GÉANT Trust & Identity services update

Vincenzo Capone

Head of Research Engagement and Support

MAGIC Meeting

Dallas, 14 November 2018

About GÉANT

GÉANT
Networks • Services • People

GÉANT supports and represents over 40 NRENs across Europe.

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

The Challenge

eduGAIN ecosystem

eduTEAMS

AAI as a Service for communities

A service to enable use of federated identities in research communities

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

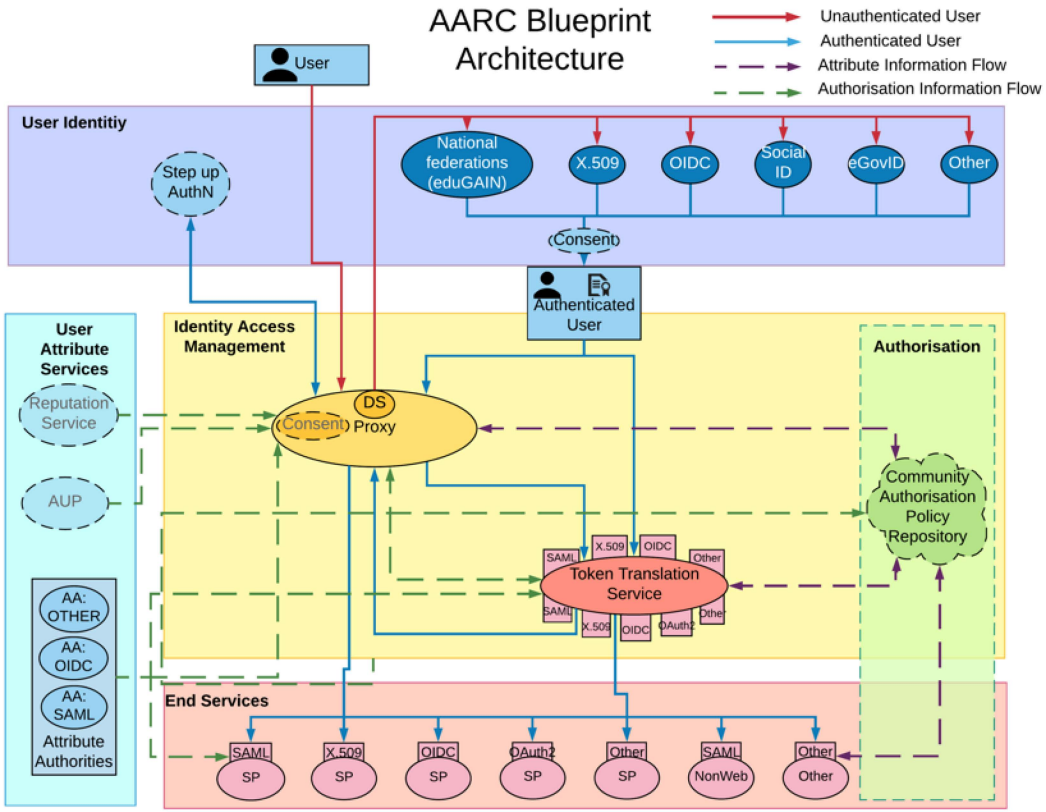
Components

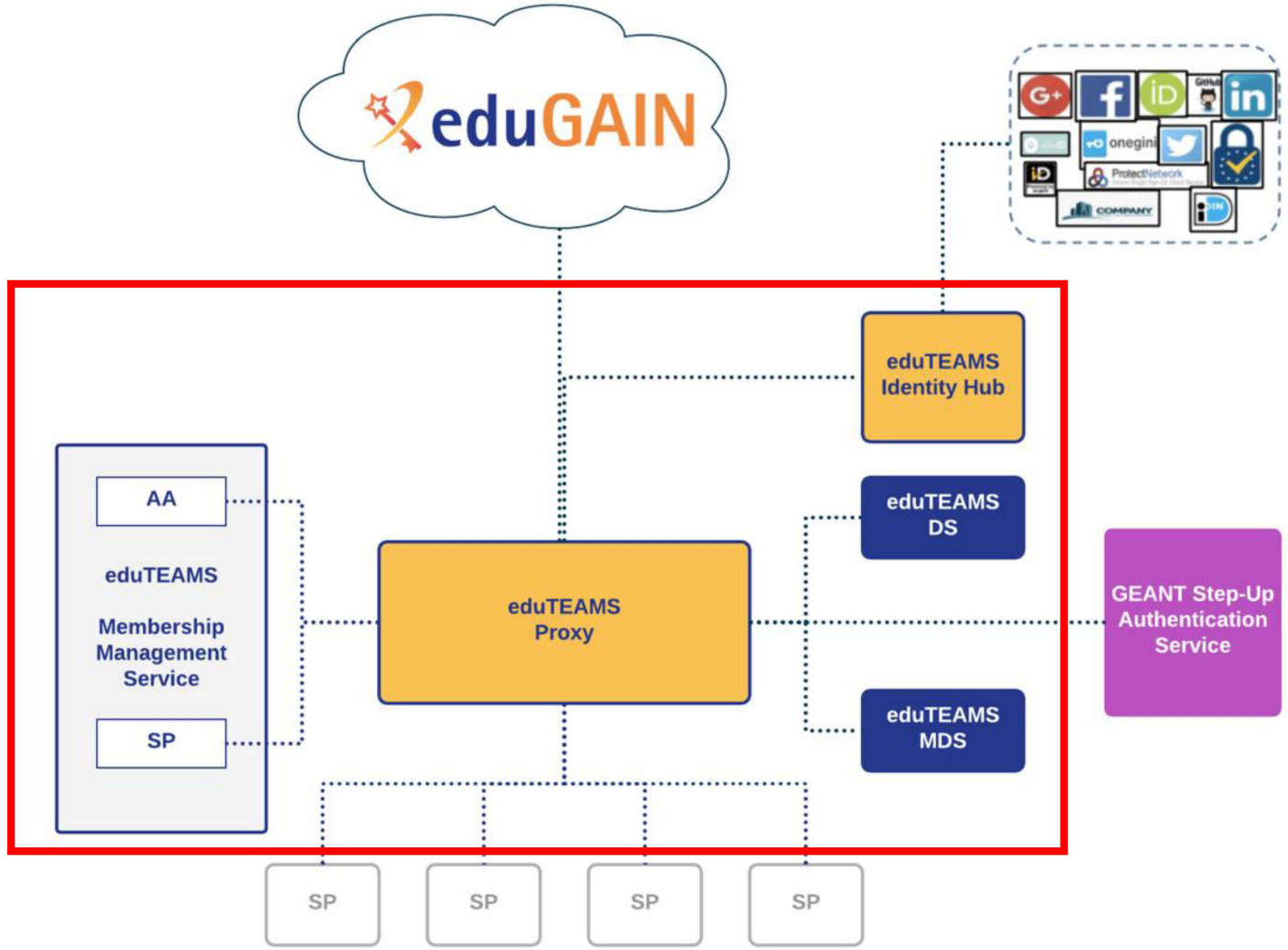
- Proxy & Identity Hub
- Membership Management service
- Discovery Service
- Metadata Service
- Second Factor Authentication (Pilot!)

Characteristics

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

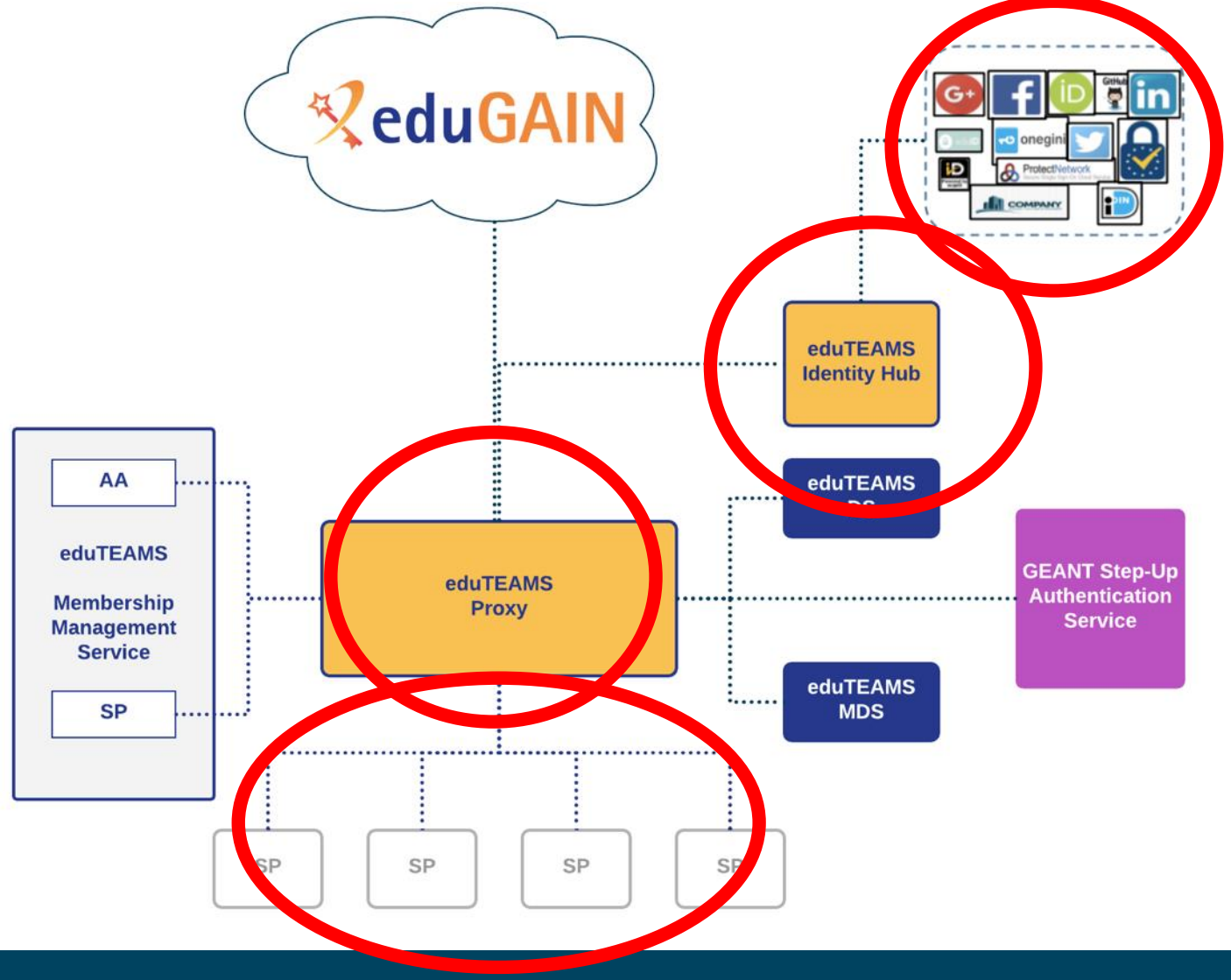
eduTEAMS for communities





eduTEAMS for communities

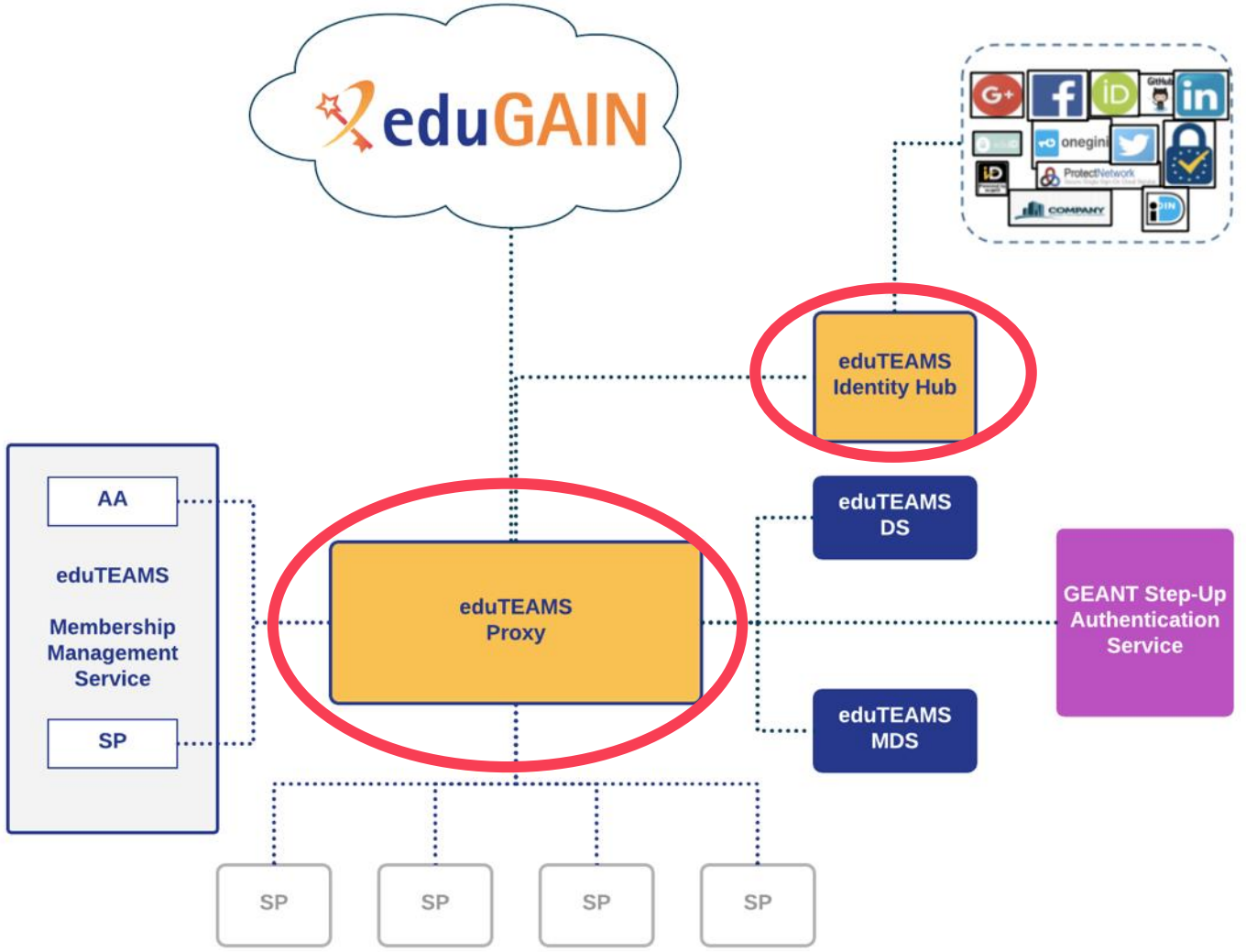
- Users sign in to services with their **community identity** via eduTEAMS
- Users **register once and access any service** (available to the their community)
- Reduces complexity for Service Providers by providing **one integration point for all services**
- **Integration with GÉANT, EOSC and other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



eduTEAMS for communities

Proxy & Identity Hub

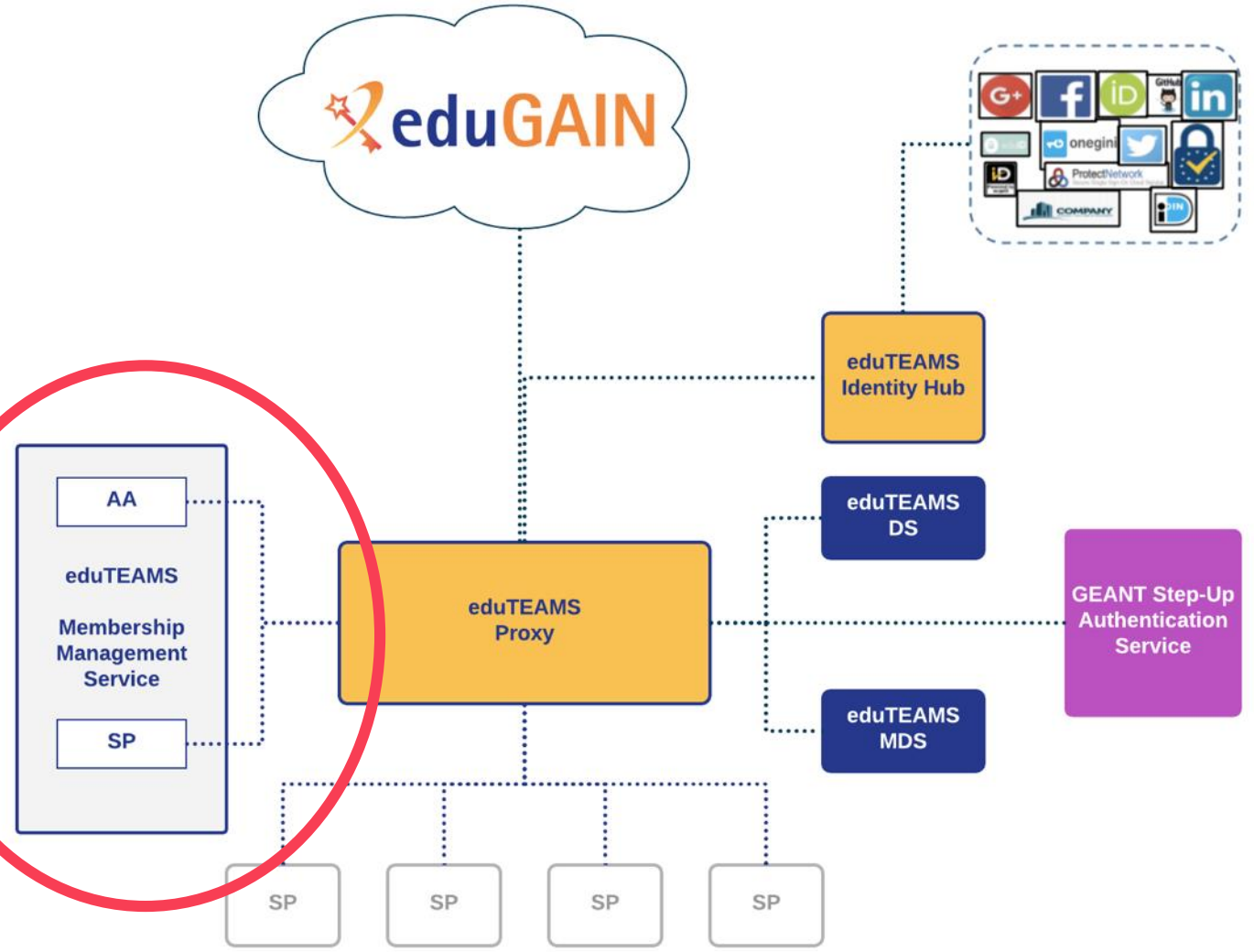
- Single **integration point for all SPs** (with support for both SAML and OIDC)
- **Attribute aggregation** from MMS
- Central **Policy Definition and Enforcement** point
- Support for **OIDC** Providers and non-eduGAIN **SAML** Identity Providers
- Supports **Research and Scholarship (R&S)** Entity Category



eduTEAMS for communities

Membership Management services

- VO specific **workflows for onboarding members**
- Registry for **user persistent Identifiers**
- Support for **R&S attributes** to maximize interoperability
- Use of **eduPersonEntitlement**(s) to express groups, roles and Service Entitlements
- Choice between **COmanage, HEXAA and Perun**



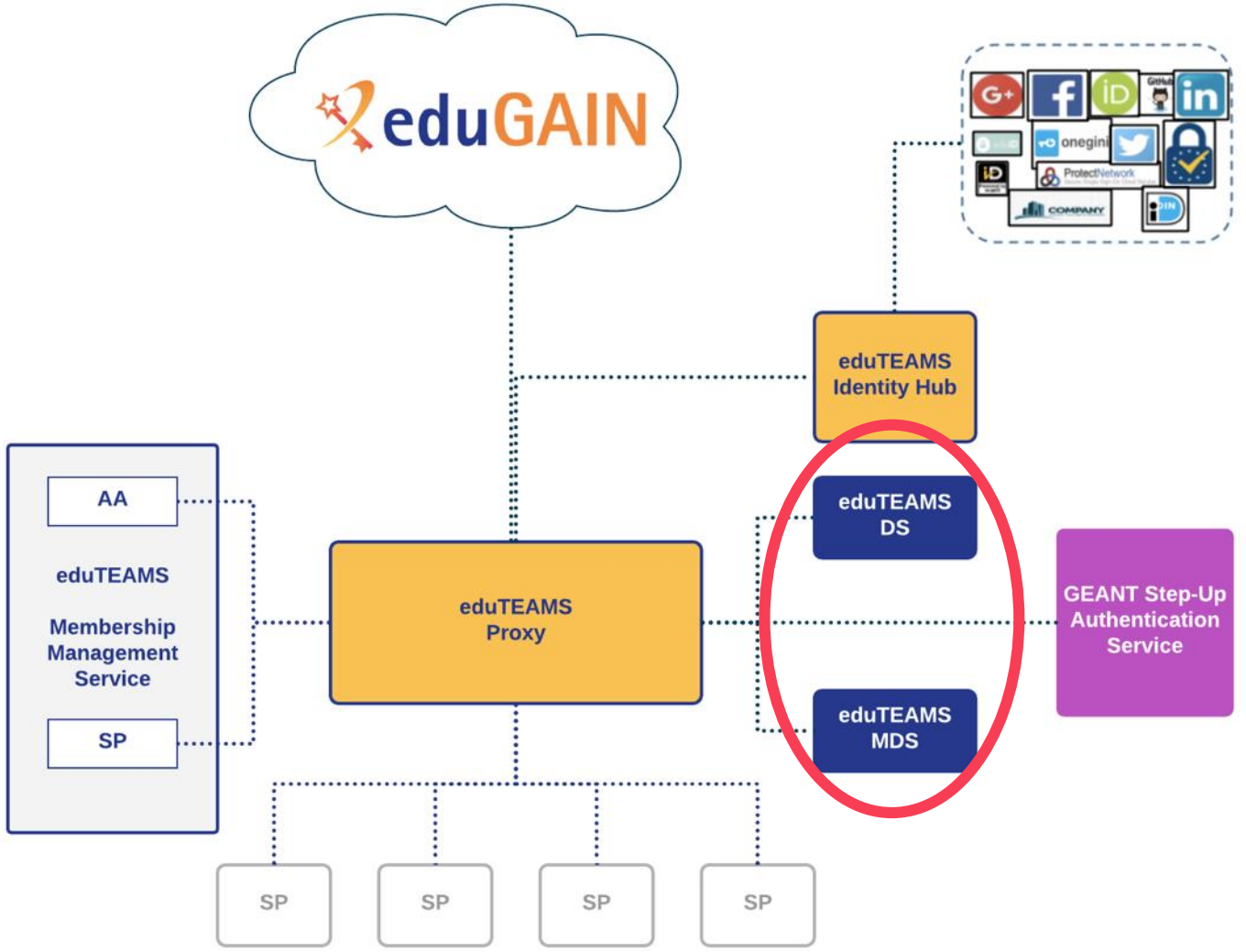
eduTEAMS for communities

Discovery Service

- Emphasis on **user friendliness** (implements RA21 guidelines)
- Integrates directly with the metadata service
- **Flexible import mechanism** for SAML entities (eduGAIN and non-eduGAIN)

Metadata Service

- Integrates directly with the eduTEAMS Proxy and the Discovery Service
- Single point of trust for all (SAML) metadata



eduTEAMS Service Offerings

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

eduTEAMS Service

eduTEAMS Dedicated Service

eduTEAMS Bespoke Service

eduTEAMS Service Offerings

- 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 defined
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Service

eduTEAMS dedicated Service

eduTEAMS bespoke Service

eduTEAMS Service Offerings

- Dedicated 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

eduTEAMS dedicated Service

eduTEAMS bespoke Service

eduTEAMS Service Offerings

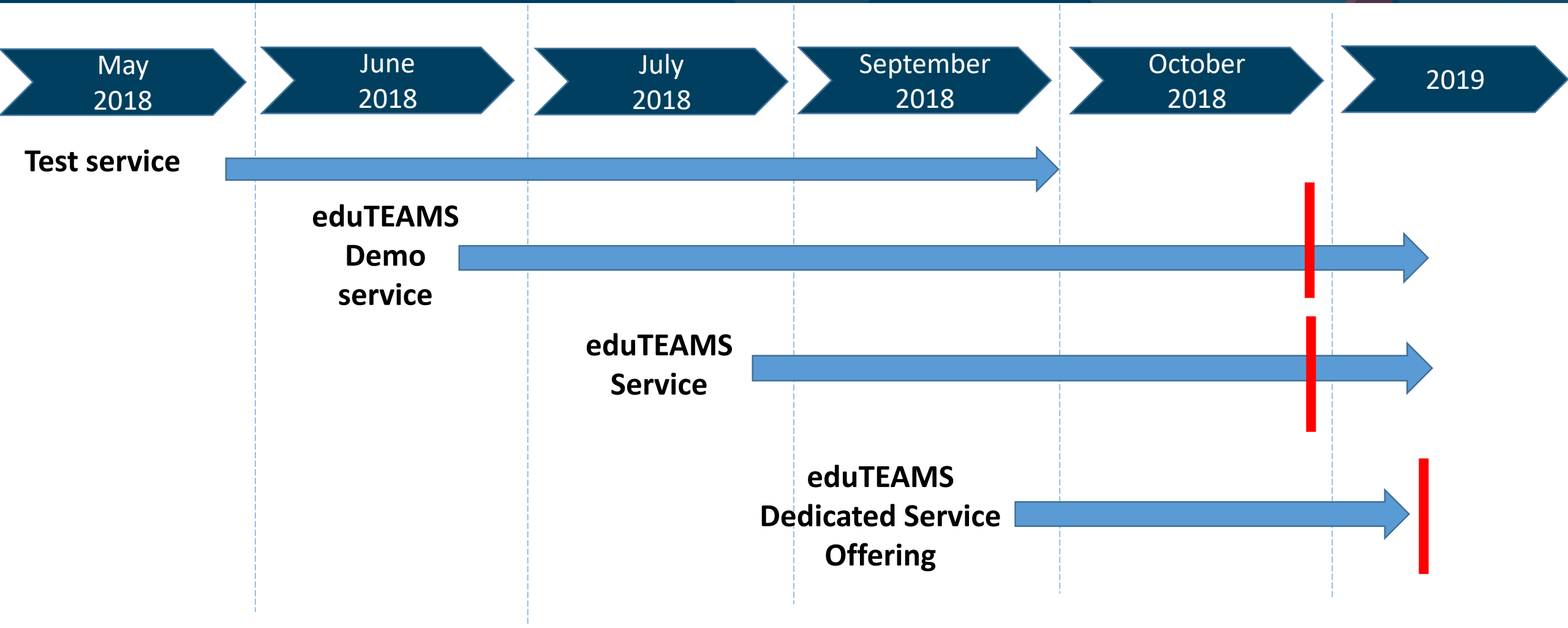
- Bespoke solution with tailor-made functionality
- Ownership model depended on the solution, operated by GÉANT
- Consultancy, development and hosting of the service.

eduTEAMS Service

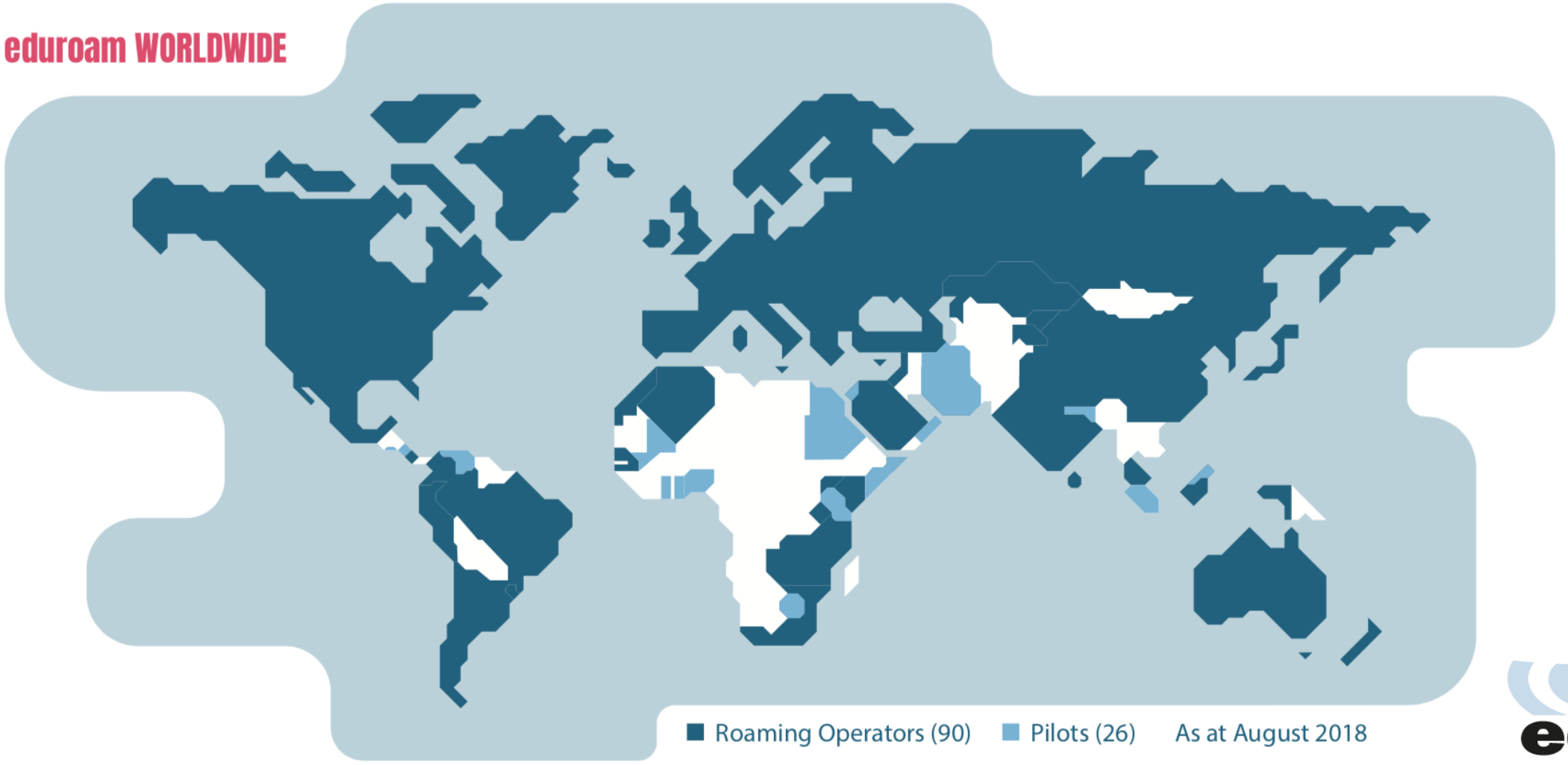
eduTEAMS dedicated Service

eduTEAMS bespoke Service

eduTEAMS for communities Roadmap



eduroam Managed IdP



eduroam Managed IdP

- Cloud based institutional eduroam IdP infrastructure
- Secure and Managed by experts from eduroam Operations Team
- High availability, professionally managed central infrastructure
- Controlled by the institution from a web browser

GÉANT
Networks • Services • People

eduVPN

Safe and trusted

Securing access for remote staff and students

eduVPN

helping to secure users and their data when online

PLUG AND PLAY

Users

Easy-to-use – no technical skills required for client installation.

Campus IT

No on-site HW or software required

PRIVACY BY DESIGN

Based on open standards and designed for authenticated private access. and secure browsing

SECURE BY DEFAULT

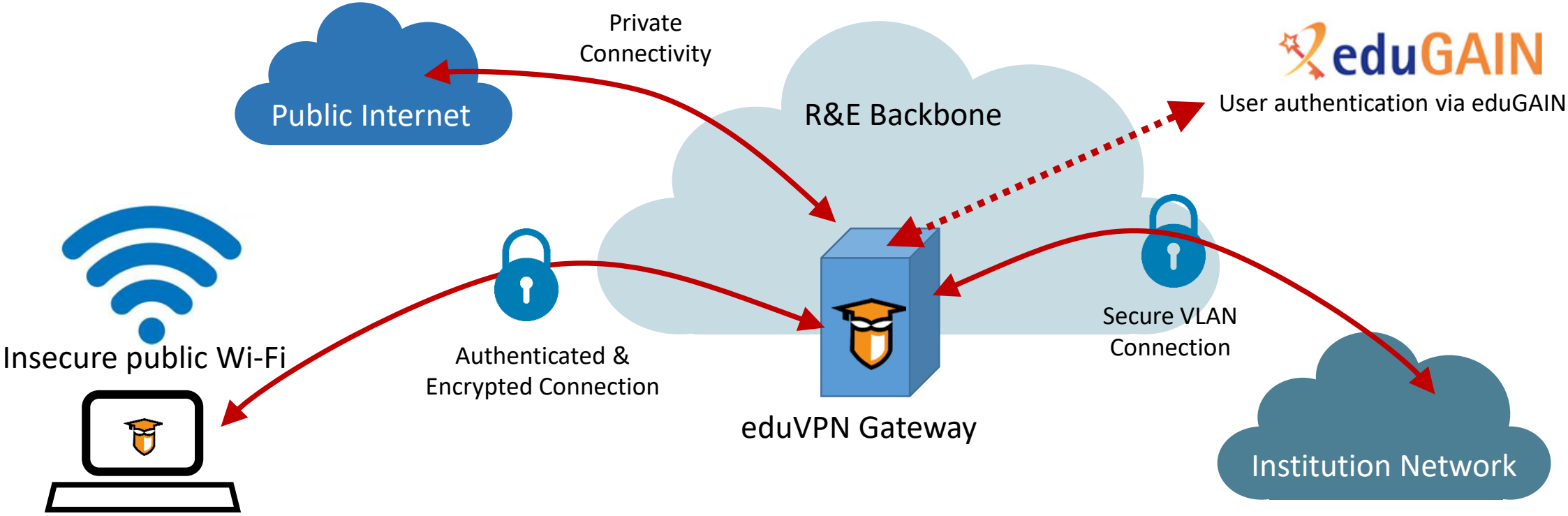
Enhances privacy of public Internet access

Provides end-to-end protection for remote staff and students

eduVPN

securing access for remote users

eduVPN provides easy-to-use client software and a secure gateway to authenticate users and encrypt data



eduVPN – Next Steps

The eduVPN project is looking for additional partner NRENs to work on the next phase

https://www.eduvpn.org

Thank you

Any questions?

vincenzo.capone@geant.org

@EnzinoCapone

www.geant.org

@GEANTnews

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov