GÉANT Trust & Identity

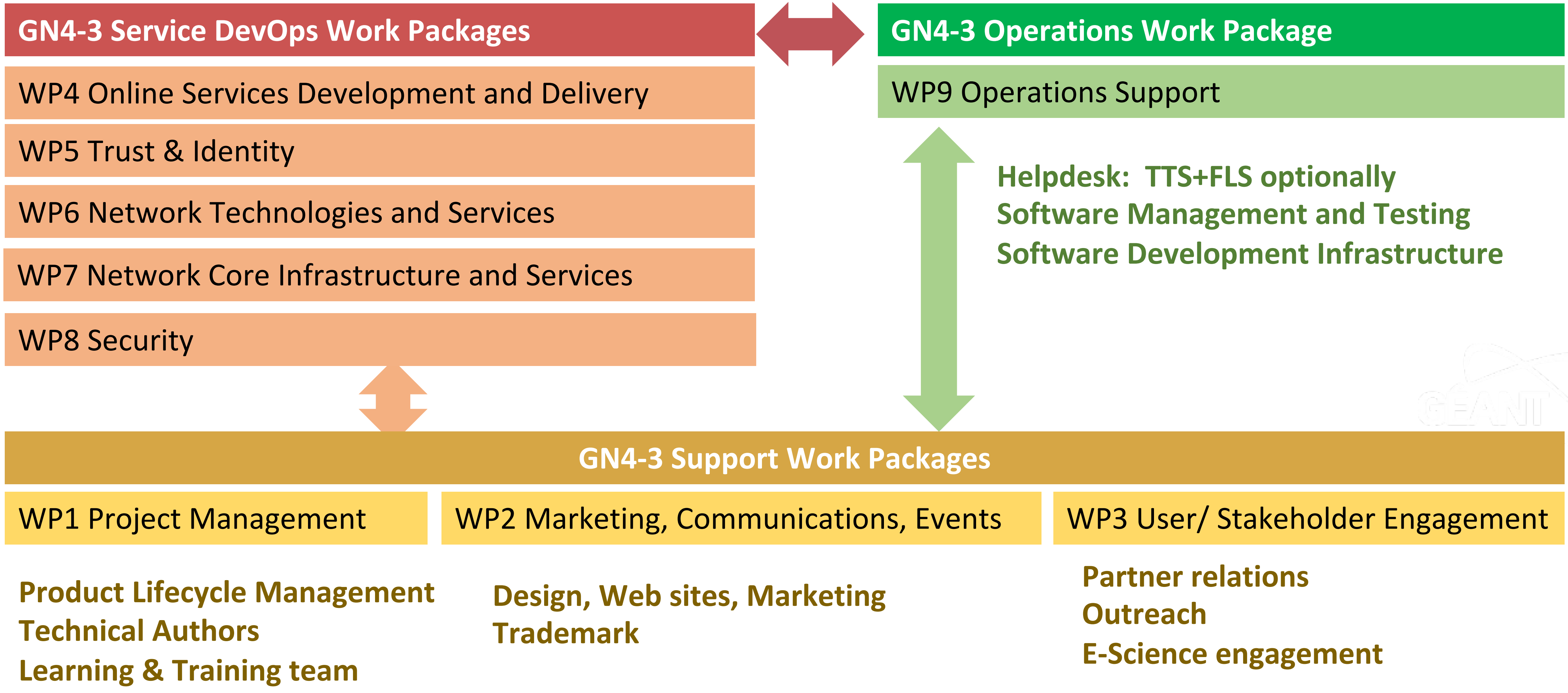
Overview for SIG-MSP

19th January 2021
Marina Adomeit, SUNET

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. 856728 (GN4-3).

Work Packages in GN4-3

GN4-3 : Jan 2019 – Dec 2022



GN4-3 Service DevOps Work Packages

- WP4 Online Services Development and Delivery
- WP5 Trust & Identity
- WP6 Network Technologies and Services
- WP7 Network Core Infrastructure and Services
- WP8 Security

GN4-3 Operations Work Package

- WP9 Operations Support

Helpdesk: TTS+FLS optionally
Software Management and Testing
Software Development Infrastructure

GN4-3 Support Work Packages

- WP1 Project Management
- WP2 Marketing, Communications, Events
- WP3 User/ Stakeholder Engagement

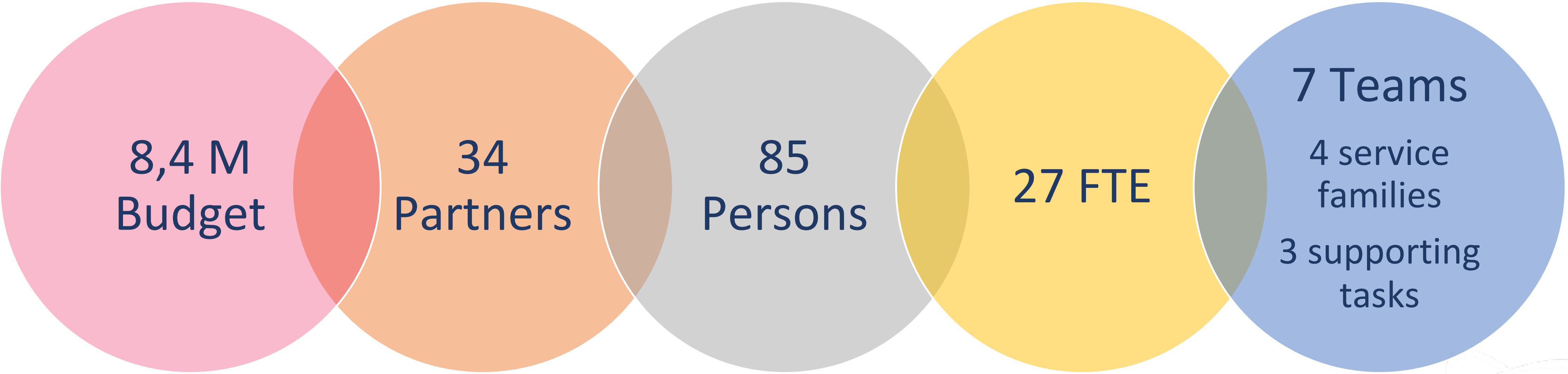
Product Lifecycle Management
Technical Authors
Learning & Training team

Design, Web sites, Marketing
Trademark

Partner relations
Outreach
E-Science engagement

The TEAM!

GÉANT
Networks • Services • People



8,4 M Budget

34 Partners

85 Persons

27 FTE

7 Teams

4 service families

3 supporting tasks

Partners

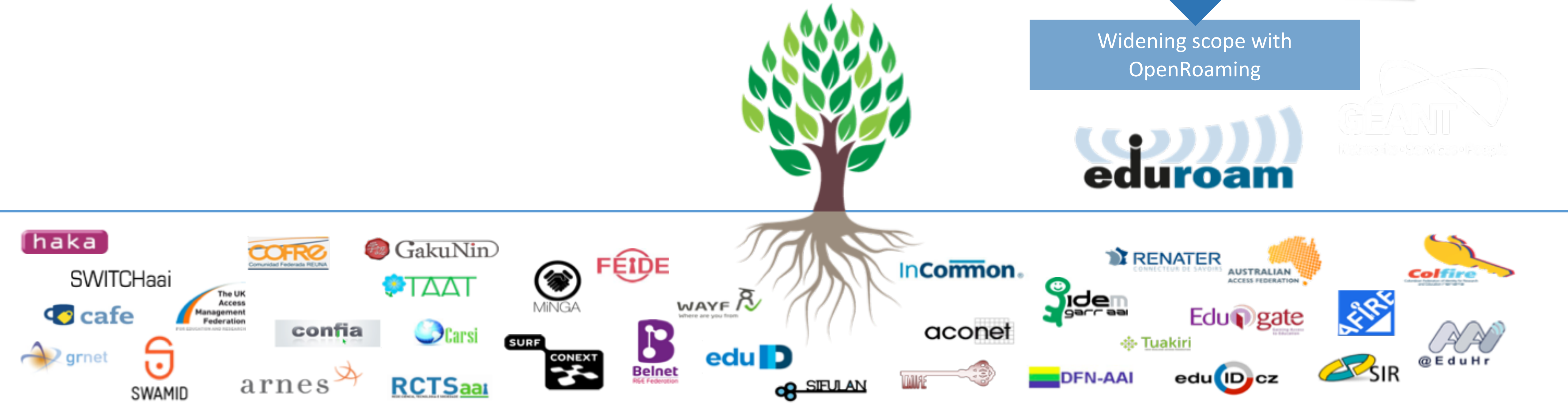
GÉANT, CARNet, RedIRIS, SURFNET, AMRES, CESNET, NORDUnet, Consortium GARR, Asnet AM, DFN, KIFÜ, MARNET, RENATER, grnet, PSNC, RASH, CSC, LitNET, RENAM, SWITCH, Jisc, DeiC, RESTENA, UNINETT, SUNET

T&I service portfolio

The big picture

T&I service portfolio

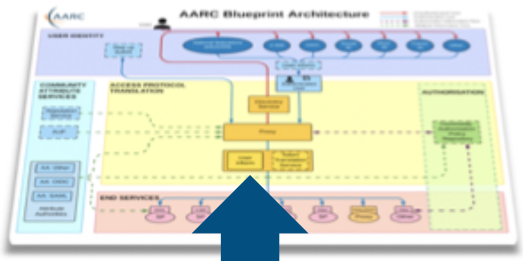
The big picture


Widening scope with OpenRoaming

T&I service portfolio

The big picture

eduTEAMS



Support virtual teams and share resources

InAcademia ONLINE STUDENT VALIDATION

Offering a validation service based on the "studentness"

Widening scope with OpenRoaming

eduGAIN

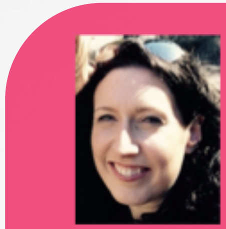
eduroam

haka · SWITCHaai · cafe · grnet · The UK Access Management Federation · SWAMID · COFRe · confia · arnes · GakuNin · TAAT · Carsi · RCTSaai · MiNGA · SURFCONEXT · FEIDE · Belnet · WAYF · eduID · SIFULAN · InCommon · aconet · idem garr aai · DFN-AAI · RENATER · AUSTRALIAN ACCESS FEDERATION · Tuakiri · Edugate · eduID.cz · AFIRE · SIR · Colfire · @EduHr

T&I Team and Key Collaborations

Expanding the reach of T&I to the broader community

T2 Incubator



InAcademia
Michelle Williams
GÉANT

eduTEAMS
Christos Kanellopoulos
GÉANT

eduGAIN
Davide Vaghetti
GARR

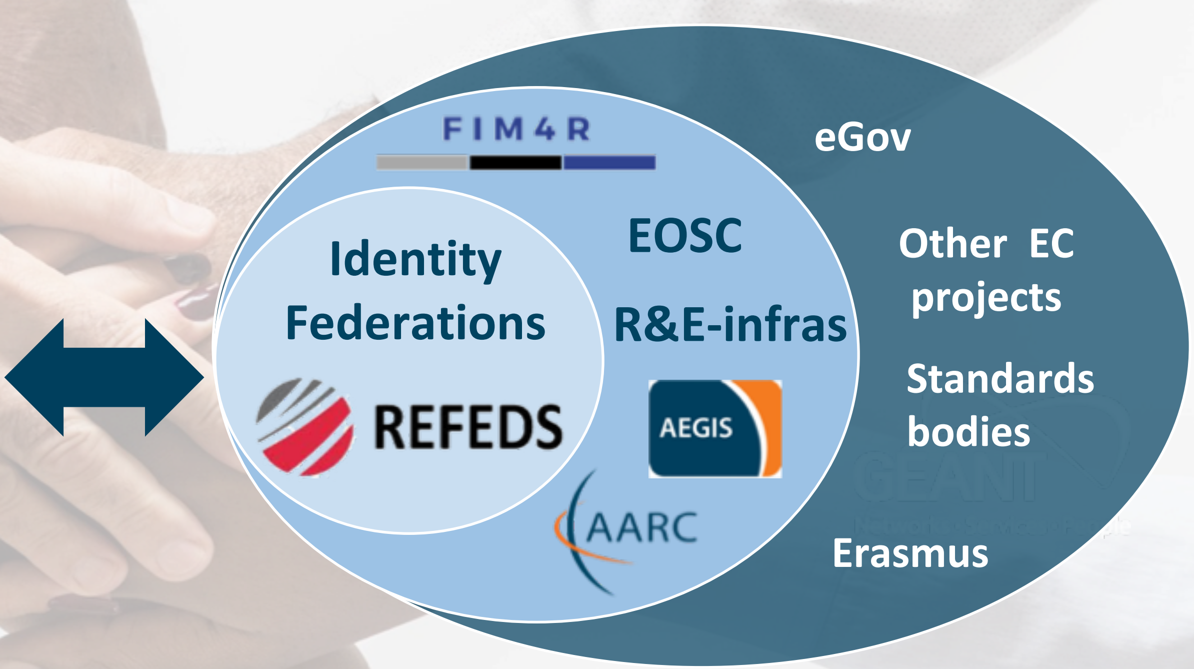
eduroam
Miroslav Milinović
CARNet/SRCE

T1 **T&I Services**

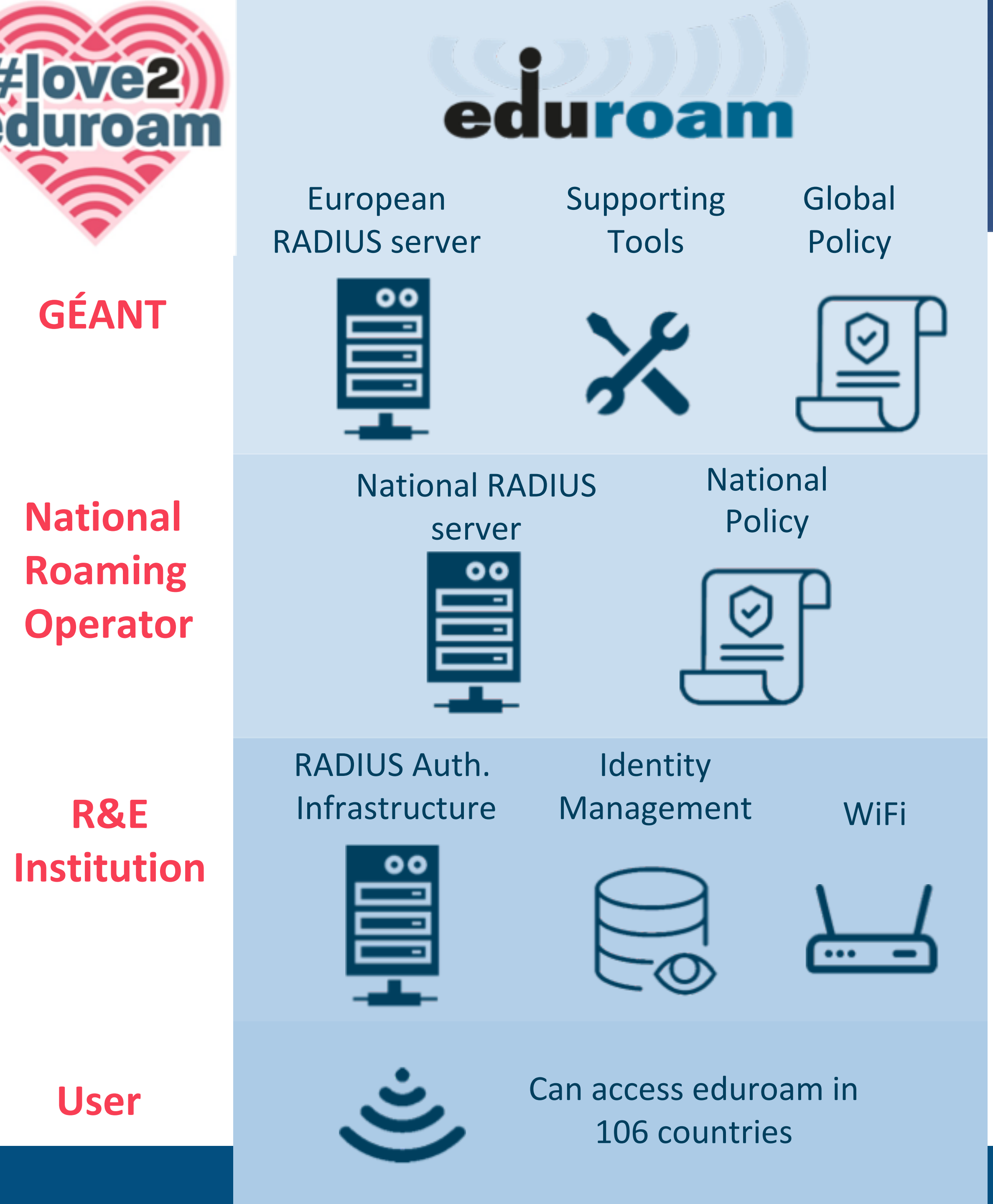
Enabling Communities

T4

T3 Operational Support



https://wiki.geant.org/display/gn43wp5/Trust+and+Identity+Services+Roadmaps



eduroam

GÉANT

European RADIUS server

Supporting Tools

Global Policy

National Roaming Operator

National RADIUS server

National Policy

R&E Institution

RADIUS Auth. Infrastructure

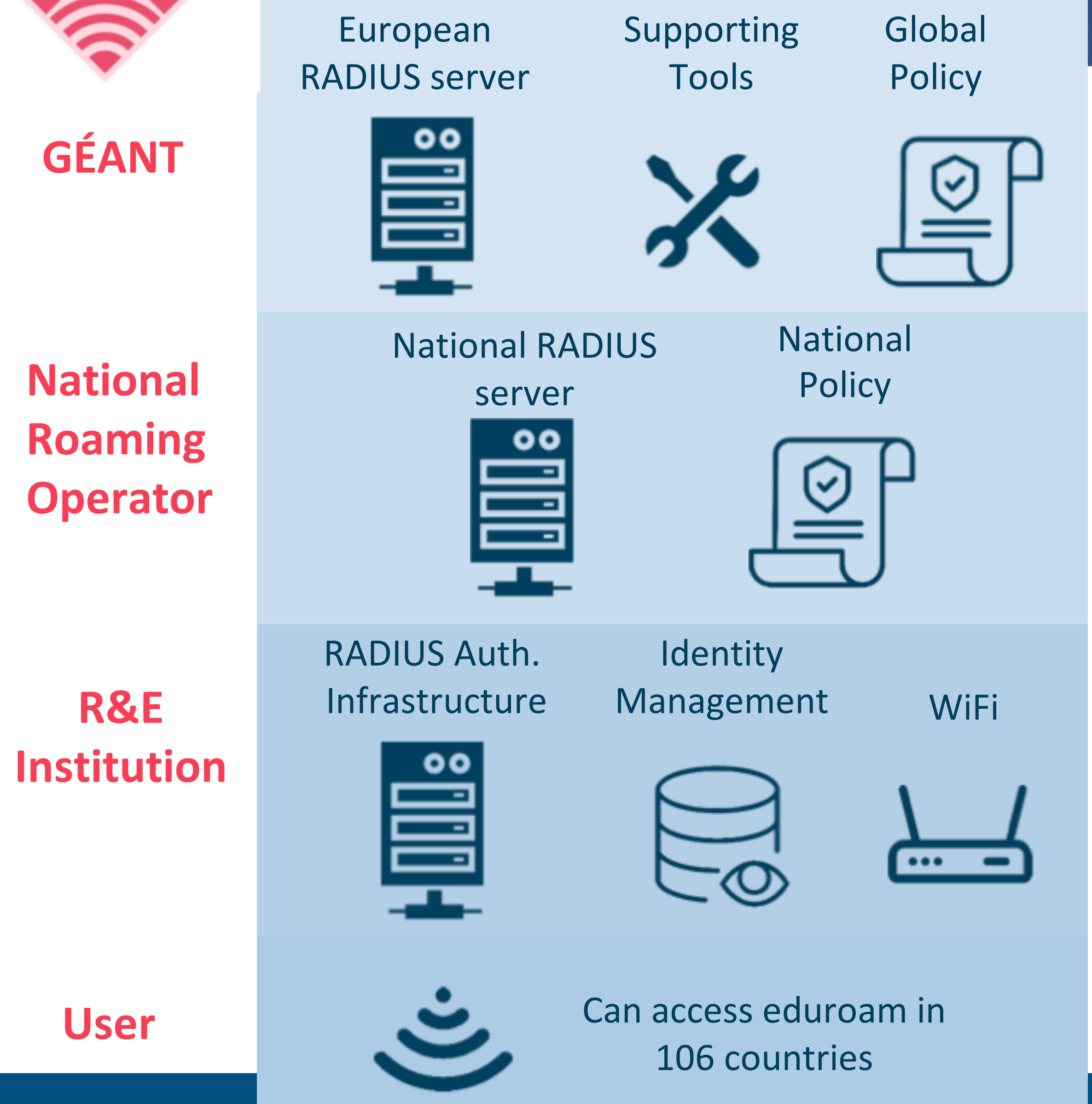
Identity Management

WiFi

User

Can access eduroam in 106 countries

Access to thousands of eduroam WiFi locations worldwide, with R&E institutional identity



GÉANT

European RADIUS server

Supporting Tools

Global Policy

National Roaming Operator

National RADIUS server

National Policy

R&E Institution

RADIUS Auth. Infrastructure

Identity Management

WiFi

User

Can access eduroam in 106 countries

Access to thousands of eduroam WiFi locations worldwide, with R&E institutional identity

Operation of Core Service Elements

- European top-level RADIUS server in Netherlands
- European top-level RADIUS server in Denmark

Operation of Support Service Elements

- Monitoring, diagnostics and metering tools: monitor.eduroam.org
- Database: monitor.eduroam.org/db_web/
- Configuration Assistant Tool: cat.eduroam.org
- eduroam Managed IdP: hosted.eduroam.org

Support and Community

- Main site: www.eduroam.org
- Wiki pages: wiki.eduroam.org
- L1 support : help@eduroam.org
- L2 support in various channels
- Participation to the GeGC
- Steering Group chairing

Standardisation bodies

- Open Roaming (WBA)
- WiFi Alliance
- Internet Engineering Task Force (IETF)

eduroam

Focus on activities

Managed eduroam IdP launch

Delivered Managed eduroam SP prototype

geteduroam pilot

eduroam database v2.0 implemented

Tools adaptation started after critical adoption reached

Development of eduroam audits in progress

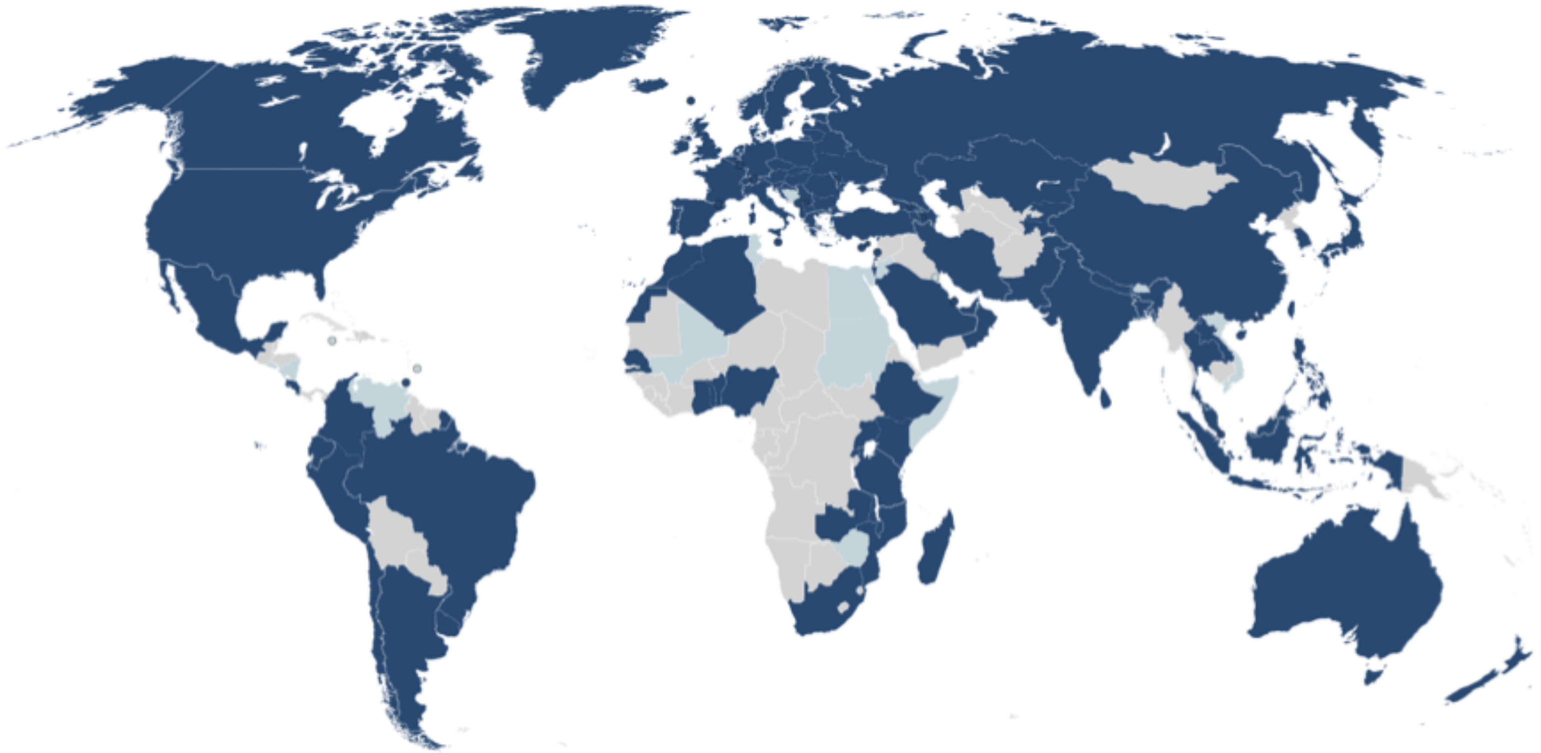
Regular releases of CAT

eduroam policy change in progress

OpenRoaming™ WIRELESS BROADBAND ALLIANCE

WBA Integrator Participant

Service uptake – National Roaming Operators (NROs)



106

Countries

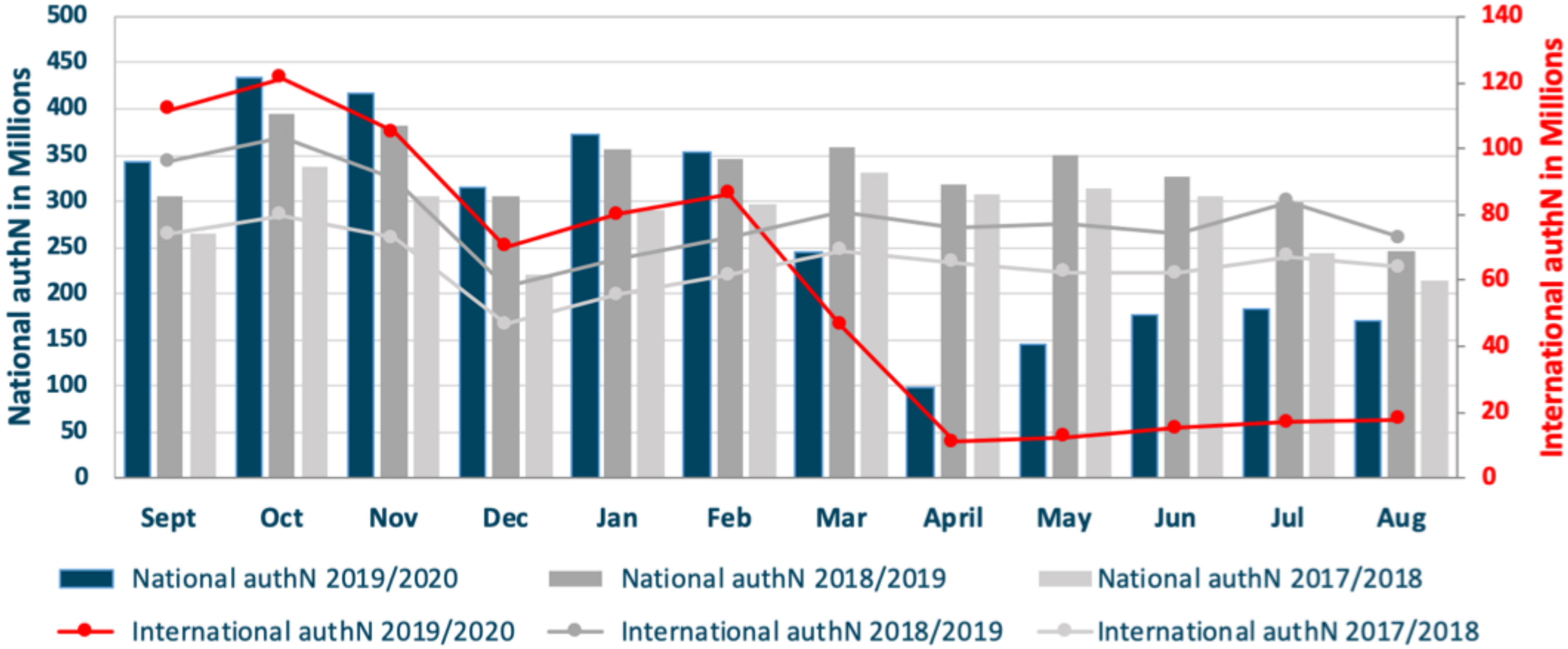
6000+

Institutions

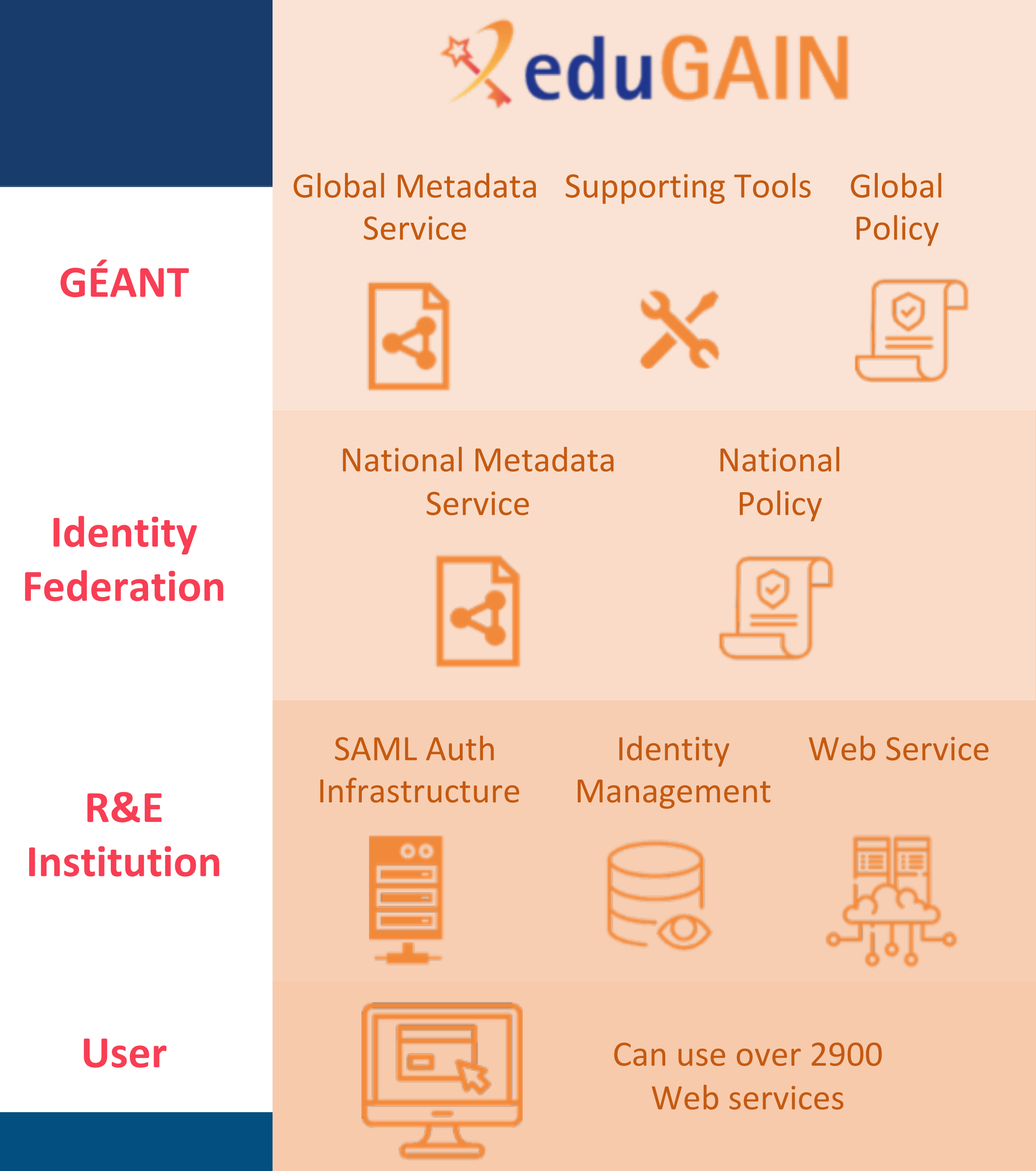
28,000+

Service Locations

Service uptake – number of user authentications



Fall of traffic during COVID-19 lockdowns



eduGAIN

GÉANT

Global Metadata Service

Supporting Tools

Global Policy

Identity Federation

National Metadata Service

National Policy

R&E Institution

SAML Auth Infrastructure

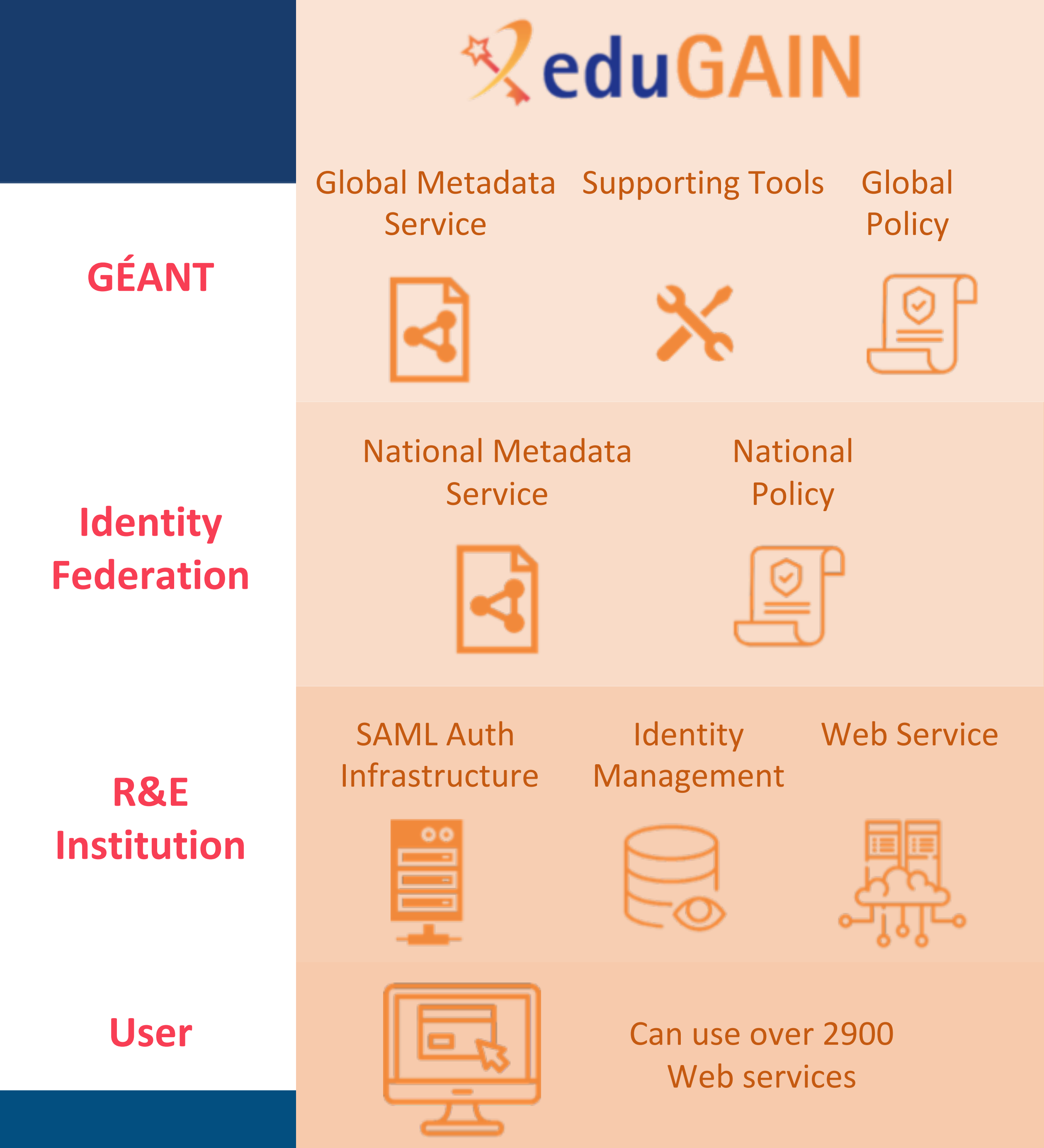
Identity Management

Web Service

User

Can use over 2900 Web services

Access to thousands of WebSSO services available via eduGAIN, with R&E institutional identity



GÉANT Networks · Services · People

Access to thousands of WebSSO services available via eduGAIN, with R&E institutional identity

Operation of Core Service Elements

- Metadata Service (MDS): mds.edugain.org
- Metadata Validator: validator.edugain.org

Operation of Support Service Elements

- Technical site: technical.edugain.org
- Entities database: technical.edugain.org/entities
- Federation as a Service

Support and Community

- Main site: edugain.org
- Wiki pages: wiki.edugain.org
- Support contact: support@edugain.org
- Security contact: abuse@edugain.org

Collaboration

- REFEDS
- FIM4R
- Seamless access

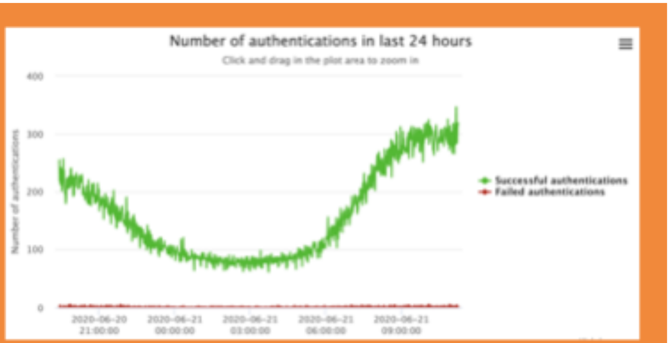
eduGAIN

Focus on activities

eduGAIN metering

Started business pilot

Success depends on federation adoption



f-ticks.edugain.org

eduGAIN signing strategy

Certificate with the signing key close to expiry

Short-term strategy for certificate renewal defined and executed

Long-term strategy to change and straighten the signing key defined

eduGAIN support team – in GN4-3 period 1

193 tickets resolved

60 errors resolved by proactive support

Training and Outreach

ASREN training material

eduGAIN security team

Established team

Security response procedure developed with SIRTFI WG

edugain.org/edugain-security

eduGAIN operations

Metadata aggregation practice statement published

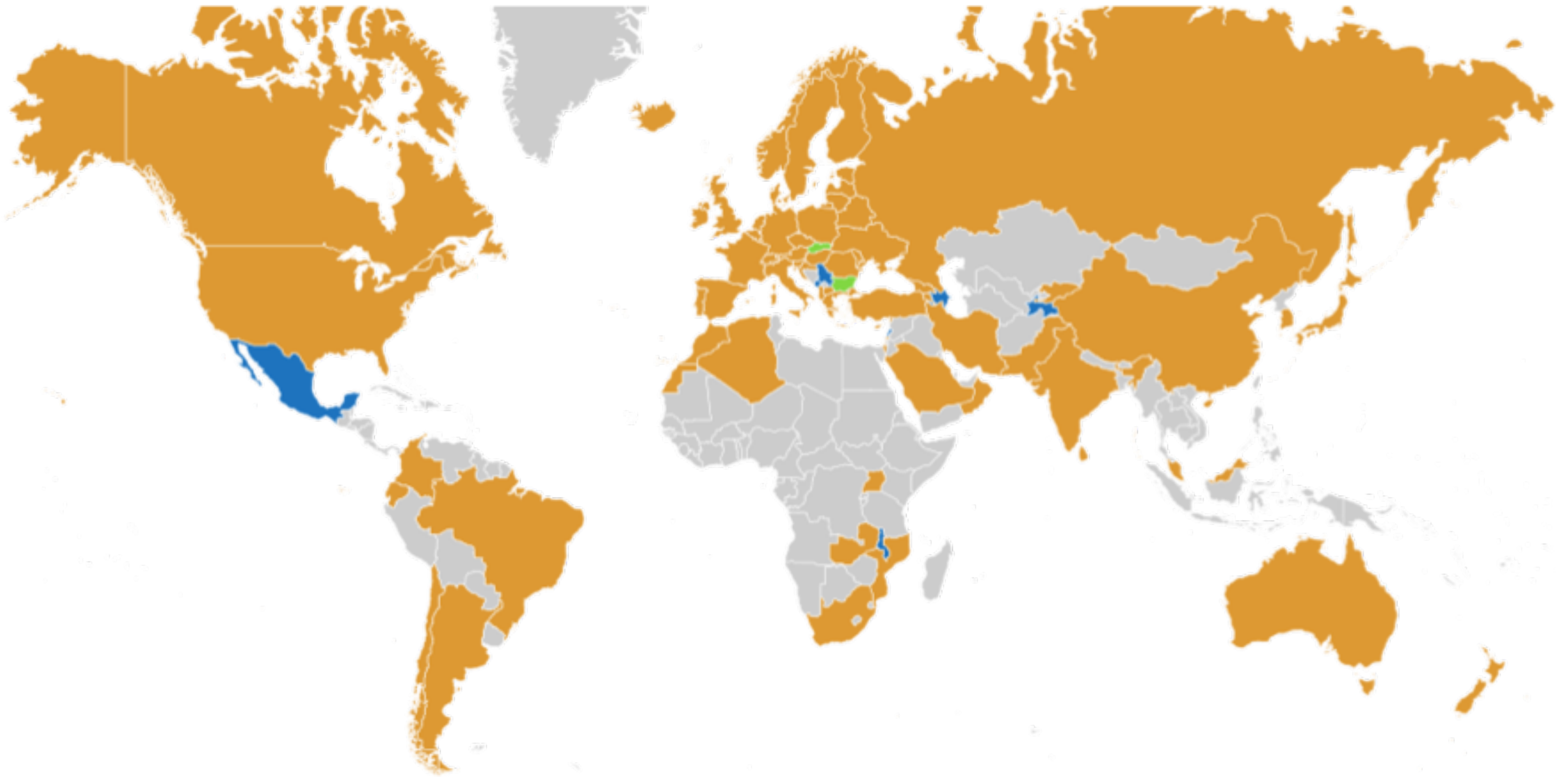
Operational Practice Statement published

Periodical updates to the MDS and introduced versioning of metadata feeds

eduGAIN

Service uptake – Identity Federations

GÉANT Networks · Services · People



71

Identity Federations

4127

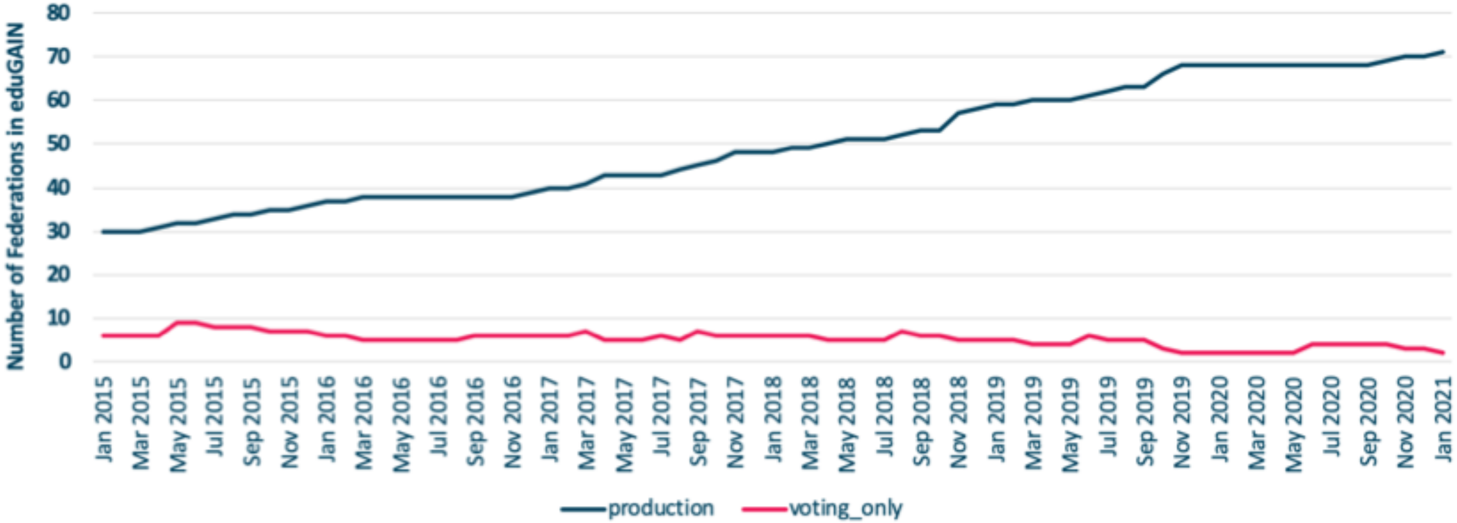
Identity Providers

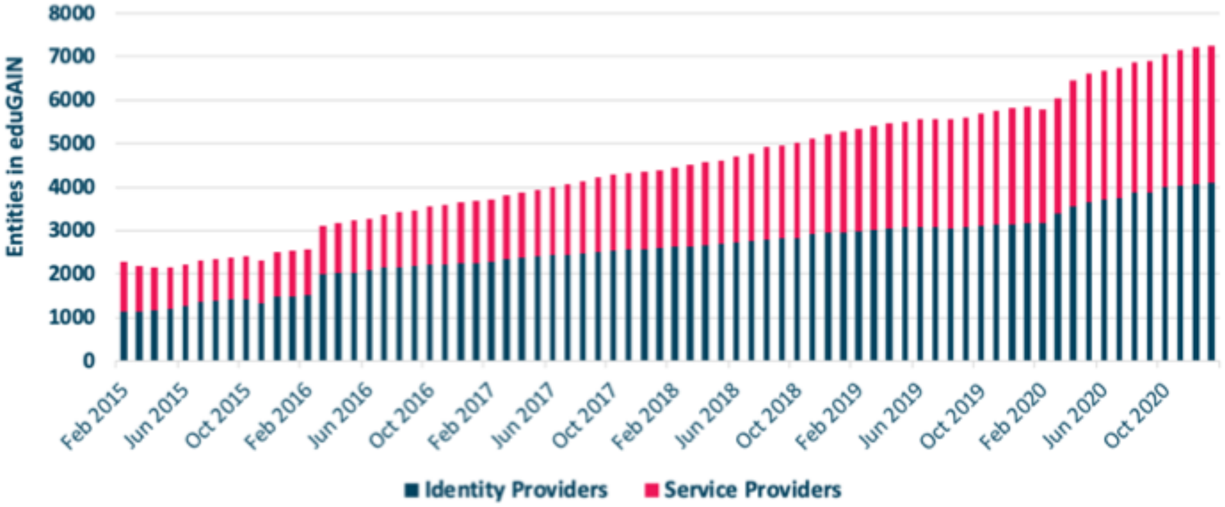
3164

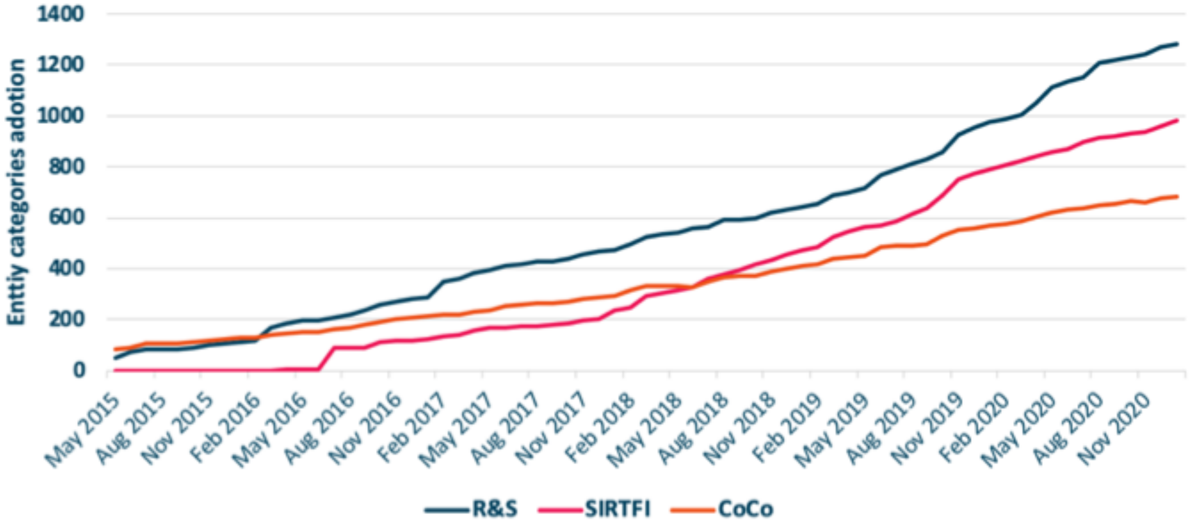
Service Providers

eduGAIN

Service uptake – number of identity federations







3600+ IdPs in eduGAIN

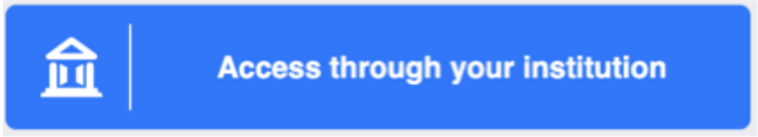
Challenge to properly implement IdP discovery

Many SPs, such as publishers, still rely on IP-based authorisation

3600+ IdPs in eduGAIN

Challenge to properly implement IdP discovery

Many SPs, such as publishers, still rely on IP-based authorisation



1 SA Button

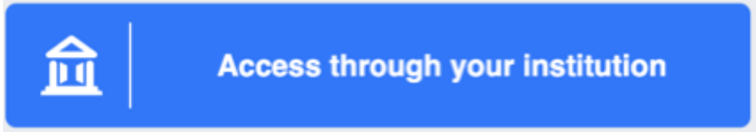
UX experts proven design

Retains user’s IdP choice and presents it next time

Privacy by design

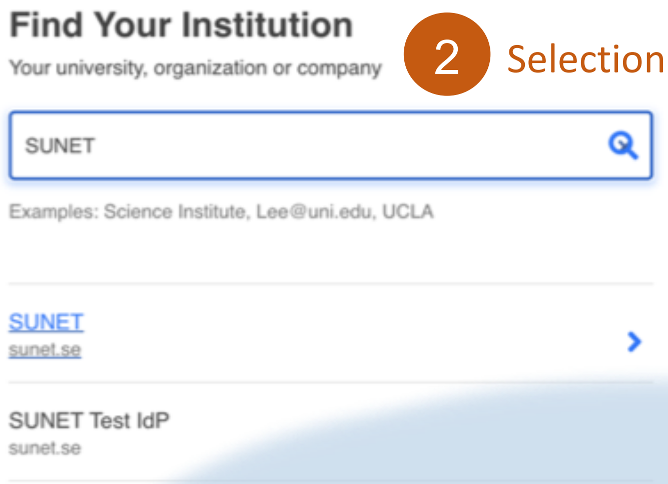
eduGAIN *SeamlessAccess*

- 3600+ IdPs in eduGAIN
- Challenge to properly implement IdP discovery
- Many SPs, such as publishers, still rely on IP-based authorisation



Access through your institution

1 SA Button



Find Your Institution

Your university, organization or company

SUNET

Examples: Science Institute, Lee@uni.edu, UCLA

SUNET
sunet.se

SUNET Test IdP
sunet.se

2 Selection of IdP

UX experts proven design

Retains user’s IdP choice and presents it next time

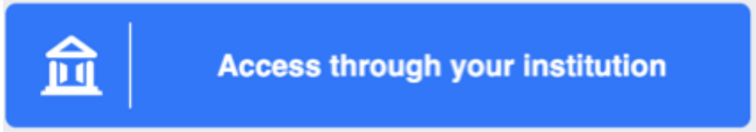
Privacy by design

eduGAIN
SeamlessAccess

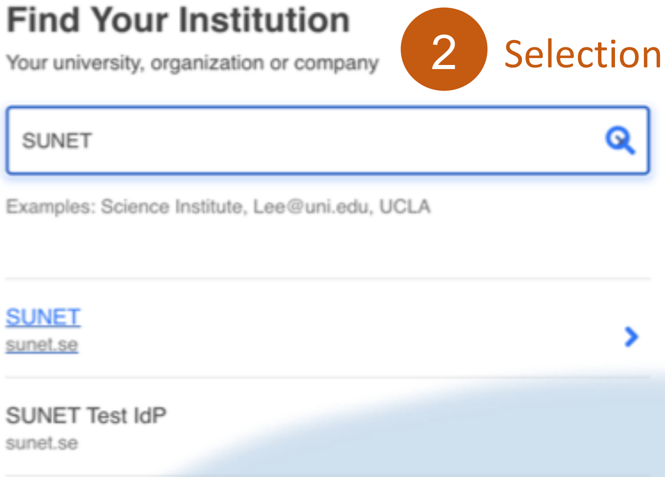
3600+ IdPs in eduGAIN

Challenge to properly implement IdP discovery

Many SPs, such as publishers, still rely on IP-based authorisation


Access through your institution

1 SA Button


Find Your Institution

Your university, organization or company

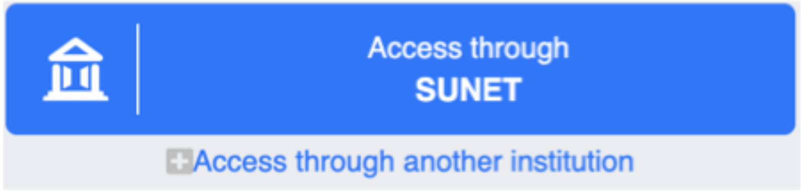
SUNET

Examples: Science Institute, Lee@uni.edu, UCLA

SUNET
sunet.se

SUNET Test IdP
sunet.se

2 Selection of IdP


Access through
SUNET

Access through another institution

3 IdP Selection
saved in SA button

UX experts
proven design

Retains user's IdP
choice and presents it
next time

Privacy by
design

eduGAIN

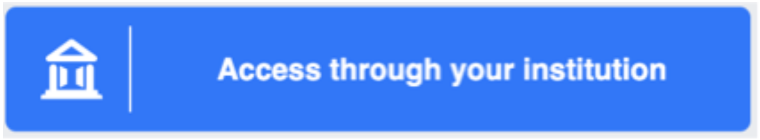
SeamlessAccess

SeamlessAccess.org GÉANT Networks · Services · People

3600+ IdPs in eduGAIN

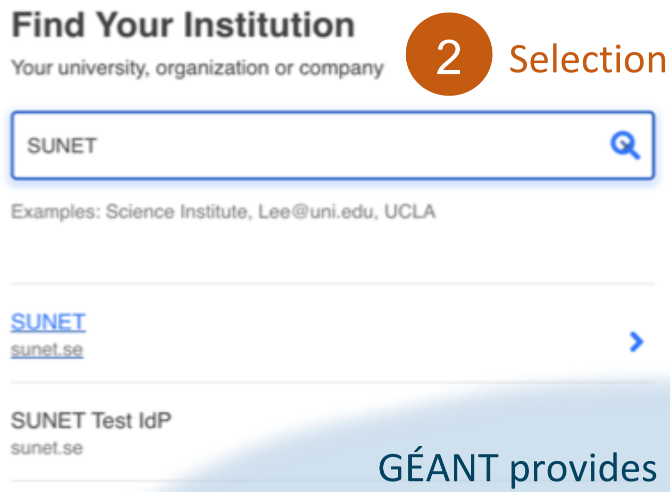
Challenge to properly implement IdP discovery

Many SPs, such as publishers, still rely on IP-based authorisation



Access through your institution

1 SA Button



Find Your Institution

Your university, organization or company

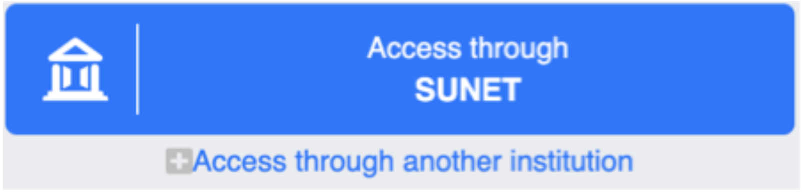
SUNET

Examples: Science Institute, Lee@uni.edu, UCLA

SUNET
sunet.se

SUNET Test IdP
sunet.se

2 Selection of IdP



Access through
SUNET

Access through another institution

3 IdP Selection saved in SA button

UX experts proven design

Retains user's IdP choice and presents it next time

Privacy by design

Delivered via coalition: NISO, Internet2, GÉANT and STM

GÉANT provides beta service operations

Robust infrastructure for mission critical service

Beta service since July 2019

Delivered production grade service

eduTEAMS

GÉANT
Networks • Services • People

GÉANT

AAIaaS

Research collaborations or NRENs

Manages groups

Connects services

Manages access

Users

Federated access to research resources

Implements AARC Blueprint Architecture and expands eduGAIN to support virtual teams to share resources

eduTEAMS *Service Offerings*

eduTEAMS Service

- Shared platform that can be used by small- to medium-size communities and the long tail of science
- Managed and operated by GÉANT
- eduTEAMS branding
- eduTEAMS service policies
- Connected to EOSC
- Onboarding of community-specific services

eduTEAMS Dedicated

- Dedicated, white-label service offering, specific to a community
- Managed by the community, operated by GÈANT
- Community branding and customisation
- Community managed policies
- Can be connected to EOSC
- Onboarding of community specific services

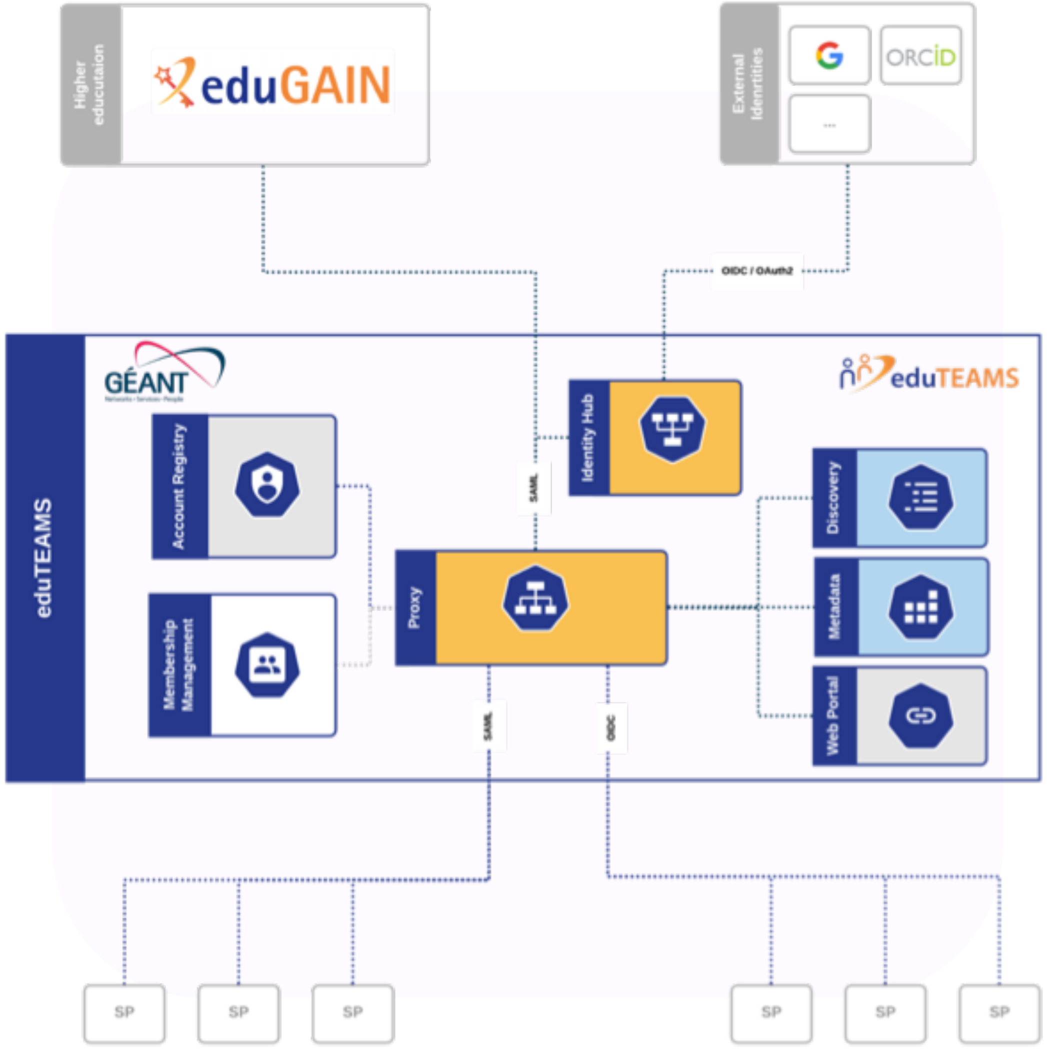
eduTEAMS Bespoke

- For communities that need tailor-made functionalities (i.e. integration with other tools)
- Ownership model depended on the solution, operated by GÉANT
- Consultancy and development as needed

eduTEAMS

Managing virtual teams made easy

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**

Deployments and Achievements

eduTEAMS Service	Production
FENIX Research Infrastructure	Production
PaNOSC (UmbrellaID)	Production
RedIRIS | NextGEOSS	Production
VESPA (EuroPlanet)	Production
LAGO	Production
SURF Research Access Management	Production
EOSC Life	Transition to Production
GN4-3	Implementation
EUROFusion	Implementation
OCRE	Implementation
ARCHIVER	Implementation

eduTEAMS one of the components of EOSC AAI

eduTEAMS technology underpins AAI for Student mobility

eduTEAMS solution for HPC community

InAcademia ONLINE STUDENT VALIDATION

GÉANT

SaaS to validate "studentess"

Community Governed

Merchants

OIDC Auth Infrastructure

Student tailored offerings

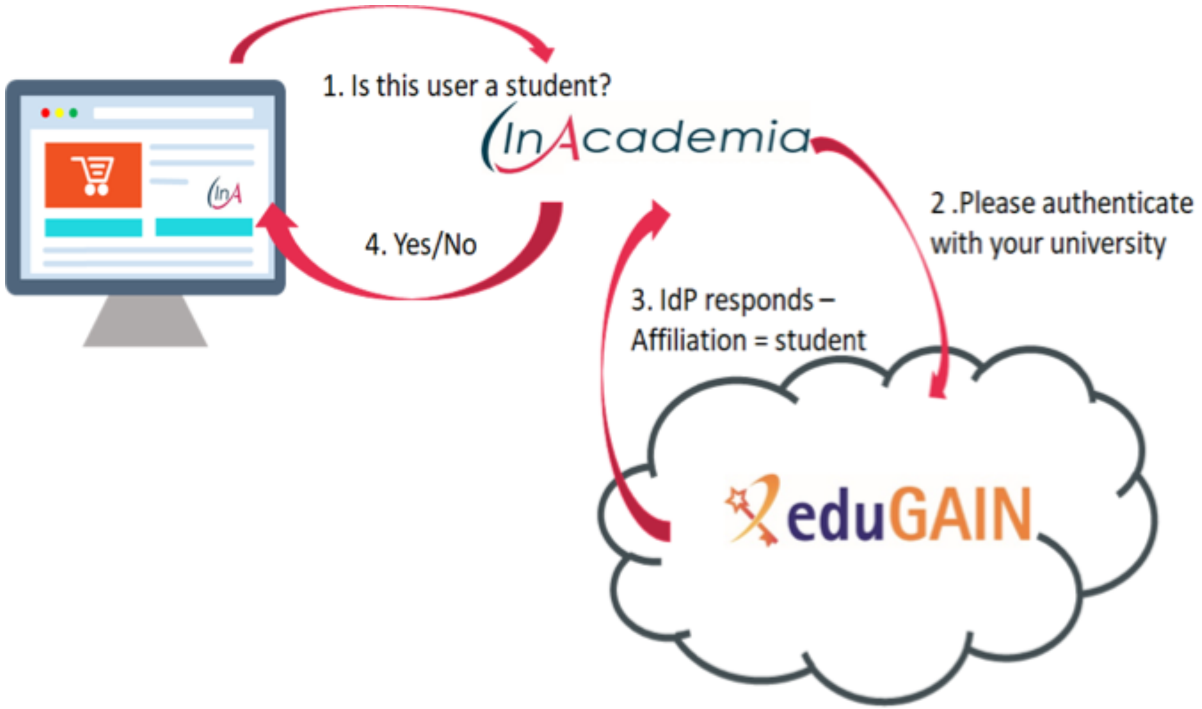
Students

Can make use of student tailored offerings, without disclosing any additional privacy details

The real-time, digital equivalent of asking a student to show their student card to access or buy discounted or specialist services and products

InAcademia
ONLINE STUDENT VALIDATION

Adding value to identity federations


1. Is this user a student?
InAcademia
2 .Please authenticate with your university
3. IdP responds – Affiliation = student
4. Yes/No
eduGAIN
InA

Reduces burden for IdPs and identity federations

Support and connect merchants

Lighter-weight option for service providers (SPs)

Quick, reliable and secure way to verify academic identities

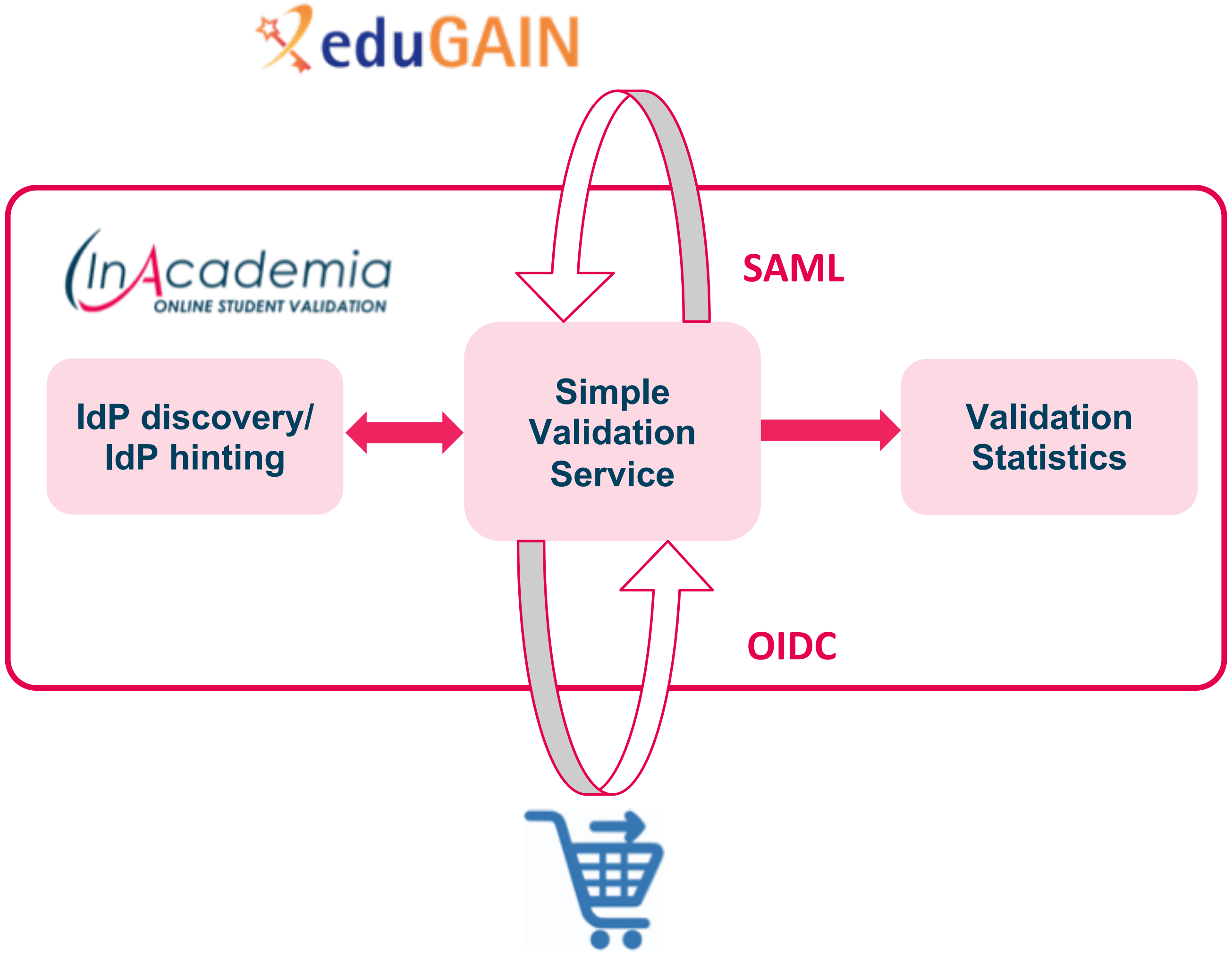
Source of income for T&I

Designed to support Identity Federations and eduGAIN to achieve sustainability

Privacy by design to protect end users

Helps with GDPR compliance

Validating students made easier


eduGAIN
InAcademia ONLINE STUDENT VALIDATION
SAML
IdP discovery/ IdP hinting
Simple Validation Service
Validation Statistics
OIDC

- Merchant integrates validation as part of its process (typically during check out)
- One integration point for all eduGAIN IdPs
- Users validates affiliation to academia in the same way they use their federated identity
- Service infrastructure designed to be highly available
- Collect statistics that are necessary for invoicing model

InAcademia
ONLINE STUDENT VALIDATION

Production service

GÉANT
Networks • Services • People

- Production service since February 2020 - over 200.000 validations
- Two service editions: 'Commercial' and 'Community'
    - Same governance and operational infrastructure
    - Two different models: paid and free to use
    - [Defined eligibility criteria and service Constitution]()

- Designed to be promoted in collaboration with national identity federations and NREN outreach/marcomms teams
- Actively participating federations - Netherlands, Germany, Denmark, Spain, Sweden, France
- Steering Committee composed of participating federation, meets quarterly to discuss strategy

Contact info@inacademia.org to get your federation involved!

%STUDENTEN RABATT.COM

KB national library of the netherlands

SheerID

Team and work organisation

TRUST & IDENTITY INCUBATOR

Develop, foster & mature new ideas in technical & business case development or enhancement to data protection and privacy

Core teams (alfa and beta) with a scrum master and developers
Mentors (one per topic)
Main incubator board (community provided)

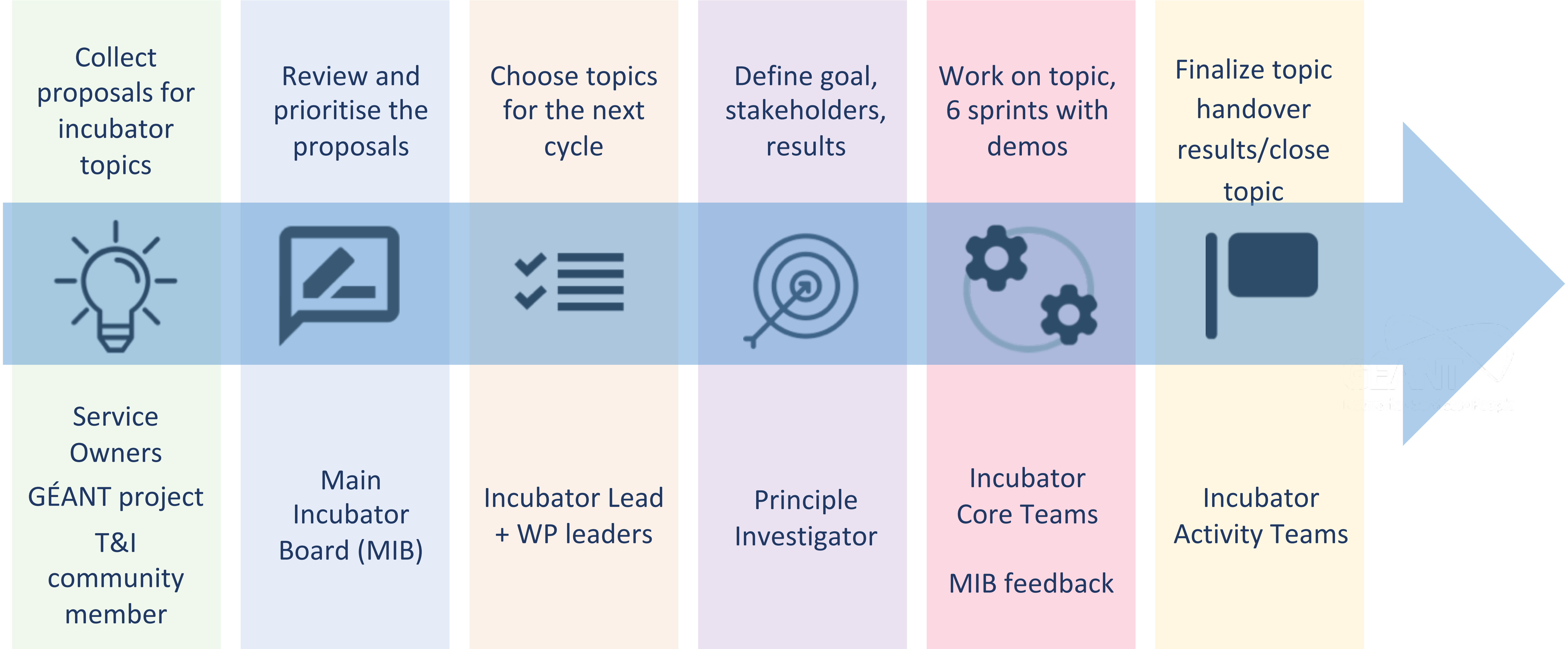
Ongoing activities in parallel
6 sprints
Monthly sprints
Sprint demos (open to all)

https://wiki.geant.org/display/gn43wp5/T2+-+Trust+and+Identity+Incubator

TRUST & IDENTITY INCUBATOR

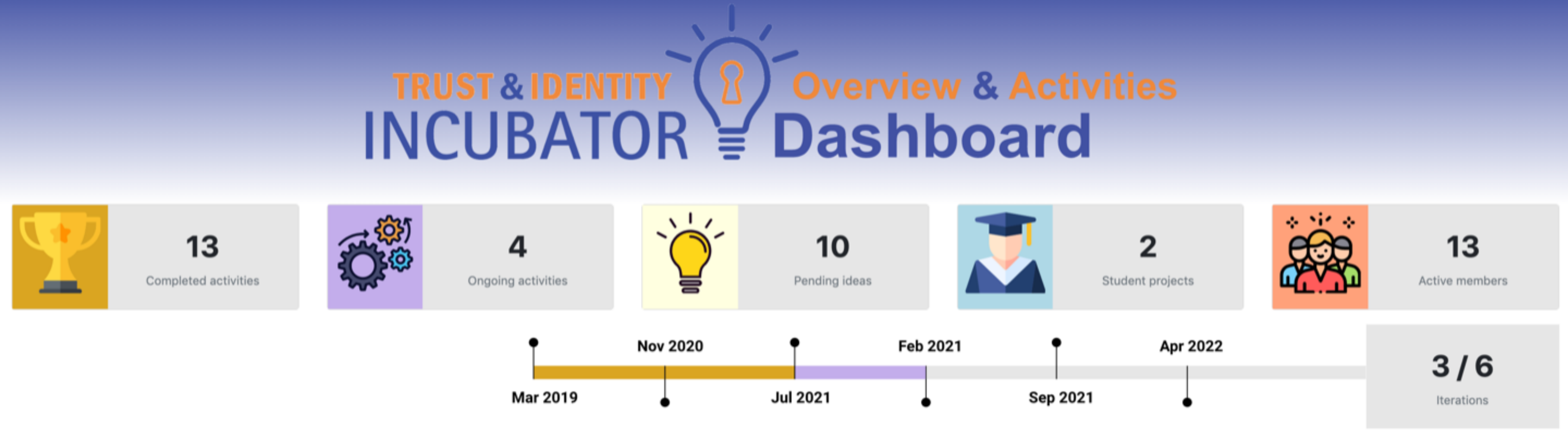
Methodology

GÉANT Networks · Services · People



Collect proposals for incubator topics	Review and prioritise the proposals	Choose topics for the next cycle	Define goal, stakeholders, results	Work on topic, 6 sprints with demos	Finalize topic handover results/close topic
Service Owners GÉANT project T&I community member	Main Incubator Board (MIB)	Incubator Lead + WP leaders	Principle Investigator	Incubator Core Teams MIB feedback	Incubator Activity Teams

Dashboard



TRUST & IDENTITY INCUBATOR Overview & Activities Dashboard

13 Completed activities

4 Ongoing activities

10 Pending ideas

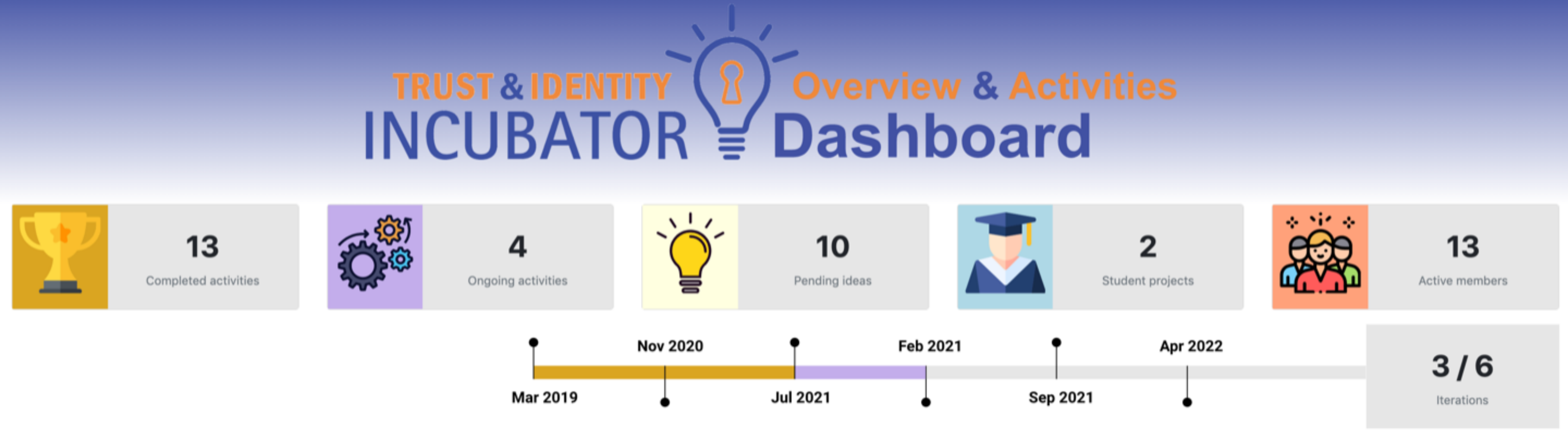
2 Student projects

13 Active members

3 / 6 Iterations

Dashboard - https://wiki.geant.org/display/gn43wp5/Incubator+Dashboard

Dashboard



TRUST & IDENTITY INCUBATOR Overview & Activities Dashboard

13 Completed activities	4 Ongoing activities	10 Pending ideas	2 Student projects	13 Active members

Mar 2019 – Nov 2020 – Jul 2021 – Feb 2021 – Sep 2021 – Apr 2022

3 / 6
Iterations

Dashboard - https://wiki.geant.org/display/gn43wp5/Incubator+Dashboard

Call for topics - https://wiki.geant.org/display/gn43wp5/TII+Call+for+Ideas

GÉANT Infoshare - T&I Incubator & NREN engagement - https://events.geant.org/event/463

DEVELOPING THE NEXT GENERATION OF T&I PRODUCTS AND SERVICES FOR THE EUROPEAN NREN COMMUNITY

TO FIND OUT MORE CONTACT GLAD@GEANT.ORG

GÉANT

TIM
TRUST & IDENTITY
MENTORSHIP PROGRAMME

TIM Programme - https://wiki.geant.org/display/GIG/TIM+Programme

Thank you

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. 856728 (GN4-3).