Authentication and Authorisation for Research and Collaboration

AARC Blueprint Architecture

Christos Kanellopoulos, GÉANT

11th FIM4R, Montreal, Canada

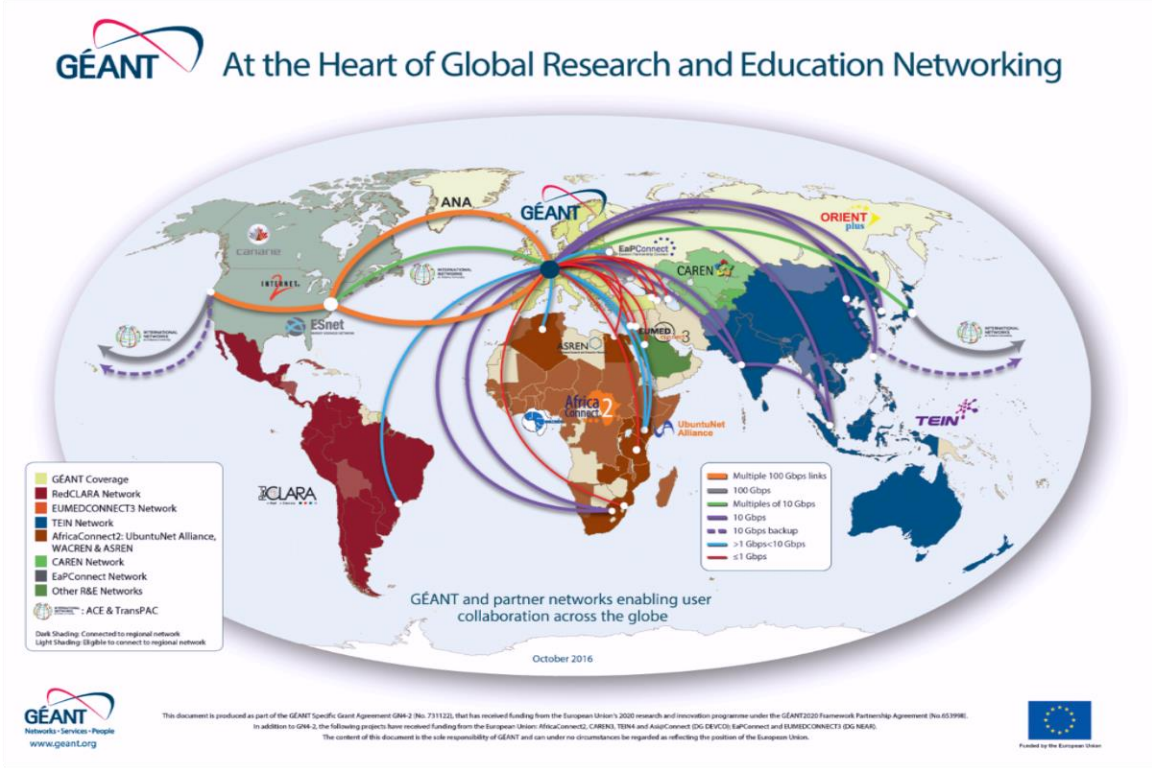
September 19th , 2017

Research Communities

- The way researchers collaborate within scientific communities can vary significantly from community to community
- The ability to access and share resources is crucial for the success of any collaboration
- Advanced Research and Education (R&E) needs advanced IT services

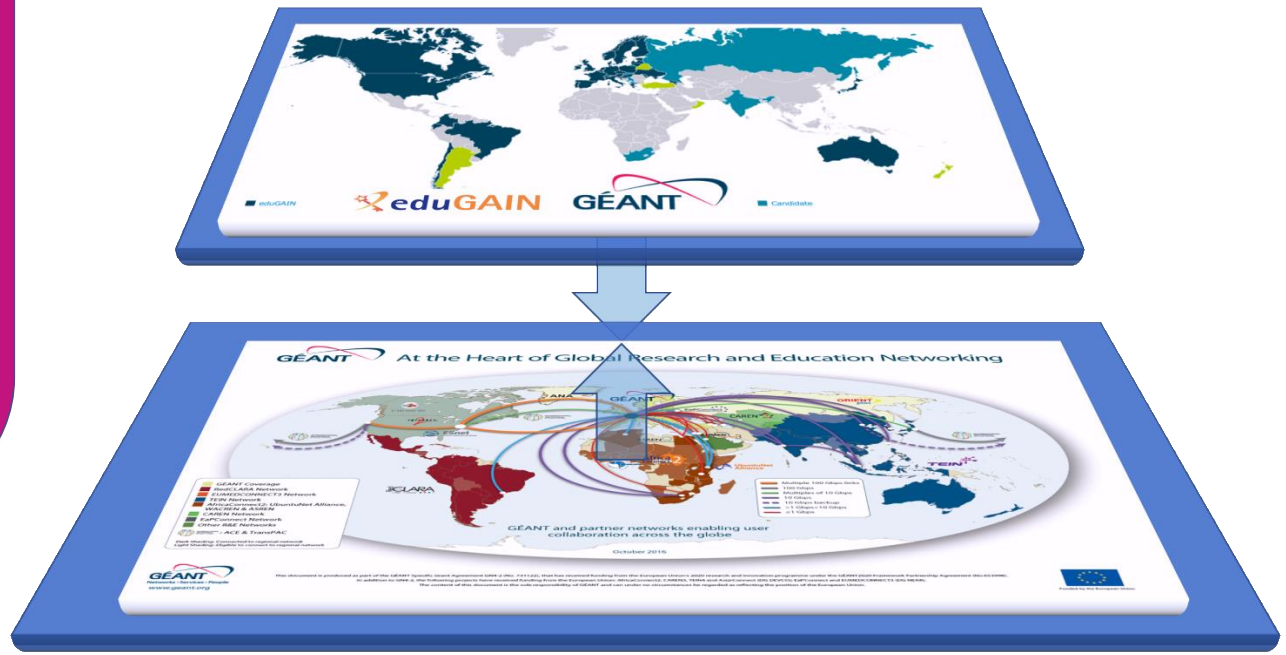
GÉANT Network – A global infrastructure enabling collaboration on a global scale

- GÉANT and the NRENs connect over 50 million users at 10,000 institutions across Europe
- Interconnecting with all world regions, reaching to over 100 countries.
- A global infrastructure enabling European researchers to collaborate on a global scale



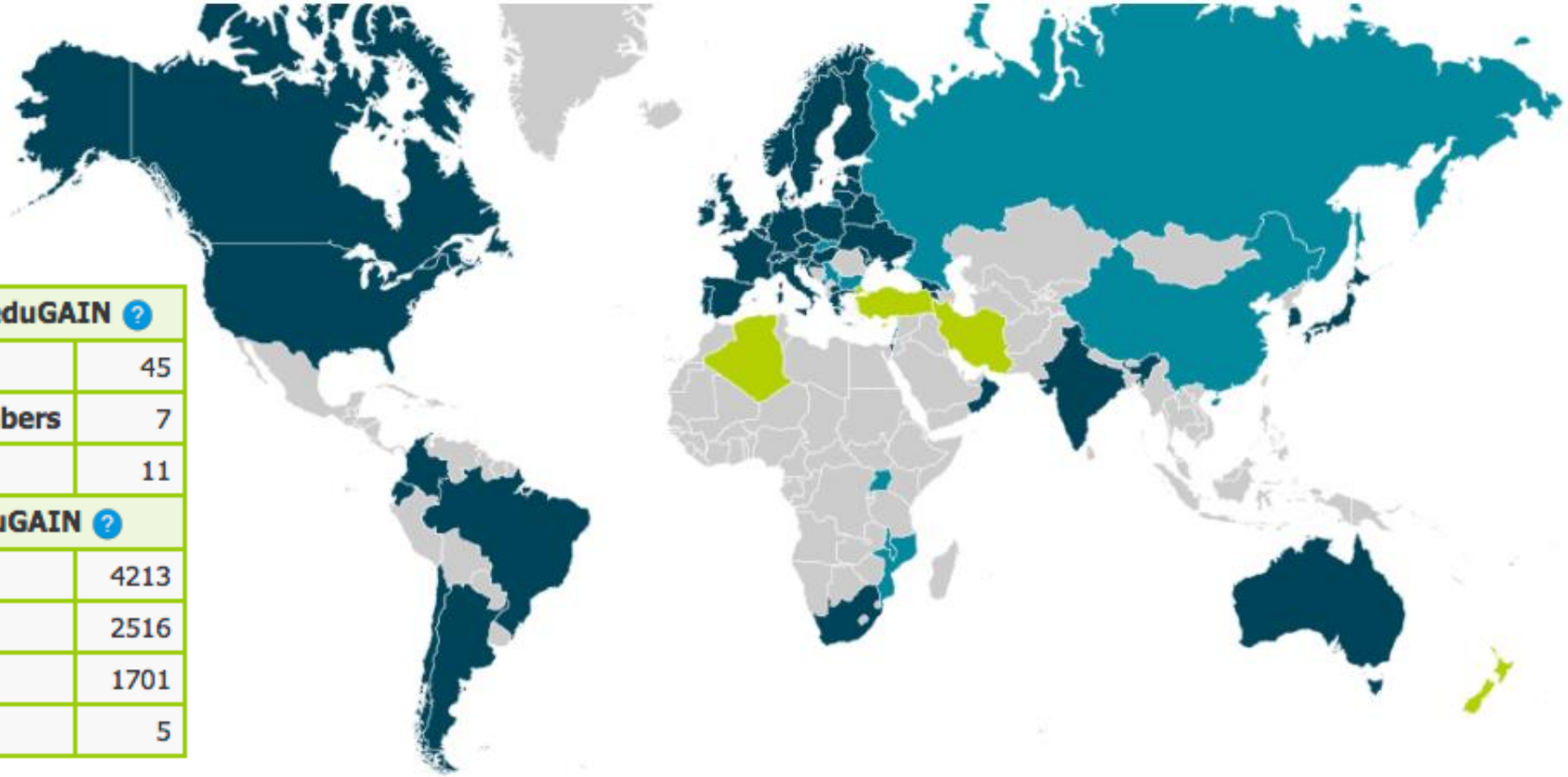
eduGAIN – A global network of academic identities

- Interconnects identity federations around the world, simplifying access to content, services and resources
- Researchers can use a single digital identity provided by the home organization



eduGAIN – A global network of academic identities

Federations in eduGAIN	
Members	45
Voting-only Members	7
Candidates	11
Entities in eduGAIN	
All	4213
IdPs	2516
SPs	1701
Standalone AAs	5

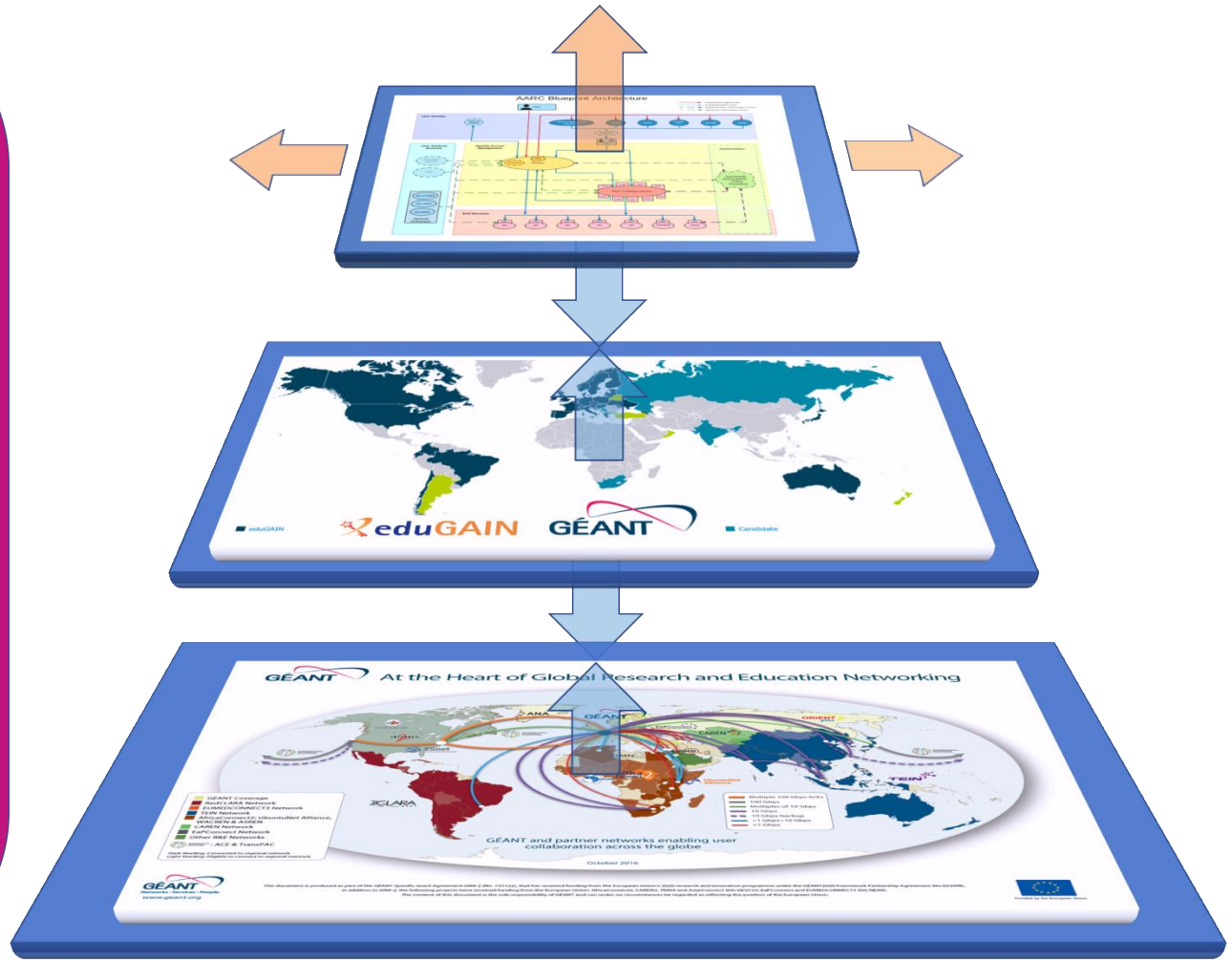


Federated Identity Management for Research

- Access services using **identities from their Home Organizations** when available.
- Secure integration of **guest identity solutions** and **support for stronger authentication** mechanisms when needed.
- **Access** to the various services should be granted **based on the role(s)** the users have in the collaboration.
- Users should have **one persistent identity** across all community services when needed.
- **Ease of use for users and service providers**. The complexity of multiple IdPs/Federations/Attribute Authorities/ - technologies should be hidden.

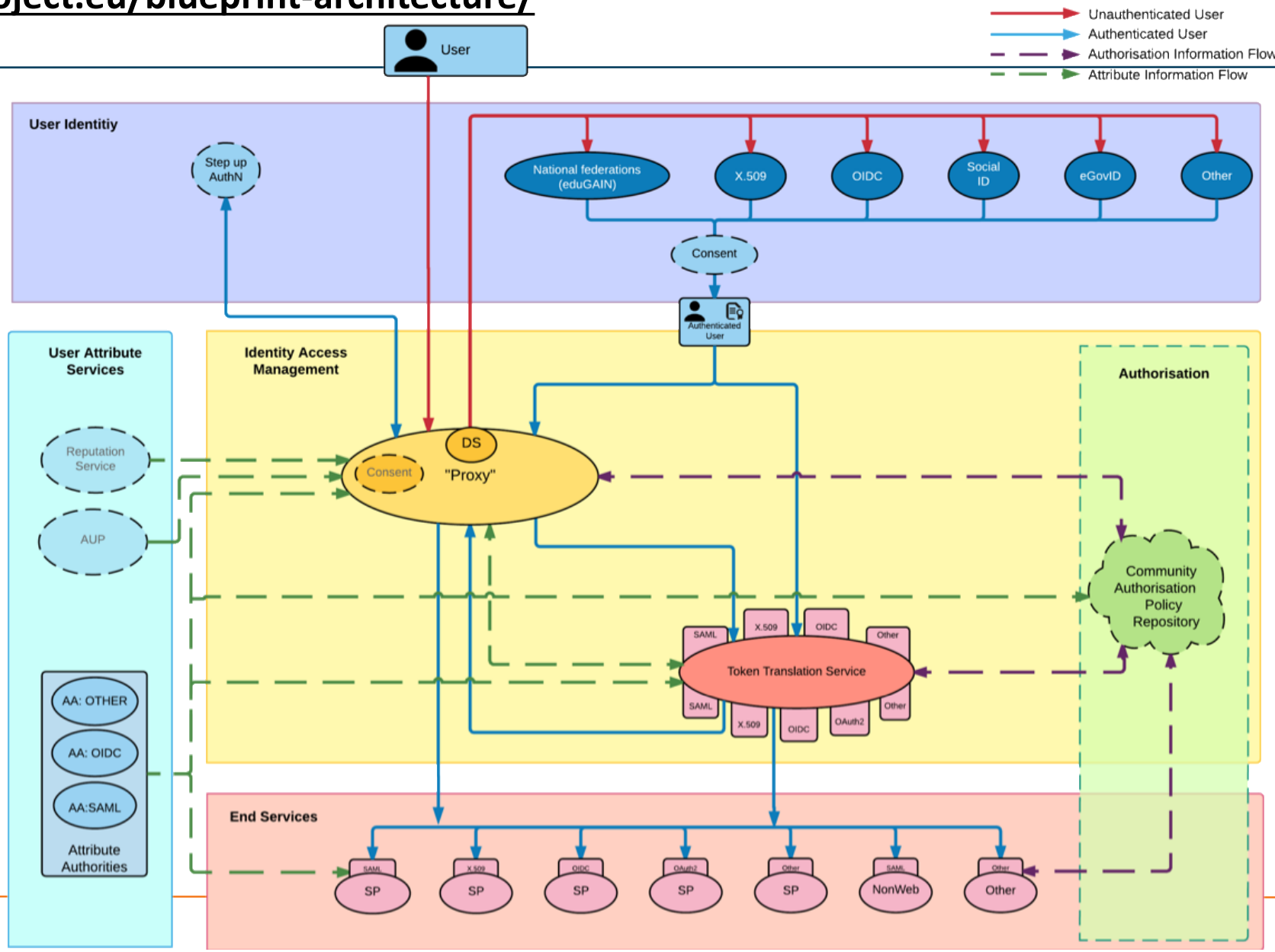
AARC Blueprint Architecture - Enabling an ecosystem of solution on top of eduGAIN

- 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



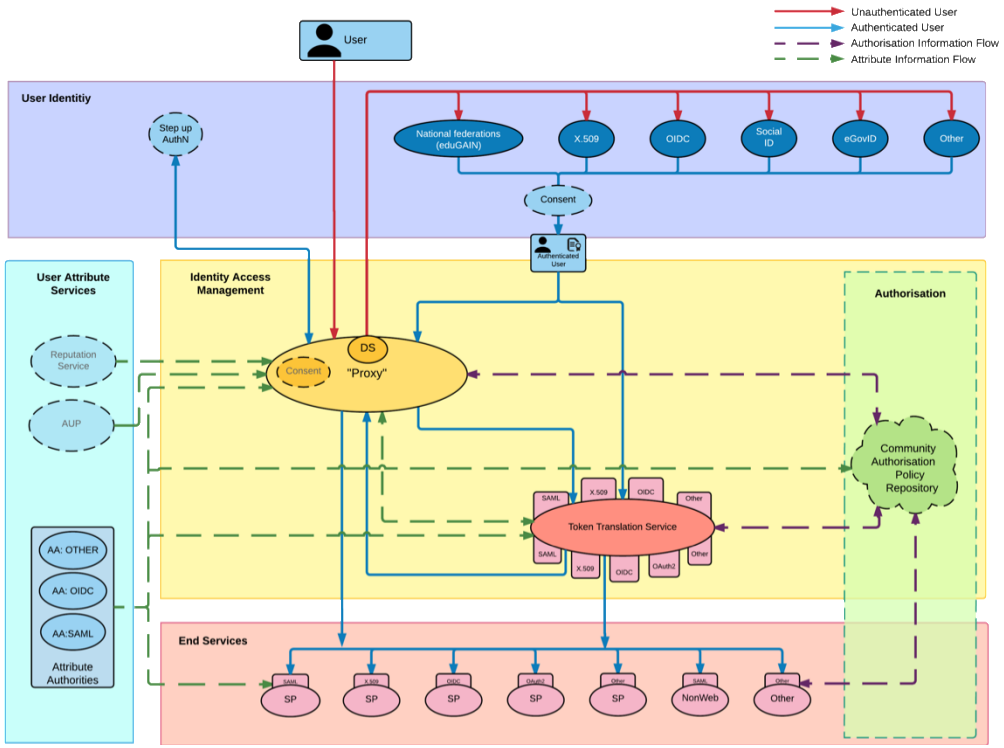
AARC Blueprint Architecture

https://aarc-project.eu/blueprint-architecture/



AARC Blueprint Architecture

https://aarc-project.eu/blueprint-architecture/

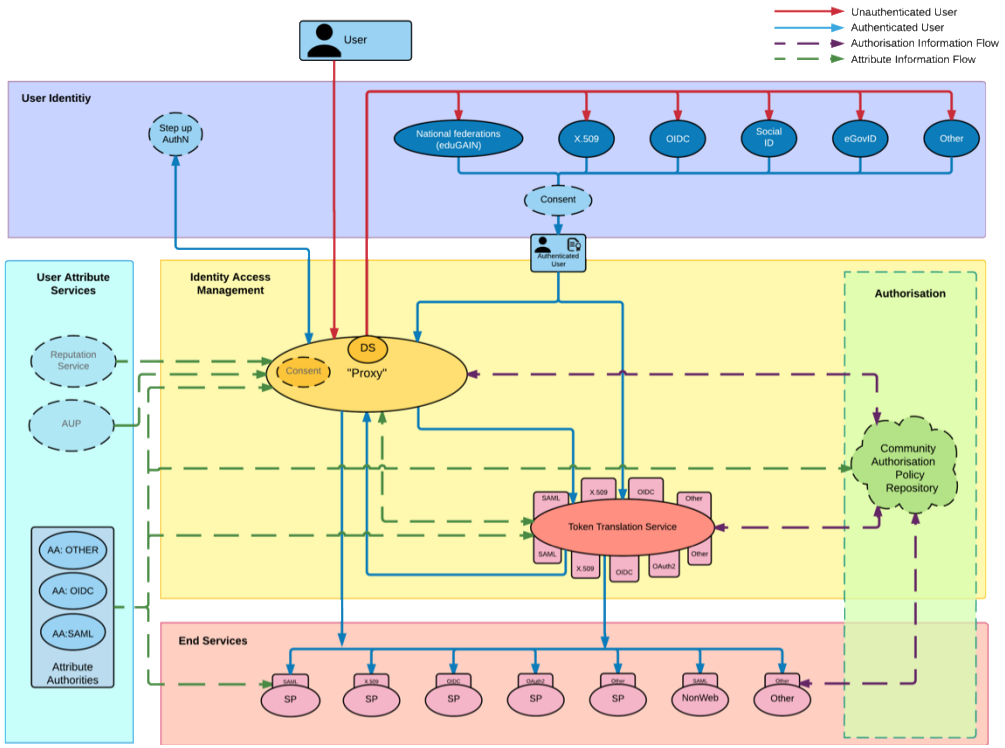


Guidelines and support documents

- Best practices for managing authorisation
- Expressing group membership and role information
- Scalable attribute aggregation
- Implementation of token TTS
- Credential delegation
- Non-web access
- Social media IdPs
- Use cases for account linking
- Use cases for LoA elevation via step-up authentication

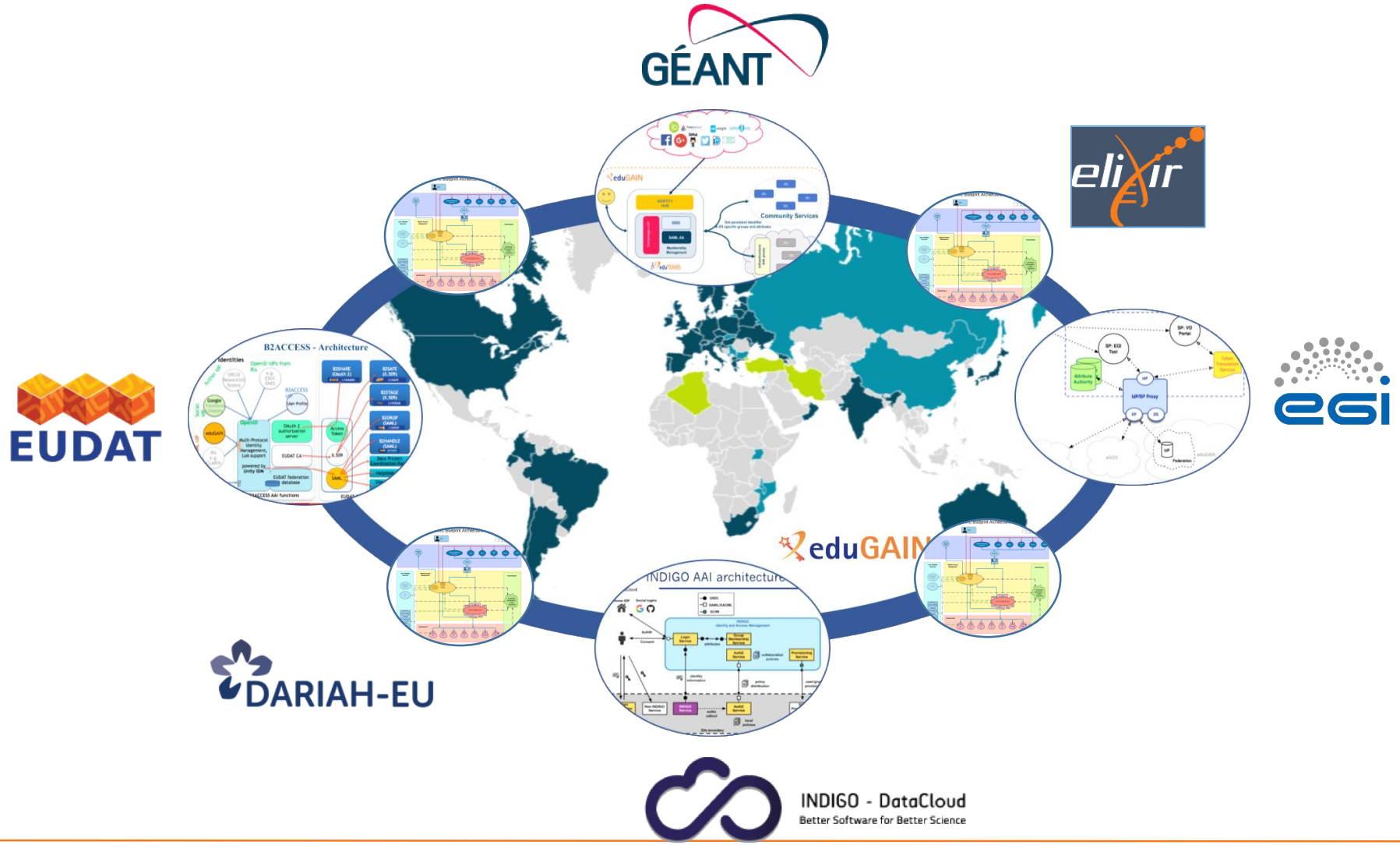
AARC Blueprint Architecture

https://aarc-project.eu/workpackages/policy-harmonisation/

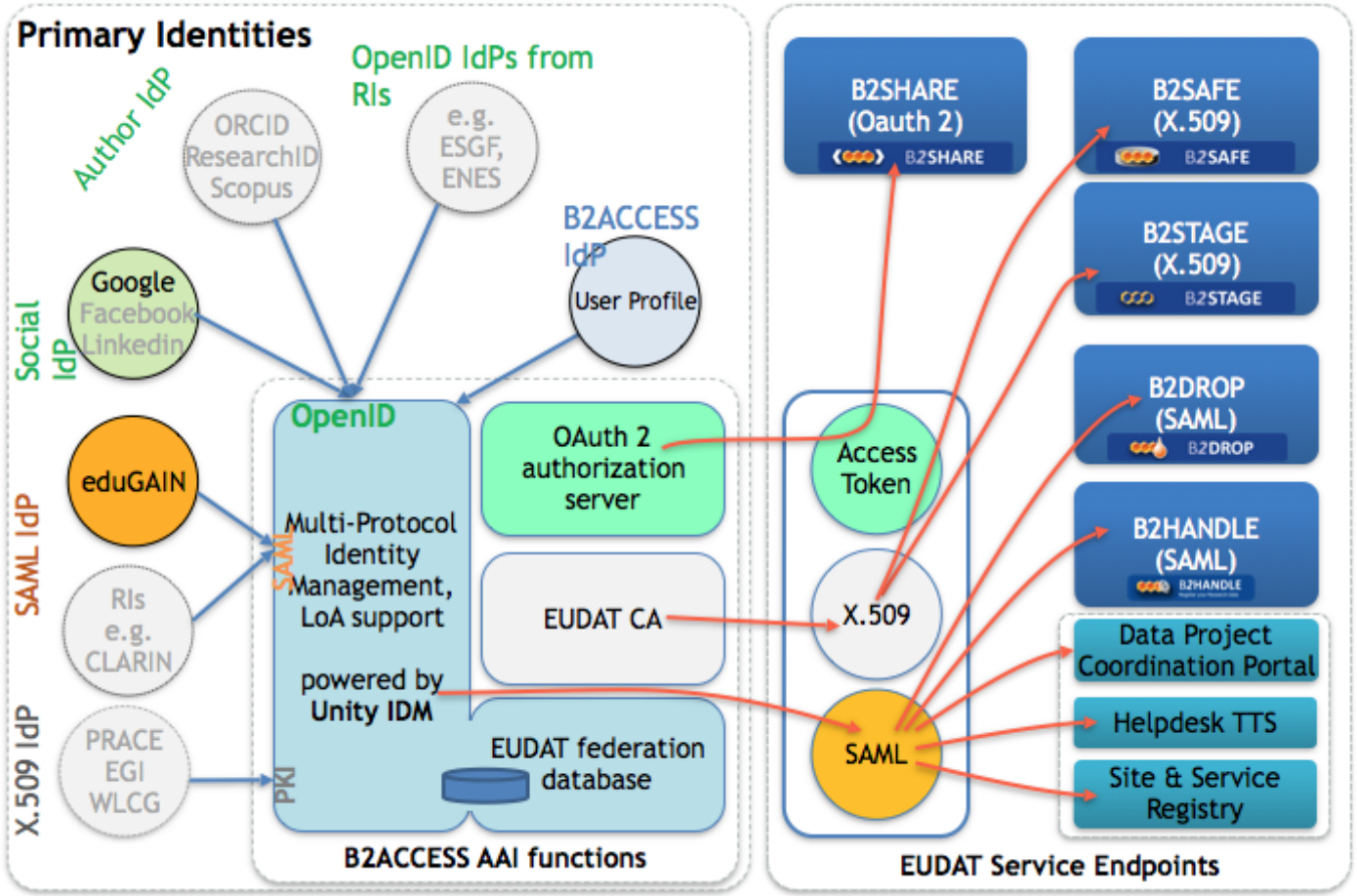


Policy recommendations & frameworks

- Security Incident Response Trust Framework for Federated Identity – Sirtfi
- Scalable Negotiator for a Community Trust Framework in Federated Infrastructures – Snctfi
- Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases
- Differentiated LoA recommendations for policy and practices of identity and attribute providers
- Recommendations and template policies for the processing of personal data by participants in the pan-European AAI

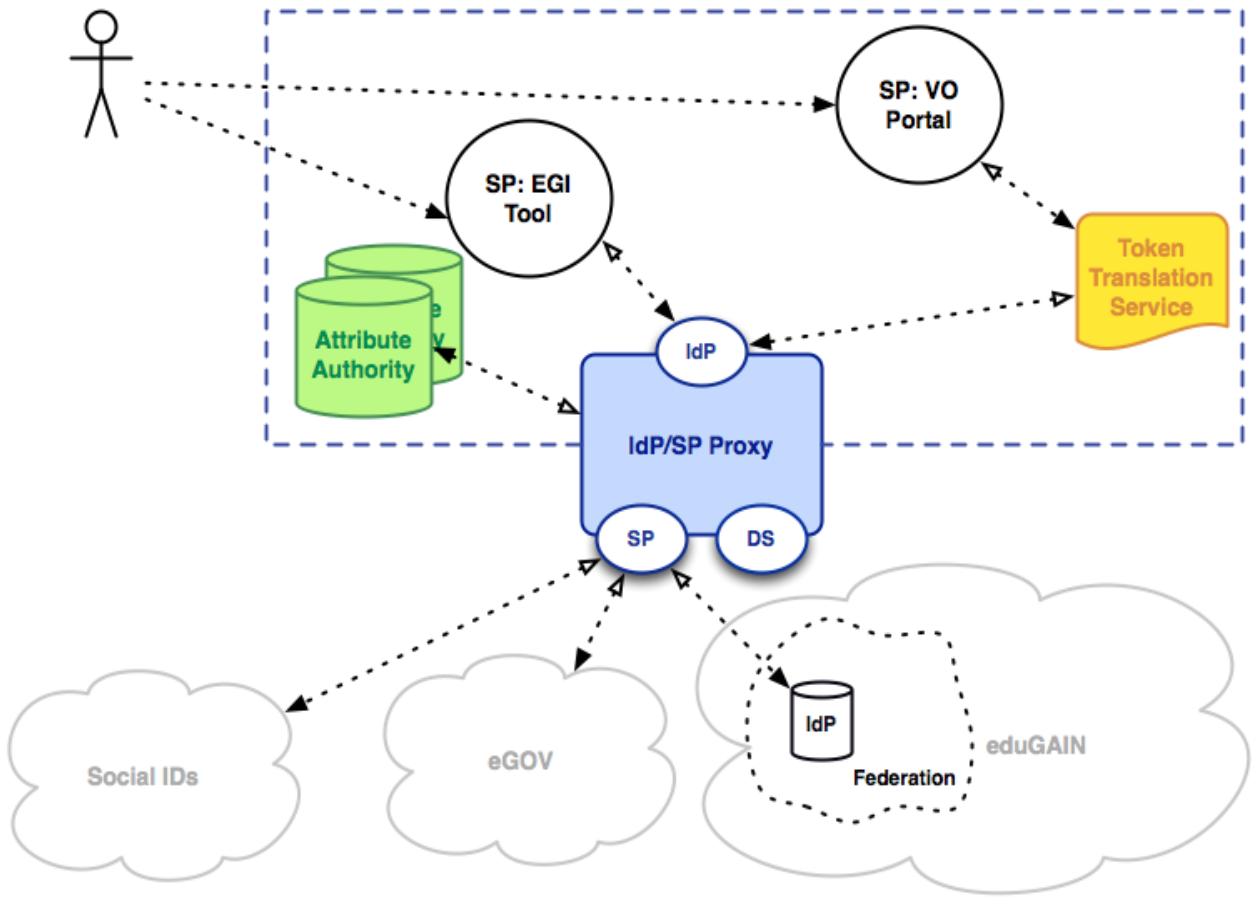

GÉANT
eduGAIN
Community Services
eliXir
B2ACCESS - Architecture
EUDAT
SP: EGI Tool
SP: VO Portal
IdP/SP Proxy
EGI
eduGAIN
INDIGO AAI architecture
DARIAH-EU
INDIGO - DataCloud
Better Software for Better Science

EUDAT B2ACCESS Service



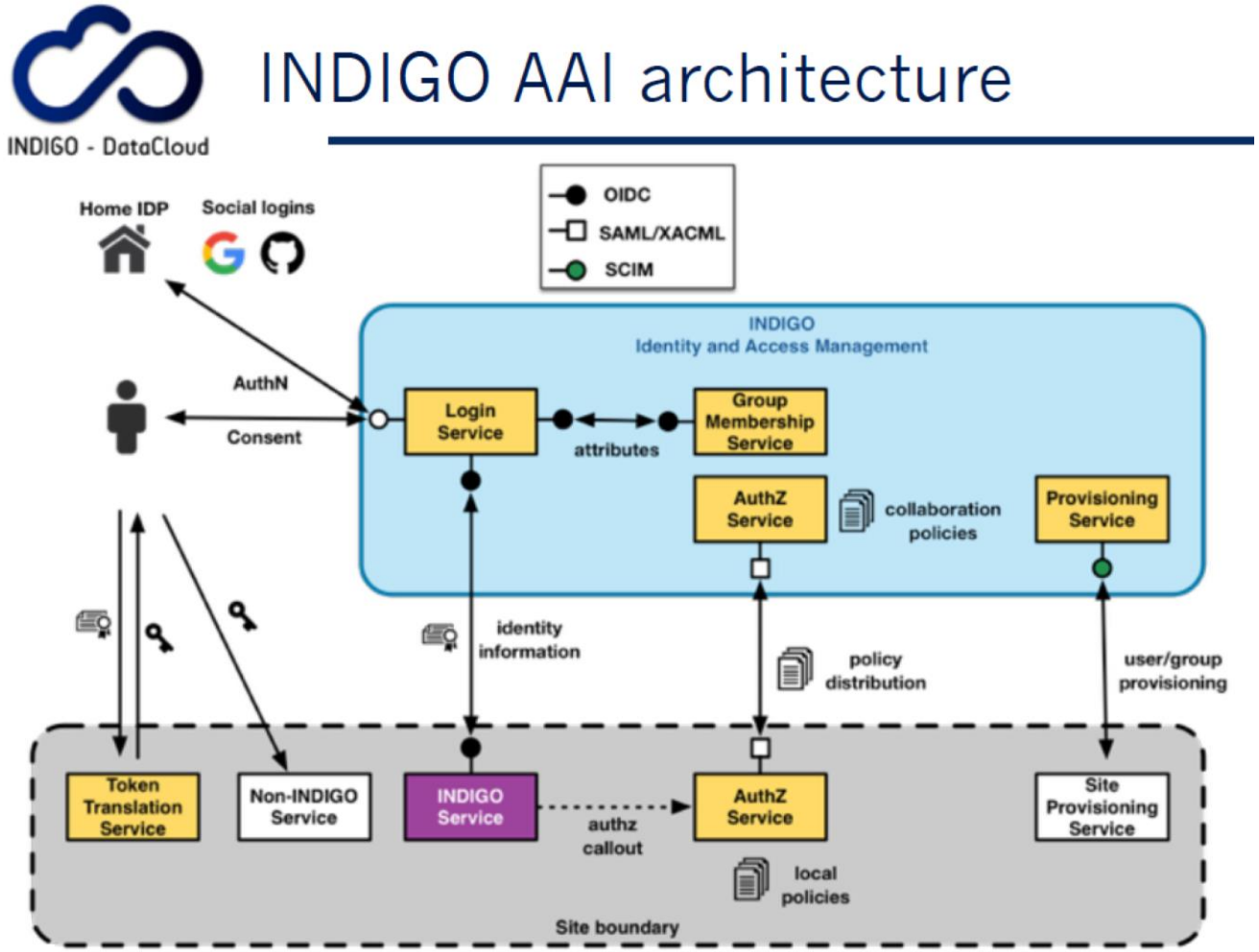
- Enables communities to use federated identities to access EUDAT services
- Connects to **eduGAIN** to enable users use their existing accounts at their home organisations
- Supports social ID logins and integration with token translations services for enable non-web access
- Communities can connect their community management systems as Attribute Authorities

EGI Check-In Service



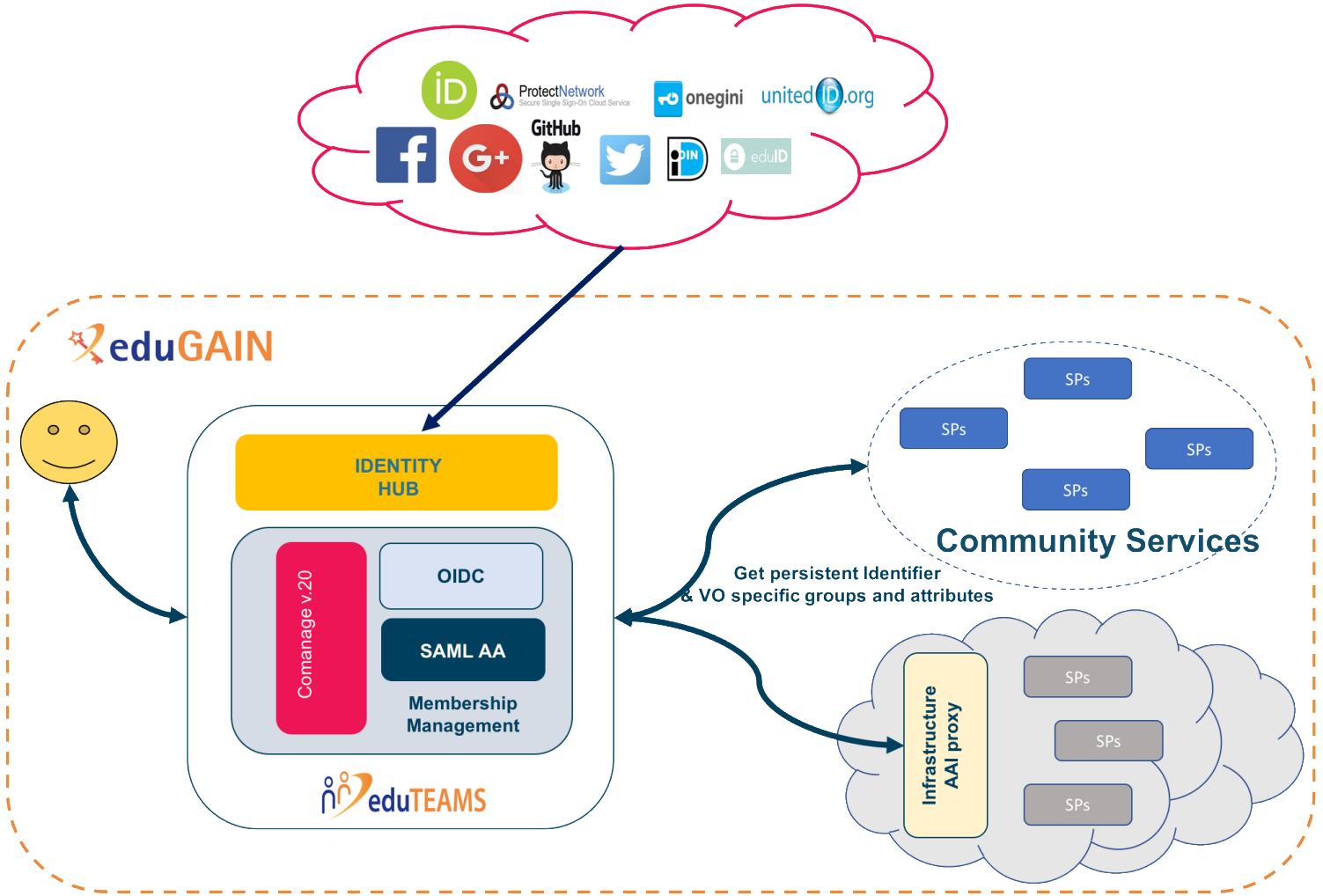
- Enables communities to use federated identities to access EGI services
- Connects to **eduGAIN** to enable users use their existing accounts at their home organisations
- Supports social ID logins and integration with token translations services for enable non-web access
- Communities can connect their community management systems as Attribute Authorities

INDIGO AAI



- Enables communities to use federated identities to access services using OIDC
- Connects to **eduGAIN** to enable users use their existing accounts at their home organisations
- Supports social ID logins and integration with token translations services for enable non-web access
- Communities can connect their community management systems as Attribute Authorities

GÉANT eduTeams



- A suite of services to support research collaboration
- Built on top of eduGAIN, takes full advantage of federated AAI
- Simplify the management of group and authorization information
- Enables the integration of users from a wide range of environments
- Service Providers in eduGAIN can utilize Social IDs using the identity Hub
- Connects users to services

Thank you

Any Questions?

Christos.Kanellopoulos@geant.org

http://aarc-project.eu/

© GEANT on behalf of the AARC project.
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).

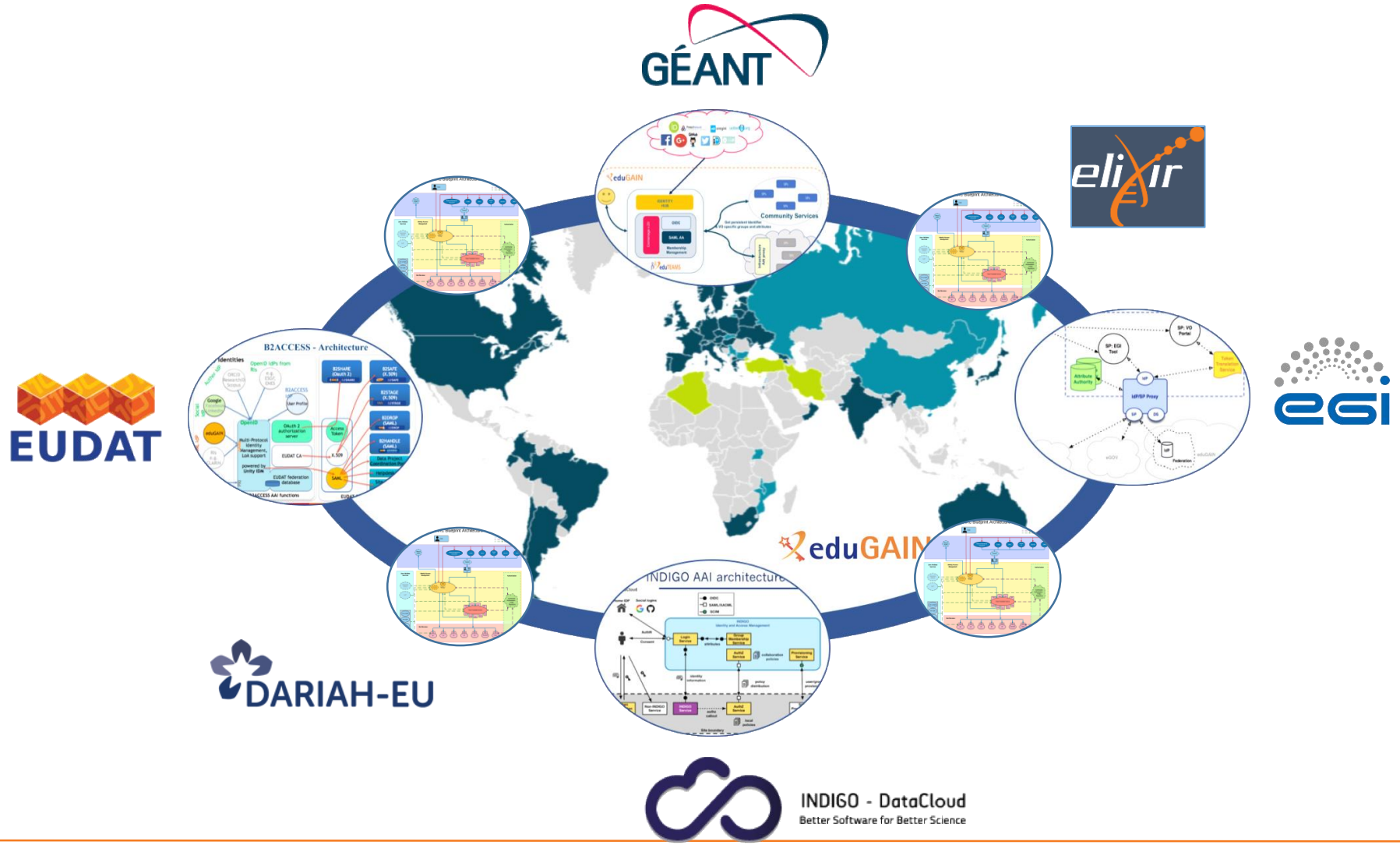
Authentication and Authorisation for Research and Collaboration

AARC Engagement Group for InfrastructureS

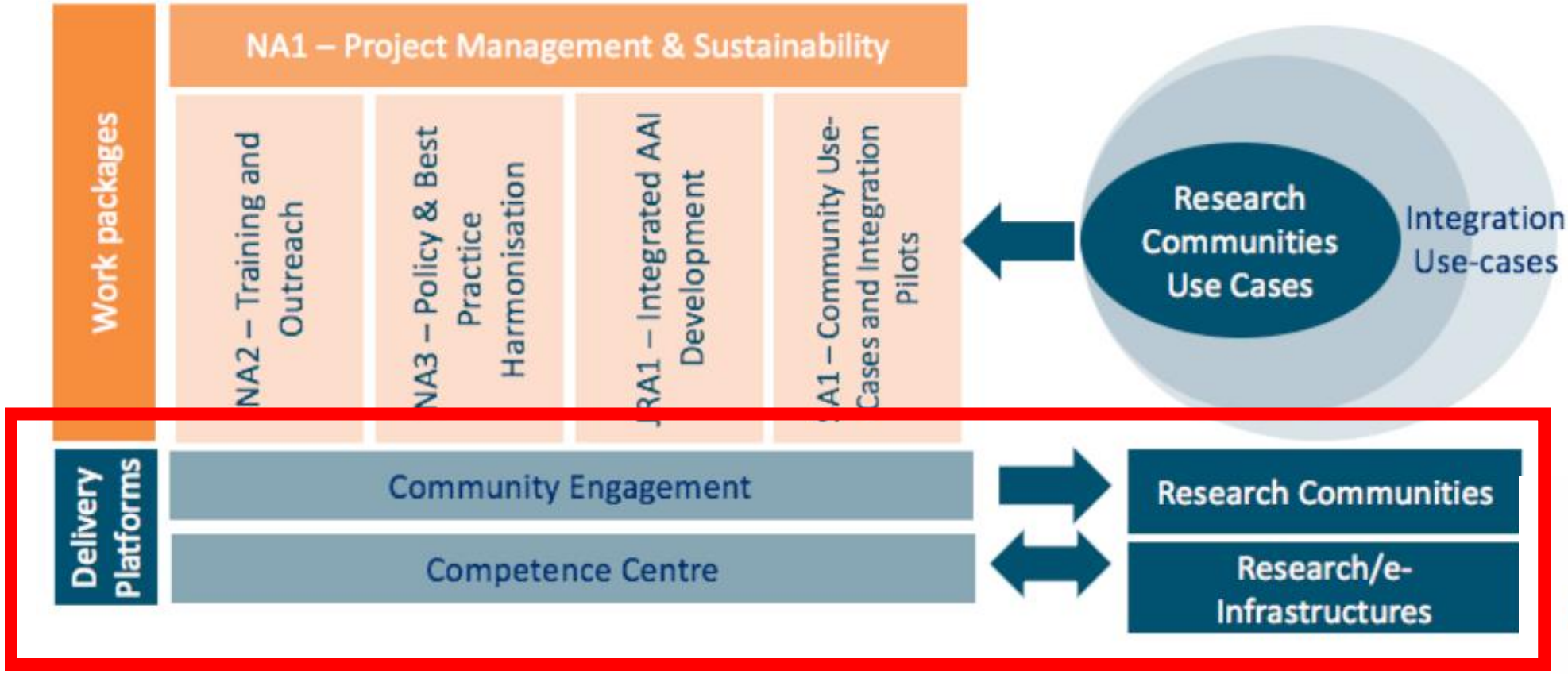
Christos Kanellopoulos, GÉANT

11th FIM4R, Montreal, Canada

September 19th , 2017


GÉANT
eduGAIN
Community Services
elixir
B2ACCESS - Architecture
EUDAT
SP: EGI Tool
SP: VO Portal
IdP/SP Proxy
egi
eduGAIN
INDIGO AAI architecture
DARIAH-EU
INDIGO - DataCloud
Better Software for Better Science

AARC 2nd edition – Working closer together



AARC Engagement Group for Infrastructures

- Representatives from research and e-Infrastructures who operate AAI services for the communities they support
- A communication channel with and across the infrastructure providers
- Promote a consistent vision for federated access
- Facilitate activities so that infrastructures implement harmonised solutions and avoid ’re-inventing the wheel”

AARC Engagement Group for Infrastructures

- **Implementation of AARC guidelines**
- **AAI platform alignment activity**
  - **Levels of Assurance**
    - How to position the LoA for social identities
    - LoA and eduGAIN IdPs
    - REFEDS assurance profiles
  - **Infrastructure identifier syntax**
  - **Acceptable Usage Policies**
  - **Home organization affiliation**
    - Syntax for home organization affiliation
    - Practices for home organization affiliation
  - **Requested attributes from HO**

Thank you

Any Questions?

Christos.Kanellopoulos@geant.org

http://aarc-project.eu/

© GEANT on behalf of the AARC project.
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).