

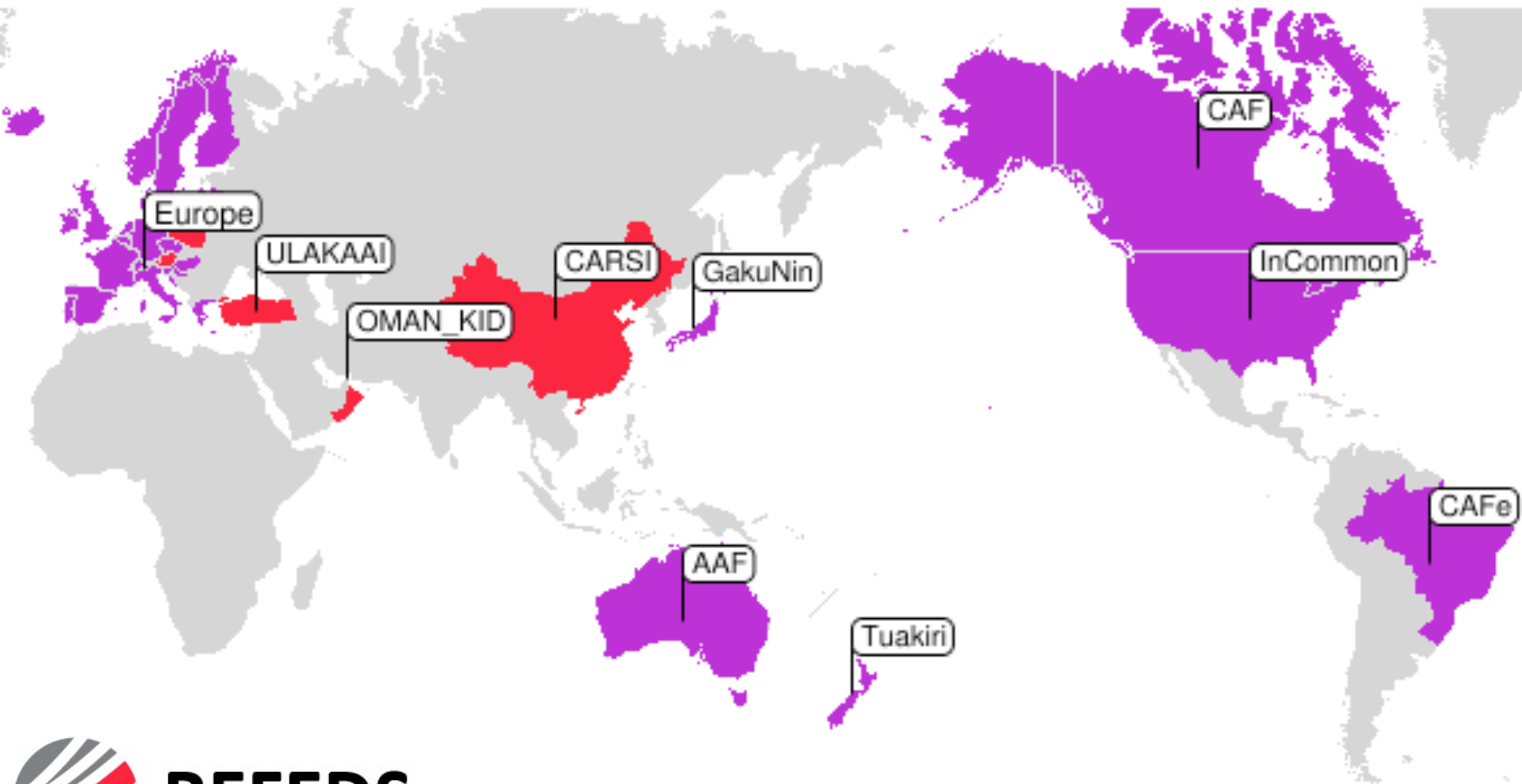
eduGAIN: services and identity

Brook Schofield
eduGAIN Task Leader, GN3 Project &
Project Development Officer, TERENA

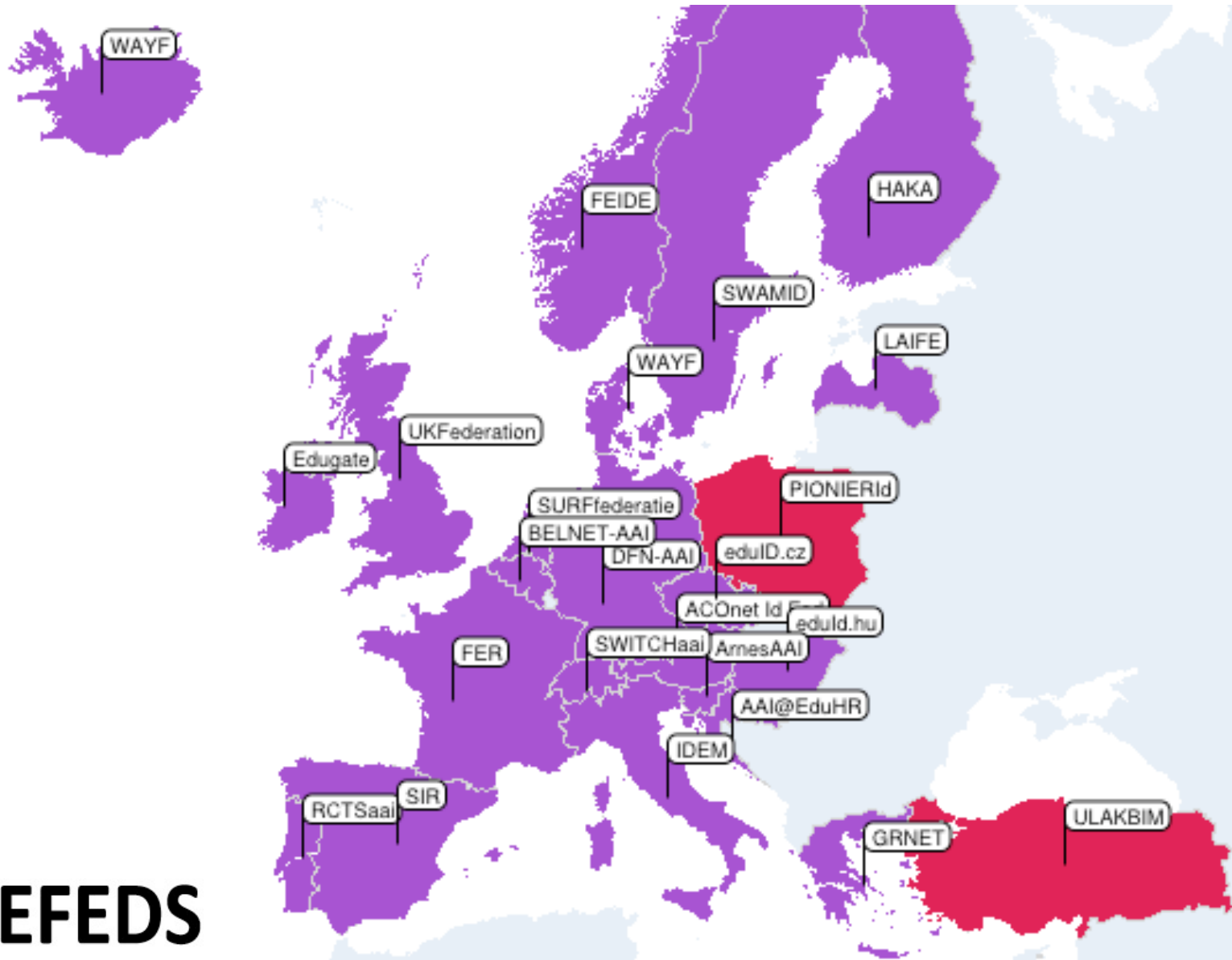
schofield@terena.org

Identity Federations

■ Pilot ■ Production



European Identity Federations



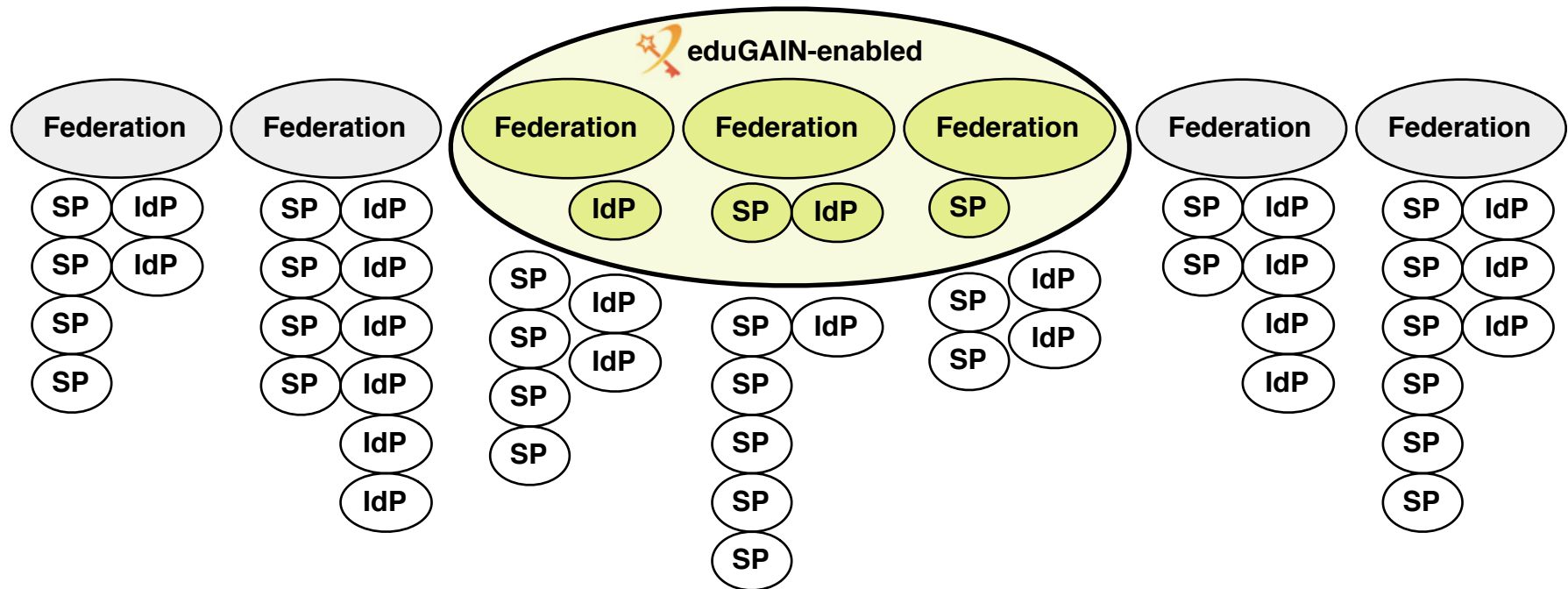
GÉANT

-

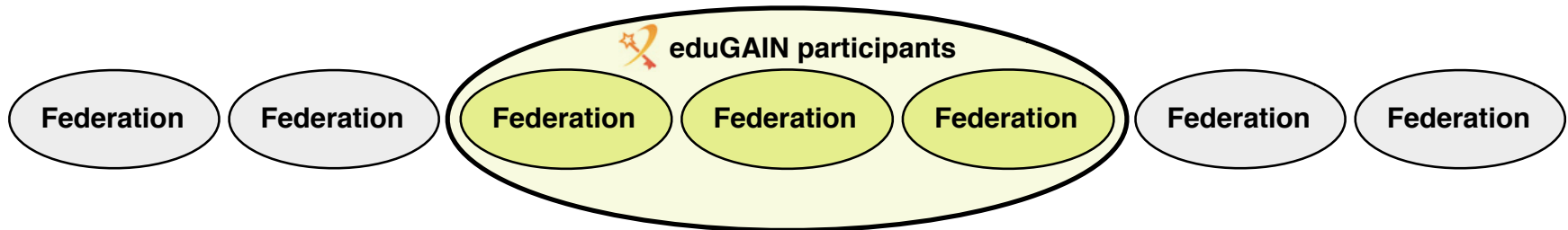
A map of Europe showing the distribution of the three main language families. The map uses a color-coded system: green for Indo-European languages, yellow for Uralic languages, and blue for Caucasian languages. Indo-European languages are the most widespread, covering most of Western and Central Europe, as well as parts of Northern Europe and the Balkans. Uralic languages are found in a band across Northern Europe, including Scandinavia and parts of Russia and Central Europe. Caucasian languages are concentrated in the Caucasus region, primarily in Georgia and Armenia.

Innovation through participation

Adoption Width vs Depth



- Good federation adoption (Width)
- Entity Adoptions (Depth) has yet to grow



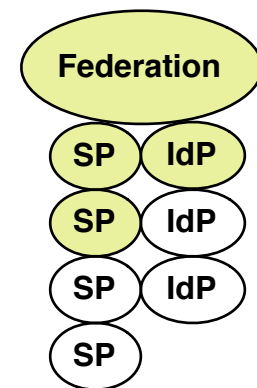
- **55% of European of national federations are eduGAIN participants**

Or 40% of total 30 national federations worldwide

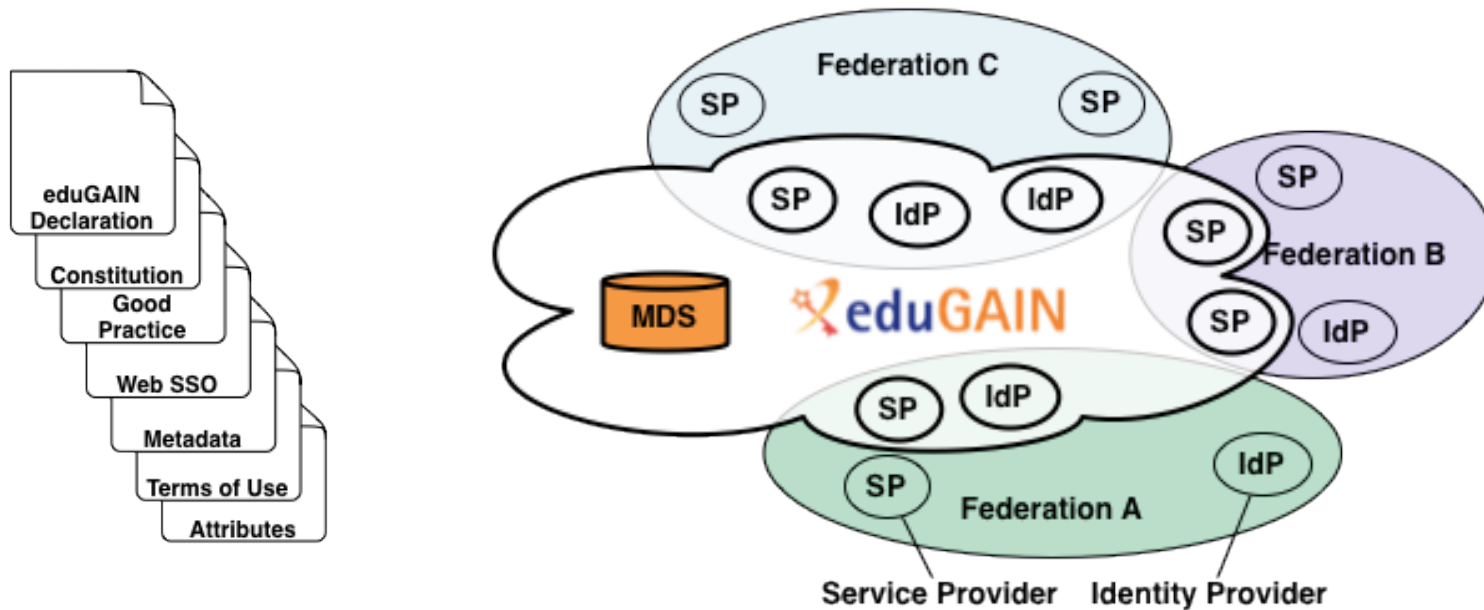
Source is Refeds Wiki: <https://refeds.terena.org/index.php/Federations>

- **About 2% entities opted-in so far**

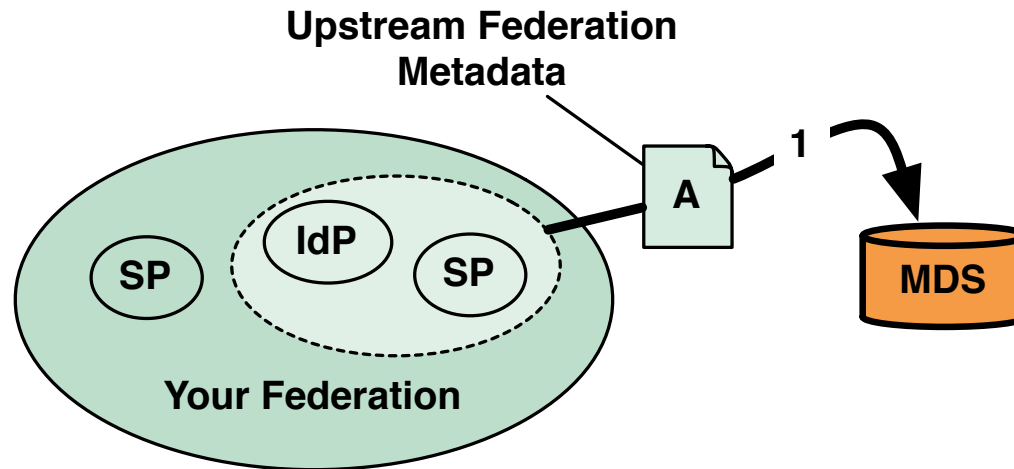
- Out of about 2500 SPs and IdPs that eduGAIN members operate
- Half of entities are SPs
- Note: It is not reasonable for every SP and IdP to interfederate!



What makes up eduGAIN?

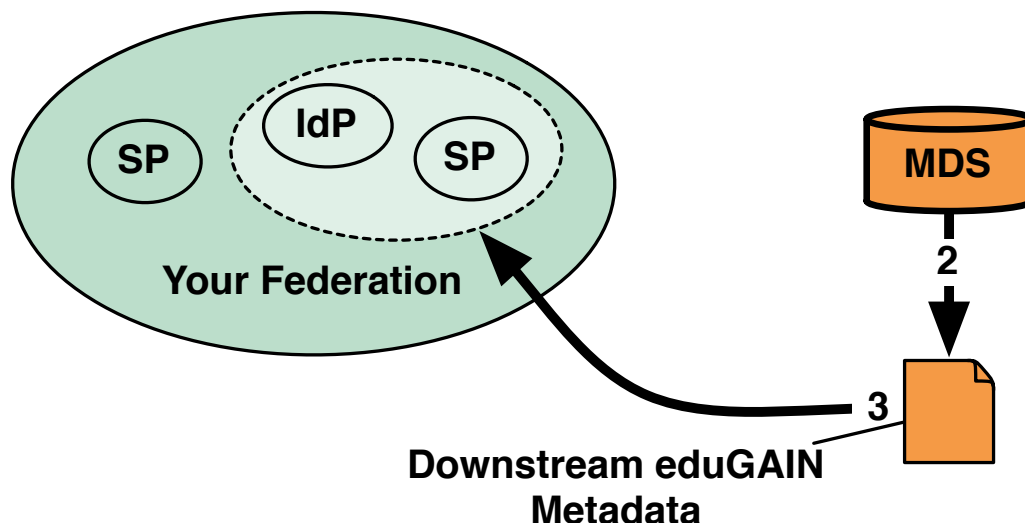


- eduGAIN entities are a subset of a national federation (via opt in)
- Profiles and policies to harmonize environment



Goal

- Generate SAML 2 metadata document and sign it
- Metadata must contain only local federation entities that opted-in
- Format and elements must meet eduGAIN Metadata Profile
- Publish metadata document online
- Send URL of document together with signing cert to OT



Goal

- Download eduGAIN metadata from MDS
- Verify signature using the eduGAIN signing certificate
- Process metadata (adding/removing/modifying entity data)
- Sign metadata using a certificate known in your federation
- Publish new metadata document to opt-in subset of your federation

Phonebook publishing tools...



Question	SWITCH RR	Fed Reg AAF	JANUS-SSP	In-House
Which Federation?	SWITCHaai, Haka, NIIF, Edugate	AAF, Tuakiri (NZ), CAFé	WAYF, SURFconext	Belnet, AConet-aa, RENATER, AAI@EduHR, SURFfederatie
Customisation	Lots	None		Lots
Language	Java, PHP	Groovy	PHP	XSLT, Perl, PHP
Missing Features	Dependent on generation of software.	eduGAIN “opt-in”, MDUI, MD Aggregation	*eduGAIN “opt-in”, MD Aggregation	Self-Service, eduGAIN “optin”, MDUI, MD Aggregate

*Process available but requires documentation.

NB:- Signing of metadata outside the scope of these tools – solutions exist.



- “Federation Infrastructure” training
 - simpleSAMLphp IdP & Shibboleth SP
 - JANUS-SSP for Metadata Management
 - Istanbul mid 2011 and Amsterdam late 2011
- “How to write a federation policy” training
 - SWAMID Policy (technology independent) + explain it
 - REFEDS research on Federation Policies
 - Template Policy as the basis for new federations (eduroam + IdFed)
 - ...“Federation-as-a-Service”
- Code of Conduct for Personally Identifiable Data Transmission
 - Stop people being scared of data protection rules
- Develop around a smaller set of MD Aggregators + MD Registries
 - Aggregators are the 1st step – Shibboleth MA1