# AAI and PaNOSC

**Christos Kanellopoulos**
christos.kanellopoulos@geant.org
*Senior Trust & Identity Manager*

PaNOSC Conference, Trieste, November 5th 2019

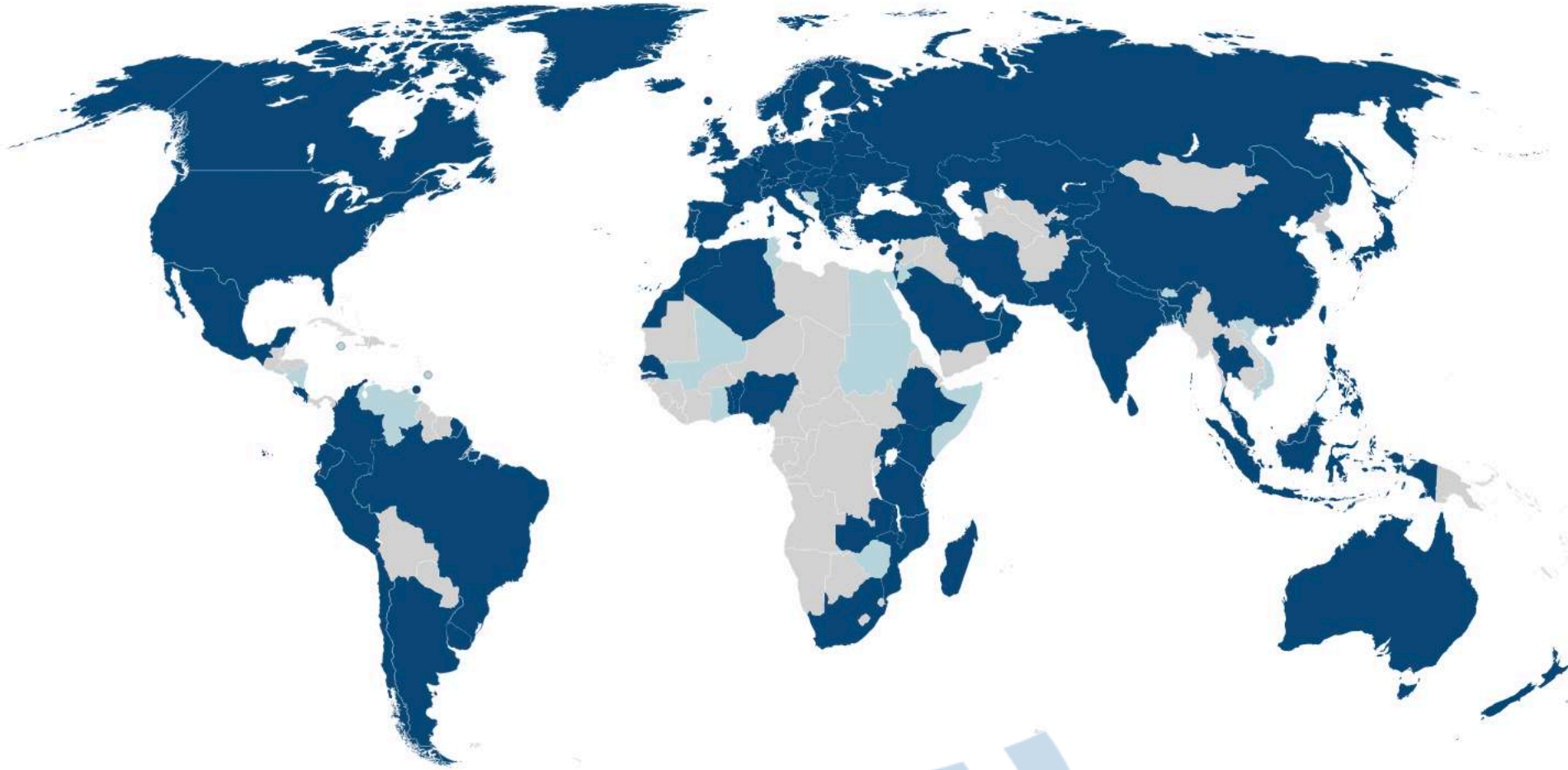
www.geant.org

# Membership Association

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

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

GÉANT
Networks • Services • People



**September 2019:**

101 Roaming Operators

18 Pilots

250+M authentications / month

eduroam

September 2019:

66 Federations active

3 Federations with voting rights
8 Federations in process of joining

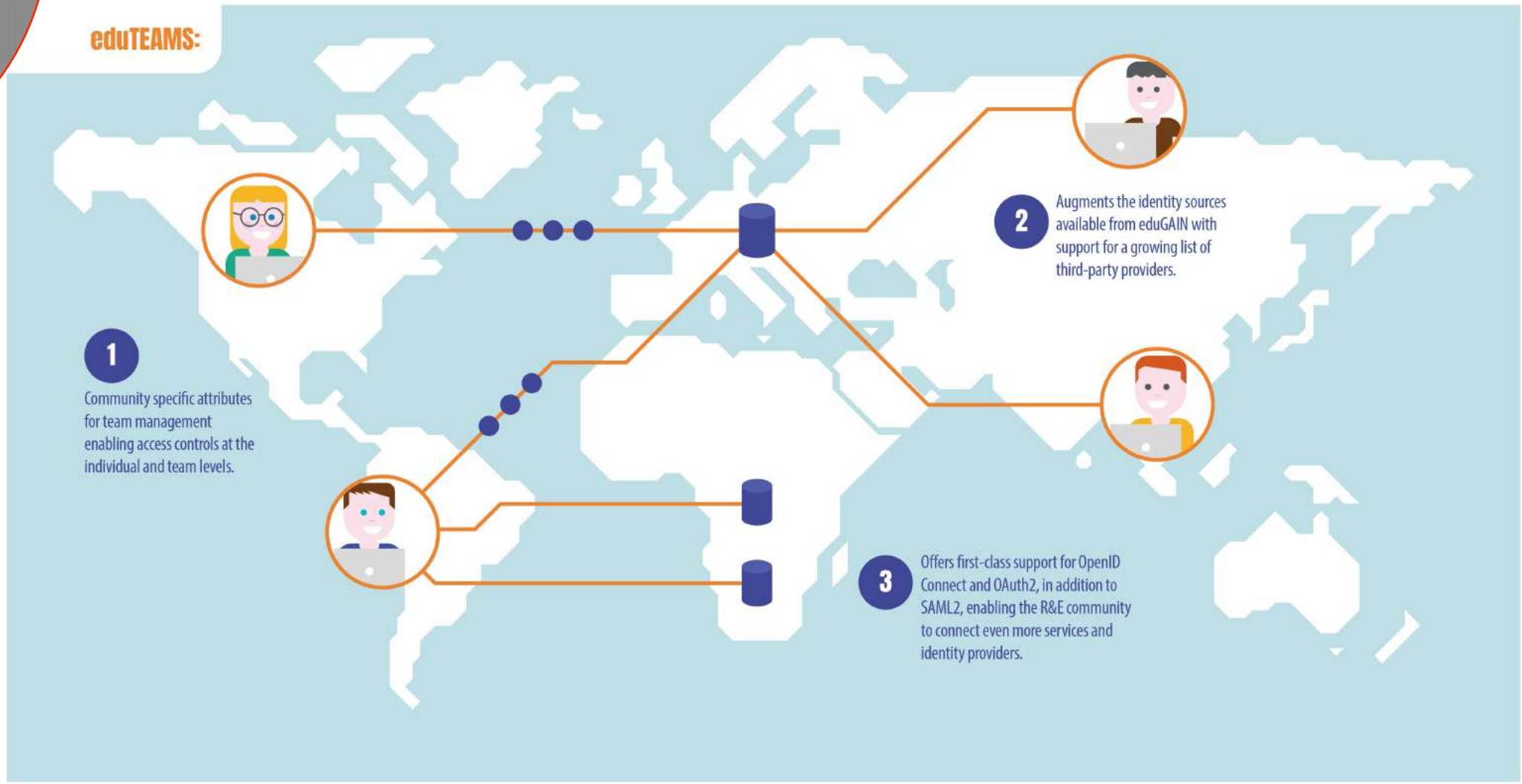
5666 entities

GÉANT
Networks • Services • People

**eduTEAMS enables the research and education community to create virtual collaborations and share common resources and services across organizational boundaries.**

eduTEAMS eduGAIN GÉANT

## eduTEAMS:



1 Community specific attributes for team management enabling access controls at the individual and team levels.

2 Augments the identity sources available from eduGAIN with support for a growing list of third-party providers.

3 Offers first-class support for OpenID Connect and OAuth2, in addition to SAML2, enabling the R&E community to connect even more services and identity providers.

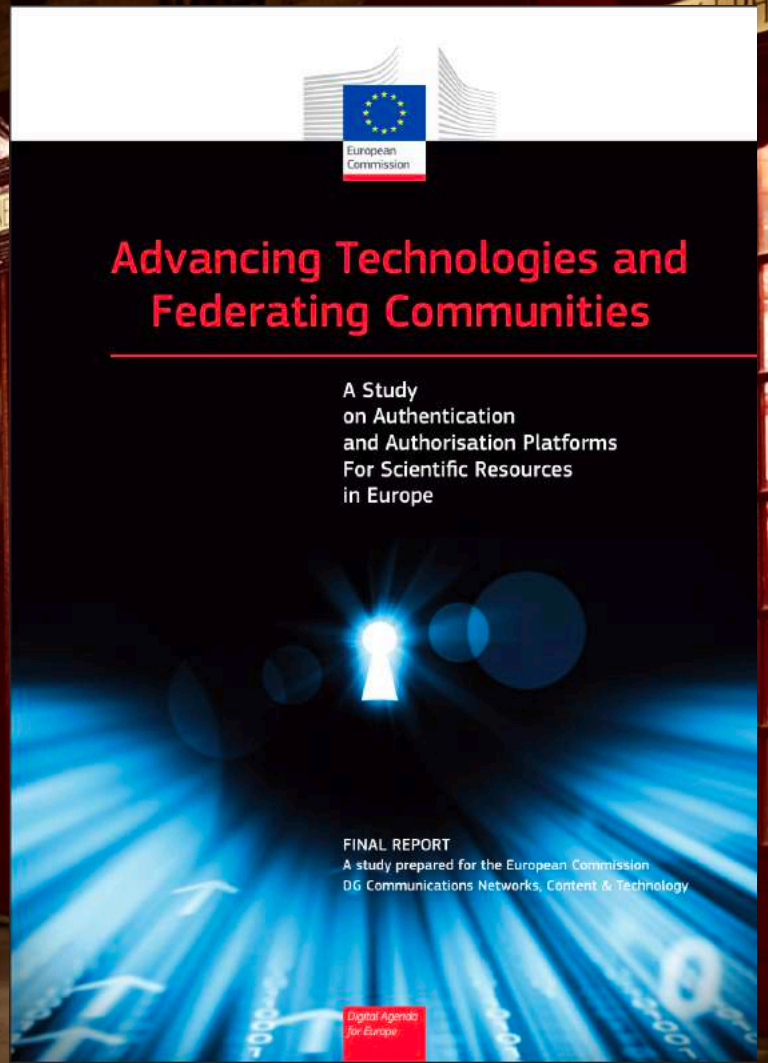
**eduTEAMS - taking the AAI to the next level**

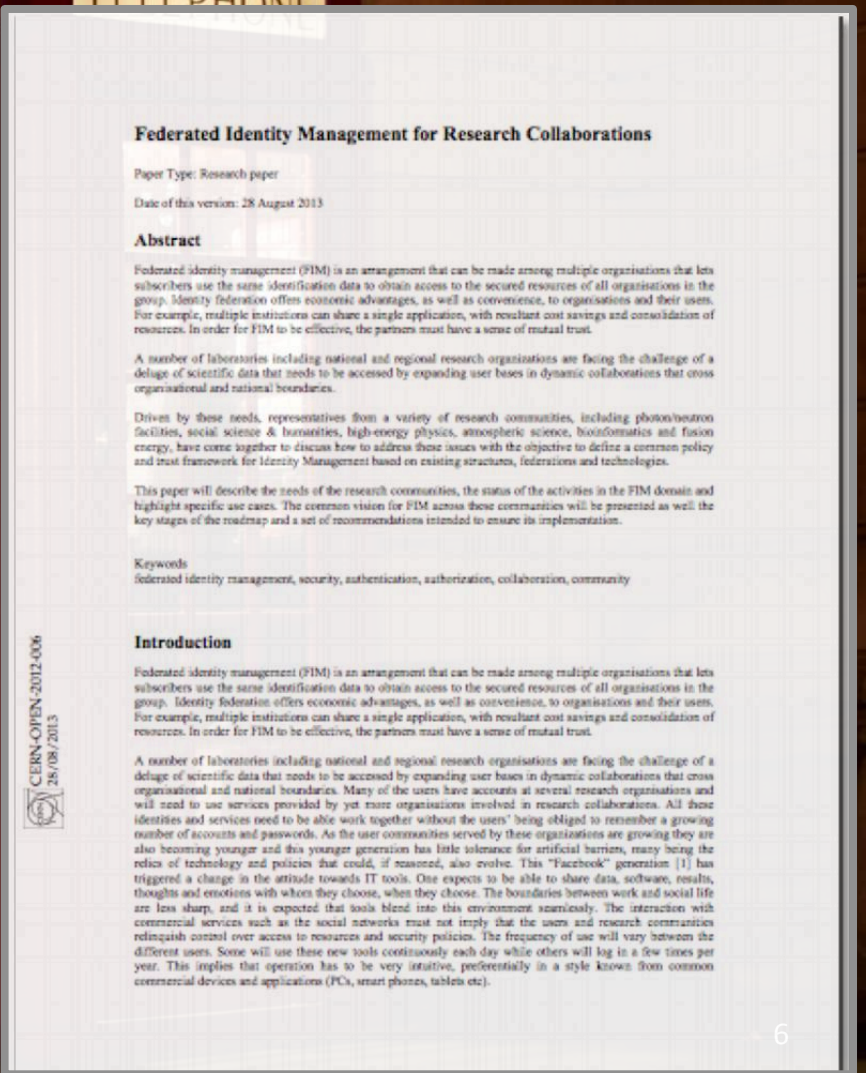
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

September 2019

eduTEAMS.org

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.

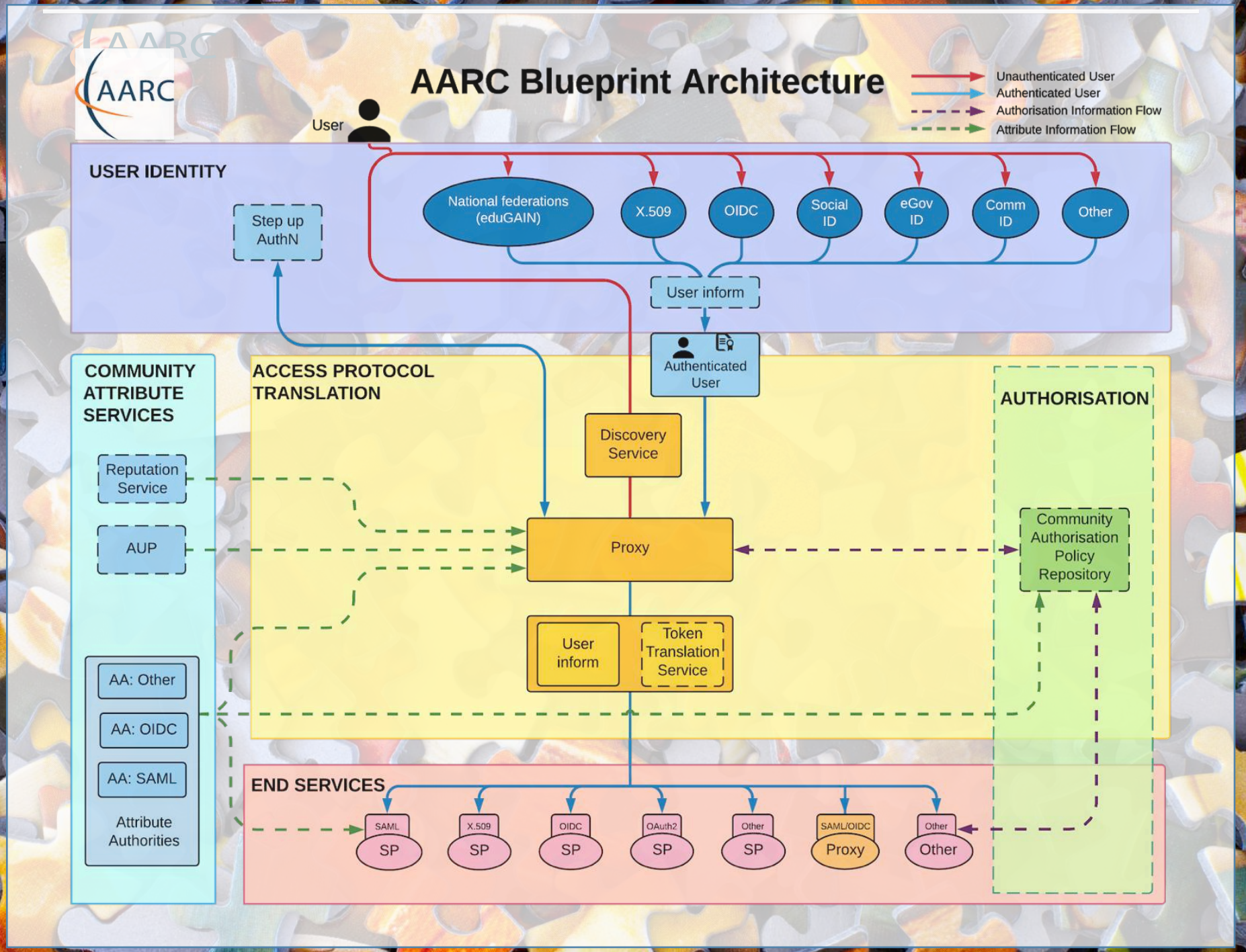
A number of laboratories including national and regional research organisations are facing the challenge of a deluge of scientific data that needs to be accessed by expanding user bases in dynamic collaborations that cross organisational and national boundaries. Many of the users have accounts at several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

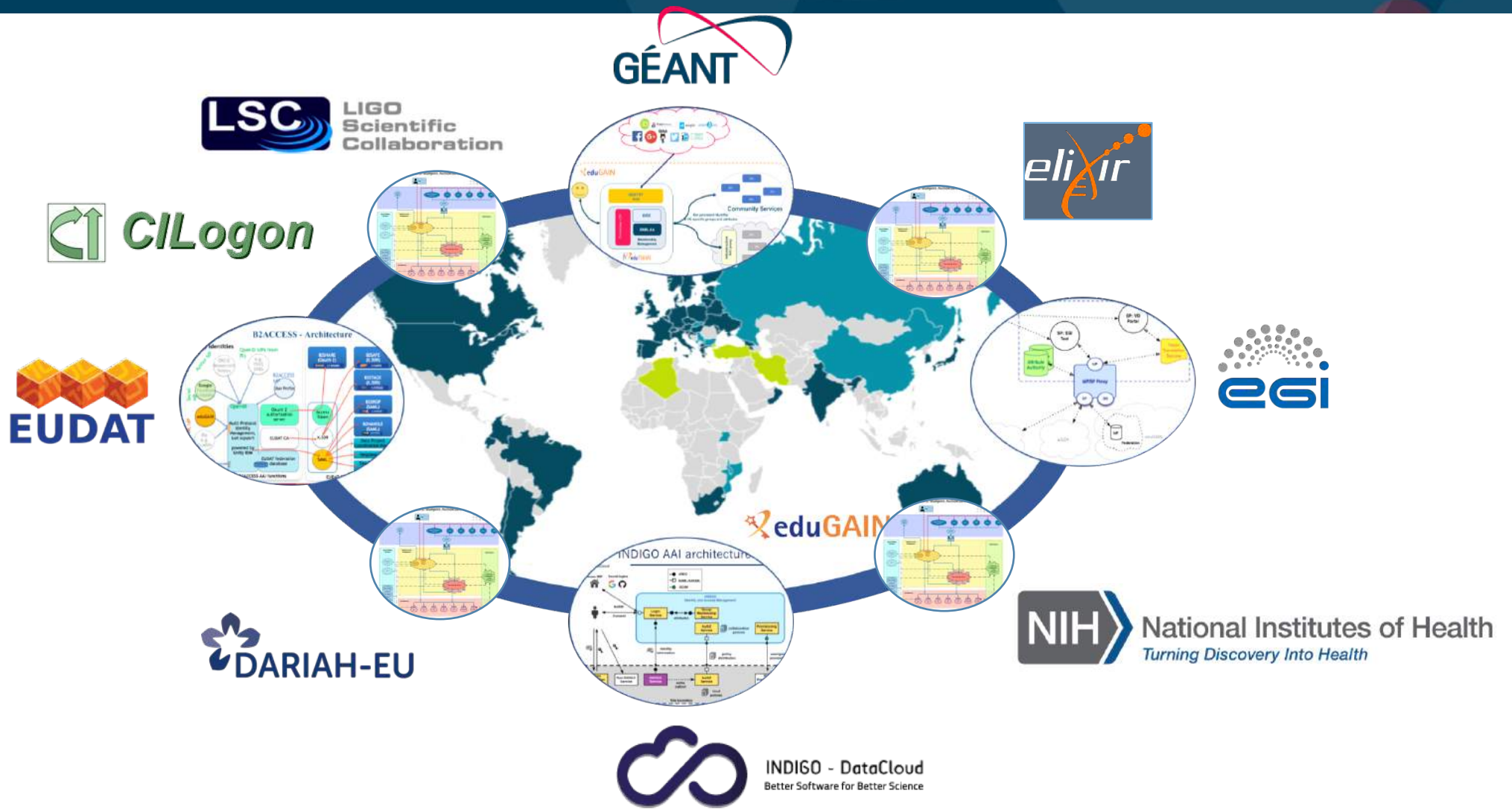

GÉANT
Networks • Services • People
AARC

GÉANT
Networks • Services • People

# BPA

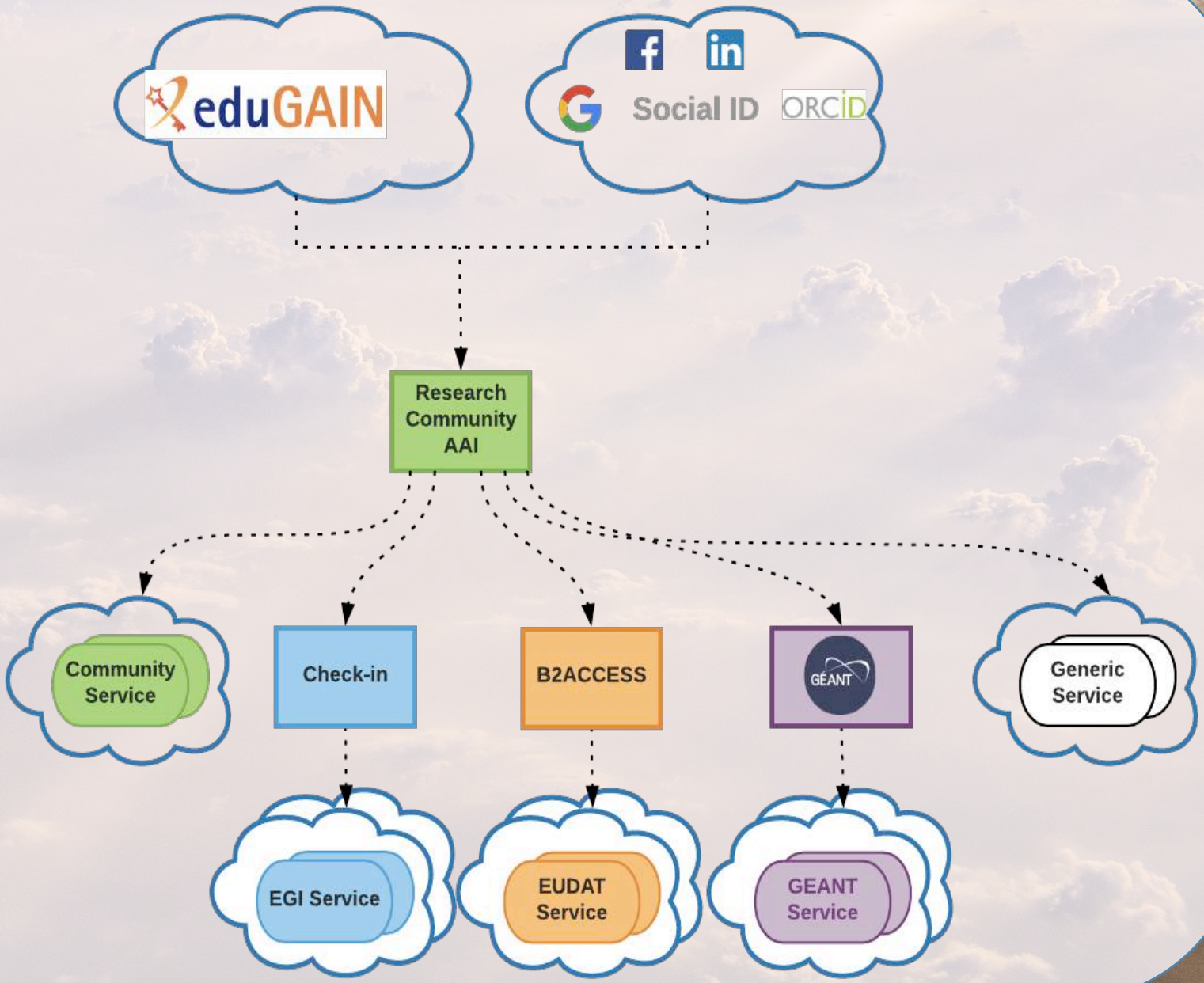


# AARC Blueprint Architecture Implementations



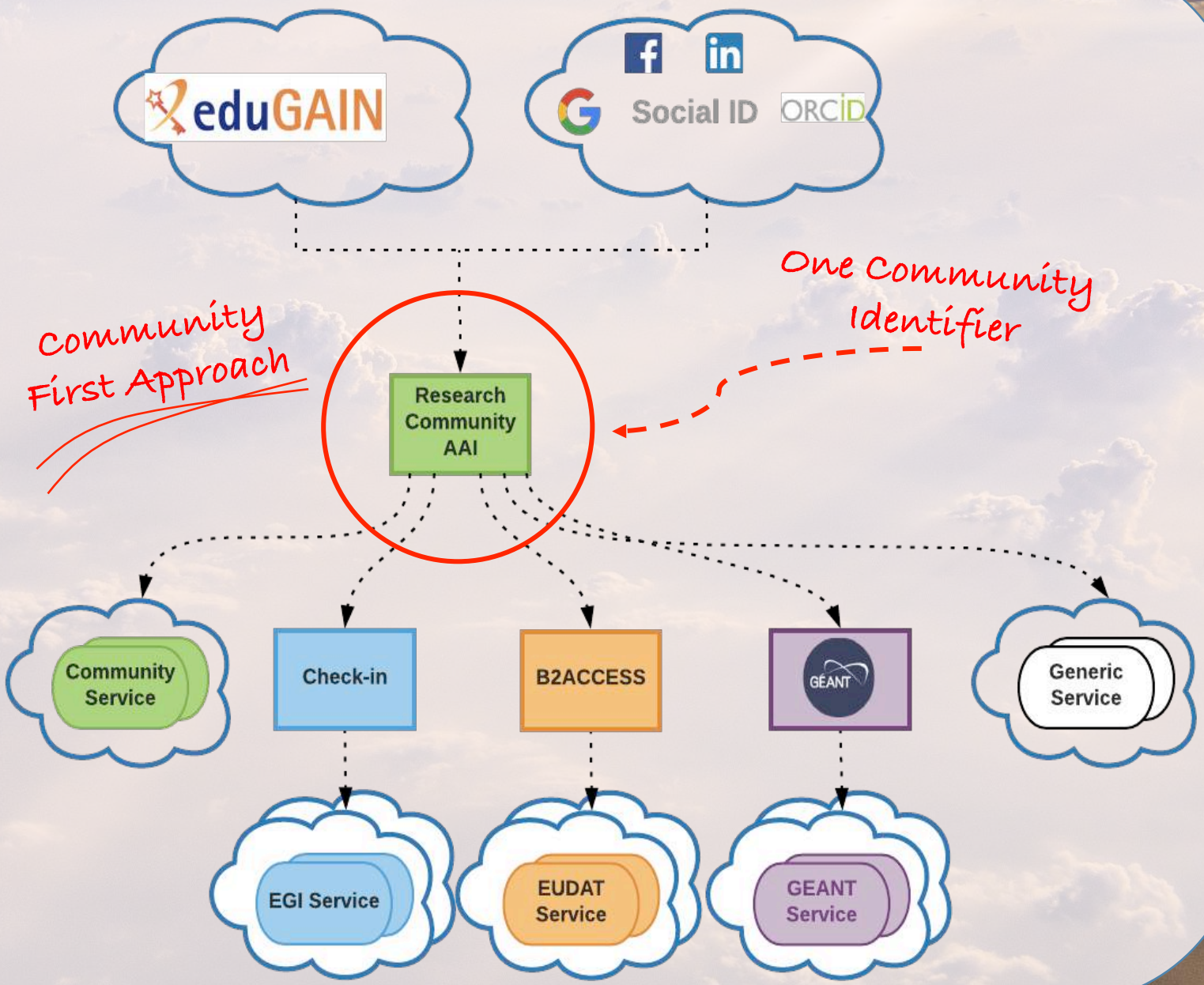
GÉANT
Networks • Services • People

# European Open Science Cloud



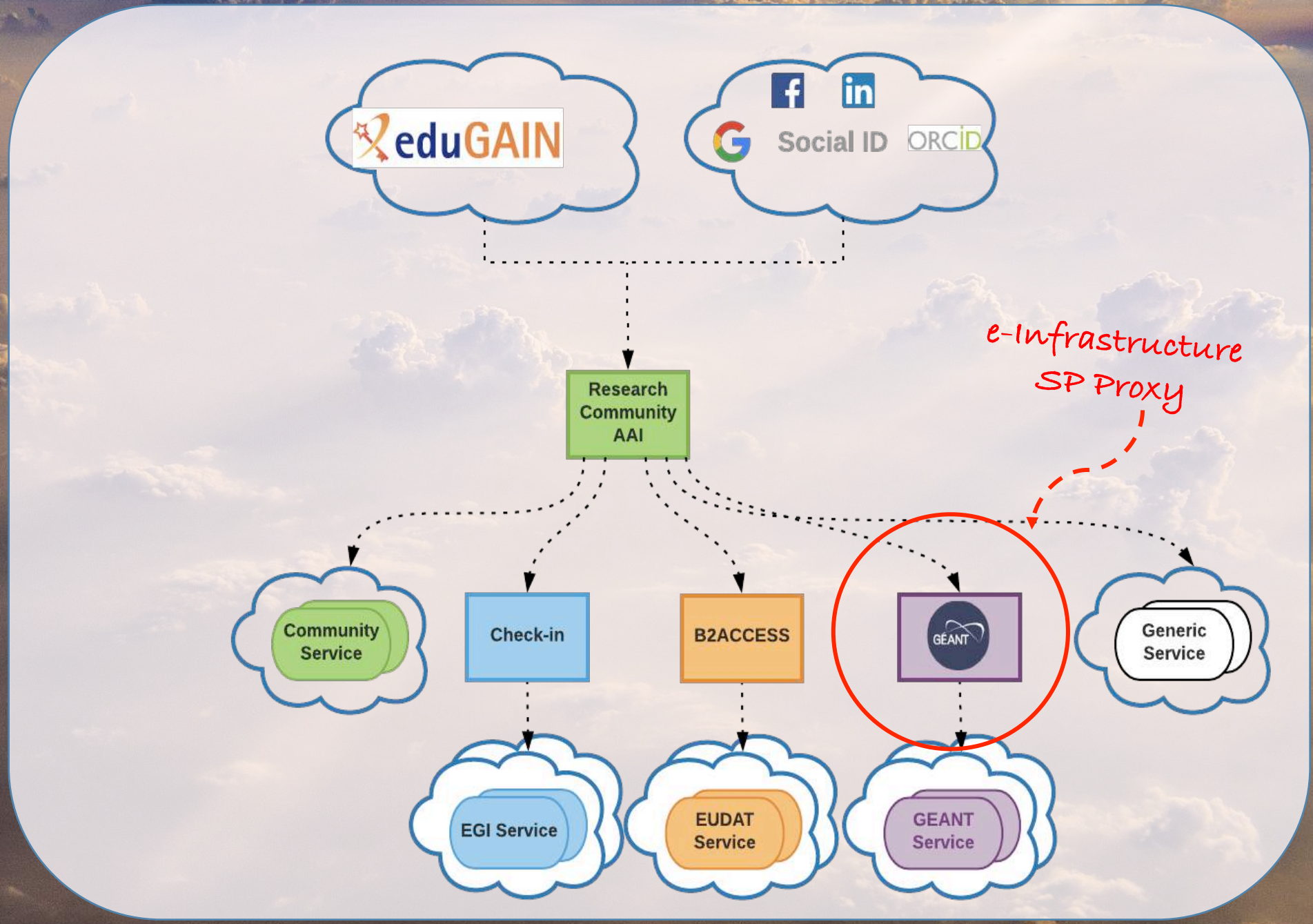
GÉANT
Networks • Services • People

# European Open Science Cloud

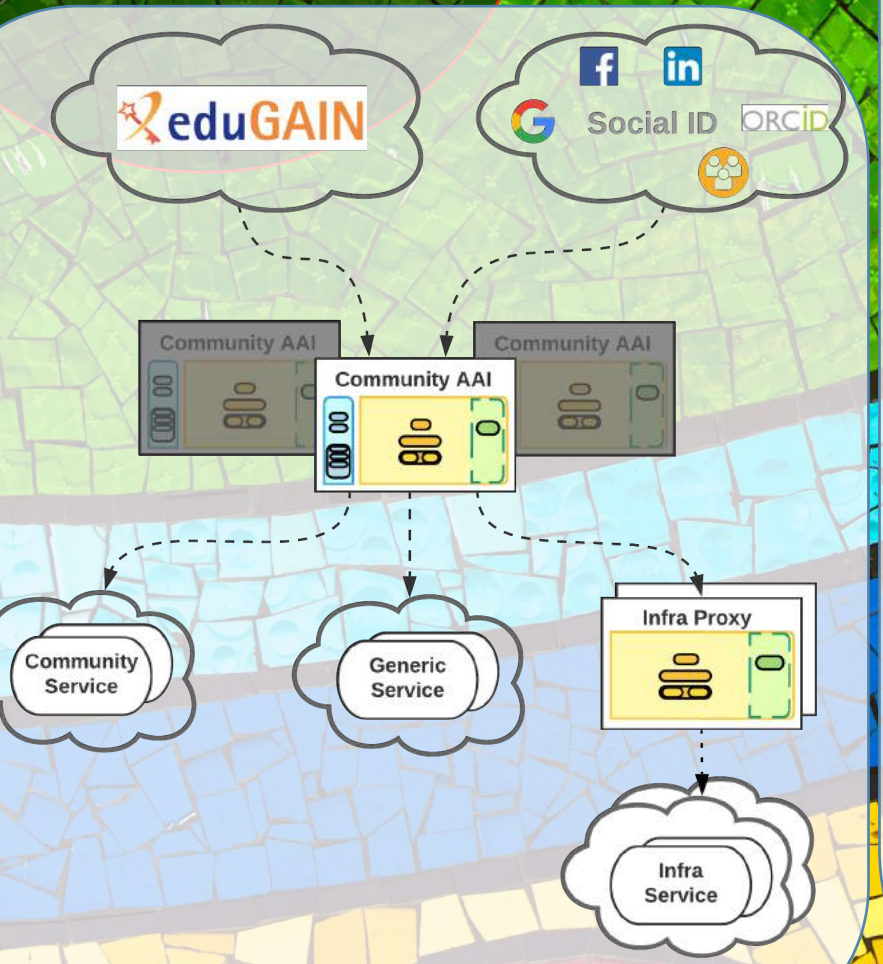


GÉANT
Networks • Services • People

# European Open Science Cloud



GÉANT
Networks • Services • People




**Researchers** sign in using their institutional (eduGAIN), social or community-managed IdP via their Research Community AAI

**Community-specific services** are connected to a single Community AAI

**Generic services** can be connected to more than one Community AAI proxies through eduGAIN

**e-Infra services** are connected to a single e-infra SP proxy service gateway


June 22, 2018

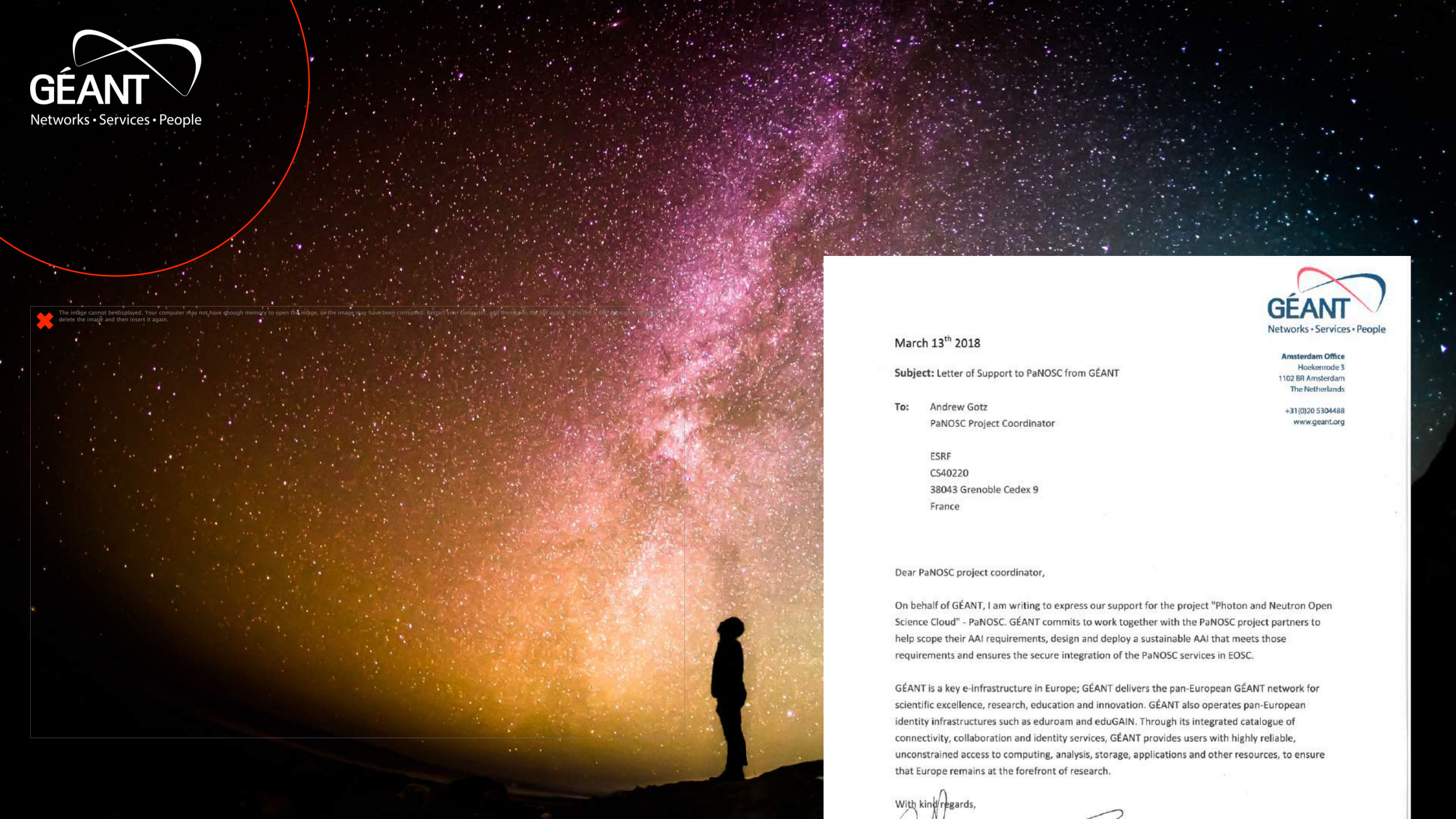
Journal article | Open Acces

# 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

**Amsterdam Office**
Hoekenrode 3
1102 BR Amsterdam
The Netherlands

+31 (0)20 5304488
www.geant.org

March 13th 2018

**Subject:** Letter of Support to PaNOSC from GÉANT

**To:** Andrew Gotz
PaNOSC Project Coordinator

ESRF
CS40220
38043 Grenoble Cedex 9
France

Dear PaNOSC project coordinator,

On behalf of GÉANT, I am writing to express our support for the project "Photon and Neutron Open Science Cloud" - PaNOSC. GÉANT commits to work together with the PaNOSC project partners to help scope their AAI requirements, design and deploy a sustainable AAI that meets those requirements and ensures the secure integration of the PaNOSC services in EOSC.

GÉANT is a key e-infrastructure in Europe; GÉANT delivers the pan-European GÉANT network for scientific excellence, research, education and innovation. GÉANT also operates pan-European identity infrastructures such as eduroam and eduGAIN. Through its integrated catalogue of connectivity, collaboration and identity services, GÉANT provides users with highly reliable, unconstrained access to computing, analysis, storage, applications and other resources, to ensure that Europe remains at the forefront of research.

With kind regards,

# UmbrellaID.org

## Facts

- Started out in 2012 as a collaboration between the main European analytical user facilities in the field of research using photons and neutrons (PaN facilities)
- Over 1000 users providing services to 16 European organisation

## Objectives

- Provide a common Authentication and Authorization Infrastructure that allows users of all PaN facilities to connect seamlessly to digital facility services with a single and unique ID.
- Authorization should remain in full control of each facility providing the services
- Users should be in full control of their personal data

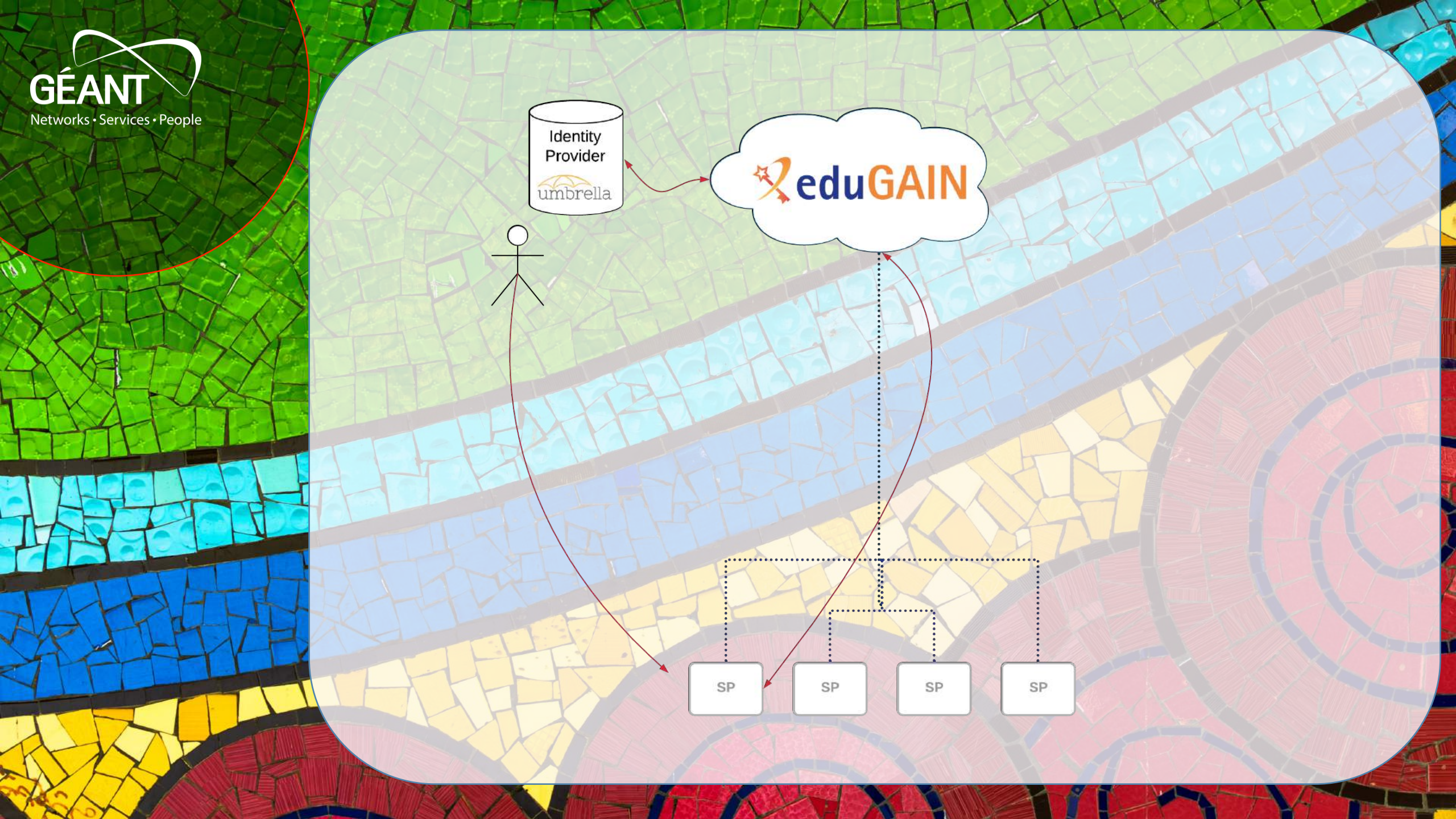
# UmbrellaID.org | Goals in PaNOSC

Increase capacity to respond to users' needs in a stable, secure and trusted environment

Cater from the growing security constraints and legal requirements

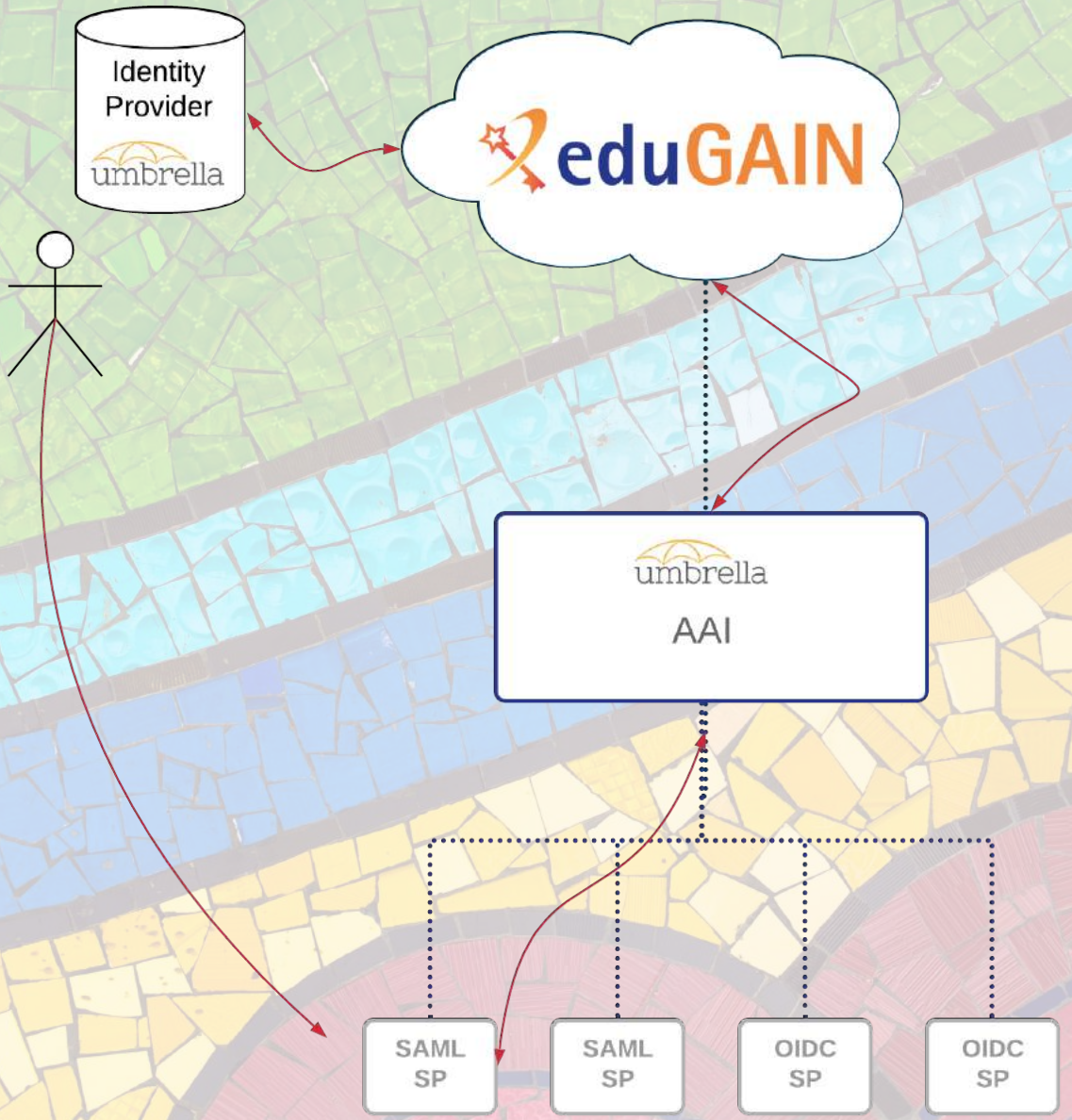
Global and comprehensive interoperability with services outside of the Photon and Neutron domain

Access to the European Open Science Cloud


GÉANT
Networks • Services • People
Identity Provider
umbrella
eduGAIN
SP
SP
SP
SP

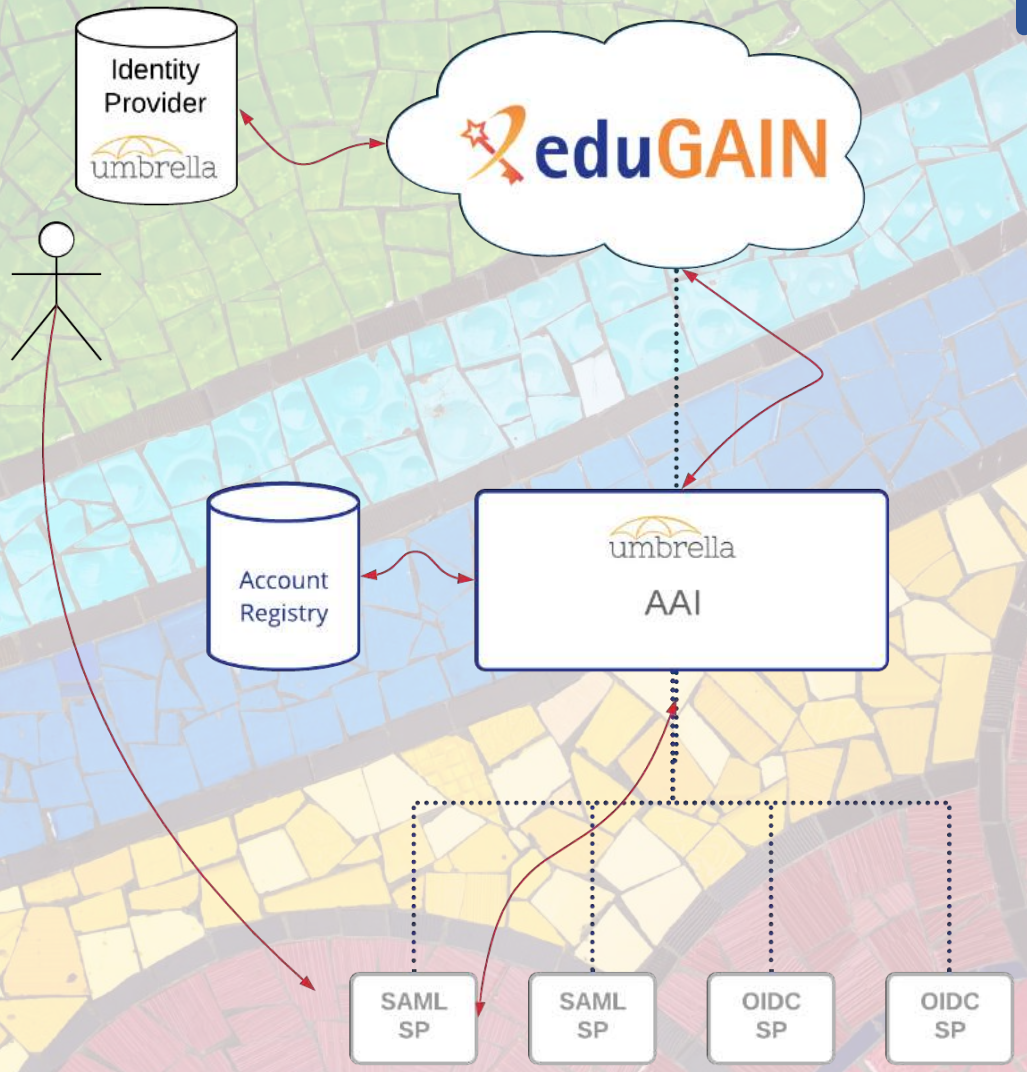
GÉANT
Networks • Services • People

# Phase 1



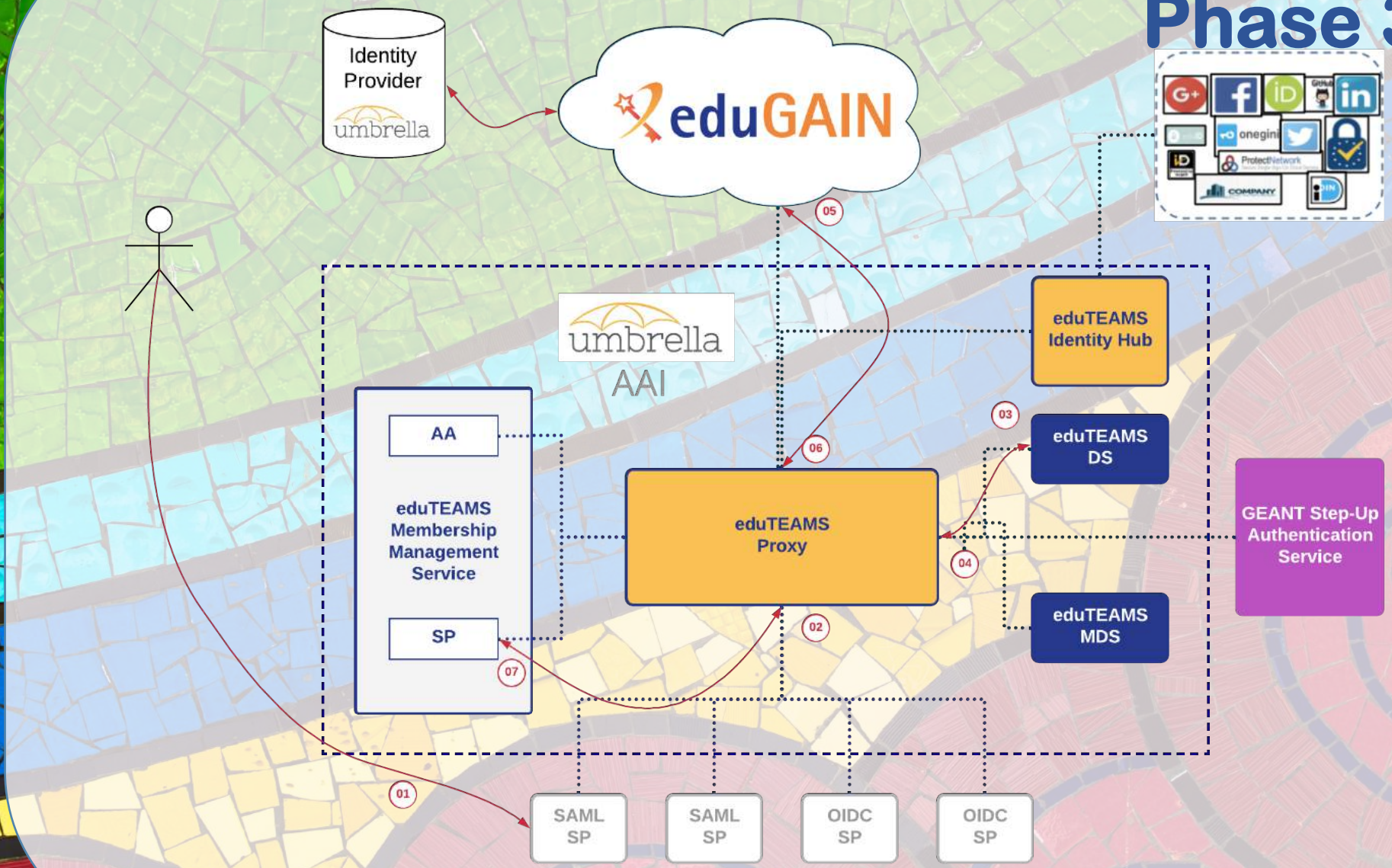
GÉANT
Networks • Services • People

# Phase 2

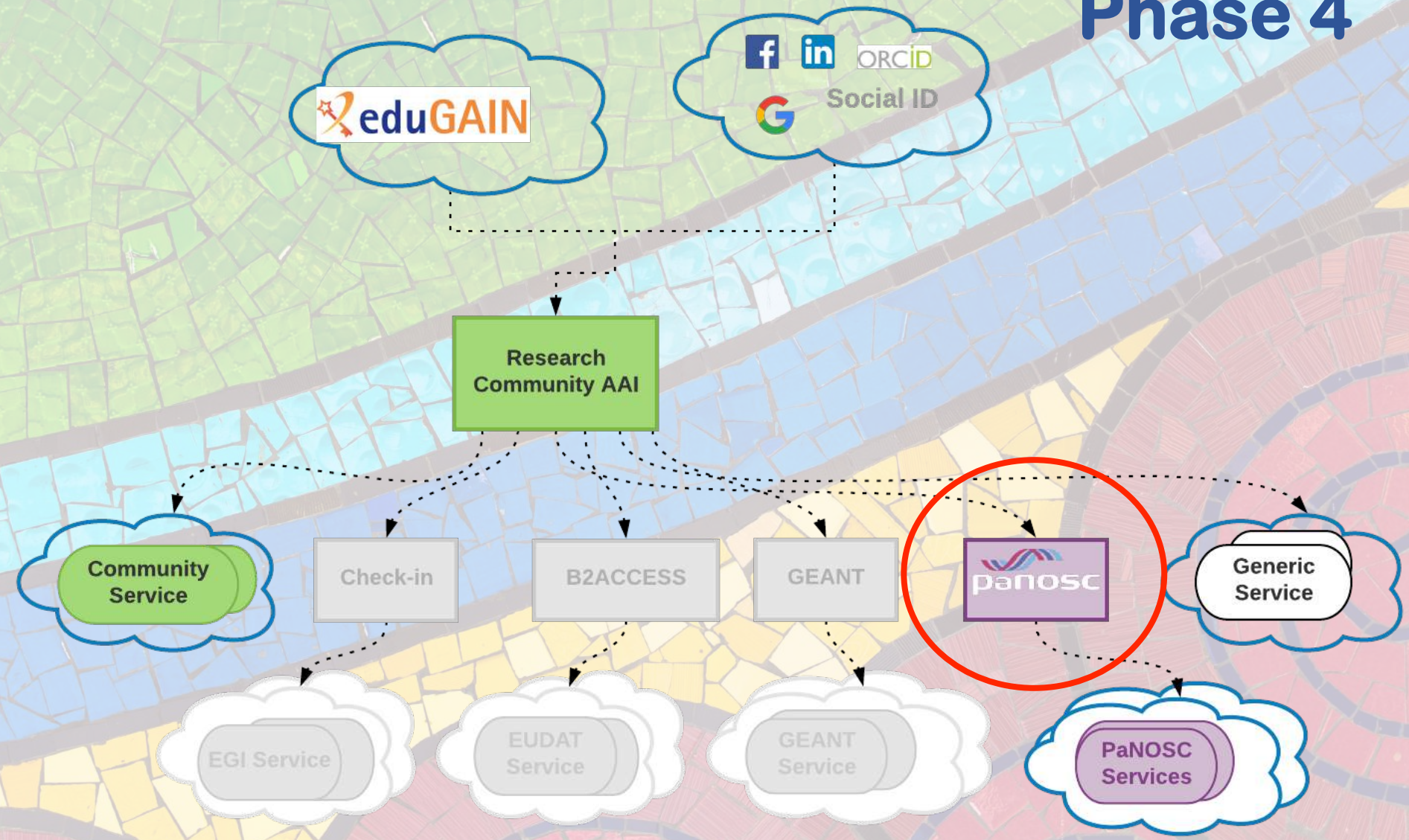


GÉANT
Networks • Services • People

# Phase 3



# Phase 4


eduGAIN
ORCID
Social ID
Research Community AAI
Community Service
Check-in
B2ACCESS
GEANT
panosc
Generic Service
EGI Service
EUDAT Service
GEANT Service
PaNOSC Services

# Thank you