Options for Joining eduGAIN

Lukas Hämmerle, SWITCH

DARIAH Workshop, Köln

18 October 2013

Outline

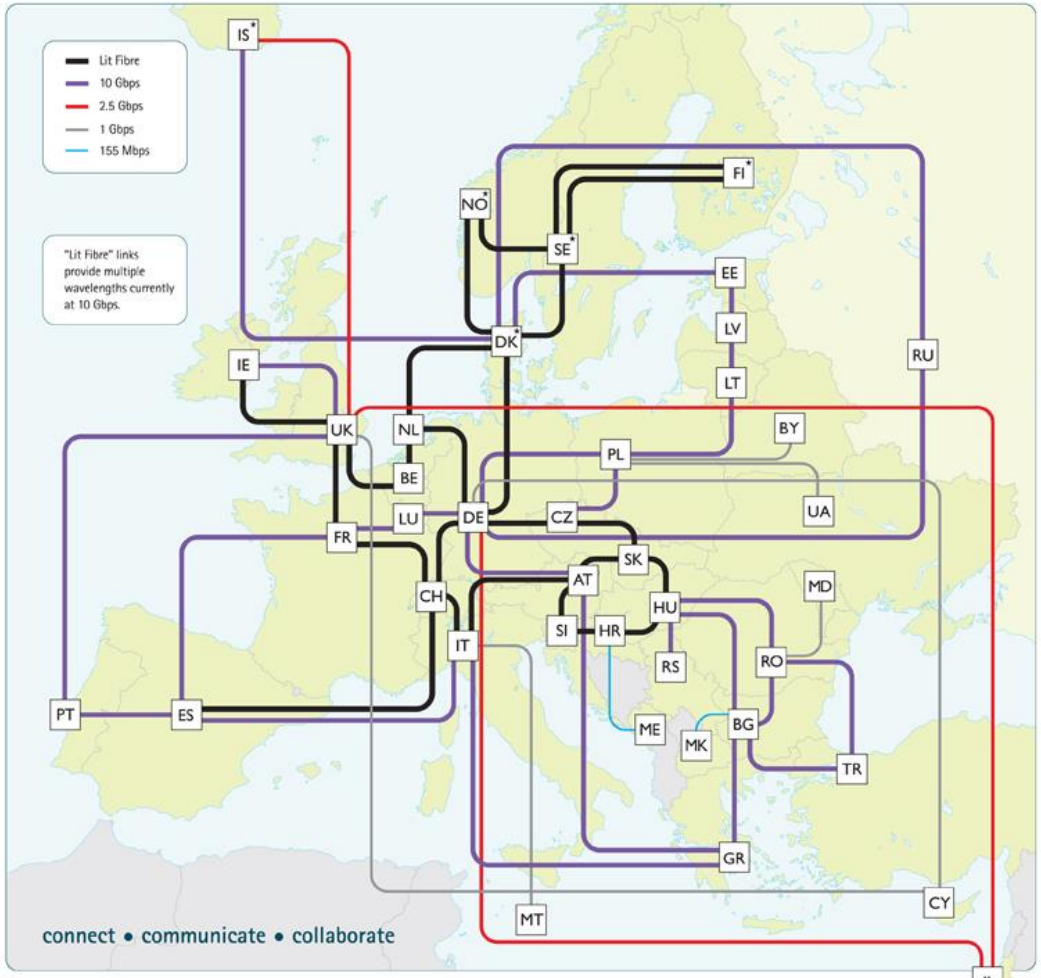
1. GÉANT and the Enabling Users task
2. Options to Join eduGAIN
3. Discussion

GÉANT (GN3plus)
- vital to the EU's e-Infrastructure strategy

Key Facts	GN3plus
Start date	April 1 2013
Duration	24 months
Total budget	€84,283,018
EC contribution	€41,800,000
Participants	250+
41 Project Partners: 38 NRENs, DANTE, TERENA, NORDUnet (representing 5 Nordic countries)	

- **GN3plus:** extension and expansion to 3rd term of the successful GÉANT networking project, vital to the EU's e-Infrastructure strategy.
- **GÉANT vision:** to become the unified ***European Communications Commons -*** driving knowledge creation as the global hub for research networking excellence
- **GÉANT Mission:** to deliver world-class services with the highest levels of operational excellence
- **Co-funded:** by the EU and Europe's NRENs

Europe's 100Gbps Network
- *e-Infrastructure for the "data deluge"*



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

- Latest transmission and switching technology
- Routers with 100Gbps capability
- Optical transmission platform designed to provide 500Gbps super-channels
- Hybrid network
  - *GÉANT IP: packet routed – and VPNs*
  - *GÉANT Plus: switched point-to-point circuits*
  - *GÉANT Lambda: dedicated wavelengths*
- 12,000km of dark fibre over 100,000km of leased capacity (inc. transatlantic links)
- 28 main sites covering European footprint

Delivering world-class services to R&E communities

JRA1: Network Architectures for Horizon 2020

JRA2: Technology Testing for Specific Service Applications

JRA3: Identity & Trust Technologies for GÉANT Services

SA1: Core Backbone Services

SA2: Testbeds as a Service

SA3: Network Service Delivery

SA4: Network Support Services

SA5: Application Services

SA7: Support to Clouds

SA6: Service Management & Operations

NA1: Management

NA2: Communications & Promotion

NA3: Status & Trends

NA4: International & Business Devpt

SA5 Application Services
For global collaboration

Service Tasks:

eduroam

eduCONF

eduPKI

eduGAIN

(Moonshot pilot)

Non-service Tasks:

- Federation-as-a-Service
- Enabling Users **<= That's us, ~6 people, present today Wolfgang and me**

"Enabling Users" Objectives

- Be **expert partner** for large EU projects with AAI requirements
- Actively collaborate with large international user communities
  - Based on well-defined, replicable use cases
  - Increase the practical use of AAI infrastructure
- Extend interfederation technology and AAI functionalities
  - Help communities **integrate their services into eduGAIN**
  - Incorporating adoption and dissemination of Federation current best- practice solutions

11 Use-Cases Submitted by FIM4R group
Initial focus on 3, later more to follow

SeaDataNet

CRISP
The Cluster of Research Infrastructures for Synergies in Physics

pandata
Photon and Neutron Data Infrastructure

(Umbrella)

BioVeL

DARIAH-DE

CLIPC

LIGO

SU:MA

VERCE

esa

WLCG
Worldwide LHC Computing Grid

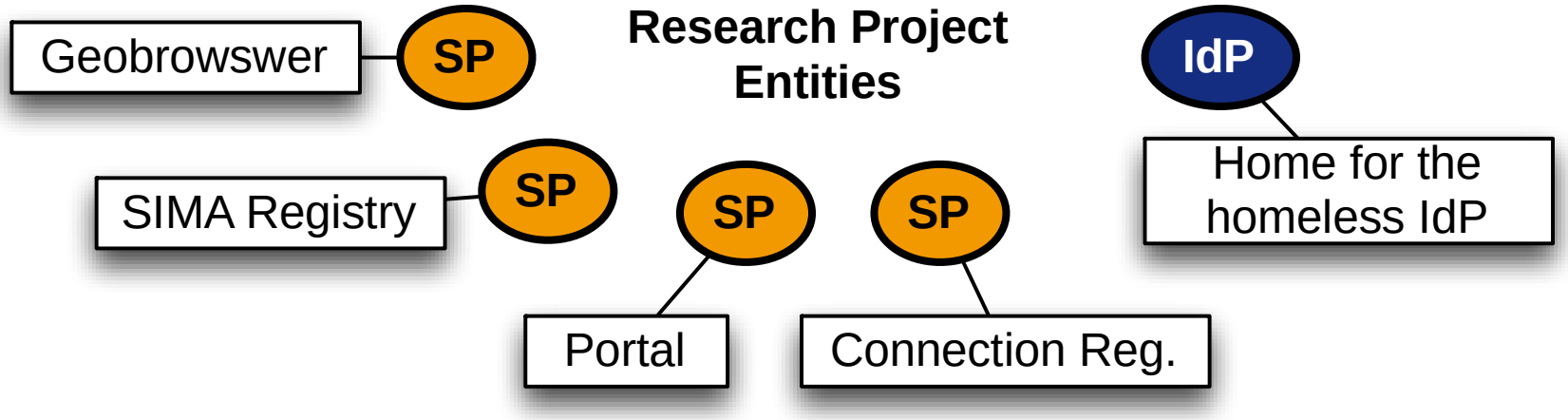
elixir Data for Life

8

DARIAH how we see it

- **DARIAH community (and other DASISH communities) are likely to operate many services (SPs) in different countries**
  - In contrast to other research communities which probably will operate only few SPs
- **Hand-full of services and Homeless IdP are already SAML-enabled**
  - Including a mechanism to deal with users where only the persistentId attribute is available
- **DARIAH LDAP and Admin Portal for permission and authorization management**
- **Main questions are:**
  - How to best integrate services/SPs into eduGAIN?
  - How to ensure SPs receive required attributes?

Situation from AAI/SAML perspective



Entities typically operated by a research community:

- **Multiple Service Providers**
  - DARIAH has so far about 5-10 Service Providers
  - Number is likely to grow
- **One Identity Provider** (home for the home-less)
  - Unless it relies on the guest Identity Provider of somebody else

Priorities

To make use of eduGAIN, it's primarily the Service Providers that have to be added to eduGAIN from one communities' point of view.

- Allows researchers accessing a service using their university/research institution account

Adding the Identity Provider(s) to eduGAIN is less important

- Allows users managed by that community to access other eduGAIN services outside of that community
- Allows bridging different communities

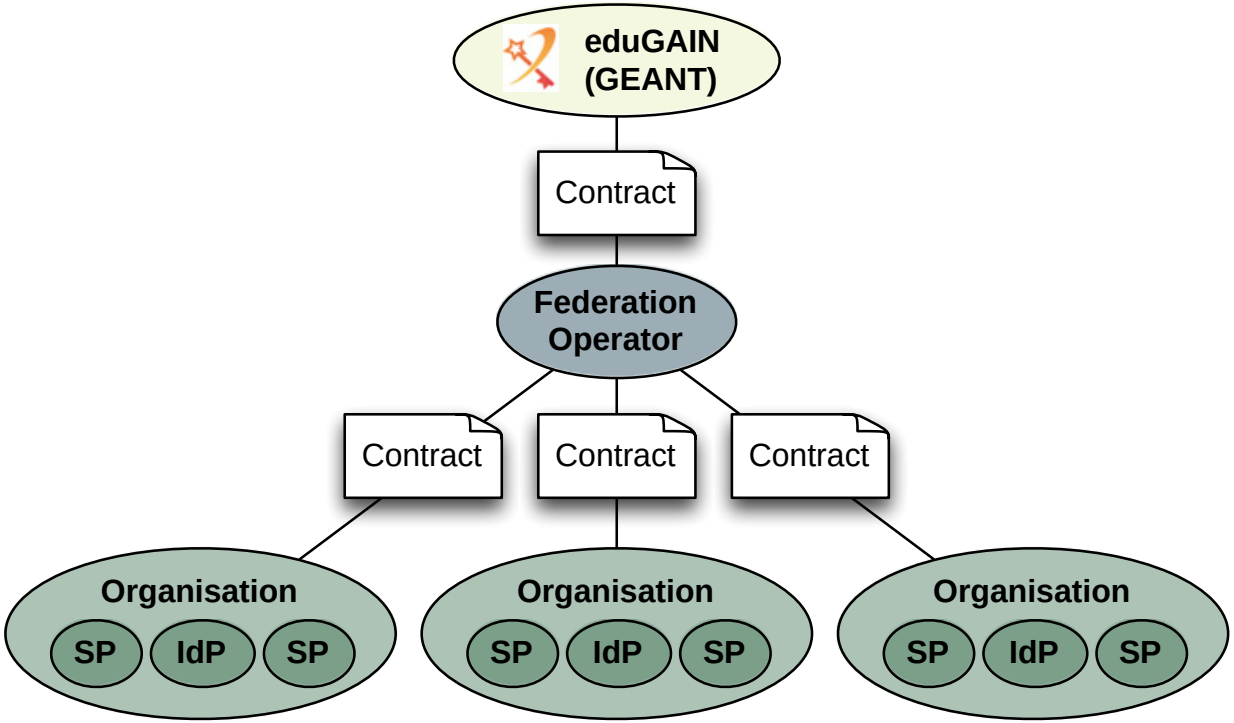
Options to join eduGAIN

- **Option A: Join via existing federation**
  Let each service join eduGAIN via an existing federation (e.g. the national federation that already exists)

- **Option B: Create your own federation**
  Organize all services in an own federation and join with the whole federation

- **Option C: Use a hub/proxy**
  Place all services behind a hub/proxy and add that proxy via an existing federation to eduGAIN

eduGAIN Membership



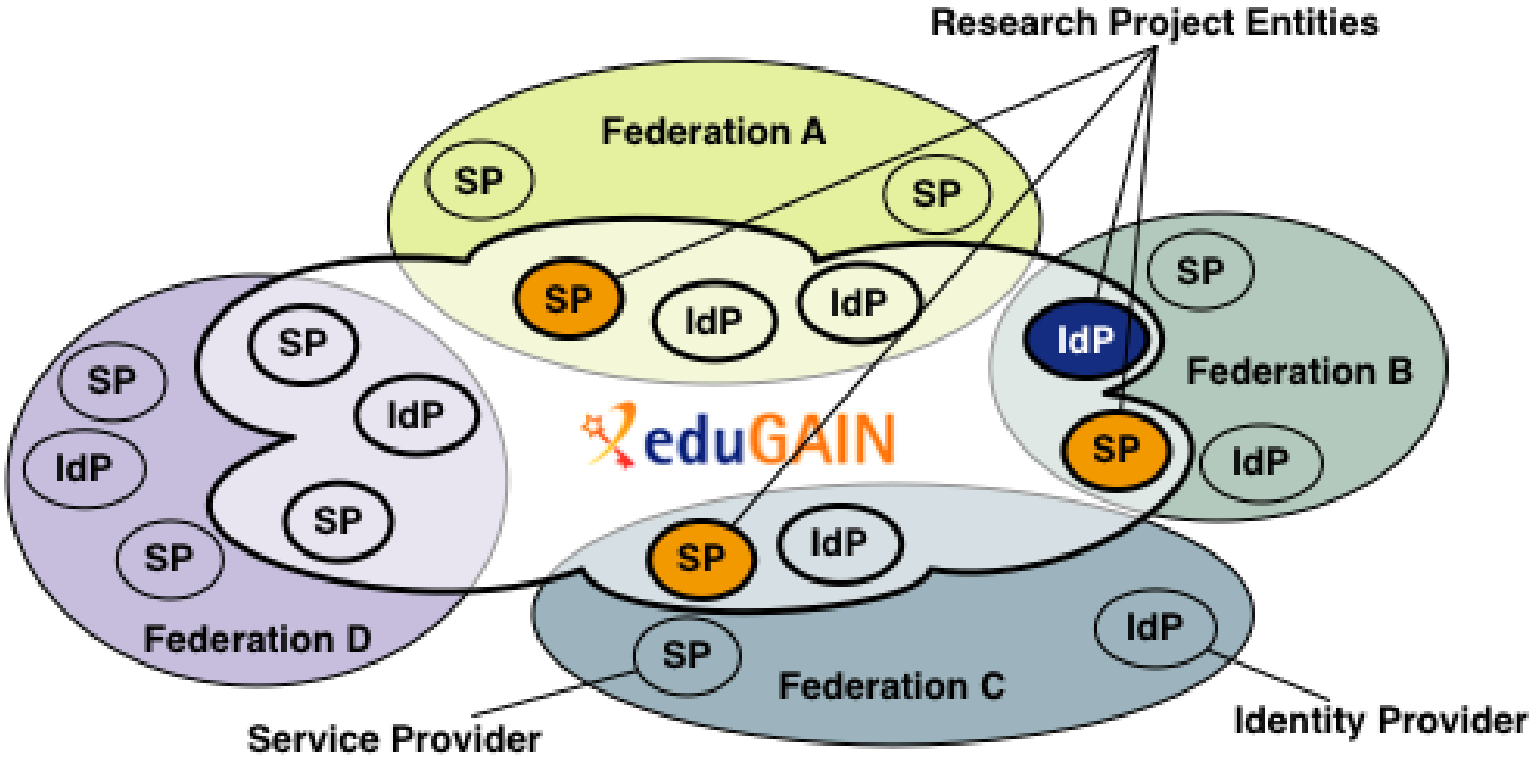
- Only **federations** can become eduGAIN members
  - eduGAIN is an interfederation service and not a federation itself
  - It is not possible for an SP or IdP to directly join eduGAIN
  - eduGAIN operations team and efforts can be kept small

Requirements to become eduGAIN member federation

- **Formal requirements:**
  http://www.edugain.org/technical/joining_checklist.php
  - Sign and agree with eduGAIN policy/constitution
  - Provide upstream metadata according to eduGAIN MD profile
  - Name representative and deputy for eduGAIN steering group
  - Federation has to primarily serve research and education
  - Must be accepted by eduGAIN steering group

- **Federations usually also:**
  - Have a name, logo, web page
  - Operates registration service to manage SPs /IdPs
  - Process and provide eduGAIN downstream metadata
  - Maintains support and helpdesk for their members
  - Provides central discovery service and home for the homeless IdP

Option A:
Add SPs via existing federation



Option A: Characteristics

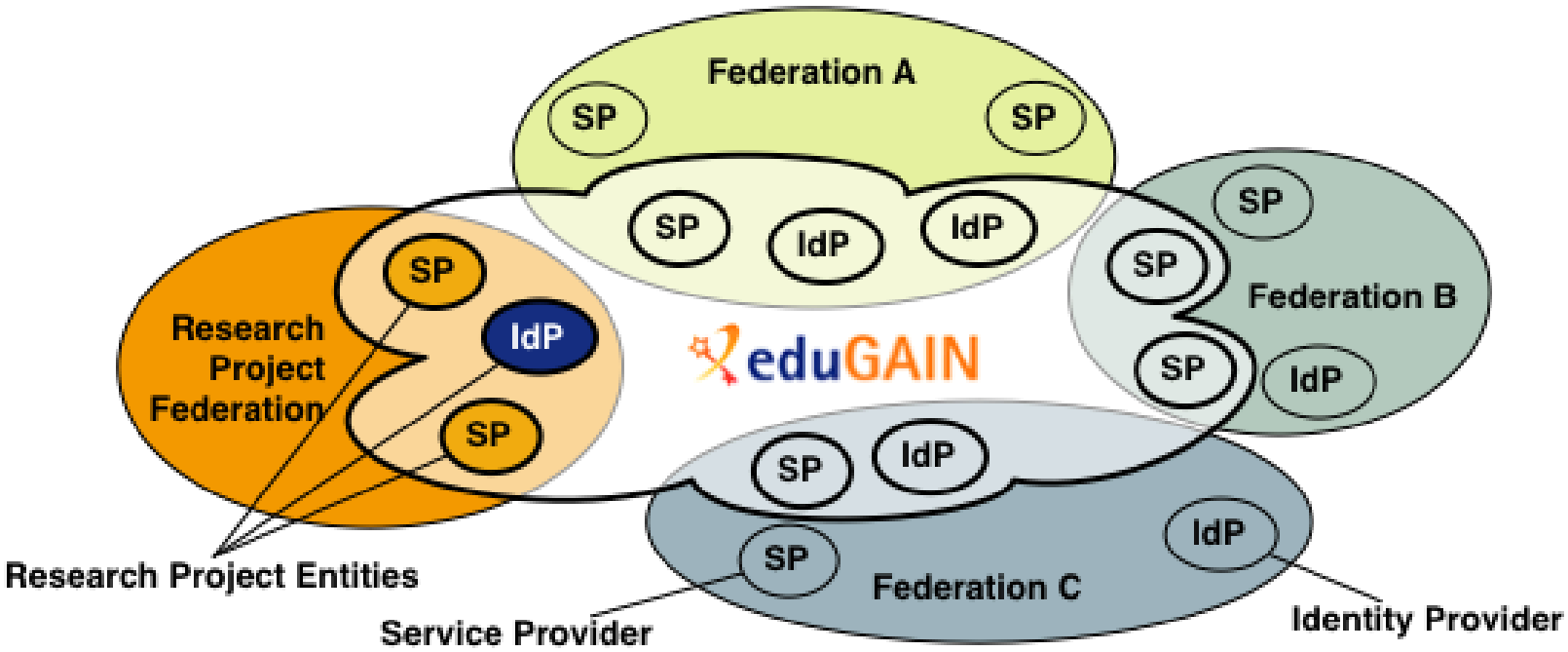
Pros/Cons:

- ⊕ Technically straight-forward
- ⊕ Re-use know-how, infrastructure, documentation, guides, policies, legal framework, processes of existing federations
- ⊕ Transparent from the user's point of view and not different from accessing any other service within the local federation
- ⊖ Deployment/registration procedures vary from federation to federation
- ⊖ Home-less-IdP might not be easy to add to eduGAIN (depends on federation: fees, liability, ...)

Examples:

Currently in eduGAIN metadata are science gateways from African Grid community, INDICATE E-Culture, agINFRA, DECIDE, EarthServer, EUMEDGRID, GISELA and IGI

Option B:
Create an own federation



Federation Types

- Three federation architectures are currently used for national federations:
  - Full-mesh federation
  - Hub-and-spoke with distributed login
  - Hub-and-spoke with central login

- Choice depended on:
  - Political/financing situation in a country
  - (Trust) Relation between participating organisations and federation operator

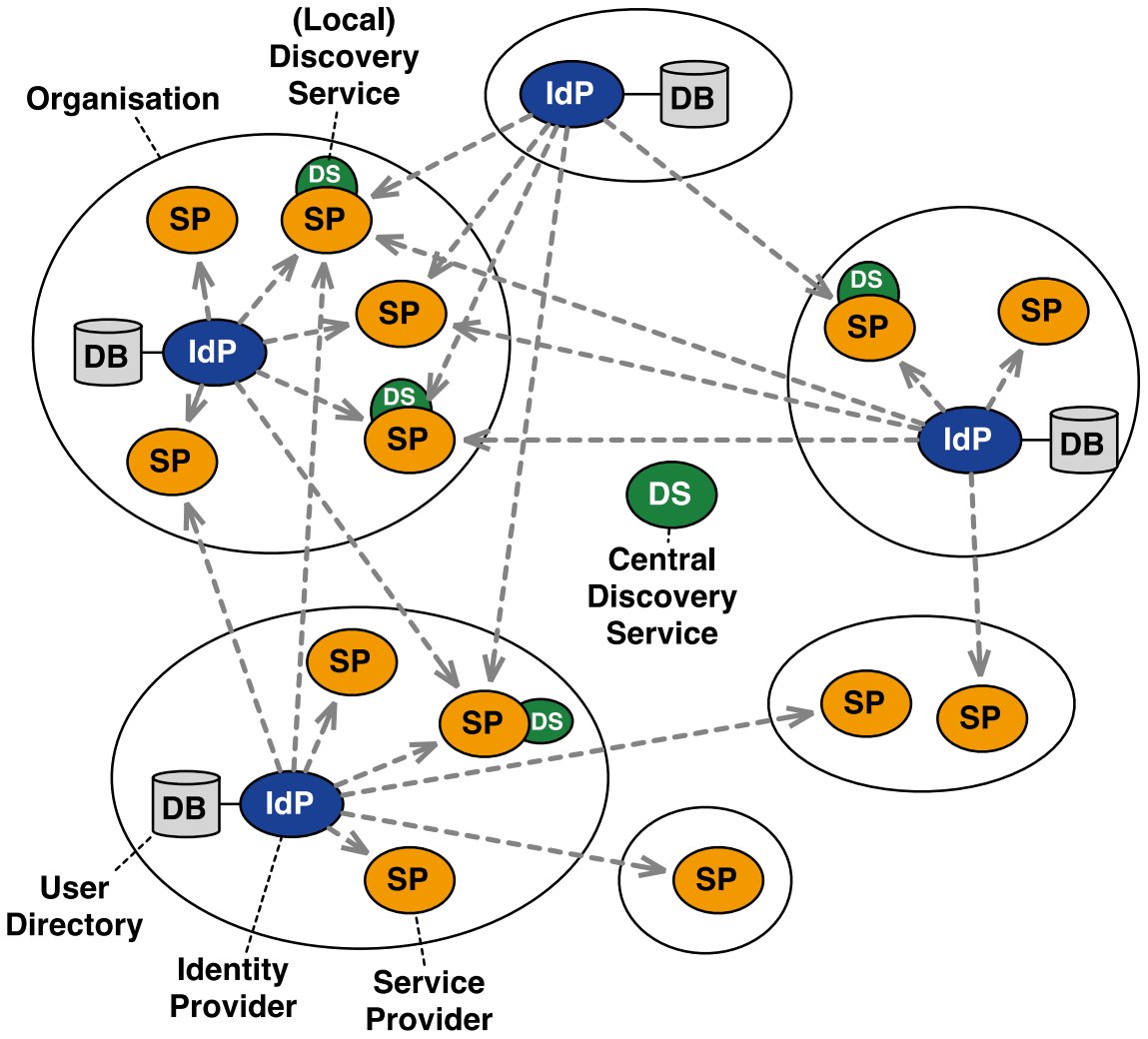
Same models could be used by a research community that decided to create an own federation.

Full Mesh Federation

~80% of all NREN Federations (June 2013)

E.g

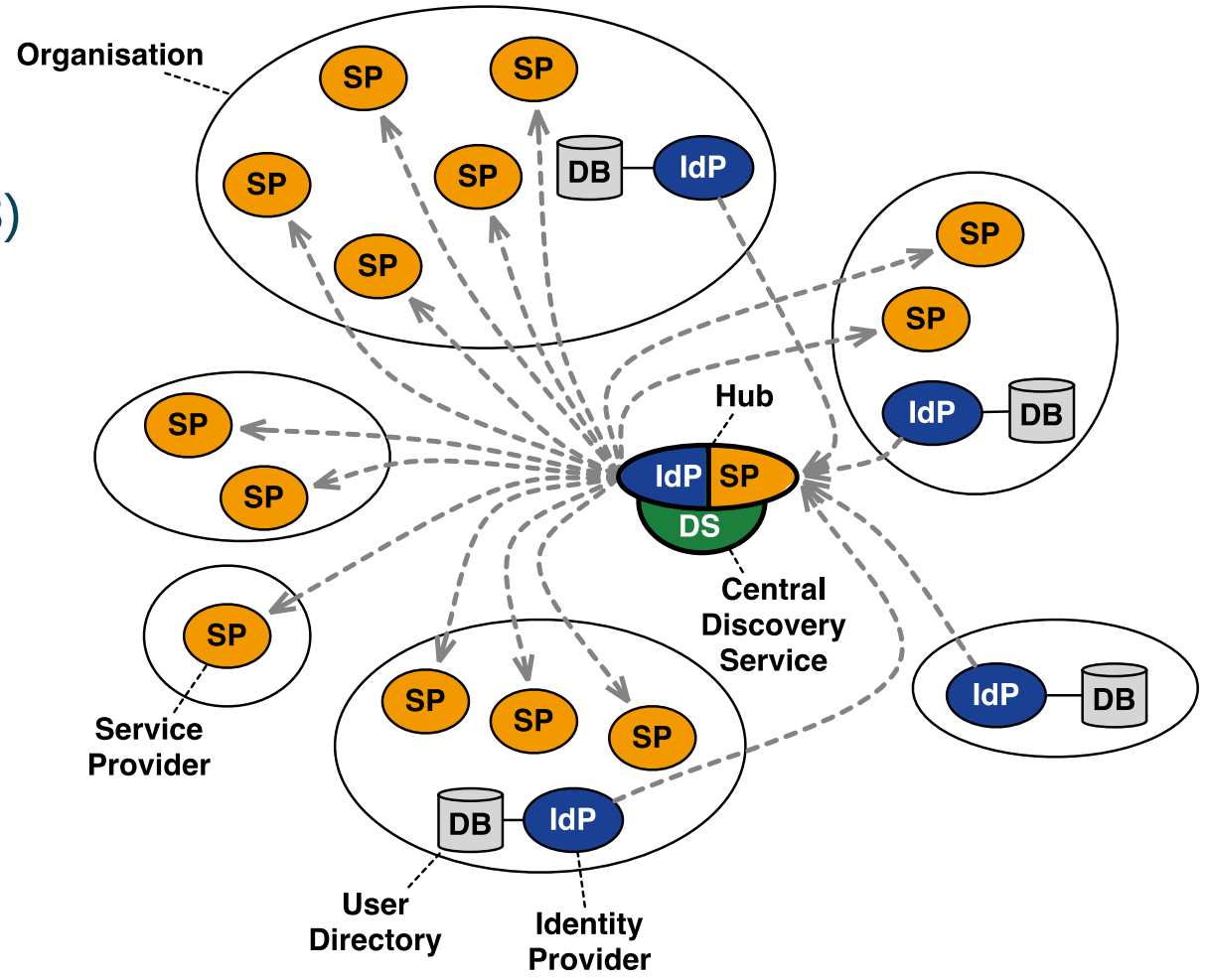
- InCommon
- UKAMF
- SWAMID
- HAKA
- DFN-AAI
- SWITCHaai
- ...



Hub-and-Spoke Federation with Distributed Login

~15% of all NREN Federations (June 2013)

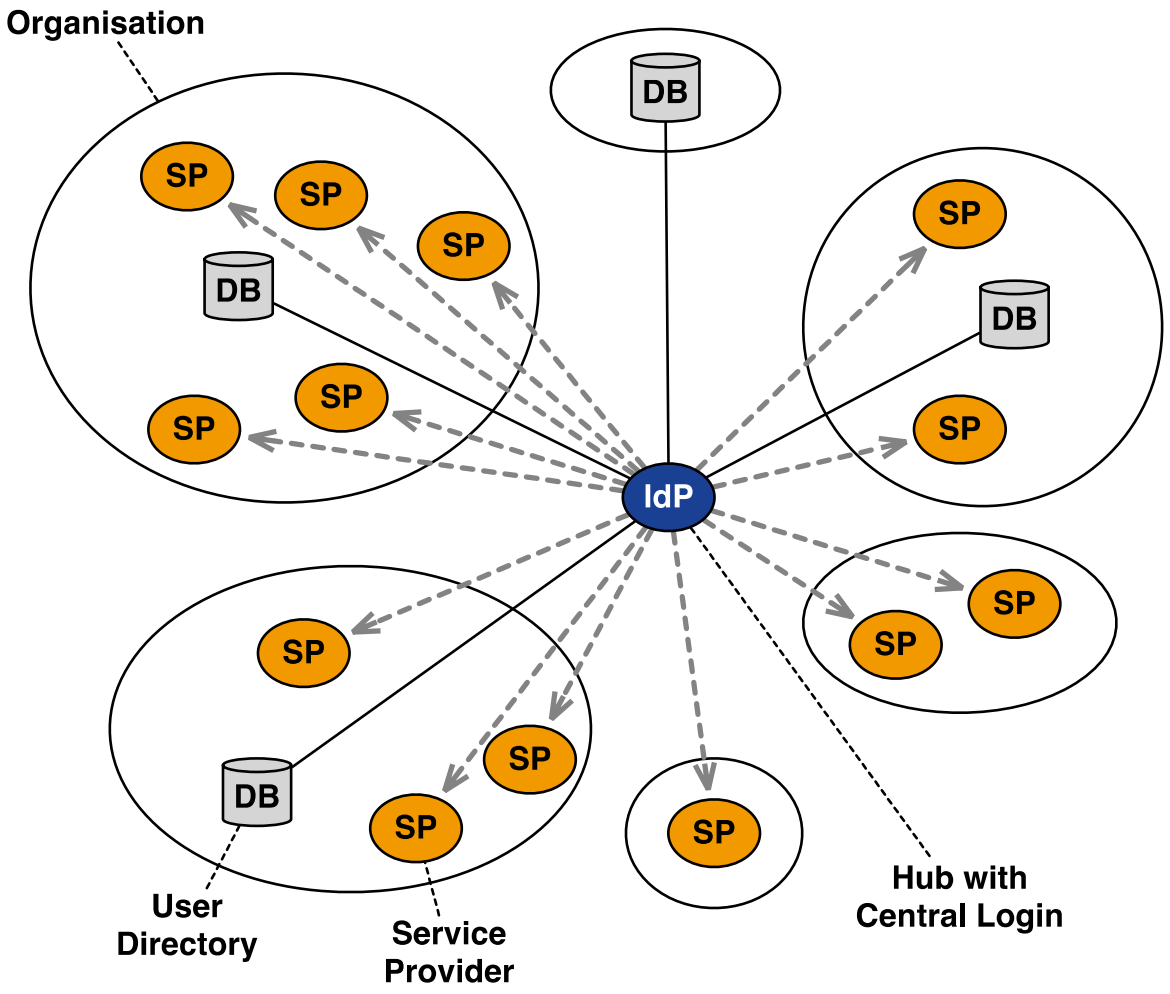
- SURFconext
- WAYF.dk
- SIR
- TAAT
- Confia



Hub-and-Spoke Federation with Central Login

~5% of all NREN Federations (June 2013)

- FEIDE
- AAI@EduHr



Option B: Characteristics

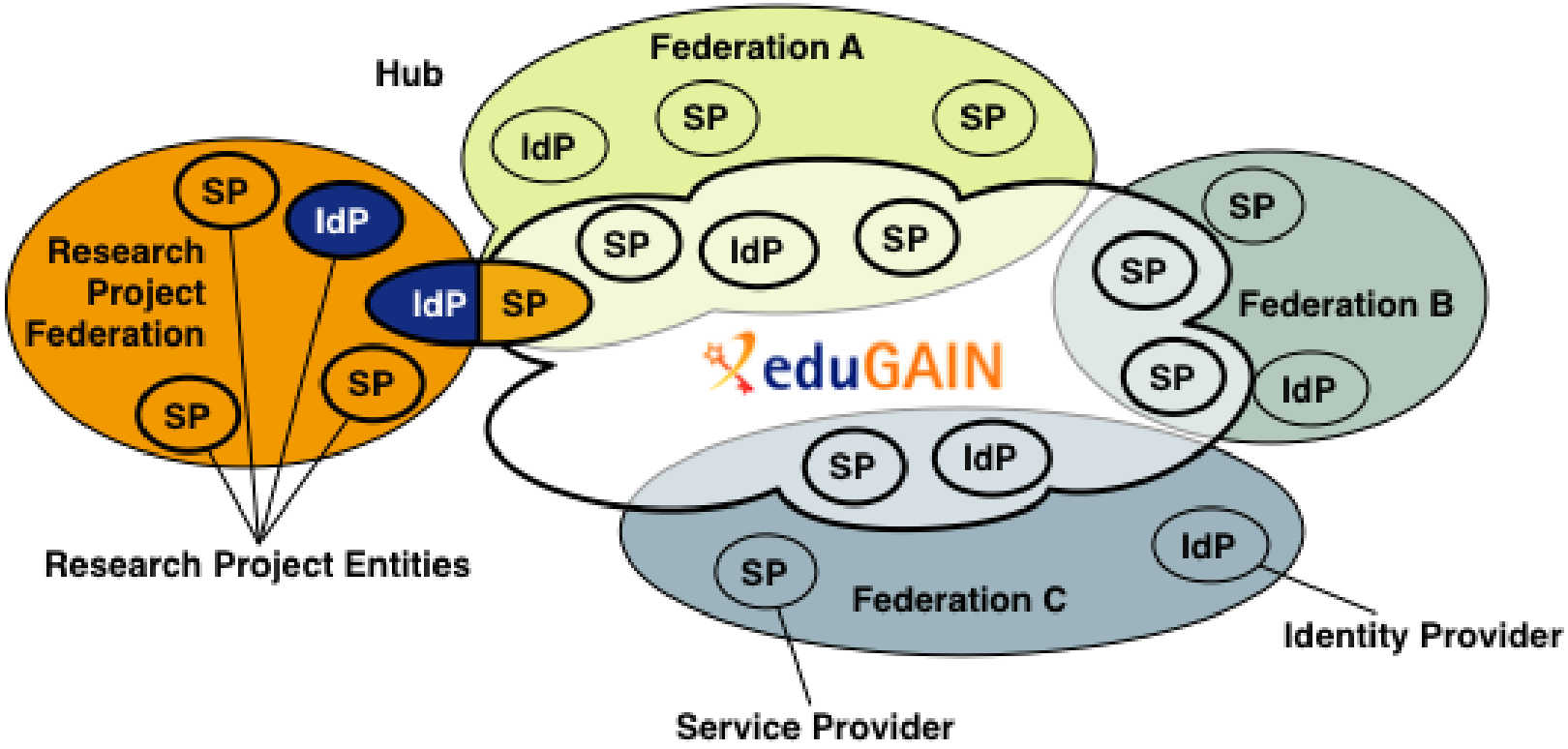
Pros/Cons:

- ⊕ Influence on eduGAIN via the eduGAIN Steering Group
- ⊕ Consistent registration of SPs/IdPs across national boundaries
- ⊕ Potentially beneficial for getting more user attributes
- ⊕ Transparent from the user's point of view and not different from accessing any other service within the local federation
- ⊕ Technically straight forward. No problem adding IdPs to eduGAIN.
- ⊖ Potentially quite some overhead to manage the federation (metadata management, deployment guides, helpdesk/support, policies). Will require some permanent service unit

Examples:

CLARIN Service Provider Federation (SPF). Not in eduGAIN as a federation currently.

Option C1:
Join via a Hub



Option C1 Characteristics

Similar like model B (Own federation) using a hub-and-spoke federation with a central login.

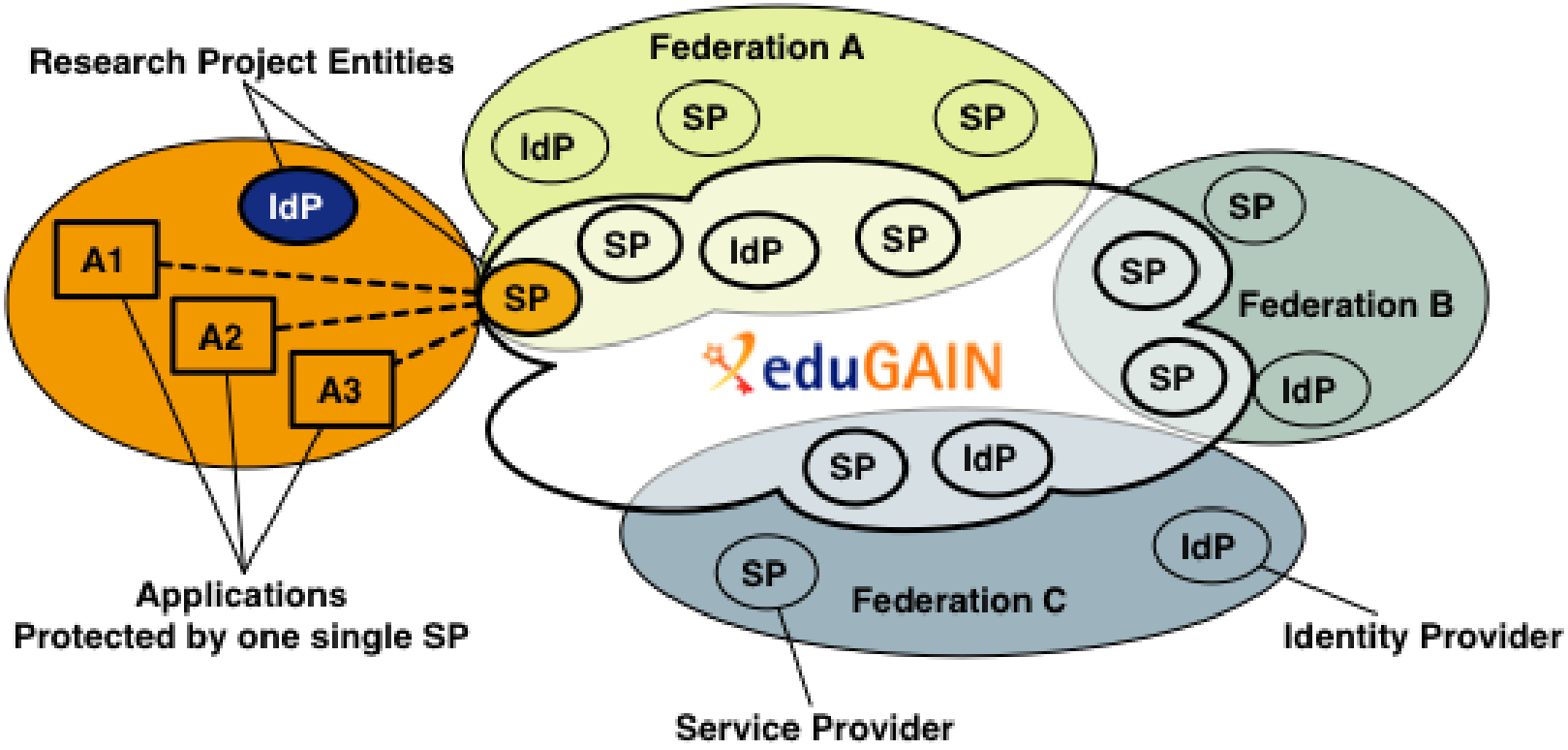
Pros/Cons:

- ⊕ Extend/Transform/enrich user data at the hub
- ⊕ Bridging communities becomes easier if hub supports multiple protocols
- ⊕ Unique identifier attribute sufficient for a user
- ⊕ Registration of only a single SP (and potentially an IdP)
- ⊖ Requires development work because no out-of-the-box solution exists
- ⊖ Hub becomes single point-of-failure
- ⊖ Hub hides all services behind it -> intransparent for user

Examples:

Umbrella (CRISP/PaNdata) large photon and neutron research community

Option C2:
Join via a (Web) Proxy



Option C2 Characteristics

One (Web) proxy with an SP protects multiple applications on different hosts behind the proxy. Sub-type of C1. Relatively easy to deploy using Apache and Shibboleth. Also combines with Options A,B and C1.

Pros/Cons:

- ⊕ Operate only one SP with a moderately complex configuration.
- ⊕ Can be operated completely transparent or hide all applications
- ⊕ Unique identifier attribute sufficient for a user
- ⊕ Registration of only a single SP (and potentially an IdP)
- ⊖ Proxy becomes single point-of-failure
- ⊖ If applications are hidden -> intransparent for user
- ⊖ Increased complexity and harder to debug problems

Examples:

Number of universities chose this approach for their services.

3 Recommendations for DARIAH

1. **Choose option A or B**
   - It's basically a question of commitment: How much long-term financial and personal resources are available to operate an own federation?

1. **Implement the GÉANT Data Protection Code of Conduct**
   - No silver bullet to get all attributes immediately but currently the best chance.
   - DARIAH already has a technical solution to cope with missing attributes issue

2. **Be patient**

Thank you!

Connect | Communicate | Collaborate

www.geant.net

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