

Experiences in Supporting Service Providers and User Communities

Lukas Hämmerle, GÉANT/SWITCH
AAI@eduHR Conference
26 November 2014

Who am I



- Work almost 10 years for SWITCH (Swiss NREN)
- Mostly involved building SWITCHaai, now also (life-long) Swiss edu-ID
- Have been involved since GEANT 2 to build eduGAIN

GÉANT/GN3plus

- Who are we?

eduGAIN

- Interfederation in action

Work with Research Communities

- Collaborations to make use of eduGAIN

Summary and Conclusion

- Lessons learned

GÉANT/GN3plus

Who are we?

- **GÉANT:** the pan-European research and education network that interconnects Europe's National Research and Education Networks (NRENs). Together we connect over 50 million users at 10,000 institutions across Europe, supporting research in areas such as energy, the environment, space and medicine.
- **GN3plus:** extension and expansion to 3rd term of the successful GÉANT project, vital to the EU's e-Infrastructure strategy.
- **GÉANT Mission:** to deliver world-class services with the highest levels of operational excellence
- **Co-funded:** by the EU and Europe's NRENs

Key Facts	GN3plus
Start date	April 1 2013
Duration	24 (+1) months
41 Project Partners: 38 NRENs, DANTE, TERENA, NORDUnet (representing 5 Nordic countries)	

Federation	Services
eduGAIN	Interfederation
eduroam	Network SSO
Federation as a Service	In development

GÉANT is more than just the network!



Activity Leader

- Ann Harding, SWITCH
- ann.harding@switch.ch



Deputy Activity Leader

- Valter Nordh, SUNET
- valter.nordh@gu.se



T1: eduPKI

- Reimer Karlsen-Masur, DFN,
- edupki@geant.net



T2: eduroam

- Miroslav Milinović, SRCE,
- eduroam-ot@geant.net



T3: eduGAIN

- Brook Schofield, TERENA
- edugain@geant.net



T3.1 Moonshot

- John Chapman, JANET
- moonshot@geant.net



T4: Federation as a Service

- Valter Nordh, SUNET
- edugain@geant.net



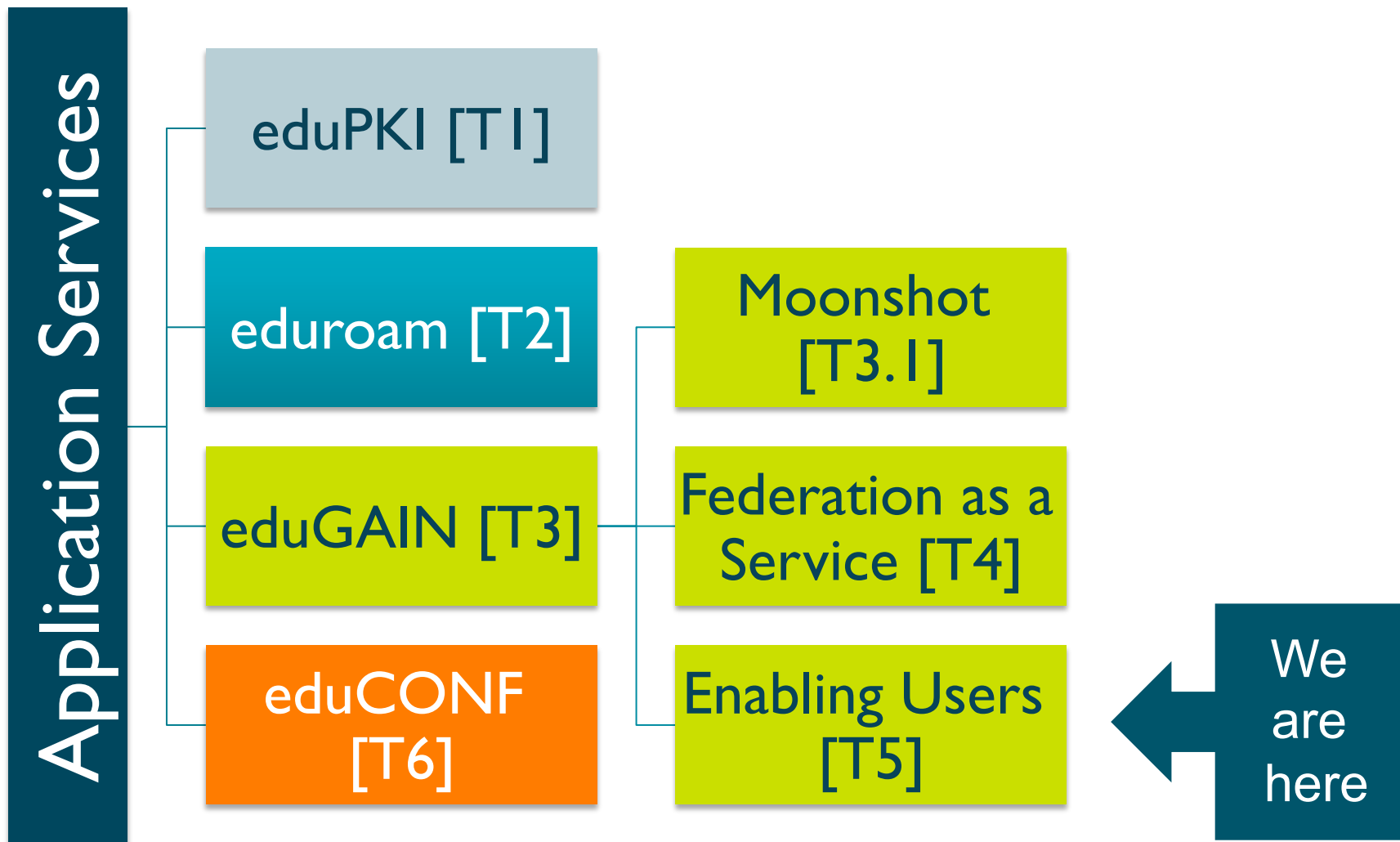
T5: Enabling Users

- Lukas Hämmerle, SWITCH
- enabling-users@geant.net



T6: eduCONF

- Tim Boundy, JANET
- educonf@geant.net



Enabling Users Task Participants and Partners



- Mandeep Saini, DANTE
- Barbara Monticini, GARR
- Maria "Lalla" Laura Mantovani, GARR
- Simona Venuti, GARR
- Marco Malavolti, GARR
- Mikael Linden, CSC
- Olivier Salaün, RENATER
- Thomas Bärecke, SWITCH
- Thomas Lenggenhager, SWITCH
- Wolfgang Pempe, DFN



Federation Operators of:

- DFN-AAI (DE)
- FER (FR)
- HAKA (FI)
- IDEM (IT)
- SWITCHaai (CH)

- Our partners:
 - REFEDS: Research and Education FEDerationS
 - GÉANT3plus Federation-as-a-Service (FaaS) task
 - GÉANT3plus eduGAIN/Moonshot Task

eduGAIN

Interfederation in action

eduGAIN Concept



Many established **national** Identity Federations

- but research projects are **international**
- but content publishers' customers are **international**
- but audience of research wikis and blogs is **international**



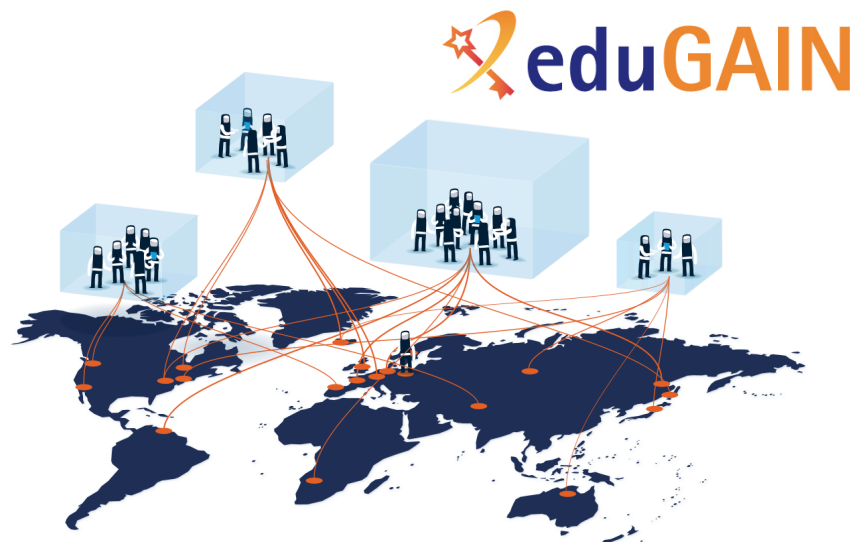
Interconnecting national federations → Interfederation

- Interfederation service facilitates international research collaboration
- International collaboration can be facilitated
- eduGAIN is an interfederation service

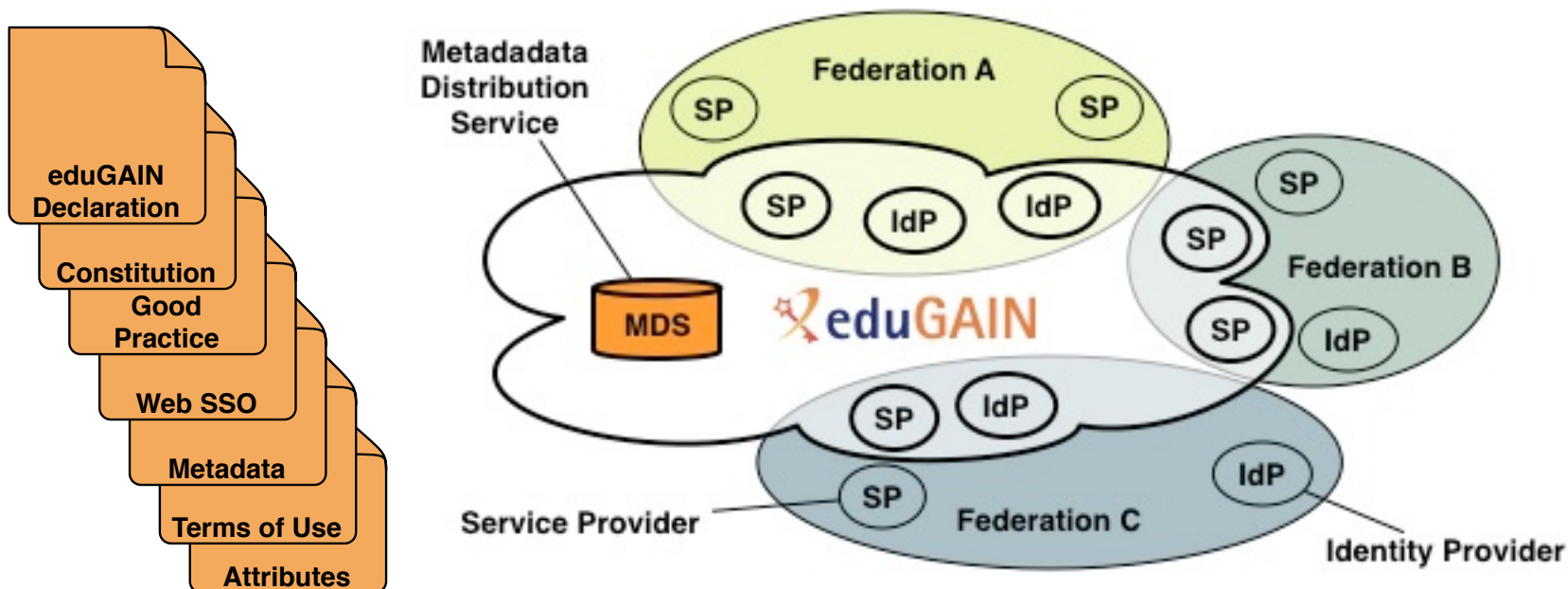
eduGAIN Key Facts



- eduGAIN ~= "AAI world-wide"
 - Launch 2011
- Interfederation service
 - Connects national federations
- Developed by GÉANT
 - All member federations are represented in steering group
- Interfederation-enabled organisations gain:
 - Their users can access web services abroad with organisation account
 - Their AAI services are accessible by students/researchers abroad

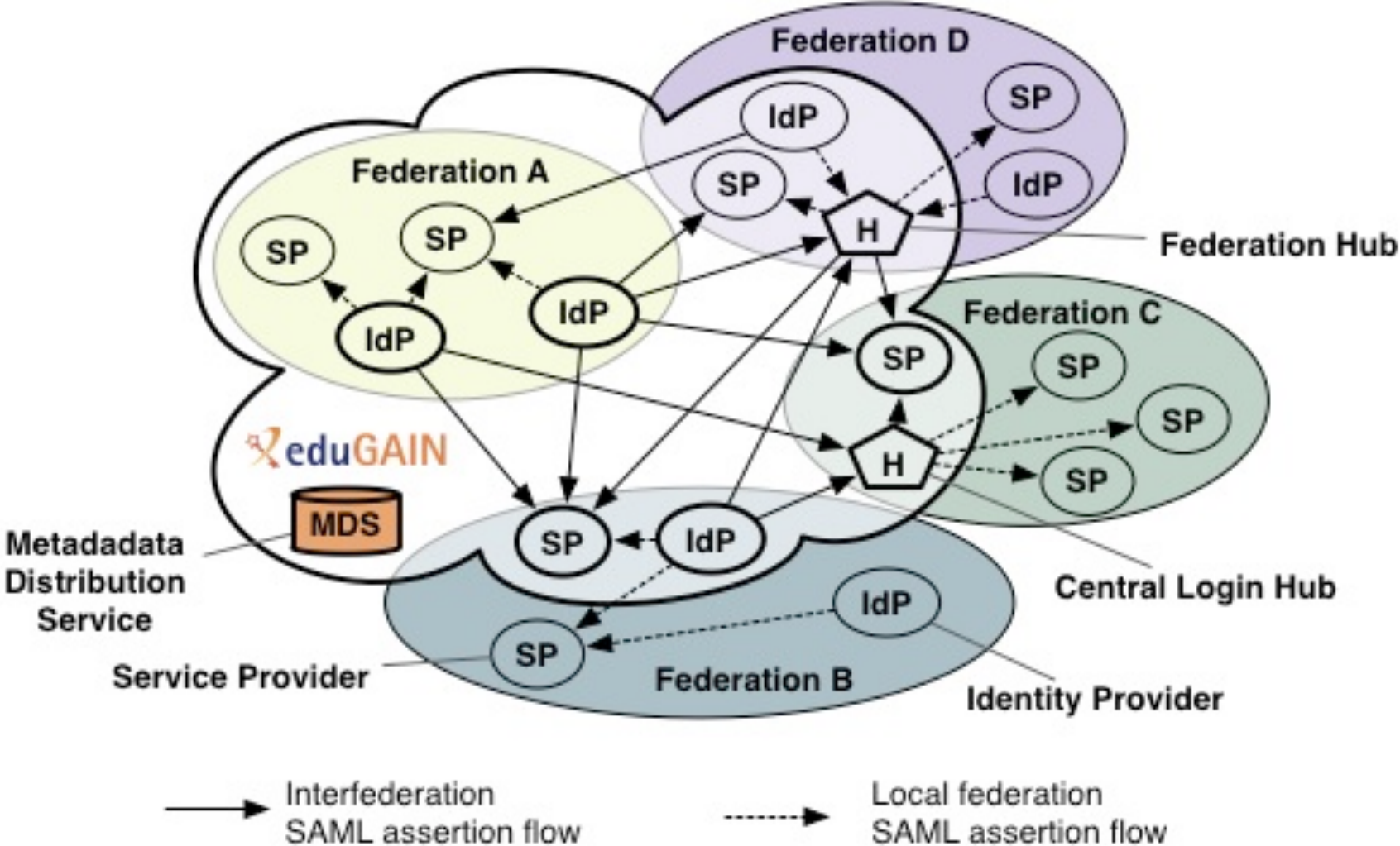


eduGAIN Basics: What is it, how does it work?

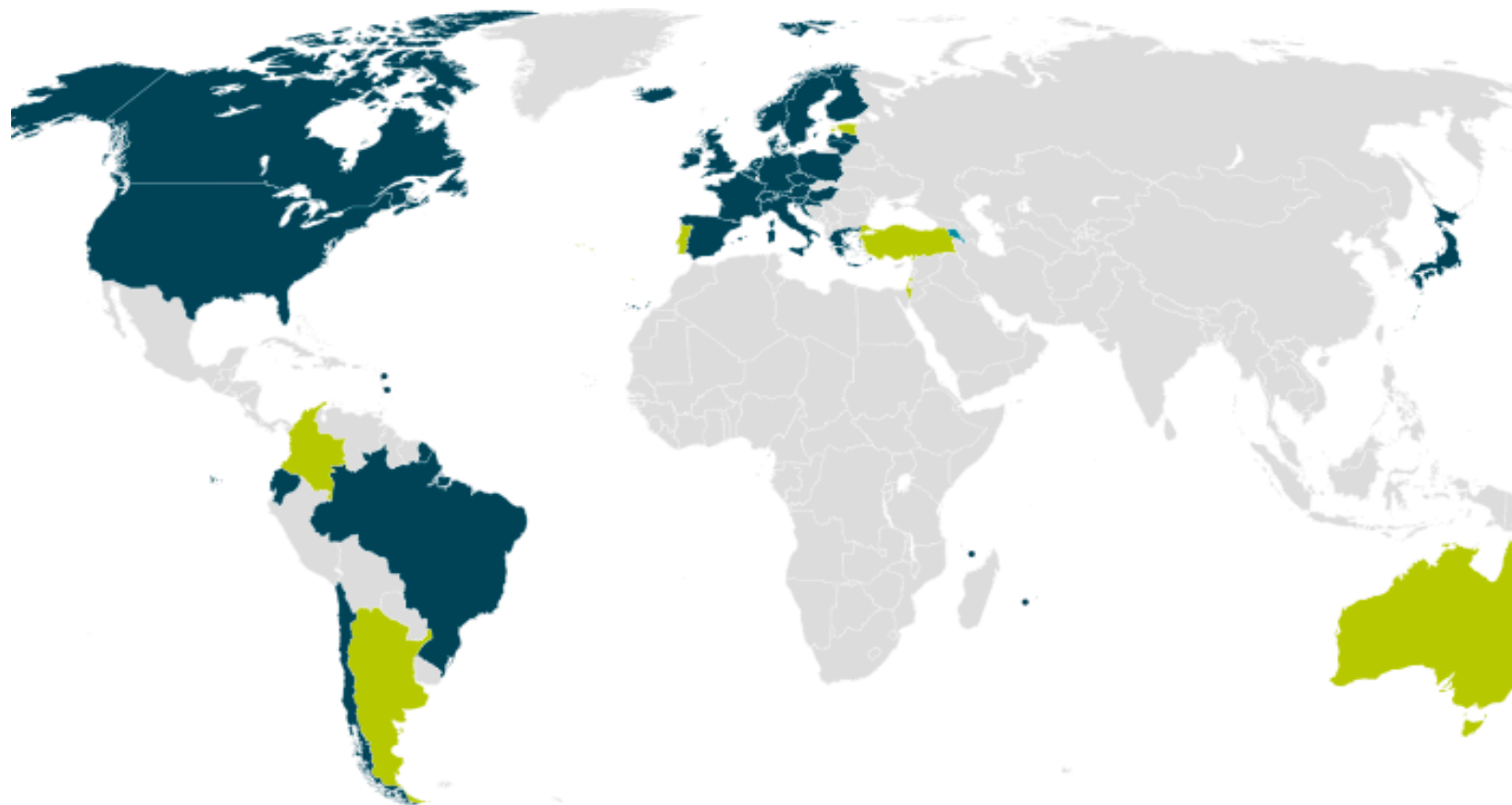


- eduGAIN provides policy framework and standards to build trust
- Subset of SPs and IdPs of participating federations opts-in for eduGAIN
- Their metadata is retrieved, aggregated and republished by MDS, consumed by other eduGAIN SP/IdPs

Actual Graphic



eduGAIN Member Federations



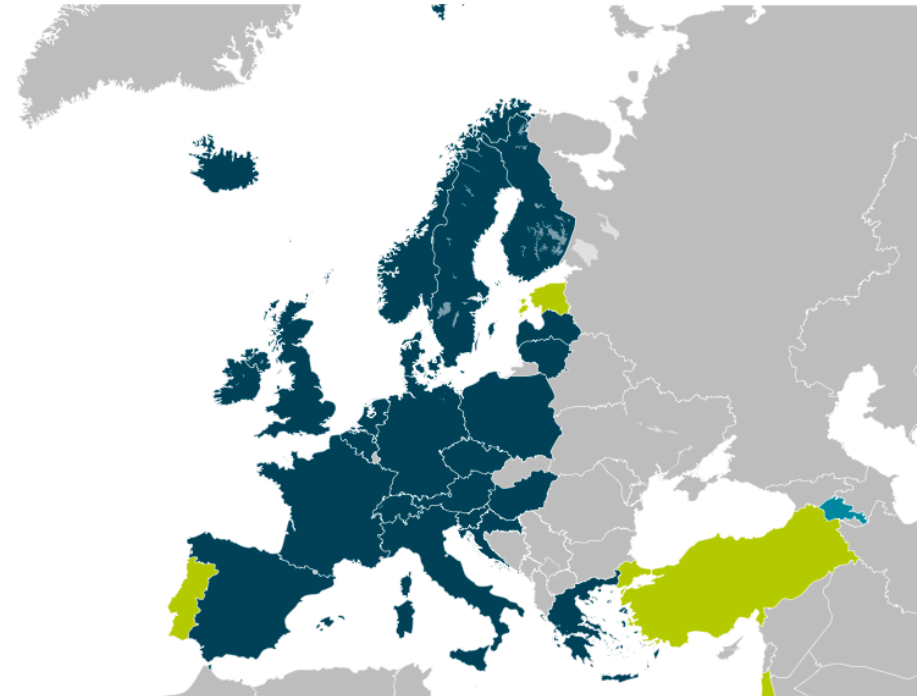
■ 29 Member Federations

■ 7 Joining Federations

eduGAIN Organisations and Services (9. November)



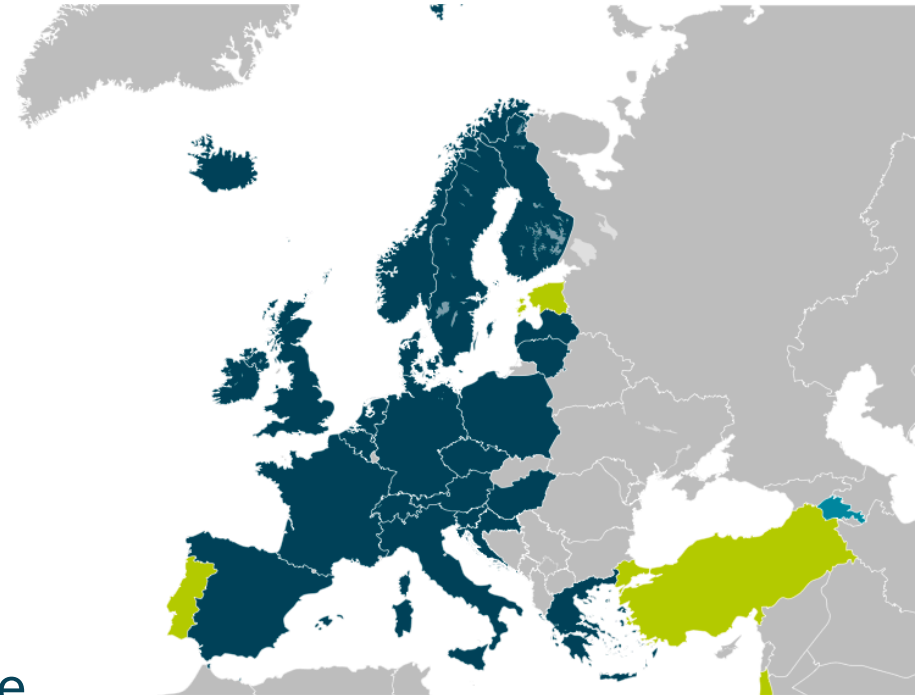
- 529 Identity Providers
+260% since Nov. 2013
- 147 Service Providers
+100% since Nov. 2013



eduGAIN Organisations and Services (19. November)



- 1'077 Identity Providers
+100% within 10 days
- 1'120 Service Providers
+160% within 10 days
- UK Federation added all their
IdPs and SPs
to eduGAIN
- By the end of 2014,
eduGAIN likely to contain more
entities than any other national federation
InCommon (US) currently has ~ 2300 entities



Work with Research Communities

Collaborations to make use of eduGAIN

Enabling Users Task: Who are the users?



Users = Researchers, who primarily want to do research but have to deal with some federated identity management challenges

Enabling Users Objectives

Helping communities benefit from federated identity/eduGAIN



Collaborate with the wider GÉANT project and with international user communities to increase usage of AAI infrastructure

Act as an expert partner for large, pan-European projects with AAI requirements

Coordinate a set of two or three projects between GÉANT and user communities, addressing their federated-identity concerns

Provide support such that four GN3plus project tools/services are AAI-enabled



Work in Close Collaborations and provide Basic support

- **Basic support**
 - Provide to all interested research communities
 - Basic "Hand-holding" and consultancy on eduGAIN

- **Close Collaborations**
 1. Collect use-cases
 2. Evaluate use-cases
 3. Collaborations with research community on 2-3 use-cases
 4. Start more collaborations at later phase if possible

- **Build knowledge-database and tools** based on feedback

How to Identify Use-Cases and Work Areas?

Fortunately some work has already been done by **FIM4R**:

- Interest group of several large European Research Communities
- Started to meet and discuss FIM topics in 2011
- Was transformed to a Research Data Alliance Interest Group in 2014:
<https://www.rd-alliance.org/fim-interest-group.html>
- Wrote paper "Federated Identity Management for Research Collaborations" (a.k.a. "FIM4R paper")
<https://cdsweb.cern.ch/record/1442597>
- Paper described challenges and requirements for each participating research community



Requirements/Important of Areas in FIM4R Paper



Requirement Area	Importance
User friendliness and Ease of use	High
Browser federated access	High
Non-browser federated access	High
Bridging communities	Med.
Technology translators	Med.
Open standards and sustainable licenses	High
Levels of Assurance	High
Authorisation under community control	High
Well defined and harmonised attributes	Med.
Flexible and scalable attribute release	Med.
Attributes that cross national borders/Data Protection	High
Attribute aggregation for authorisation	Med.
Privacy and data protection	Med.

Use-Case Submission for Close Collaborations



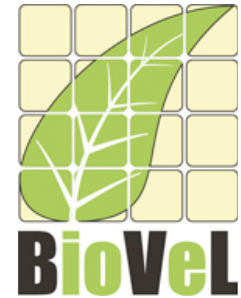
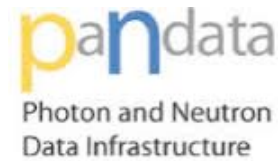
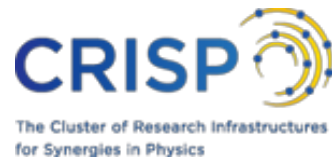
Research communities were via FIM4R and REFEDS mailing list invited to submit their use-cases

- **March 2013**: FIM4R workshop in Villigen, CH
 - Suggestion to collect use-cases

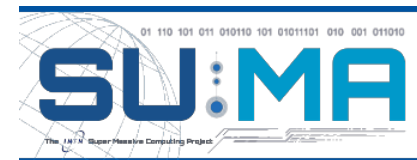
- **April 2013**: GÉANT3plus started
 - GÉANT3plus Enabling Users Task + REFEDS invited to submit use-cases

... and what use-cases were submitted?

11 Use-Cases Submitted by May 2013



CLIPC



- Too many to work with all of them at the same time
- Focus on 3 use-cases initially, add further later on if possible
 - But we also promised to provide basic support, consulting and expertise to all interested research groups in the mean time (via edugain-integration@geant.net)
- **Criteria for use-cases:**
 - Time frame, variety, reproducibility, existing SAML know-how, contribution, feasibility, ...
 - Only web-based use-cases in context of eduGAIN
 - *Non-browser use-cases covered in GÉANT Moonshot pilot*
 - Use-cases with heavy use of credential translation (e.g. X.509 to SAML) postponed because we (still) lack knowledge there

Year 1 Collaborations



- **DARIAH**

Humanities and
Social Sciences.

Bring ~ 4 services to eduGAIN and help
establishing GÉANT Data Protection Code
of Conduct



- **ELIXIR**

Life Sciences

Access to European Genome Archive (REMS)
and integration of Resource Entitlement
Management System (REMS)



- **UMBRELLA**

Photon/Neutron research

Bridging for Umbrella/eduGAIN. Moonshot pilot to provide SSH login
with final goal to remotely control experiments.



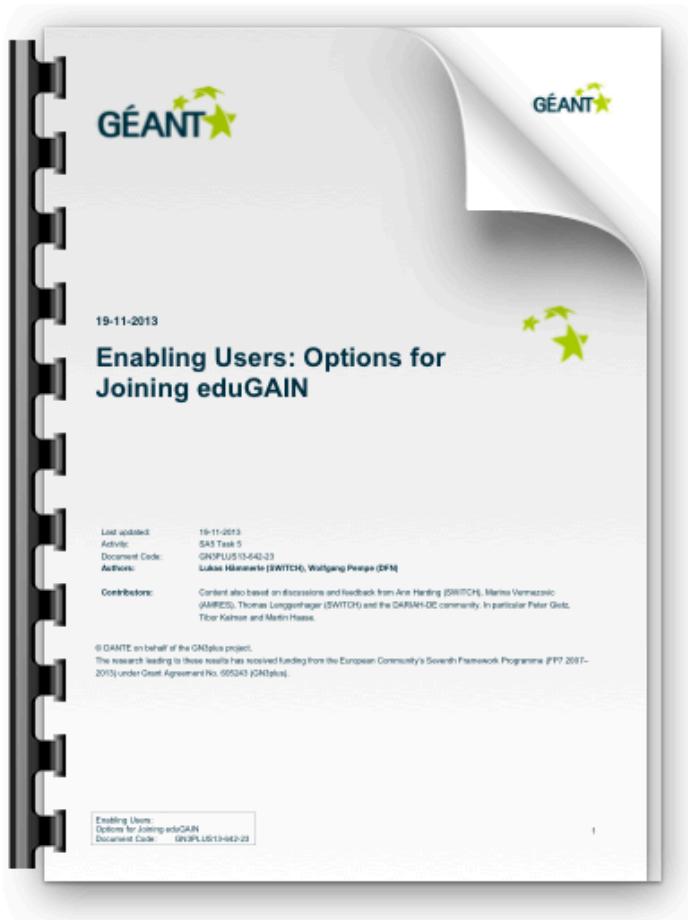
- **May 2013**: Use-case review and evaluation
- **June 2013**: Decision on use-case collaboration and initial discussions
 - Focus on DARIAH, ELIXIR, Umbrella (CRISP/PanData)
- **July 2013**: Agreed work plan with Umbrella
- **August/September 2013**:
 - Work with DARIAH on Document "Options to join eduGAIN"
No agreed-on workplan was possible because preliminary questions had to be answered first
- **October/November**:
 - Agreed with Elixir on work plan

FIM4R Requirements/Importance Status (November 2014)



Requirement Area	Import.	Status
User friendliness and Ease of use	High	Active
Browser federated access	High	Active
Non-browser federated access	High	Active
Bridging communities	Med.	Active
Technology translators	Med.	Partially active
Open standards and sustainable licenses	High	Active
Levels of Assurance	High	Partially active
Authorisation under community control	High	Active
Well defined and harmonised attributes	Med.	Not active
Flexible and scalable attribute release	Med.	Partially active
Attributes that cross national borders/Data Protection	High	Active
Attribute aggregation for authorisation	Med.	Active
Privacy and data protection	Med.	Active

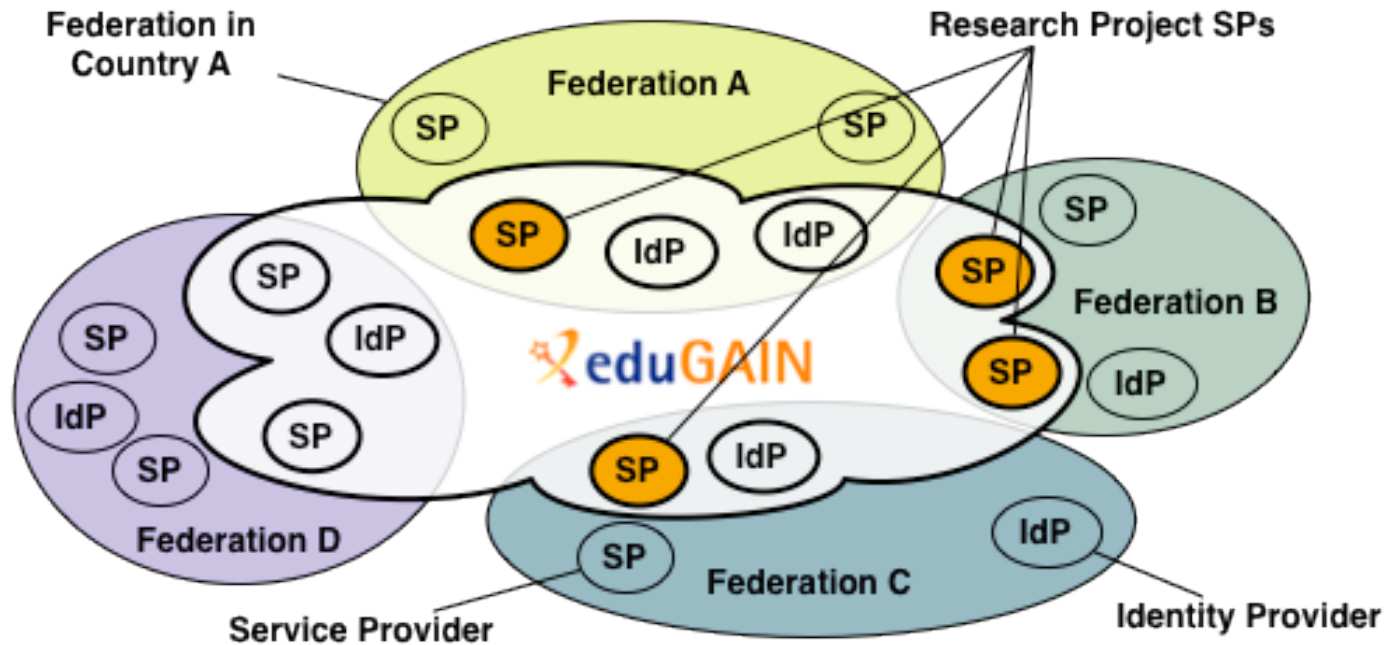
Example Result of Collaboration with DARIAH



- DARIAH as well as other Social Sciences and Humanities communities operate a large number of SPs in many countries.
- Therefore, our work first focused on the three options (A, B, C) research collaborations can operate their services in eduGAIN
- Resulted in a white paper:

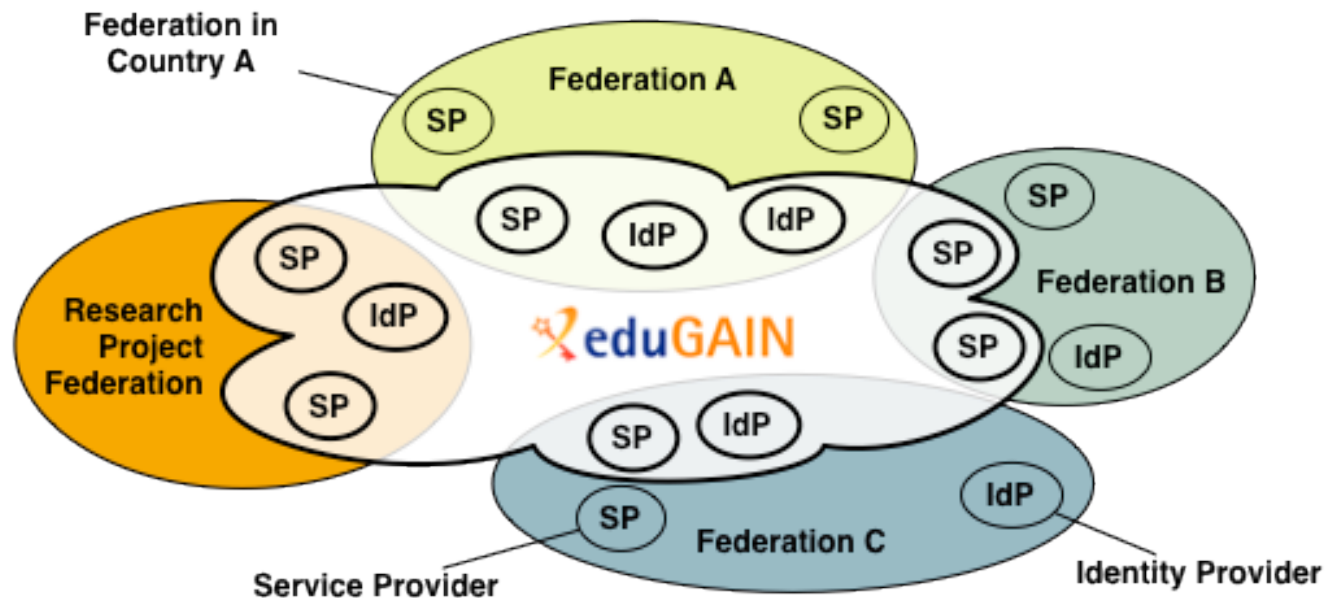
<https://wiki.edugain.org/File:Options-for-Joining-eduGAIN.pdf>

Option A: All SPs of a research project join eduGAIN via federations



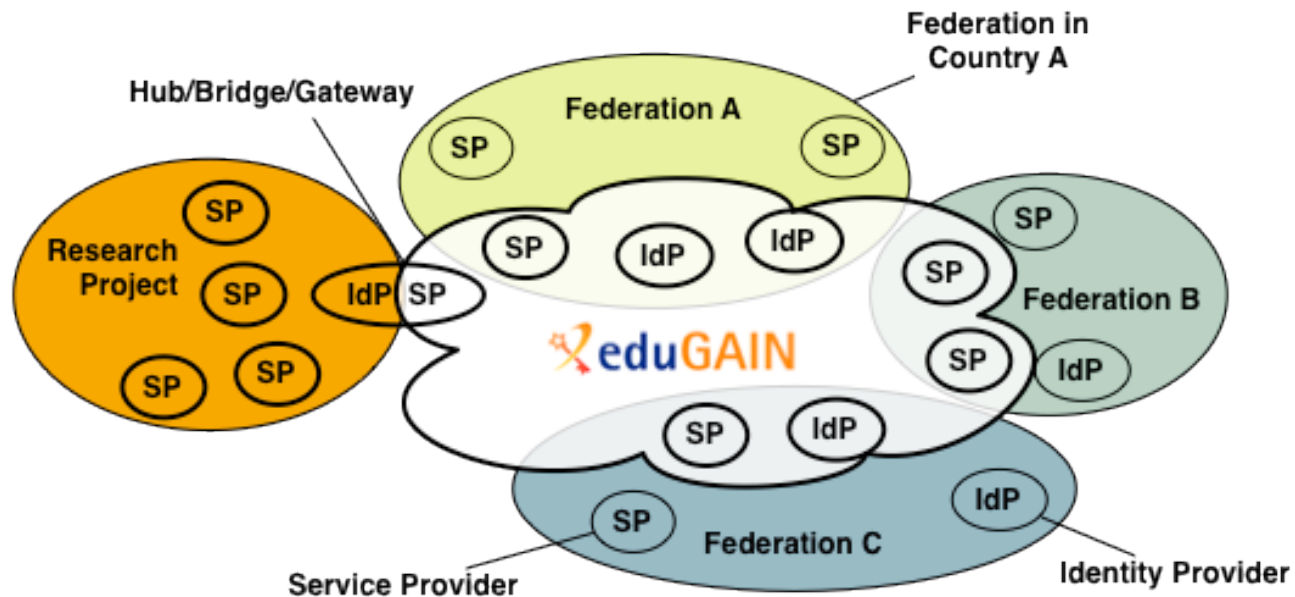
- Probably the easiest option for few SPs
- Probably the best option in the long term

Option B: Research project operates own federation and joins eduGAIN



- Probably best suited for large number of SPs
- Requires some overhead to operate federation


Option C: Research project operate single SP as hub in eduGAIN



- Probably best suited some large research projects
- Requires translating credentials/identities/trust but provides flexibility

New Collaborations in Year 2



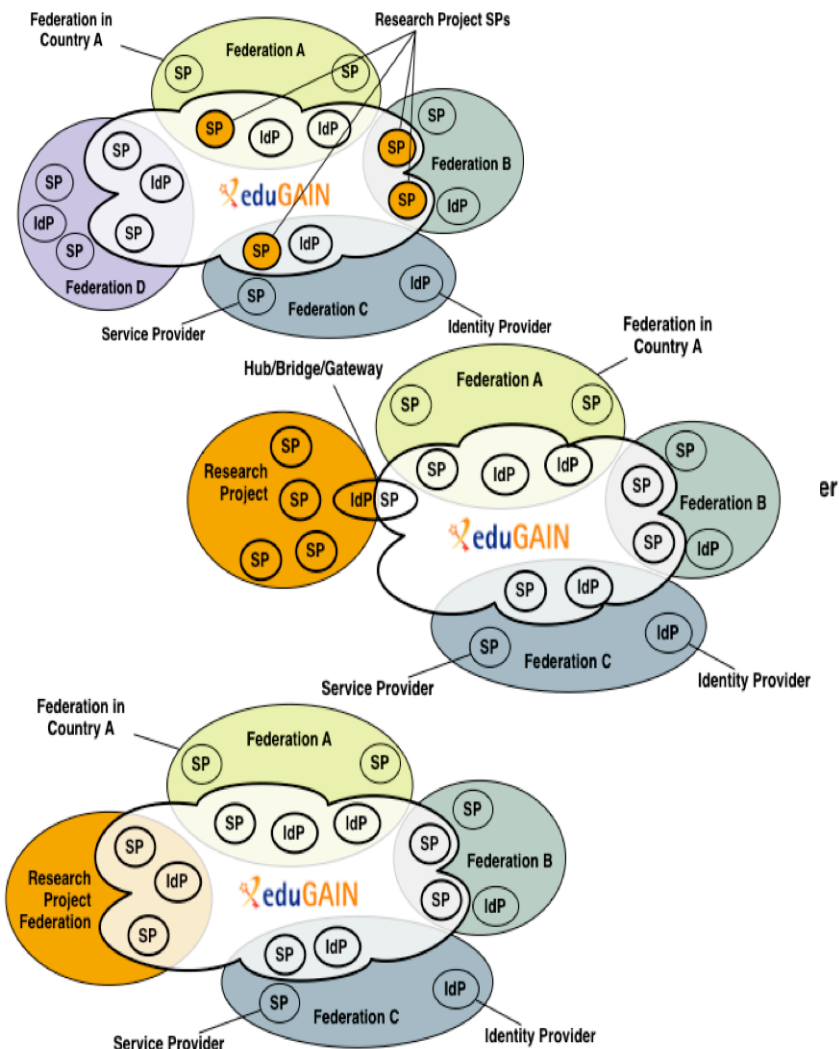
- **CERN**  Connect CERN's ADFS-based web single sign-on system via SWITCHaai to eduGAIN Bilateral login now technical possible.



- **ESA**  "Distributed" organisation in 5 countries. Pilot project started in October. First step for ESA joining eduGAIN via IDEM (IT).



Outcome from pilots



Pilot experience:
Better understanding = better
services for everyone

White paper: Options for
joining eduGAIN

Knowledge base of
community-relevant
experience collated and stored
in one place

Additional contact, support/
advice to projects,
e.g. neuGRID, ESA, CERN

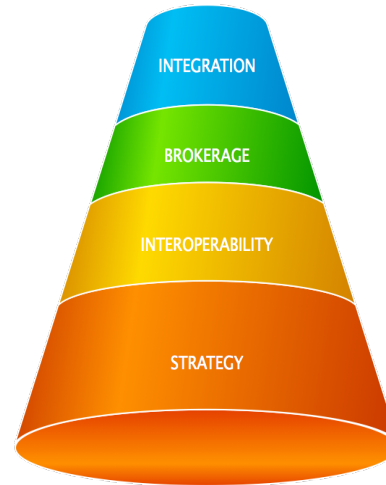
Enabling some of GÉANT's own services



GÉANT Intranet
(and other
GÉANT Sharepoint
instances)

Cloud integration

Facilitate the technical integration and implementation work needed to connect cloud services to the IT infrastructure of NRENs.



Cloud
with
SA7



AutoBAHN with SA3



eduCONF with SA5



eduroam
Supporting
Services
with SA5



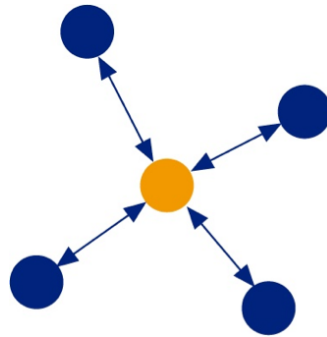
perfSONAR with
SA4

Further Collaboration Results: eduGAIN Helper Tools

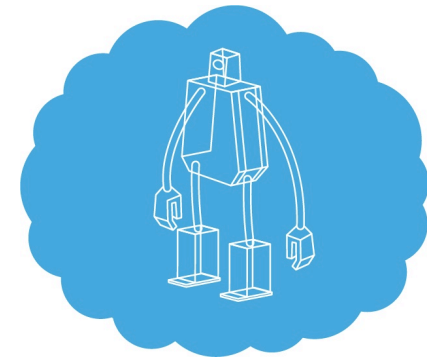
Collaboration with research communities result in valuable inputs for evolution of eduGAIN and other GEANT services.



eduGAIN
Use-cases

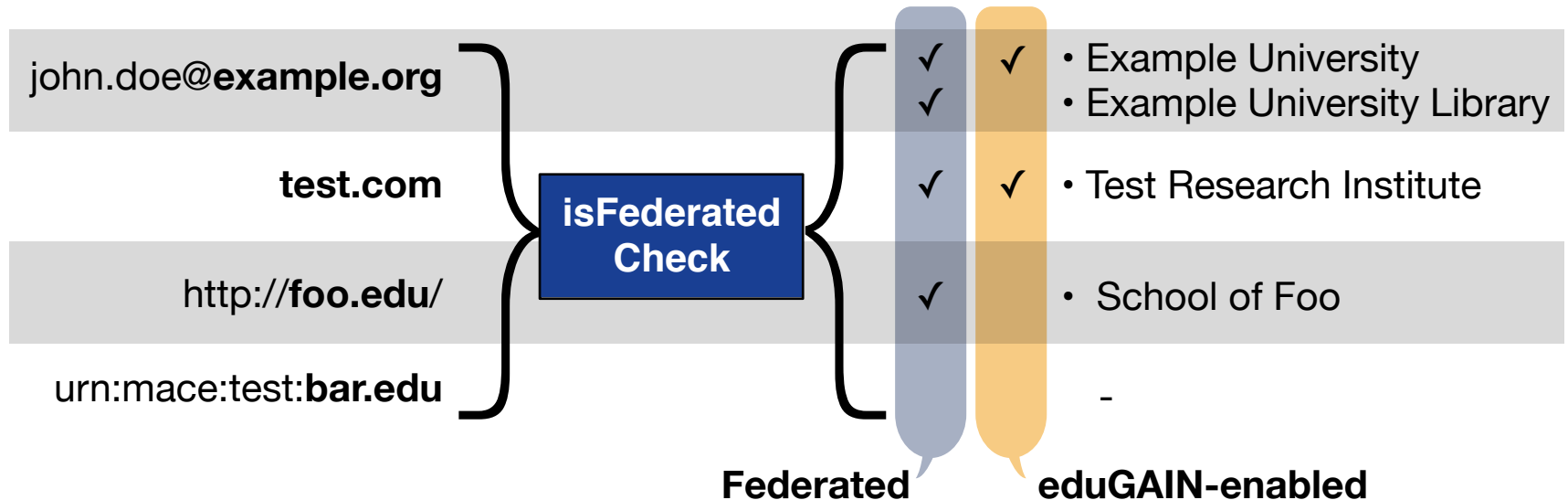


Collaboration

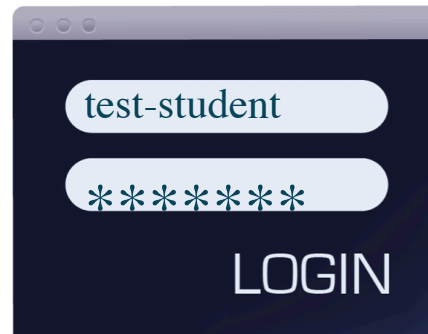


Ideas for
Improvements
and Tools

IsFederated Check Tool



- Shows if users' organisations are already federated and eduGAIN-enabled
- Great for research groups to find out how many of their users could already login to their services via eduGAIN
- URL: <https://wiki.edugain.org/isFederatedCheck/>



Create service-specific **test accounts** with different profiles

Use them for login on **own service only**

Check if access works and attributes are available

Mainly useful for service operators without an own AAI/federated login (e.g. commercial cloud providers) but also for all administrators of AAI/eduGAIN services. Currently under development.

More information will be available on <http://wiki.edugain.org>

Summary and Conclusion

- Main Challenges
- Lessons learned



Missing FIM Know-how

Federated Identity Management is complex and not their core business. Some understanding is however still needed to see the benefits of AAI and to see what AAI@EduHr/eduGAIN can provide.

Some minimum awareness and knowhow has to be built up by research communities first.



Identity Provider Coverage

Still many organisations that are not federated or not in eduGAIN yet.

But this should improve quickly.

"Almost 25% of ALL federated entities (as calculated via MET) are available via eduGAIN"

18. Nov. 2014, Brook Schofield (eduGAIN Product Manager)



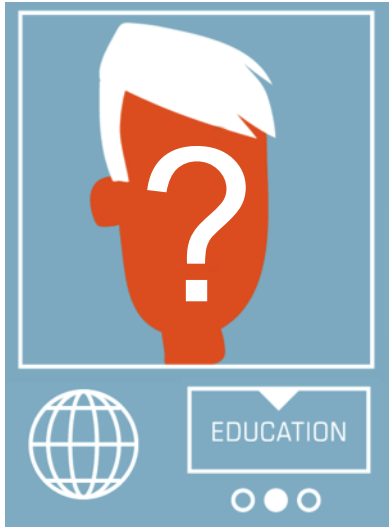
Insufficient Attribute Release

- End users arrive at an AAI service without the necessary attributes → Error message/bad user experience.
- Manual per IdP attribute release management does not scale! Central and/or rule-based automatic attribute release management is required.
- To generous attribute release collides with data privacy. Data privacy law makes some IdP administrators hesitant to release user attributes accross national borders...

Promising solution is to support entity categories:

- **GÉANT Data Protection Code of Conduct**
- **REFEDS Research & Scholarship**

Federation Operator (like AAI@EduHr) should actively propagate support (on IdP and SP side) for these entity categories!



Undefined Level of Assurances

- Identity vetting and authentication security different in every eduGAIN member federation and even every IdP
- No widely accepted standard for assurance level that is suitable for higher education
- Not possible to find out according to attributes if a user for example is a researcher (e.g. needed for ELIXIR)

Other Lessons Learned in first 18 Months



- Research groups have similar federated identity management needs but there is **no catch-all solution**
- AAI/eduGAIN expertise provided by GÉANT is well appreciated, GÉANT gets **valuable feedback & inputs**
- **Politics is often slower than technology.** Some proposed solutions first need to be discussed and approved within research communities before deployment.
- **Interest in Level of Assurance growing** but standards suitable for Higher Education still missing

- GÉANT 4 starts May 2015
- More harmonisation work:
 - Level of Assurances
 - Best-Practices for federation operators
 - Interoperability and categorization of services
- Continued Support and collaborations with research communities
 - Will include work on two new substantial use-cases
- Development of Virtual Organization Platform
 - Carry out pilots with interested research groups
 - Then prepare service package



Thank you!



Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv

