eduGAIN - How Umbrella can make the most of existing infrastructure

Ann Harding, SWITCH

5th PaN-Data & CRISP Harmonisation Meeting

27 June 2013

Overview

GÉANT/GN3plus

- Who are we?

eduGAIN

- Interfederation in action

Bridging

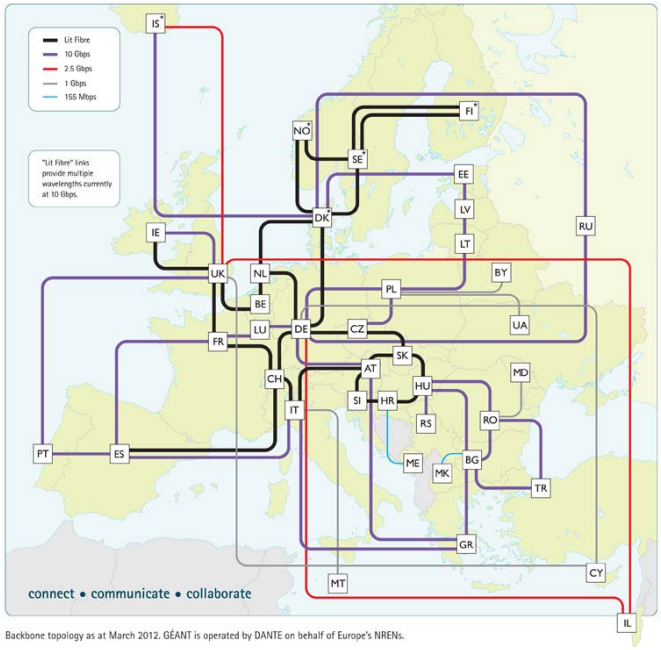
- Addressing the “Last Mile” for Umbrella with eduGAIN

GÉANT & GN3plus

- **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 months

41 Project Partners:
38 NRENs, DANTE, TERENA, NORDUnet (representing 5 Nordic countries)



Backbone topology as at March 2012. GÉANT is operated by DANTE on behalf of Europe's NRENs.

Delivering AAI Services in GÉANT

SWITCH (CH)	Nordunet (DK, SE, FI)	AMRES (RS)	Aconet (AT)	CARNET (HR)
CESNET (CZ)	DFN (DE)	GARR (IT)	Janet (UK)	HEAnet (IE)
NIIFI (HU)	PSNC (PL)	RedIRIS (ES)	RENATER (FR)	Surfnet (NL)

eduGAIN

TERENA

DANTE

eduroam

eduGAIN concept

Many established **national** Identity Federations

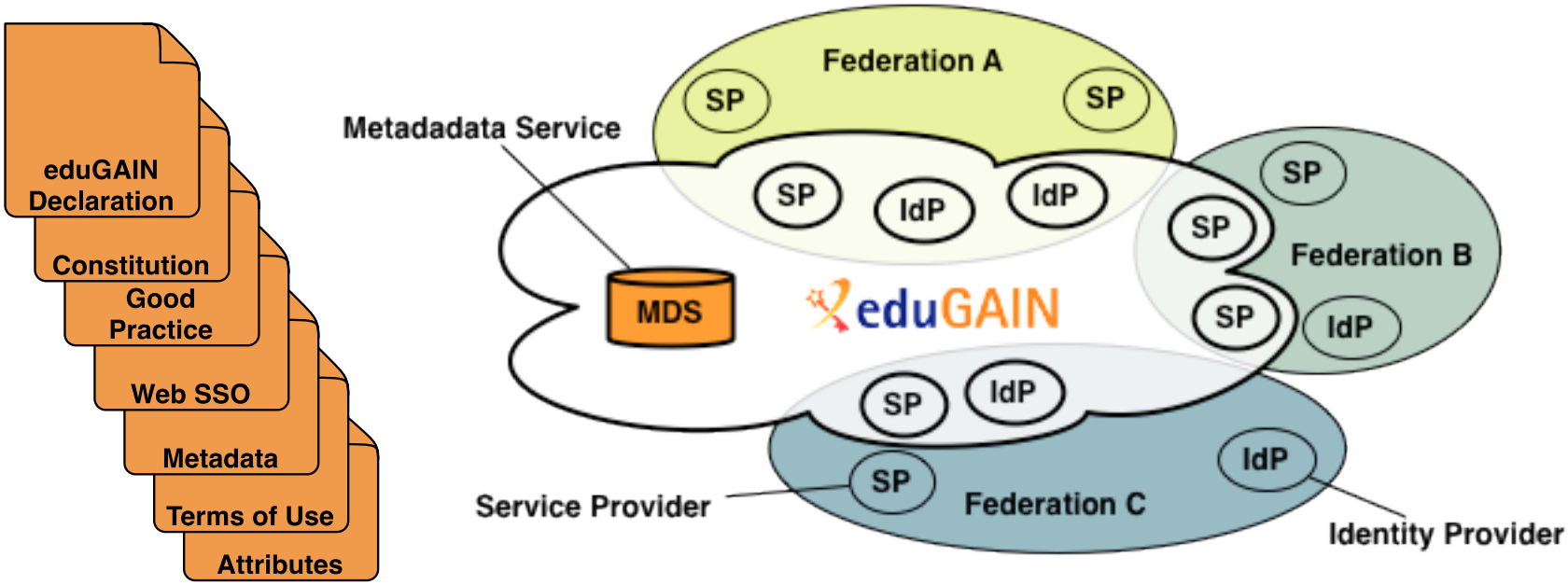
- but research projects are **international**
- but content publishers' customers are **international**
- but audience of research wikis and blogs is **international**

and many more

Interconnecting national federations → Interfederation

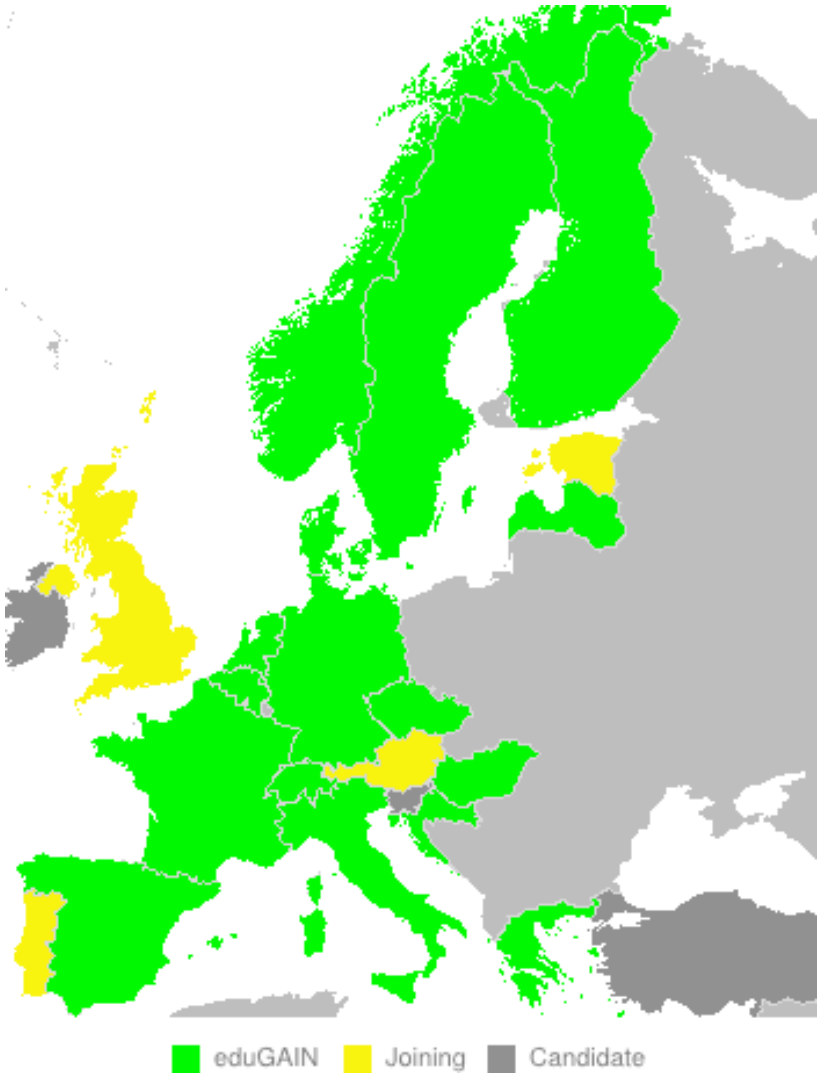
- Interfederation service facilitates international research collaboration
- International collaboration can be facilitated
- eduGAIN is an interfederation service

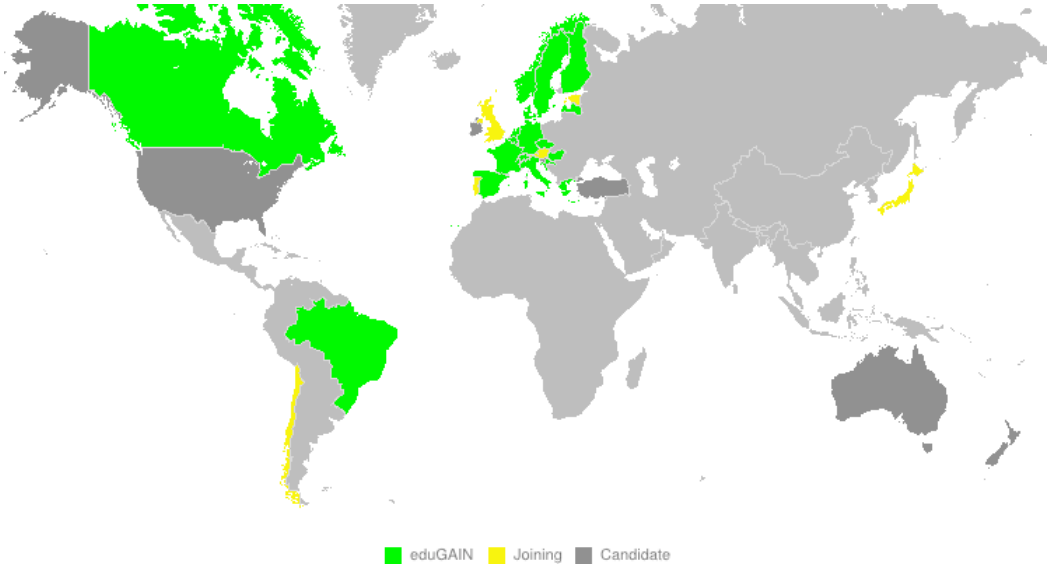
eduGAIN Basics: What is it, how does it work?



- 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

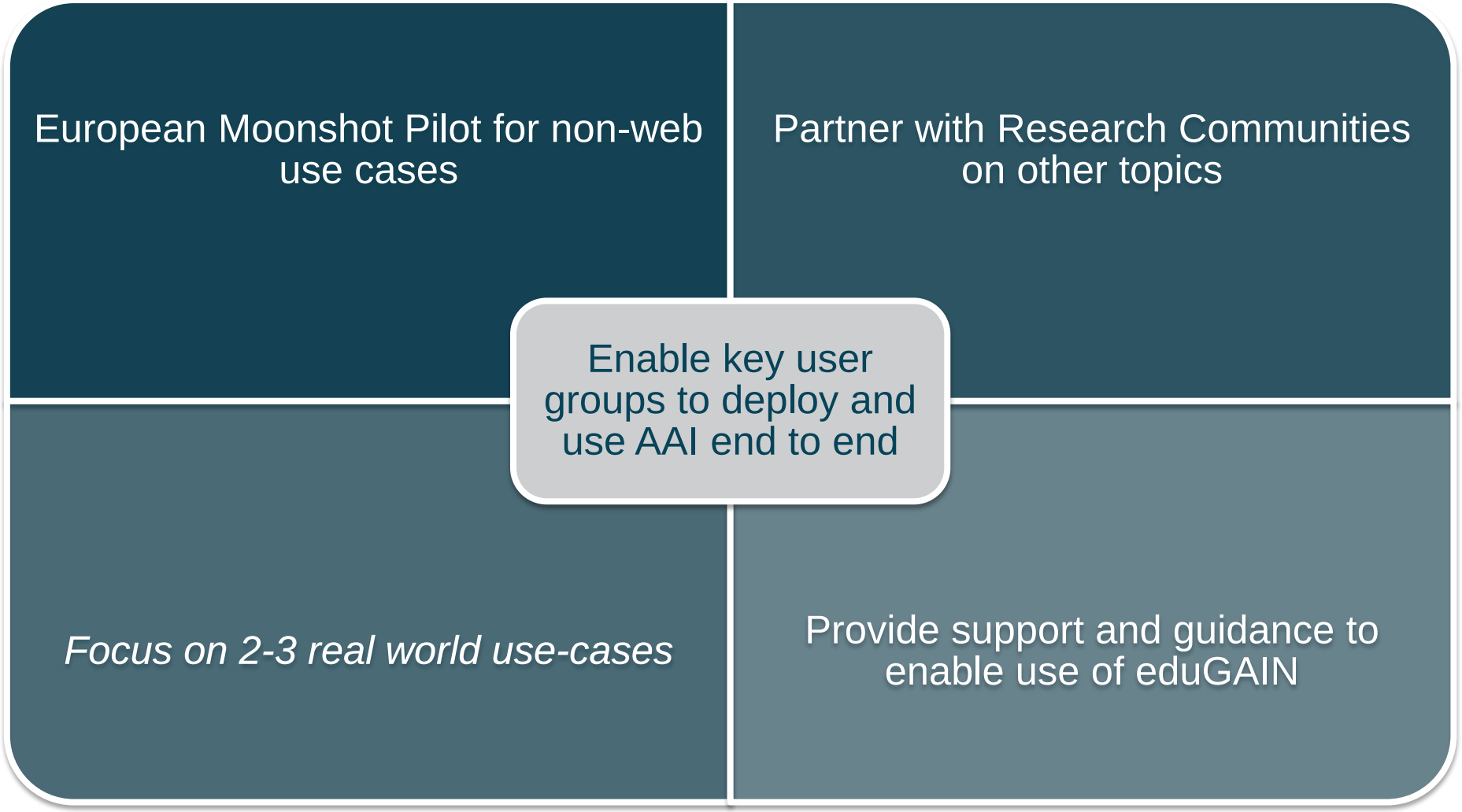
Federations Participating in eduGAIN





7

New Focus on User Communities



Bridging Umbrella and eduGAIN

Web-based use cases

Moonshot pilot for non-web

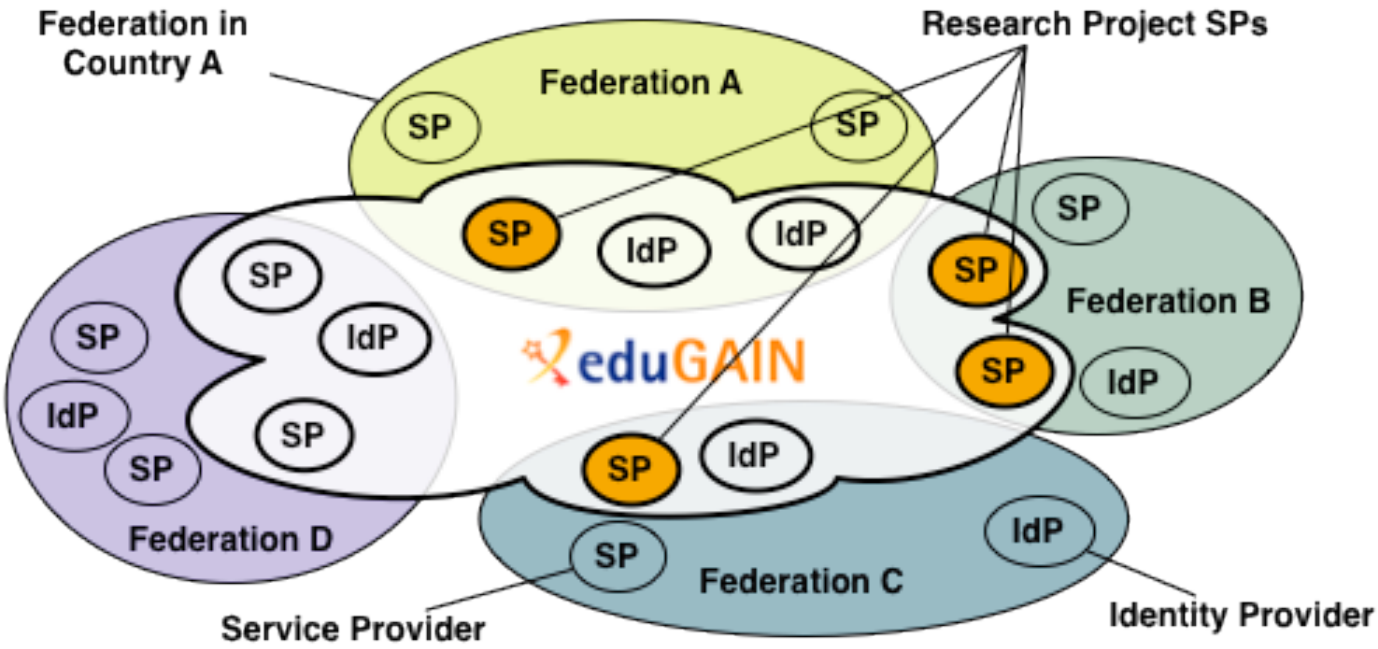
3 possible options

5 ‘simple’ steps for some, more complex for others

Some important questions

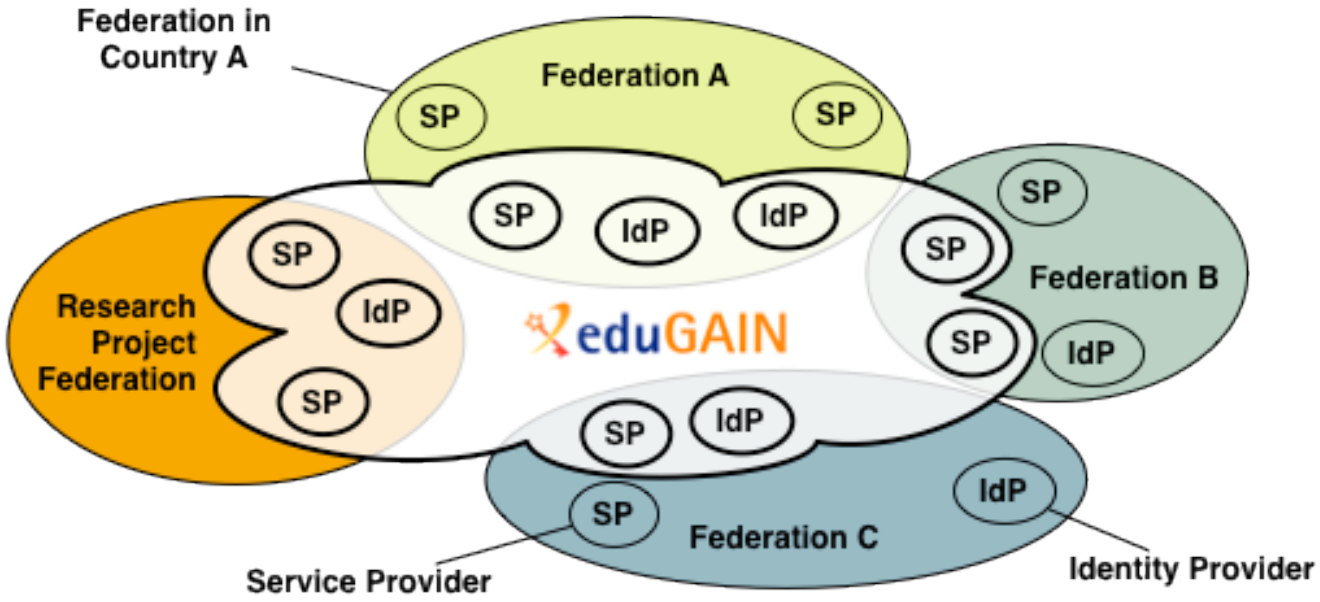
What approach do you want to take?	What help do you need?	When do you need it?	Where do you need it?

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



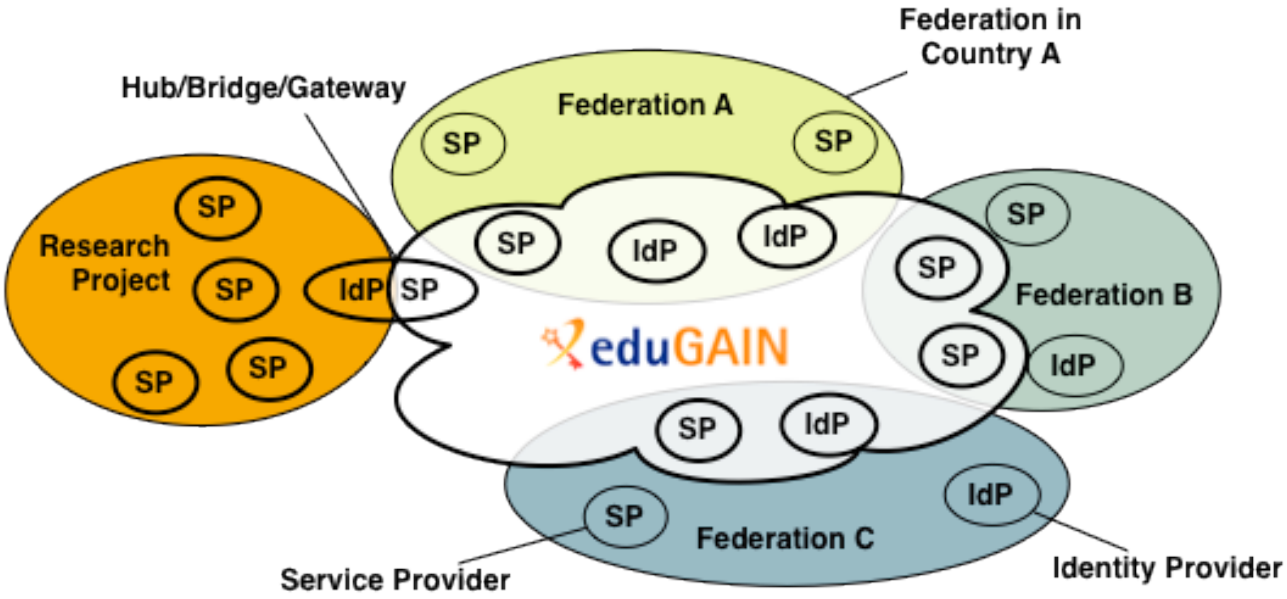
- Probably the easiest option for few SPs
- Probably the best option in the long term

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

The 5 Steps to Get a Service Connected to eduGAIN

1. Opt-in via your local federation*
2. Adapt configuration to load eduGAIN metadata
3. Adapt attribute mappings
4. Adapt access control/application
5. Adapt Discovery Service

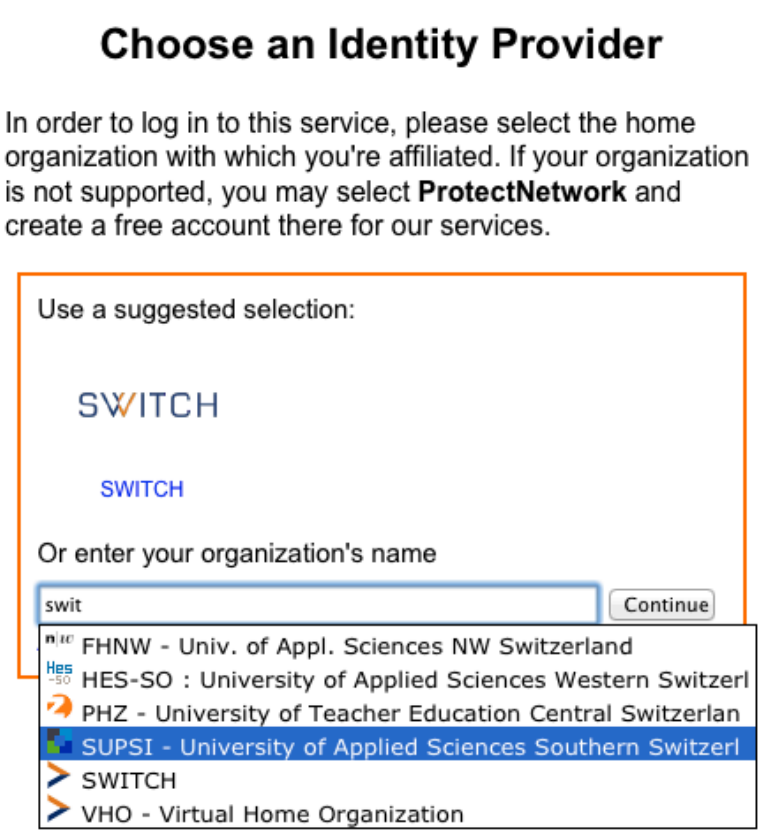
Example Guide for SWITCHaai SPs:

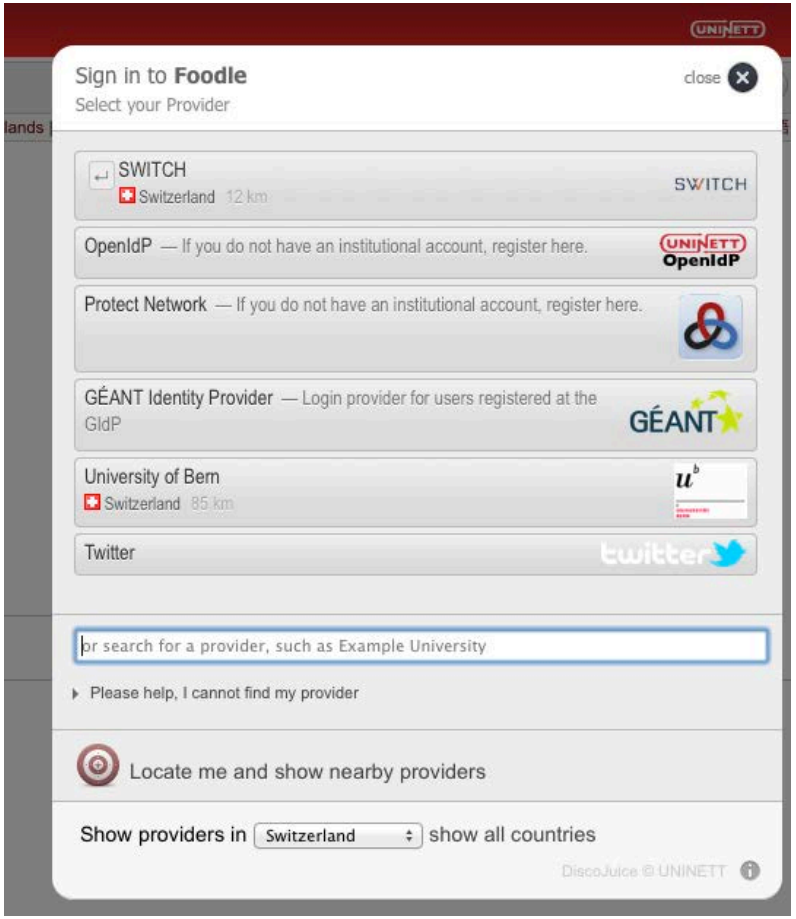
https://www.switch.ch/aai/docs/interfederation/sp-deployment.html

* Option A and C

13

Examples:
Shibboleth DS and DiscoJuice





Thank you!

Connect | Communicate | Collaborate

www.geant.net

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

Additional eduGAIN Technical Slides

Ann Harding, SWITCH

5th PaN-Data & CRISP Harmonisation Meeting

27 June 2013

Step 1:
Opt-In via local (NREN) federation

- Main goal: **Get services interfederated!**
  - Make service interoperate with entities from multiple federations
- If service is not yet part of an identity federation, join existing federation: https://refeds.terena.org/index.php/Federations
  - Or read next slide carefully
- If service is already operated in a federation, find out what steps are necessary to enable it for eduGAIN http://www.edugain.org/technical/status.php
  - Steps vary for each federation due to different laws and policies
  - Some federations might require a document to be signed
- Different Options to opt-in

Step 2:
Load eduGAIN metadata

- All common SAML implementations can process multiple metadata files
  - Most common products: Shibboleth and SimpleSAML PHP
  - This step usually requires copy&pasting a few lines into configuration and maybe downloading another X.509 certificate for metadata validation
  - Once configured, metadata is updated automatically

- Local federation will offer you (preprocessed) eduGAIN metadata
  - Don't load eduGAIN metadata directly from eduGAIN MDS

Step 3:
Adapt attribute mappings

- Make Service Provider accept common attributes used in eduGAIN
  - Attributes mostly from eduPerson and SCHAC schemas
- Involves adapting the configuration:
  - Copy&Paste a few lines according to the local federation instructions
  - E.g. for Shibboleth SP: Adapt the attribute-map.xml
- Might involve adapting the web application:
  - Different attributes might have been used in local federation than are available for eduGAIN users.
  - Mapping/transformation of names and values might be necessary

eduGAIN Recommended Attributes

eduGAIN recommends that these attributes are available (but are released only if required) for all users:

- **displayName**: Lukas Hämmerle
- **commonName** (multi-valued): Lukas Hämmerle
- **mail**: lukas.haemmerle@switch.ch
- **eduPersonAffiliation**(multi-valued): staff;member
- **eduPersonScopedAffiliation**: staff@switch.ch;member@switch.ch
- **eduPersonPrincipalName**: lhaemmerle-23yedy@switch.ch (example)
- **schacHomeOrganisation**: switch.ch
- **schacHomeOrganizationType** (multi-valued):
  - urn:schac:homeOrganizationType:ch:others
  - urn:schac:homeOrganizationType:int:nren (value currently revised)

Step 4:
Adapt access control/application

- Range of users who could access a service increases with Interfederation/eduGAIN
- Therefore, access control policy should be carefully revised
- Access control can be enforced in:
  - SAML implementation (e.g. RequestMap in shibboleth2.xml)
  - Web server (e.g. httpd.conf or .htaccess files)
  - Web application itself

- Take into account that attributes for eduGAIN users might be different/not available in all cases. Might require adaptation of access control.

Step 5:
Adapt Discovery Service

- Discovery Service (DS) lets users choose their Home Organisation
- Interfederation of a service might heavily increase the number of organisations that could access the service

- Different open source implementations available for DS:
  - Direct login links (might be suited for < 10 organisations)
  - SWITCHwayf (PHP/JS)
    http://www.switch.ch/aai/support/tools/wayf.html
  - Shibboleth Embedded Discovery Service (JS, requires Shibboleth)
    http://shibboleth.net/products/embedded-discovery-service.html
  - DiscoJuice (SaaS solution)
    http://discojuice.org/

Thank you!

Connect | Communicate | Collaborate

www.geant.net

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