eduGAIN – Updates since October 2013

Lukas Hämmerle

DASISH Strategy Workshop
Neijmegen, 10 March 2014

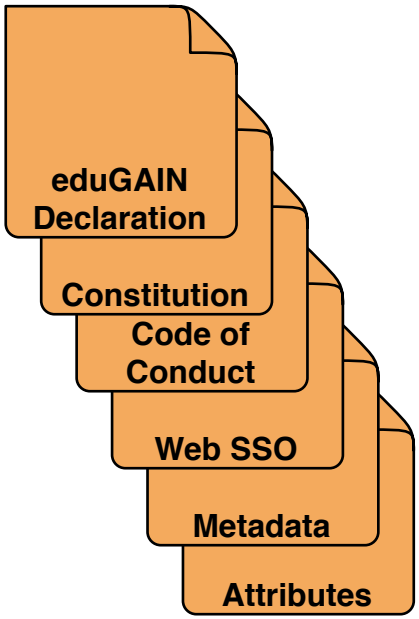
All About eduGAIN…

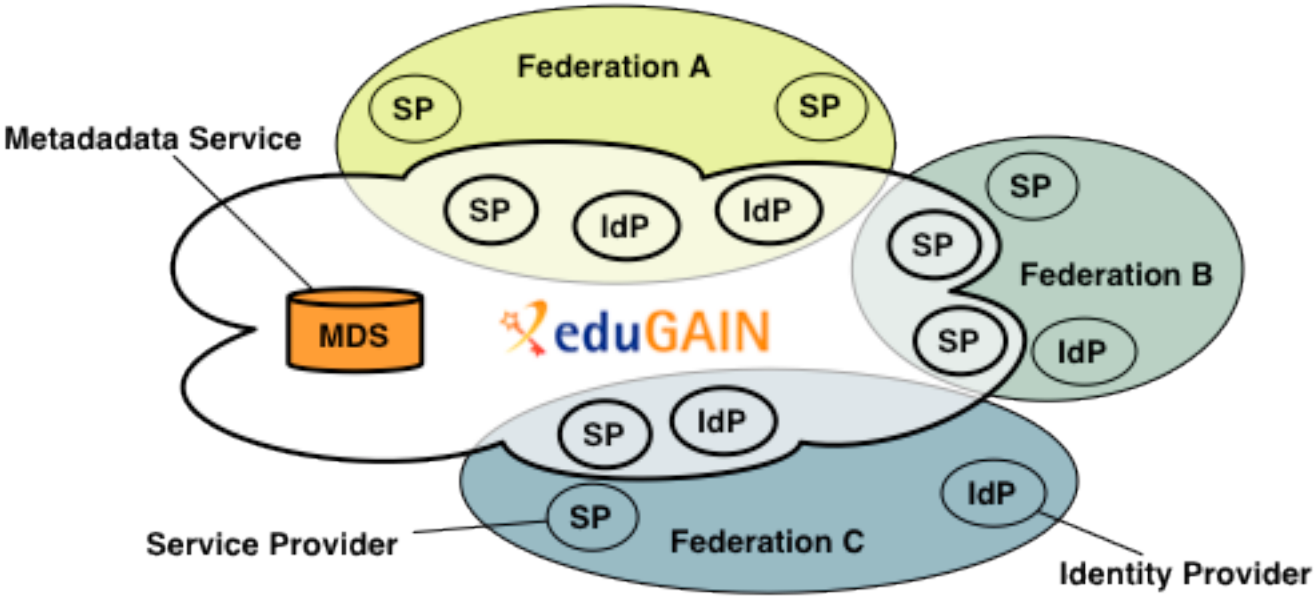
- ***G***lobal ***A***uthentication ***IN***frastructure
- Web site: http://www.eduGAIN.org
- SAML2-based
  - Currently mostly web-based services but non-web services are supported too (e.g. via SAML ECP)
- An interfederation service ***primarily*** for Research & Education
  - Connects existing SAML-based academic identity **federations**
- Developed and funded by European GÉANT projects
  - But open also to non-European federations

CLARIN Feedback on eduGAIN
GÉANT International User Advisory Com.

- "eduGAIN is currently not in a state that it can be used for production-purposes in a research infrastructure as CLARIN"
- CLARIN recommends:
  - "move from an opt-in to an opt-out policy"
  - "make the release of relevant attributes mandatory"
- Based on Tests from April 2013
- Honest and constructive feedback
- We are building eduGAIN **for you and with you**!

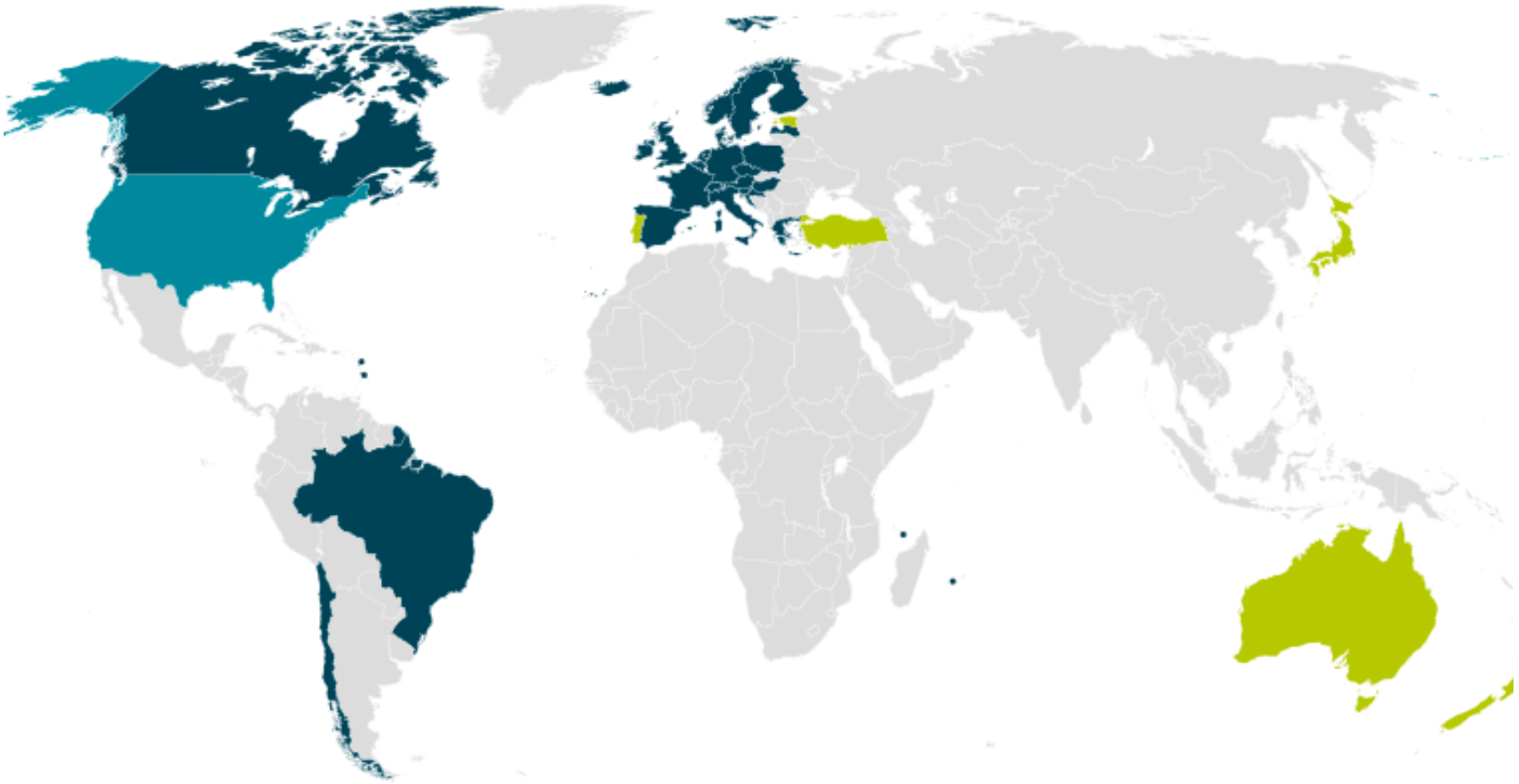
What is eduGAIN?





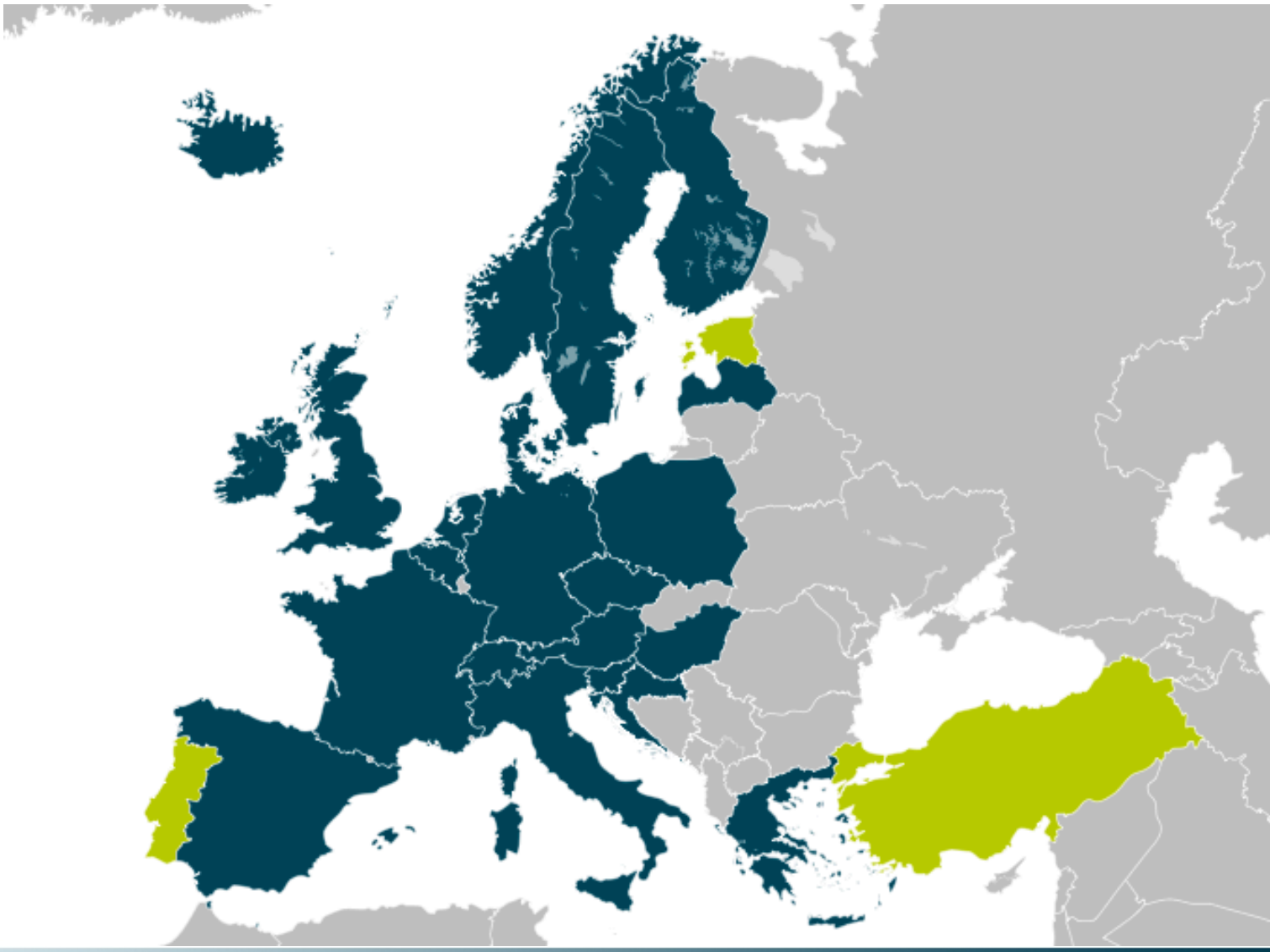
- eduGAIN provides policy framework and standards to build trust
- SPs and IdPs of participating federations should opt-in for eduGAIN
- MDS fetches, aggregates and republishes metadata

eduGAIN Interfederation Participants



24eduGAIN Members
6 Joining eduGAIN
1 Candidate Federations

And in Europe



Statistics

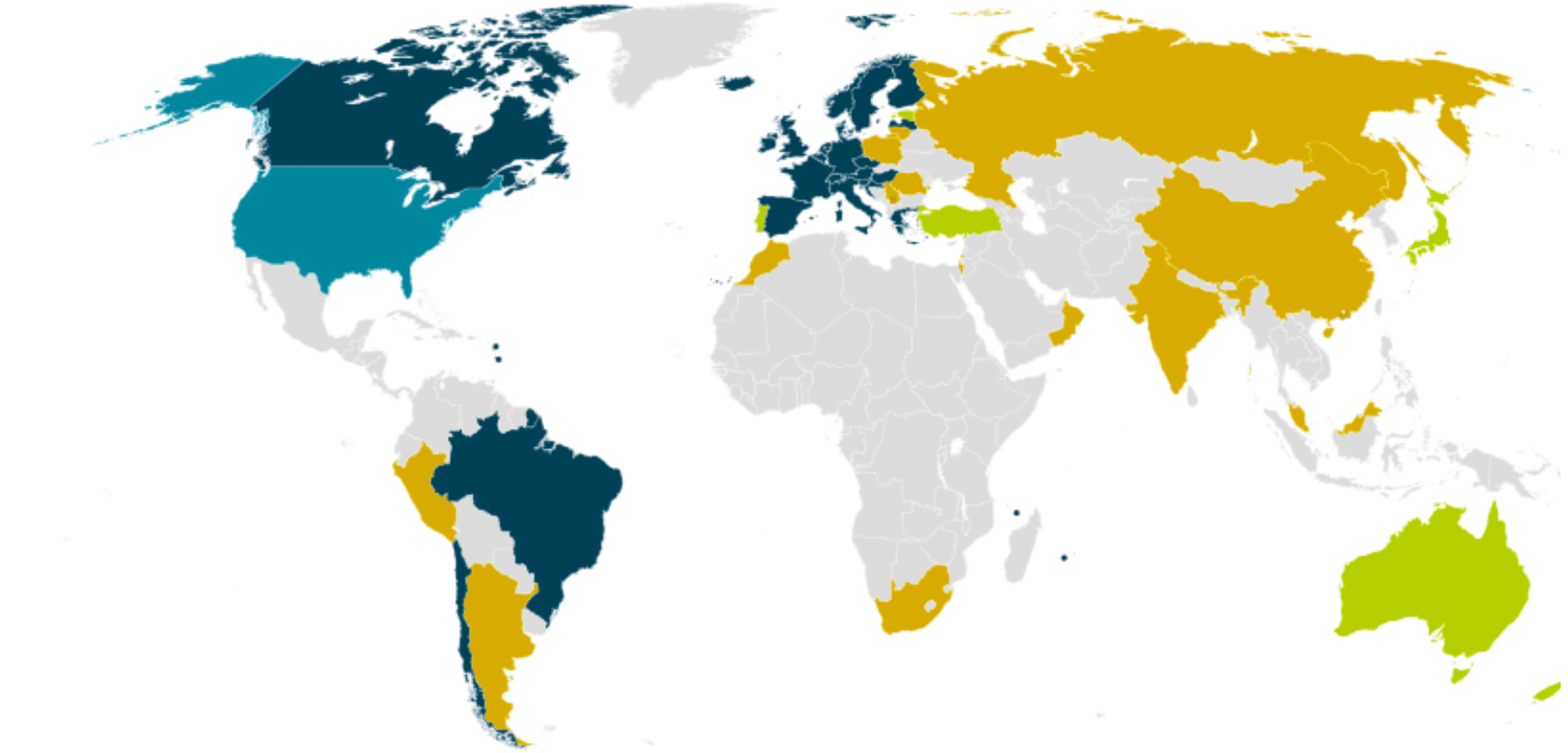
- **April 2011:** Official start of eduGAIN

- **Now: 24 Federations** (+5 since 2. October 2013 = 5 months)
  New: Ireland, Austria, Poland, Chile, Slovenia
  6 federations joining (= policy signed but some information/ technical adaptations missing)

- **Current Entities: 200 (+57 = + 40%) IdPs, 104 (+31 = +42%) SPs**
  Note: One IdP can stand for dozens of organisations depending on federation architecture (hub-and-spoke federations = 1 SP + 1 IdP)

- **Whole (academic) SAML landscape:**
  46 (+3) Federations, 2463 (+73) IdPs, 5101 (+447) SPs
  Numbers from http://www.terena.org/~schofield/servicecatalogue/
  Not all of them need to be interfederated, e.g. many internal SPs

eduGAIN & Federation Status



24 eduGAIN Members
6 Joining eduGAIN
1 Candidate Federations
15 Emerging Federations

Code of Conduct I

- GÉANT Data Protection Code of Conduct
  Describes behavioral data protection rules for Service Providers.
  Main goal is to make it easier for Identity Providers to release attributes.

- Finalized 14 June 2013 (after CLARIN tests)

- Applicable for:
  EU28, Norway, Iceland, Liechtenstein, Switzerland, Argentina, some Sectors in Canada, US Safe harbour, ...
  Currently being implemented/deployed by many federations:
  https://refeds.terena.org/index.php/Data_protection_coc

Code of Conduct II

- Endorsement letter
  Signed by heads of large research communities
  Allows federation operator to approach IdP admins and motivate them to speed up CoCo adoption

- Main focus now on international (REFEDS) CoCo:
  https://refeds.terena.org/index.php/International_dp_coc
  Applicable if service is operated in country not in EU/EAA or
  http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

- CoCo Monitoring
  Shows all SPs in eduGAIN that support CoCo (and all others)
  http://monitor.edugain.org/coc/

CoCo Monitor

eduGAIN
PART OF THE GÉANT SERVICES PORTFOLIO

Service providers | All SP test results | Instructions

					Yes	All		
entityID	**registrationAuthority**	**DisplayName**	**First seen**	**Last seen**	**CoC found**	**Status**	**Comment**	**PrivacyStatementURL**
SP data					Last test results			
http://sp.lat.csc.fi	http://www.csc.fi/haka	LAT – Language Archive Tools	2013-10-01 20:35:19	2014-03-09 17:07:04	Yes	All attributes present, privacy statement has a link to CoC		http://www.csc.fi/english/research/sciences/linguistics/lat-privacypolicy
https://clarin.ids-mannheim.de/shibboleth	https://www.aai.dfn.de	Institut für Deutsche Sprache (IDS) - CLARIN services	2013-10-01 20:35:19	2014-03-09 17:07:04	Yes	All attributes present, privacy statement has a link to CoC		https://clarin.ids-mannheim.de/privacy.html
https://filesender.funet.fi	http://www.csc.fi/haka	Funet FileSender	2013-10-01 20:35:20	2014-03-09 17:07:04	Yes	All attributes present, privacy statement has a link to CoC		https://filesender.funet.fi/privacypolicy.html
https://foodl.org/simplesaml/module.php/saml/sp/metadata.php/saml	http://feide.no/	Foodle	2013-10-01 20:35:21	2014-03-09 17:07:05	Yes	All attributes present, privacy statement has a link to CoC		https://rnd.feide.no/software/foodle/foodle-privacy-policy/
https://openskos.meertens.knaw.nl/shibboleth	https://www.aai.dfn.de	OpenSKOS | Meertens	2014-03-05 11:07:08	2014-03-09 17:07:06	Yes	All attributes present, privacy statement has a link to CoC		http://www.meertens.knaw.nl/cms/en/collections/data-protection
https://repos.ids-mannheim.de/shibboleth	https://www.aai.dfn.de	Institute for the German Language (IDS) - Respository	2013-10-01 20:35:22	2014-03-09 17:07:06	Yes	All attributes present, privacy statement has a link to CoC		https://repos.ids-mannheim.de/privacy.html
https://rr.funet.fi/attribute-test	http://www.csc.fi/haka	Haka Attribute Test Service	2013-10-01 20:35:22	2014-03-09 17:07:08	Yes	All attributes present, privacy statement has a link to CoC		https://confluence.csc.fi/x/6o4uAg
https://sp.catalog.clarin.eu	https://www.aai.dfn.de	Clarin Catalog Service Provider	2013-10-01 20:35:23	2014-03-09 17:07:08	Yes	All attributes present, privacy statement has a link to CoC		https://catalog.clarin.eu/privacy_statement.html
https://sp.korp.csc.fi/	http://www.csc.fi/haka	Concordance search service for text corpora	2013-12-20 13:07:04	2014-03-09 17:07:09	Yes	All attributes present, privacy statement has a link to CoC		https://korp.csc.fi/privacy-policy.html
https://sp.lux17.mpi.nl	https://www.aai.dfn.de	Max Planck Institute for Psycholinguistics second Service Provider	2013-10-01 20:35:23	2014-03-09 17:07:09	Yes	All attributes present, privacy statement has a link to CoC		https://lux17.mpi.nl/privacy_statement.html
https://ufal-point.mff.cuni.cz/shibboleth/eduid/sp	http://www.eduid.cz/	LINDAT/CLARIN repository and services	2013-10-01 20:35:19	2014-03-09 17:07:09	Yes	All attributes present, privacy statement has a link to CoC		https://lindat.mff.cuni.cz/privacypolicy.html

Shows which SPs have implementec CoCo and privacy statement

Move from Opt-In to Opt-Out

- The French FER federation intends to move to "opt-out" for IdPs
  - French IdPs would be published to eduGAIN metadata by default
  - Attribute filters downloaded by French IdPs, would include rules to release attributes to SPs that support the CoCo
  - All eduGAIN SPs would be published in FER metadata
  - Federation registry would allow IdP admins to opt-out
- Opt-in still would apply for SPs

- The UK/Sweden integrated all eduGAIN SPs and IdPs in their federation metadata
  - Opt-in for an IdP/SP only requires publishing their metadata in eduGAIN metadata (sending an email to the federation operator)

eduGAIN Wiki

- wiki.edugain.org
  Target group are operators of eduGAIN services
  Content still being written and added.
  Open to any (eduGAIN-)authenticated user

- Knowledge-database for eduGAIN related topics
  https://wiki.edugain.org/How_to_set_up_a_Service_Provider_for_eduGAIN

- Deployment Guides. E.g.
  - How to support the CoCo:
    https://wiki.edugain.org/Recipe_for_a_Service_Provider
  - Templates for privacy statement
    https://refeds.terena.org/index.php/Privacy_policy_guidelines_for_Service_Providers
  - How to generate metadata
    https://wiki.edugain.org/Metadata_for_eduGAIN

Test Identity Provider

- Feedback from some research groups:
  - Would be great if there were test accounts to check that eduGAIN login works.
  - Commercial (cloud) providers don't have an own federated identity

- Solution that currently is specified:
  - Special Identity Provider in eduGAIN that allows creating test accounts with arbitrary attributes.
  - Accounts can only be created by (verified) SP admins
  - Test accounts can only be used to access own SP
  - Test accounts have an expiration date

Summary

CLARIN recommends:

- **"move from an opt-in to an opt-out policy"**
  - More federations will follow the example of the UK, Sweden, France
  - With advent of Shibboleth 3 (late 2014) federations have a chance to make their IdPs deploy features/support additional attributes

- **"make the release of relevant attributes mandatory"**
  - The federations cannot "force" universities to release attributes but we can make it a lot easier for them to easily and safely release information about their users:
    - *CoCo, REFEDS CoCo, R&S, R&E entity attributes*
    - *Opt-out implementation of these in local federation*

Connect | Communicate | Collaborate

www.geant.net

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