke solution, typically involving just components
- It can be just the proxy or an MMS or the discovery or the IDhub or combinations
- Allows for combining directly with ‘external’ components, e.g. as offered nationally or as existing in the community
- Ownership model depended on the solution, operated by GEANT
- Concept tested as part of the Life Science AAI pilot
  - Presentation Christos
  - Presentation Mikael Linden  
<https://tnc18.geant.org/core/presentation/133>

eduTEAMS  
bespoke Service

## eduTEAMS Hands-On

[support@eduTEAMS.org](mailto:support@eduTEAMS.org)

<https://www.eduTEAMS.org>

<https://wiki.geant.org/display/ED>

