GÉANT Trust & Identity services update

Vincenzo Capone

Head of Research Engagement and Support

MAGIC Meeting

Dallas, 14 November 2018
GÉANT supports and represents over 40 NRENs across Europe.
Together they support over 10,000 institutions and 50 million academic users.
eduGAIN ecosystem

edugain

SWITCHaa

AUSTRALIAN ACCESS FEDERATION

Colfire

The UK Access Management Federation

grnet

Tuakiri

GakuNin

MINGA

TAAT

AAI @ EduHr

R&G Education and Research

SIFULAN

FEIDE

Belnet

arnes

eduID

SIR

rencher

confia

DFN-AAI

Wayf

aconet

cafe

SID

arNATER

CONNECTEUR DE SAVOIRS

WAYF

Where are you from

arnes

eduID
eduTEAMS
AAI as a Service for communities

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

A service to enable use of federated identities in research communities

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

• Users sign in to services with their community identity via eduTEAMS

• Users register once and access any service (available to 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 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 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 Offerings

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

Test service

- May 2018
- June 2018
- July 2018
- September 2018
- October 2018
- 2019

eduTEAMS Demo service

- eduTEAMS Service

- eduTEAMS Dedicated Service Offering
Free secure Wifi provided by NRENs between campuses. A global network of users across 89 territories. More than 2 billion international authentications and counting. A worldwide success story. From its early beginnings as a joint venture between a few European universities to today—with millions of users in more than 89 territories worldwide, eduroam has been an amazing success story and an example of research and education collaboration. eduroam.org

eduroam Managed IdP

eduroam WORLDWIDE

Roaming Operators (90)  Pilots (26)  As at August 2018
eduroam Managed IdP

1. Cloud based institutional eduroam IdP infrastructure
2. Secure and Managed by experts from eduroam Operations Team
3. High availability, professionally managed central infrastructure
4. Controlled by the institution from a web browser
eduVPN
Safe and trusted
Securing access for remote staff and students
**Users**

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

**Campus IT**

No on-site HW or software required

---

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

**Secure by Default**

Enhances privacy of public Internet access

**Privacy by Design**

Provides end-to-end protection for remote staff and students
eduVPN provides easy-to-use client software and a secure gateway to authenticate users and encrypt data.
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