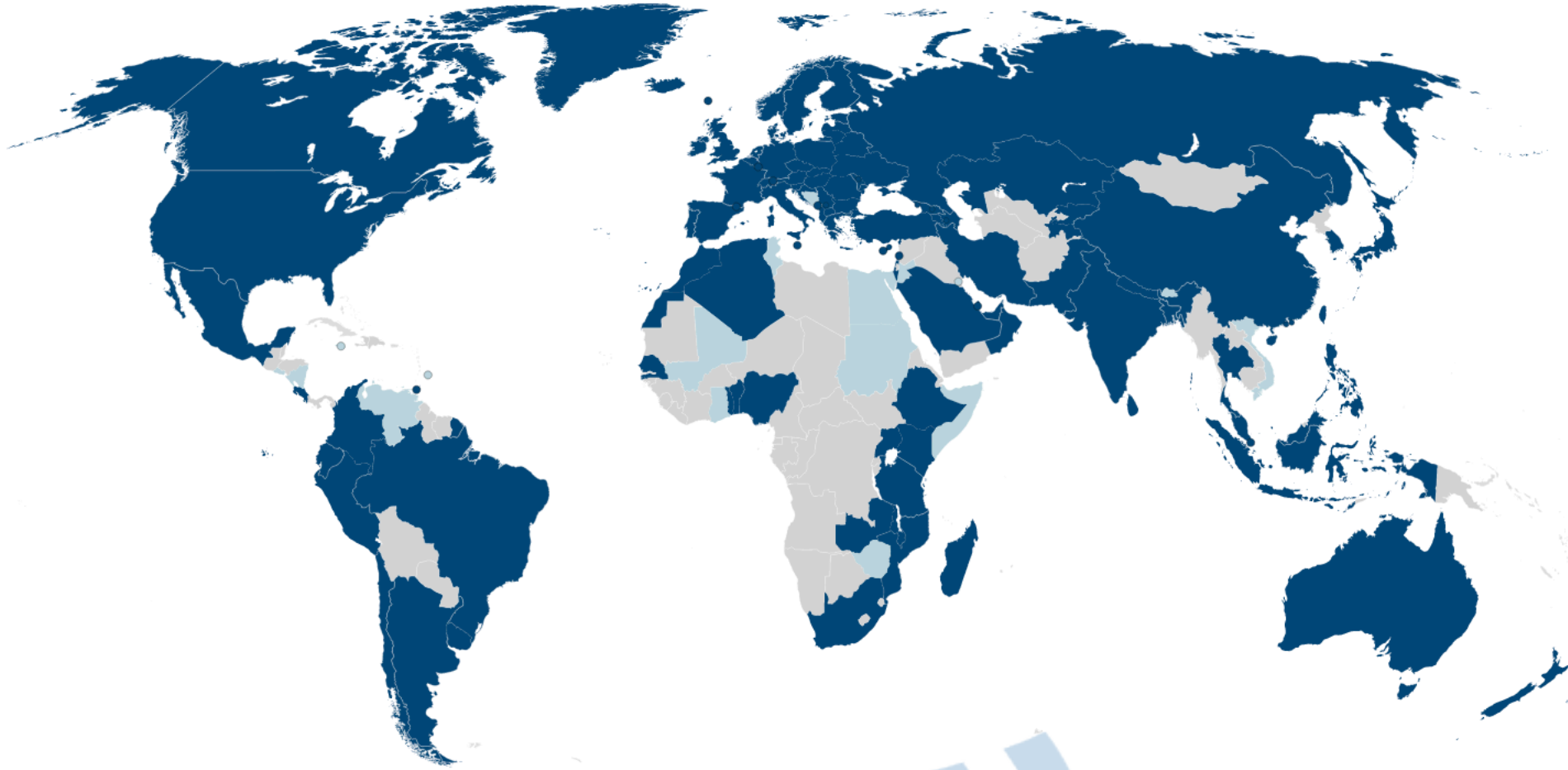
eduTEAMS: “Virtual Organizations made easy”

Christos Kanellopoulos, GÉANT

GÉANT
Networks • Services • People



May 2019:

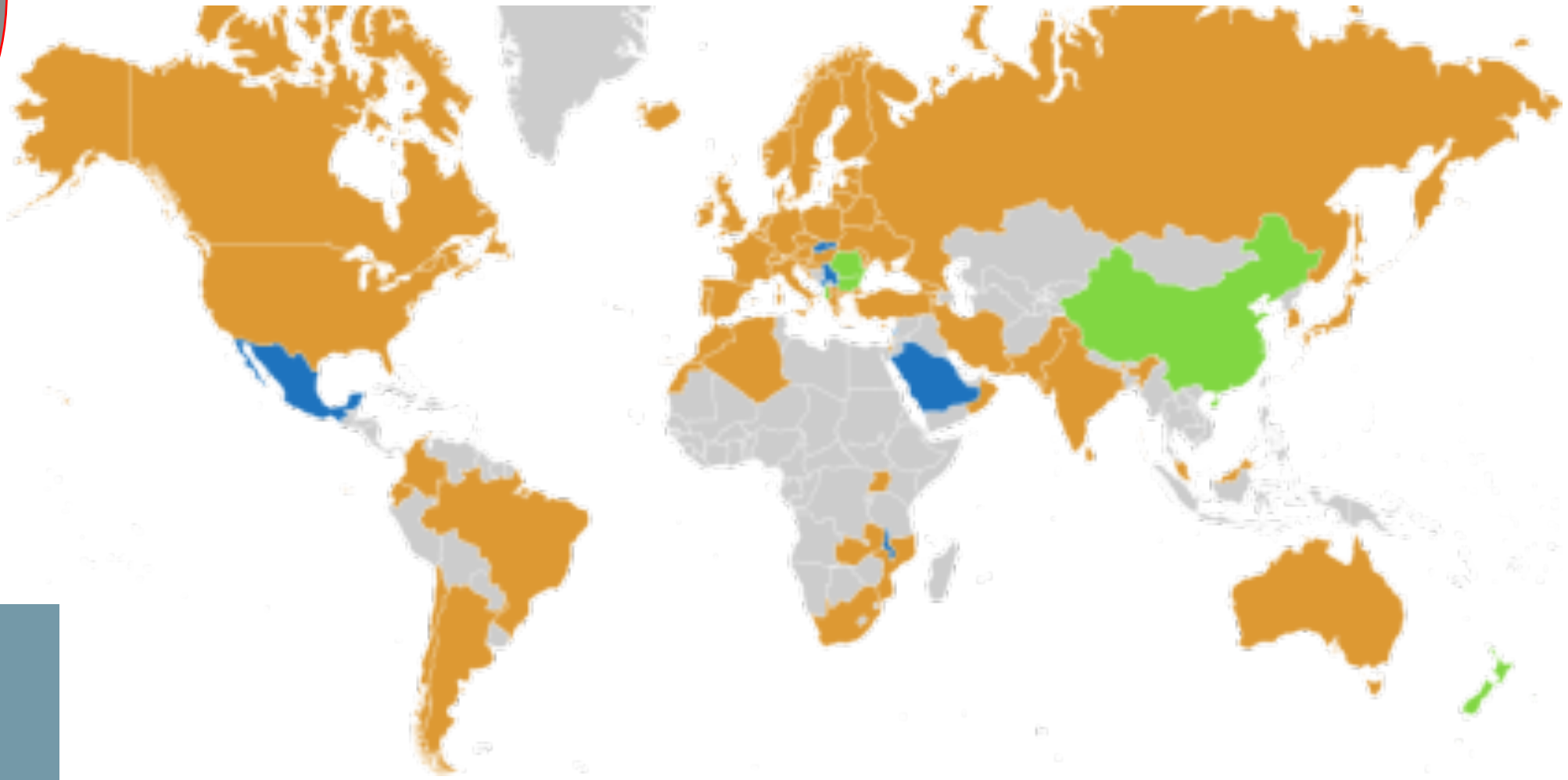
101 Roaming Operators

18 Pilots

250+M authentications / month

eduroam

GÉANT
Networks • Services • People



June 2019:

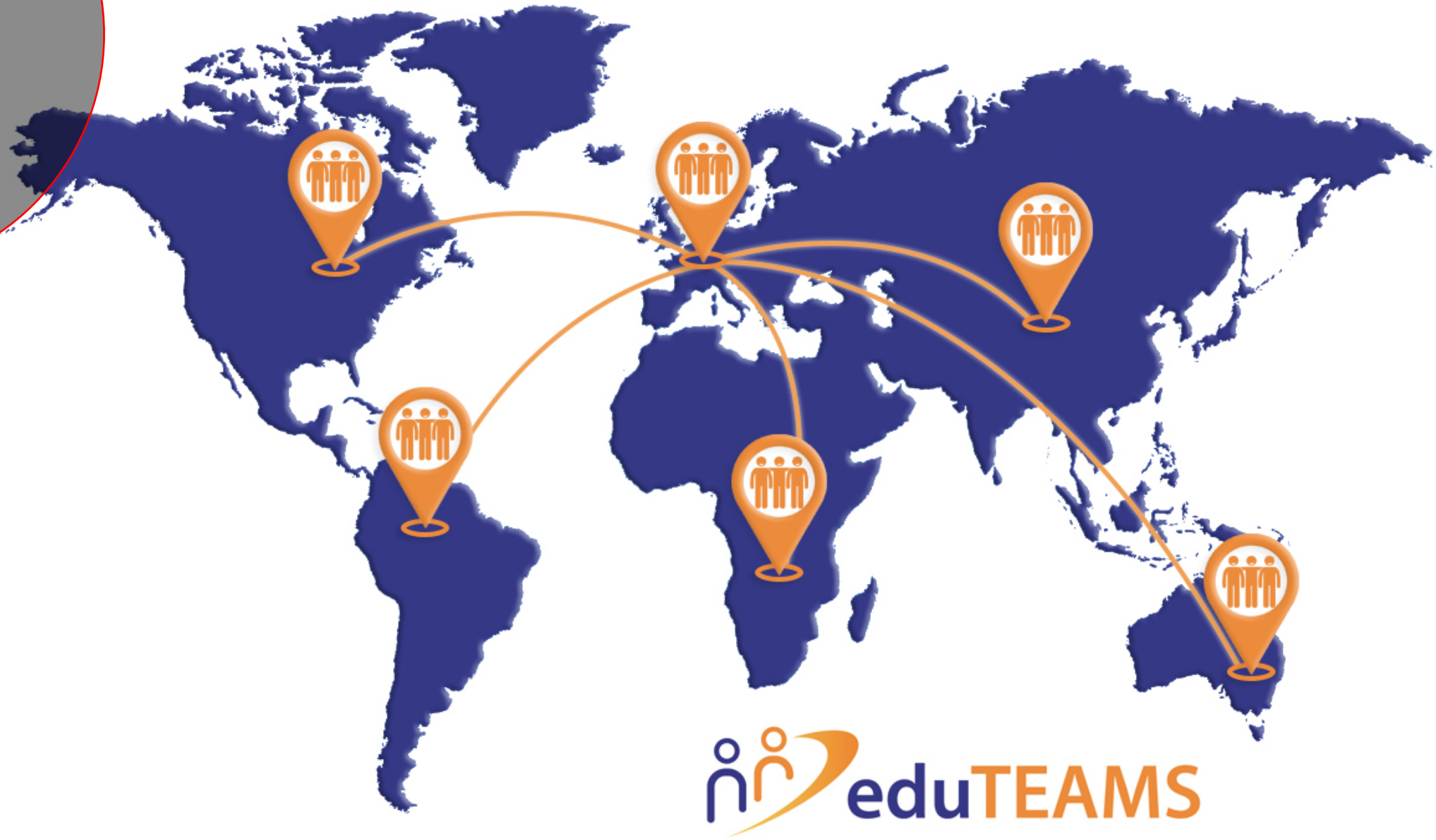
61 Federations active

6 Federations with voting rights in process of joining

5587 entities

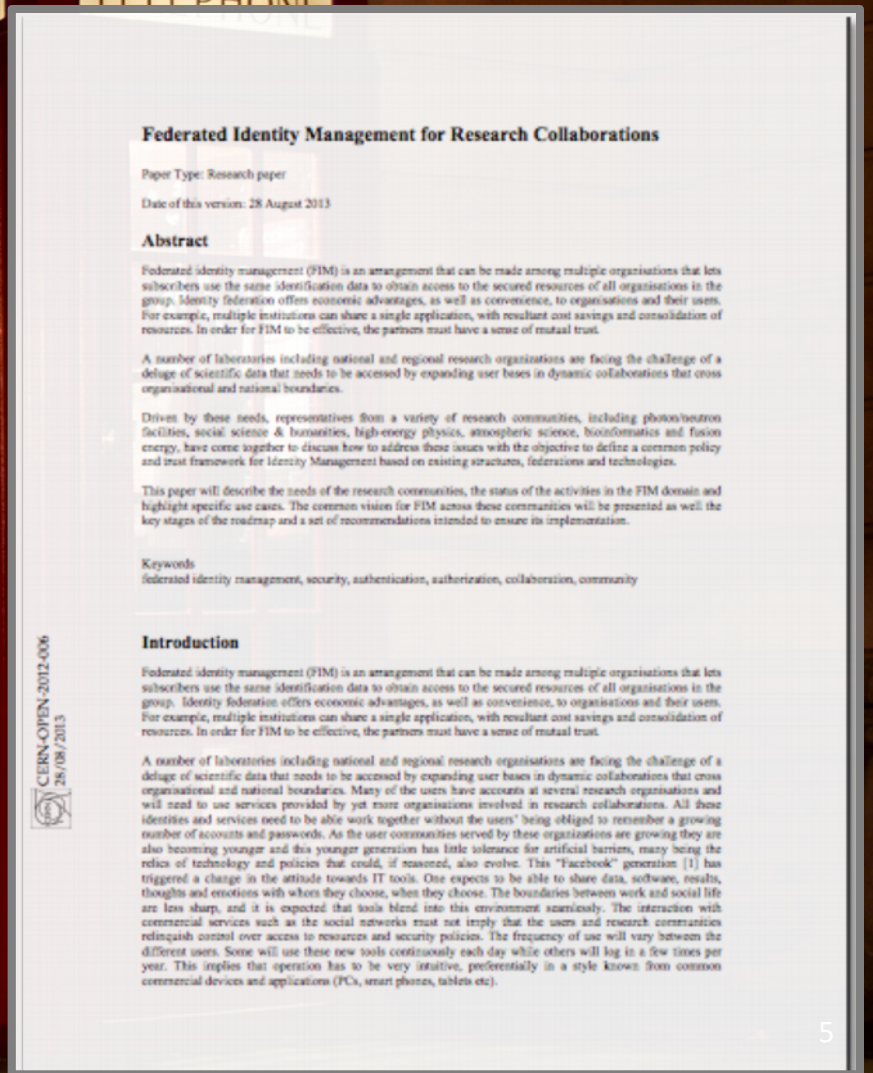
eduGAIN

GÉANT
Networks • Services • People



eduTEAMS

GÉANT
Networks • Services • People



Federated Identity Management for Research Collaborations

Paper Type: Research paper

Date of this version: 28 August 2013

Abstract

Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organizations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries.

Driven by these needs, representatives from a variety of research communities, including photon/neutron facilities, social science & humanities, high-energy physics, atmospheric science, bioinformatics and fusion energy, have come together to discuss how to address these issues with the objective to define a common policy and trust framework for Identity Management based on existing structures, federations and technologies.

This paper will describe the needs of the research communities, the status of the activities in the FIM domain and highlight specific use cases. The common vision for FIM across these communities will be presented as well the key stages of the roadmap and a set of recommendations intended to ensure its implementation.

Keywords
federated identity management, security, authentication, authorization, collaboration, community

Introduction

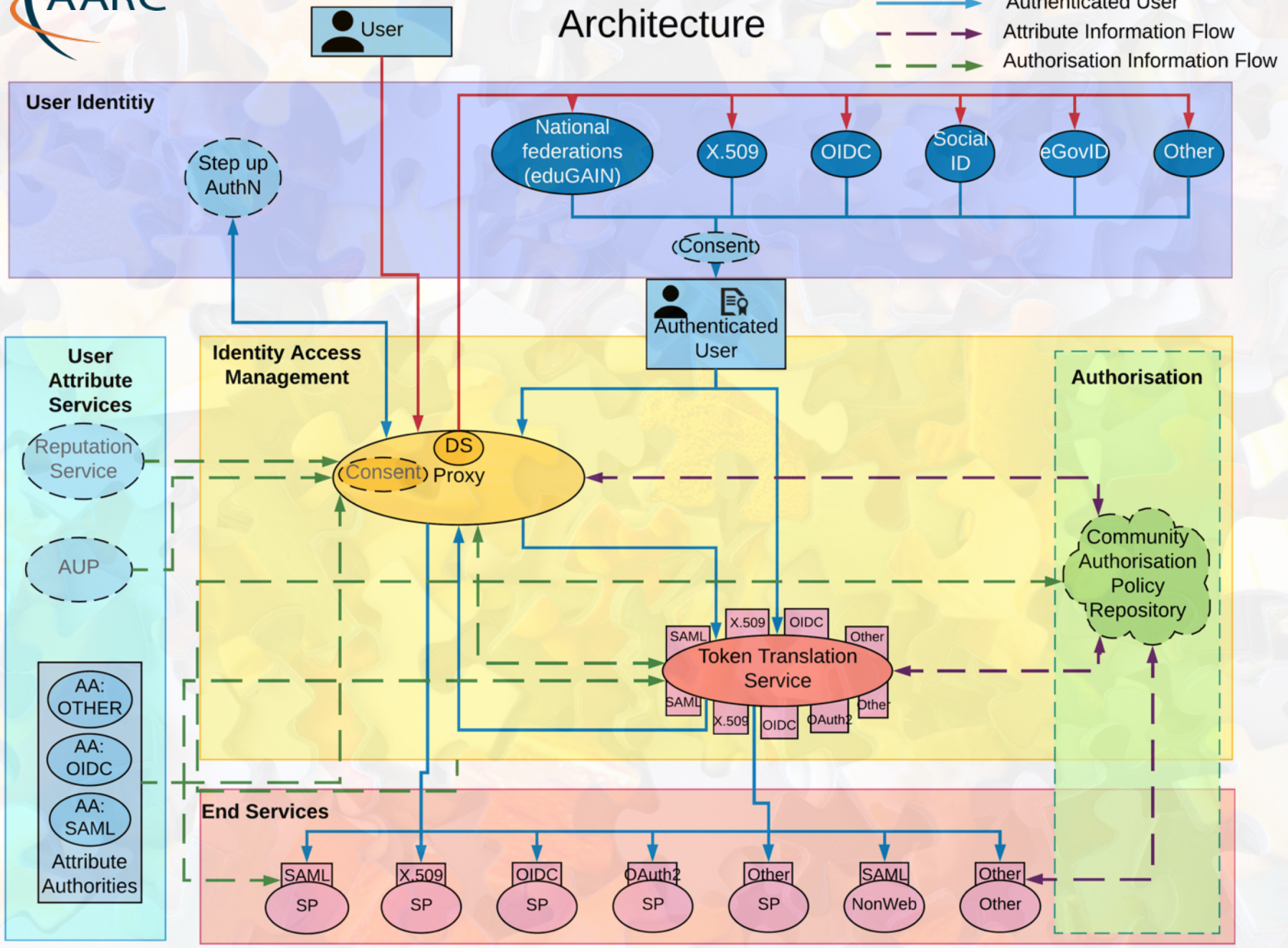
Federated identity management (FIM) is an arrangement that can be made among multiple organisations that lets subscribers use the same identification data to obtain access to the secured resources of all organisations in the group. Identity federation offers economic advantages, as well as convenience, to organisations and their users. For example, multiple institutions can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners must have a sense of mutual trust.

A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several research organisations and will need to use services provided by yet more organisations involved in research collaborations. All these identities and services need to be able work together without the users' being obliged to remember a growing number of accounts and passwords. As the user communities served by these organizations are growing they are also becoming younger and this younger generation has little tolerance for artificial barriers, many being the relics of technology and policies that could, if reasoned, also evolve. This "Facebook" generation [1] has triggered a change in the attitude towards IT tools. One expects to be able to share data, software, results, thoughts and emotions with whom they choose, when they choose. The boundaries between work and social life are less sharp, and it is expected that tools blend into this environment seamlessly. The interaction with commercial services such as the social networks must not imply that the users and research communities relinquish control over access to resources and security policies. The frequency of use will vary between the different users. Some will use these new tools continuously each day while others will log in a few times per year. This implies that operation has to be very intuitive, preferentially in a style known from common commercial devices and applications (PCs, smart phones, tablets etc).

CERN-OPEN-2012-006
28/08/2013


GÉANT
Networks • Services • People
AARC

AARC Blueprint Architecture



June 22, 2018

Journal article Open Acces

Federated Identity Management for Research Collaborations

Christopher John Atherton; Thomas Barton; Jim Basney; Daan Broeder; Alessandro Costa; Mirjam van Daalen; Stephanie Dyke; Willem Elbers; Carl-Fredrik Enell; Enrico Maria Vincenzo Fasanelli; João Fernandes; Licia Florio; Peter Gietz; David L. Groep; Matthias Bernhard Junker; Christos Kanellopoulos; David Kelsey; Philip Kershaw; Cristina Knapic; Thorsten Kollegger; Scott Koranda; Mikael Linden; Filip Marinic; Ludek Matyska; Tommi Henrik Nyrönen; Stefan Paetow; Laura A D Paglione; Sandra Parlati; Christopher Phillips; Michal Prochazka; Nicholas Rees; Hannah Short; Uros Stevanovic; Michael Tartakovsky; Gerben Venekamp; Tom Vitez; Romain Wartel; Christopher Whalen; John White; Carlo Maria Zwölf

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

The authors also acknowledge the support and collaboration of many other colleagues in their respective institutes, research communities and IT Infrastructures, together with the funding received by these from many different sources. These include but are not limited to the following: (i) The Worldwide LHC Computing Grid (WLCG) project is a global collaboration of more than 170 computing centres in 43 countries, linking up national and international grid infrastructures. Funding is acknowledged from many national funding bodies and we acknowledge the support of several operational infrastructures including EGI, OSG and NDGF/NeIC. (ii) EGI acknowledges the funding and support received from the European Commission and the many National Grid Initiatives and other members. EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777536. (iii) The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2). (iv) Work on the development of ESGF's identity management system has been supported by The UK Natural Environment Research Council and funding from the European Union's Seventh Framework Programme for research, technological development and demonstration through projects IS-ENES (grant agreement no 228203) and IS-ENES2 (grant agreement no 312979). (v) Ludek Matyska and Michal Prochazka acknowledge funding from the RI ELIXIR CZ project funded by MEYS Czech Republic No. LM2015047. (vi) Scott Koranda acknowledges support provided by the United States National Science Foundation under Grant No. PHY-1700765. (vii) GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).The research leading to these results has received funding from the European Union's

GÉANT
Networks • Services • People

eduTEAMS

A service to enable use of federated identity management in research & academic collaborations

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

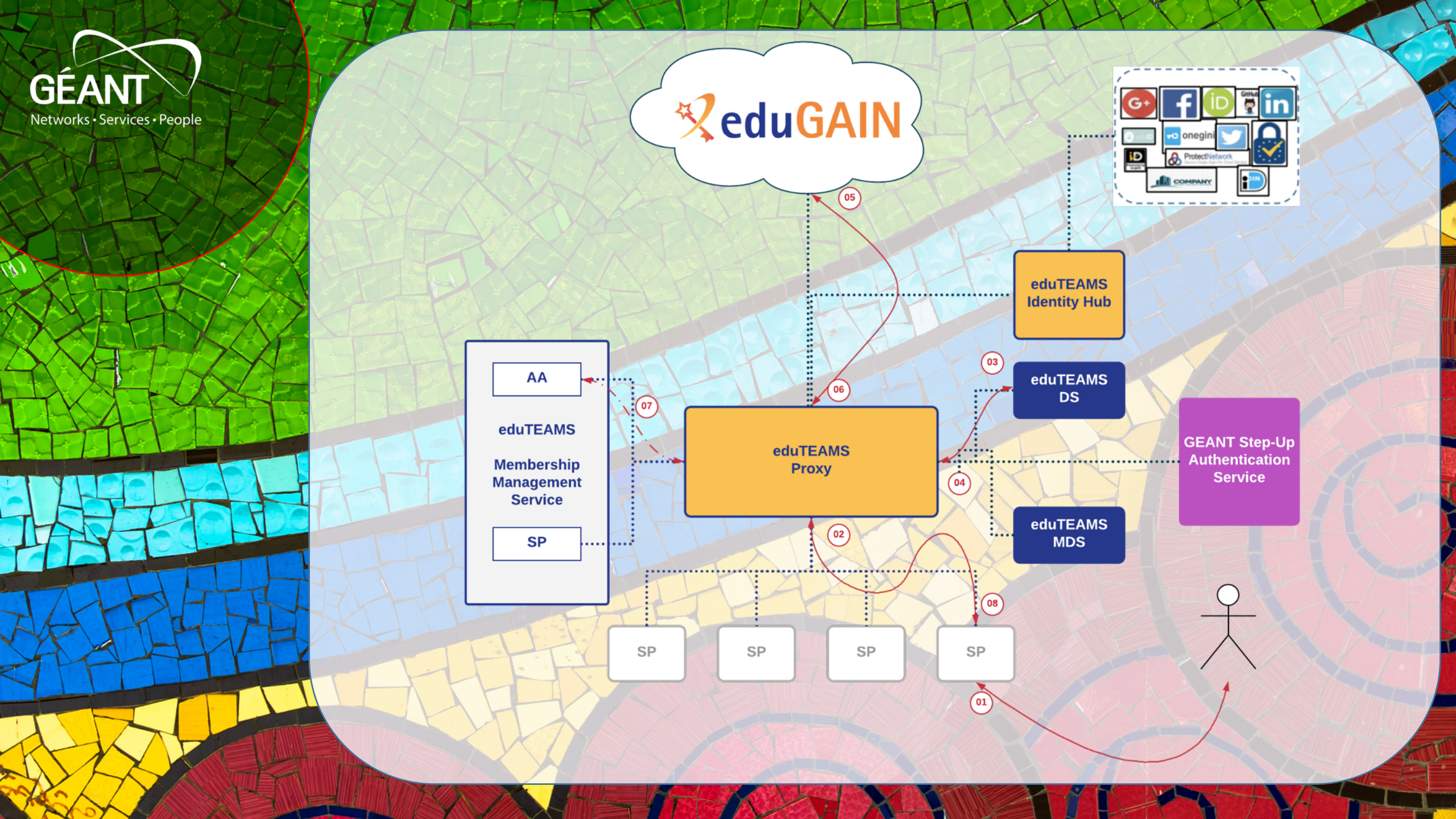
Components

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

Characteristics

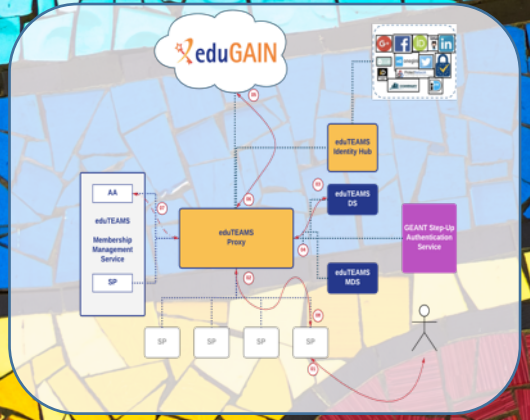
- Full implementation AARC Blueprint Architecture
- Single- and multi-tenant options
- Sustainability and strategic partnerships

https://www.eduteams.org


GÉANT
Networks • Services • People
eduGAIN
eduTEAMS
Identity Hub
eduTEAMS
DS
GEANT Step-Up
Authentication
Service
eduTEAMS
Proxy
eduTEAMS
MDS
AA
eduTEAMS
Membership
Management
Service
SP
SP
SP
SP
SP
01
02
03
04
05
06
07
08

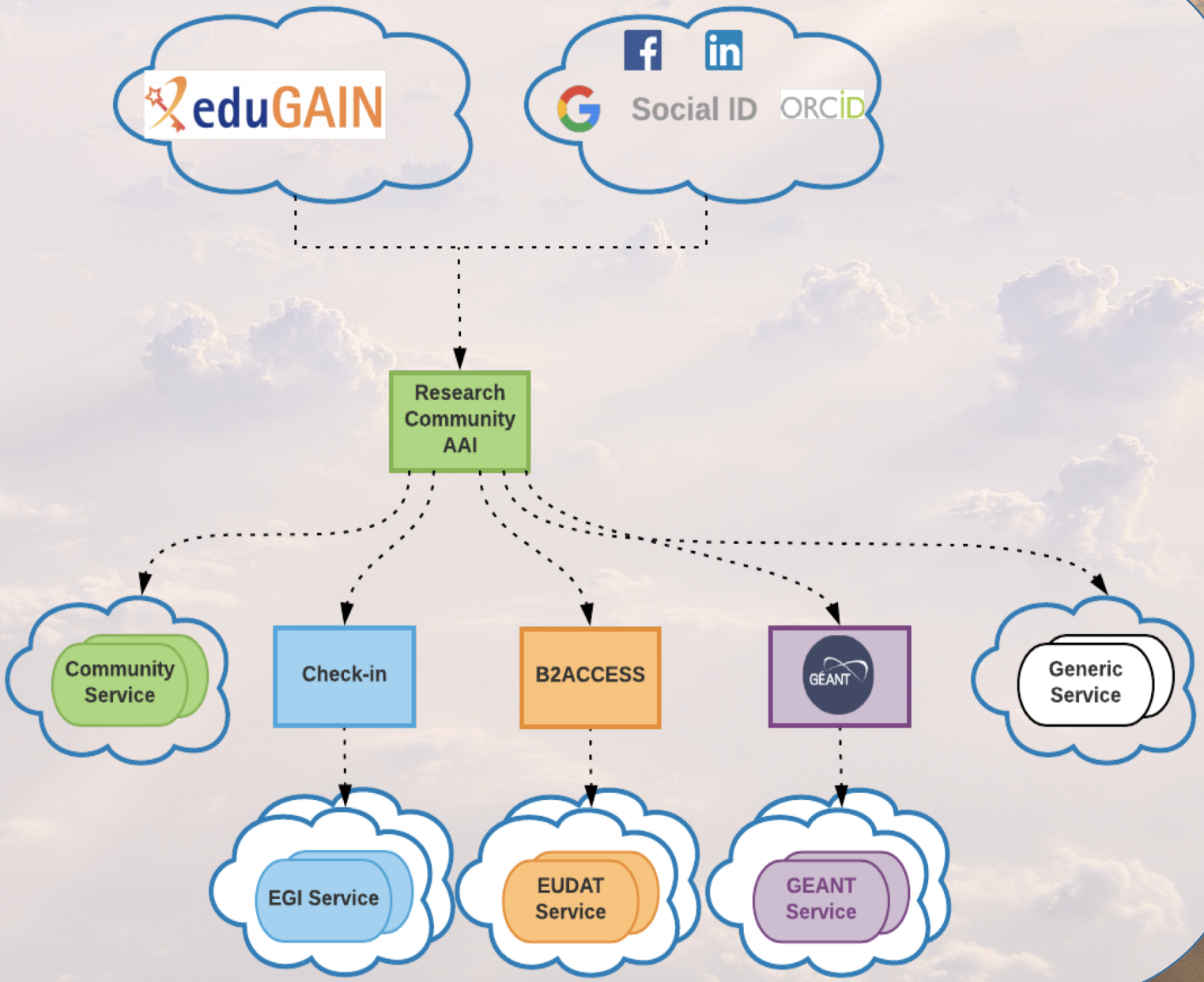
GÉANT
Networks • Services • People

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



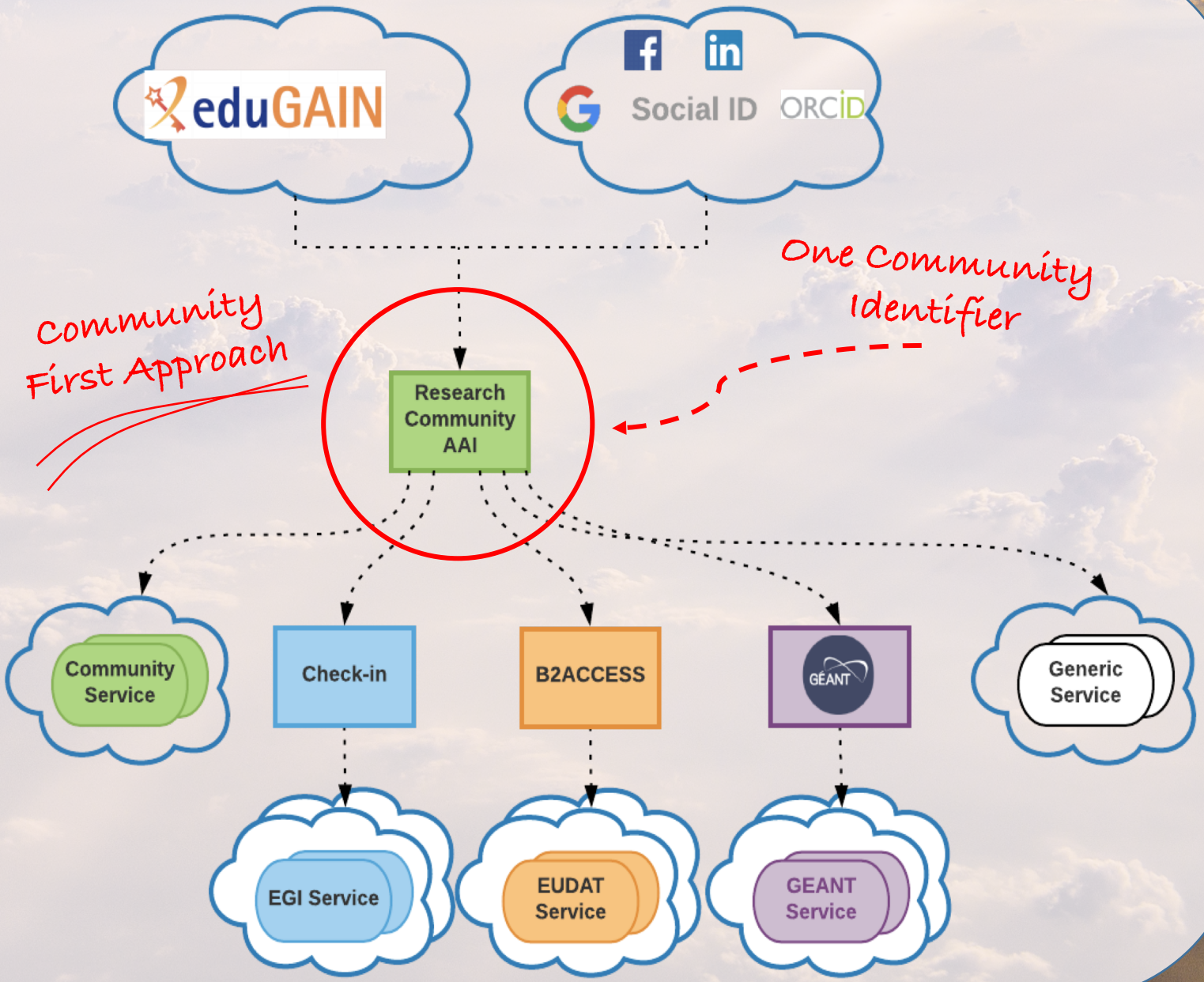
GÉANT
Networks • Services • People

European Open Science Cloud



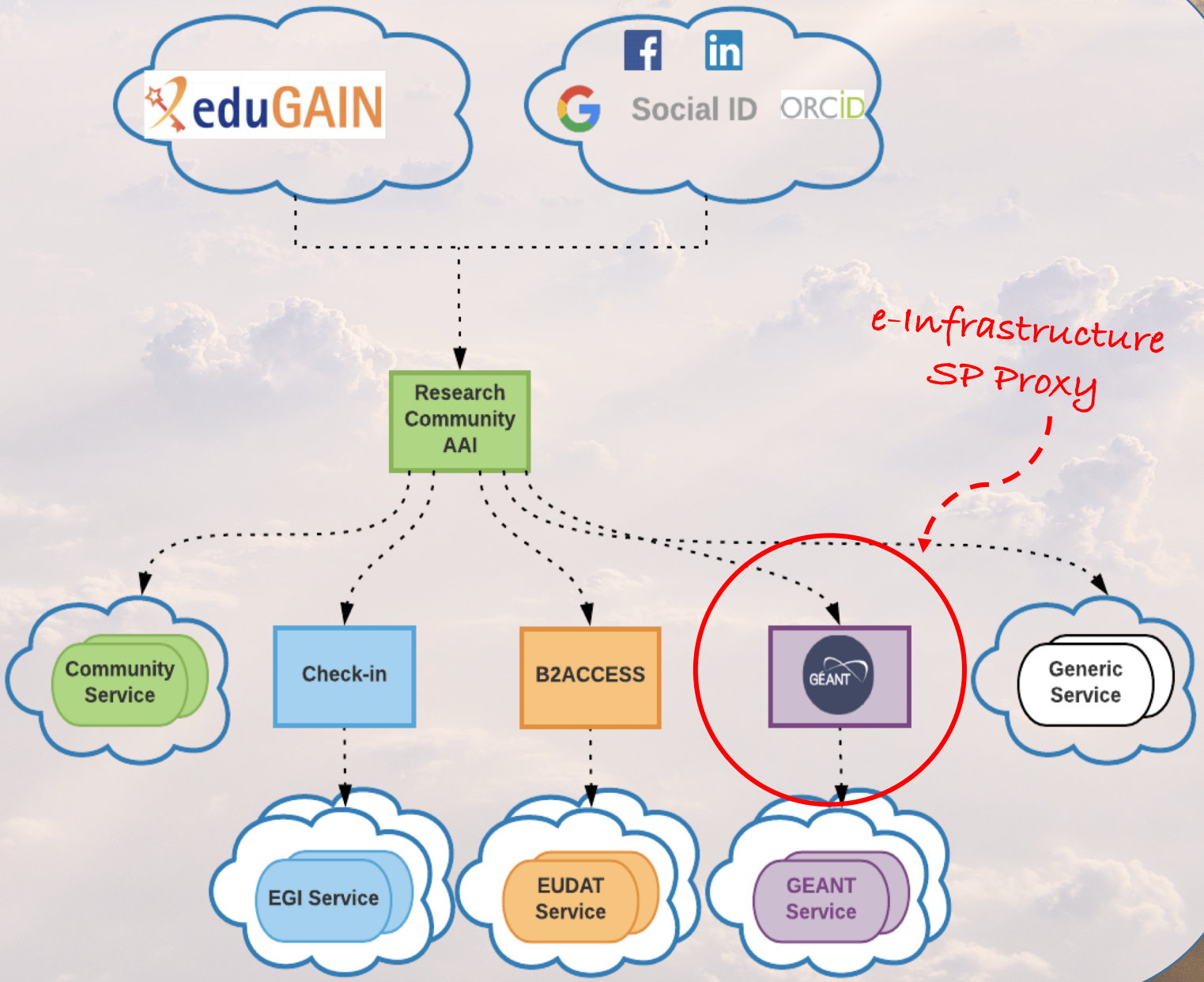
GÉANT
Networks • Services • People

European Open Science Cloud



GÉANT
Networks • Services • People

European Open Science Cloud



eduTEAMS Service

Provided by GEANT to small and medium sized communities who want to get started with their virtual collaborations and take full advantage of the federated access without having to deal with the complexity of operating and supporting their own AAI. Supports multiple communities on the same platform. Provides everything required in order to securely collaborate and use services available to the GEANT community and European Open Science Cloud.

eduTEAMS Dedicated

For communities requiring full control of their AAI, GEANT can host and operate their own, dedicated AAI Service powered by the eduTEAMS technology. Communities can rely on the operational capabilities and expertise of GEANT, while they are in full control of the policies, configuration and branding of their AAI.

eduTEAMS Bespoke

For those communities who require tailor-made functionality, such as integration with custom back-office and front-office systems, new features or enhancing their existing AAIs with new functionality available in eduTEAMS, GEANT can provide bespoke solutions based on the eduTEAMS technology, which can include a combination of consultancy,

eduTEAMS Service

- Shared platform that can be used by small - medium communities and the long tail of science
- Managed and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- eduTEAMS service policies
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Service

- Shared platform that can be used by small - medium communities and the long tail of science
- Managed and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- eduTEAMS service policies
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Dedicated

- Dedicated, white-label service offering, specific to a community
- Managed by the community, operated by GEANT
- Community branding & community specific identifier
- Community managed policies
- Can be connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Service

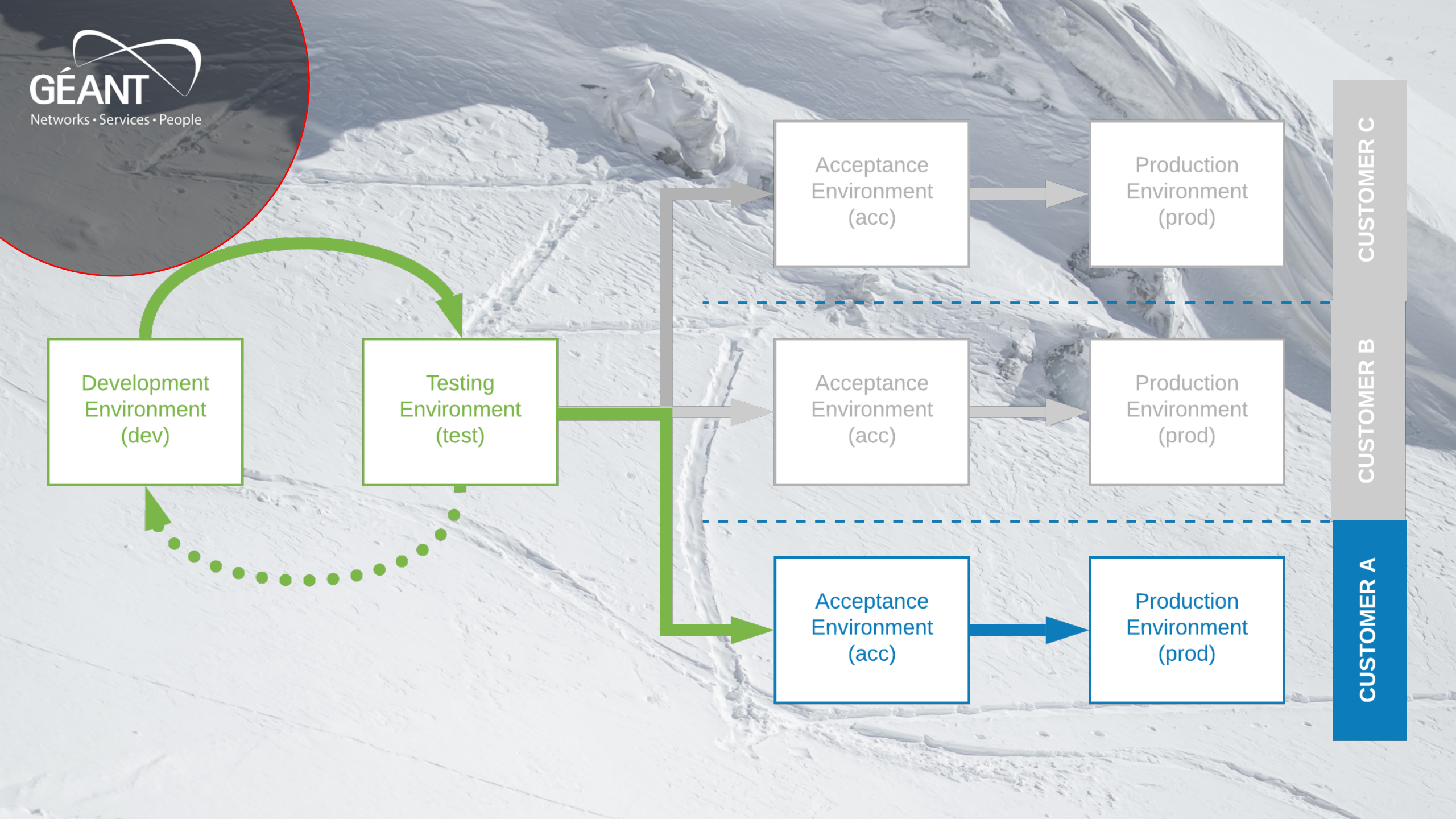
- Shared platform that can be used by small - medium communities and the long tail of science
- Managed and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- eduTEAMS service policies
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Dedicated

- Dedicated, white-label service offering, specific to a community
- Managed by the community, operated by GEANT
- Community branding & community specific identifier
- Community managed policies
- Can be connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Bespoke

- Bespoke solution with tailor-made functionality
- Ownership model depended on the solution, operated by GEANT
- Consultancy, development and hosting of the service.


GÉANT
Networks • Services • People
Development Environment (dev)
Testing Environment (test)
Acceptance Environment (acc)
Production Environment (prod)
Acceptance Environment (acc)
Production Environment (prod)
Acceptance Environment (acc)
Production Environment (prod)
CUSTOMER C
CUSTOMER B
CUSTOMER A

GÉANT
Networks • Services • People

Roadmap

https://trello.com/b/71wU60QV/eduteams-roadmap

We are working on it

- Feature, Component:Proxy — Active Role Selection
- Feature, Component:Step-up — Support for the Pilot Step-up Authentication Service
- Feature, Component:Proxy, Component:Webapp — IdP Attribute Release Check
- Feature, Component:Webapp — Improved registration flow for Service Providers
- Component:Webapp — New eduTEAMS website
- Feature, Component:TTS — Support access to services that require certificate based authentiation

+ Add another card

Coming soon

- Feature, Component:Proxy — Improvements in the generation of the eduTEAMS user identifier
- Compliance — Support for Sirtfi on the eduTEAMS Service
- Compliance — Update of the Acceptable Usage Policy for the eduTEAMS Service
- Component:MMS — Upgrade to Perun v3.3.1
- Compliance, Feature, Component:MMS, Component:Proxy — Improved AUP acceptance process
- Feature, Component:Proxy — Support of stepping up authentication flows in the eduTEAMS proxy
- Component:MMS — Upgrade to COmanage 3.2

+ Add another card

Just shipped

- Feature, Component:Proxy — Support Sirtfi declarations in the SAML metadata generation
- Feature, Component:Proxy — Improved support for entity categories in the SAML metadata
- Component:MMS — UI improvement on COmanage
- Component:MMS — UI improvements on HEXAA
- Component:MMS — UI improvements on Perun
- Compliance — New version of the eduTEAMS Privacy Policy
- Feature, Component:MMS, Component:Proxy — Improved backend integration with COmanage and HEXAA
- Component:MMS — Improved support for account linking
- Compliance, Feature, Component:Proxy — Improved support for informing the users about the attributes released to connected services

+ Add another card

Thank you

https://www.eduteams.org

support@eduteams.org