

Interfederation through eduGAIN
eduGAIN interfederation service
2011-12-01 OpenID Summit, Tokyo

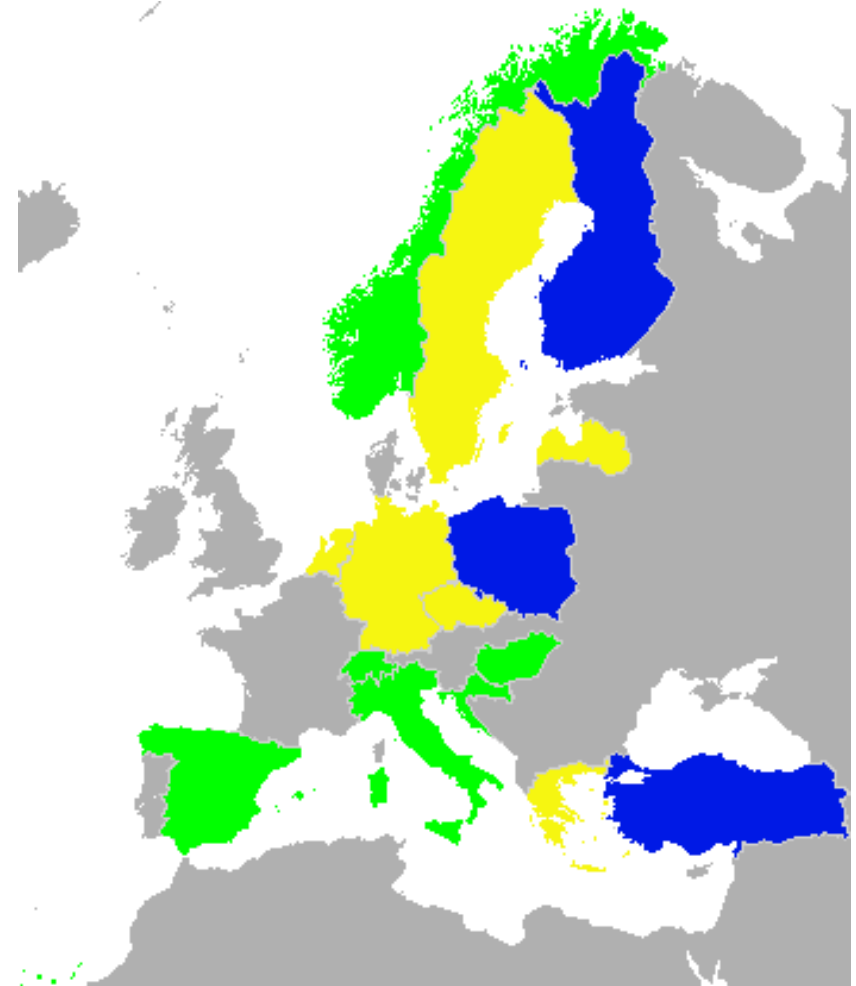
Valter Nordh, NORDUnet / GU

Introduction to the eduGAIN service



- The eduGAIN interfederation service is intended to **enable the trustworthy exchange** of information related to identity, authentication and authorisation between the GÉANT (GN3) Partners' federations. The eduGAIN service will deliver this through co-ordinating elements of the federations' technical infrastructure and a policy framework controlling the exchange of this information.

- www.edugain.org



■ Pilot ■ Declaration signed ■ eduGAIN

Introduction to the eduGAIN service



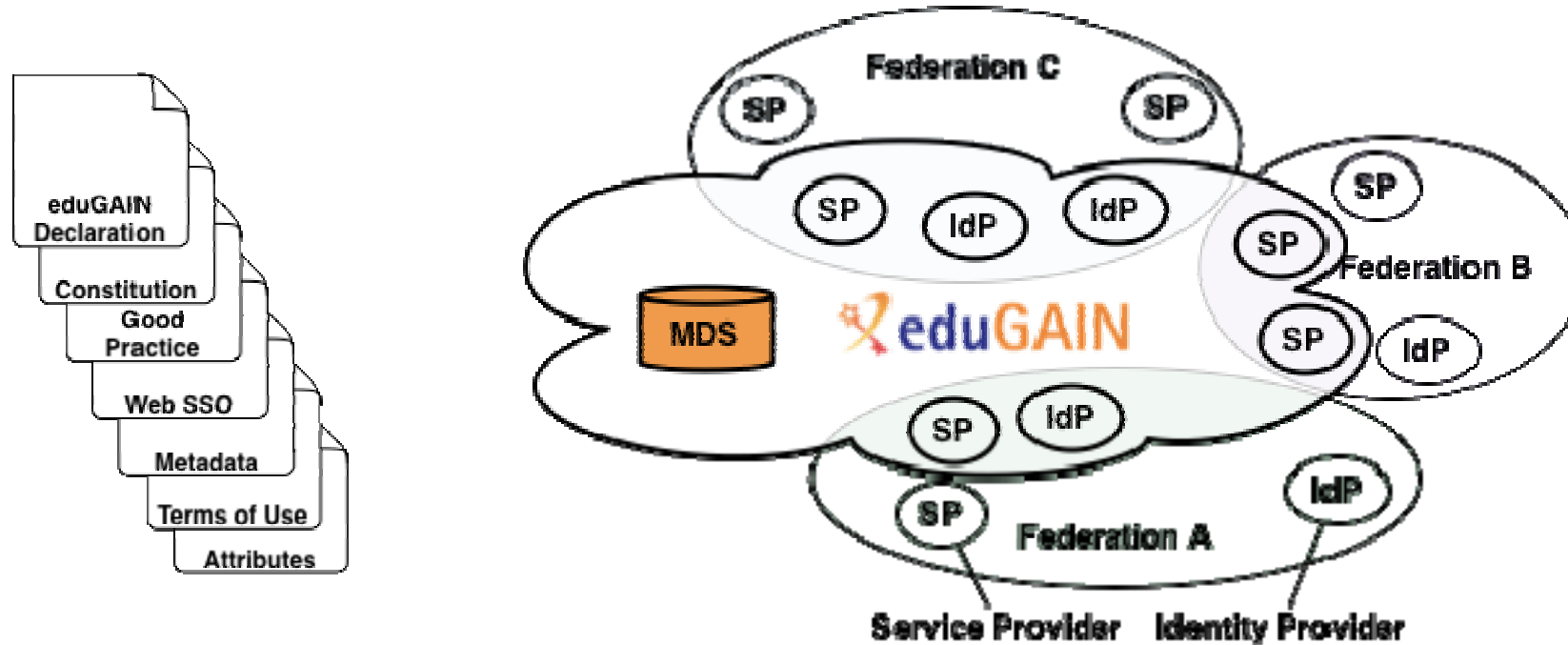
- The eduGAIN interfederation service – created and built within the GÉANT project
- Funding of the GÉANT project comes from EU NRENs and the EC
- During the development of the eduGAIN service mostly federation operators has been represented (from participant NRENs)

Introduction to the eduGAIN service



- eduGAIN in GN3 is built as a full mesh-model, where all entities talk to each other.
- Lightweight central components, both technically and process-wise, designed so that it's easy to join.
- Low bar for joining – more complex to manage all possible interactions
- Normally a federation exposes a part of it's services / identity providers to interfederation, more on this in the policy presentation (opt-in)

Introduction to the eduGAIN service



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

eduGAIN policy (and trust) framework

- Background
- eduGAIN Policy Framework
- Data protection issues and the data protection good practice profile

Federation is all about trust



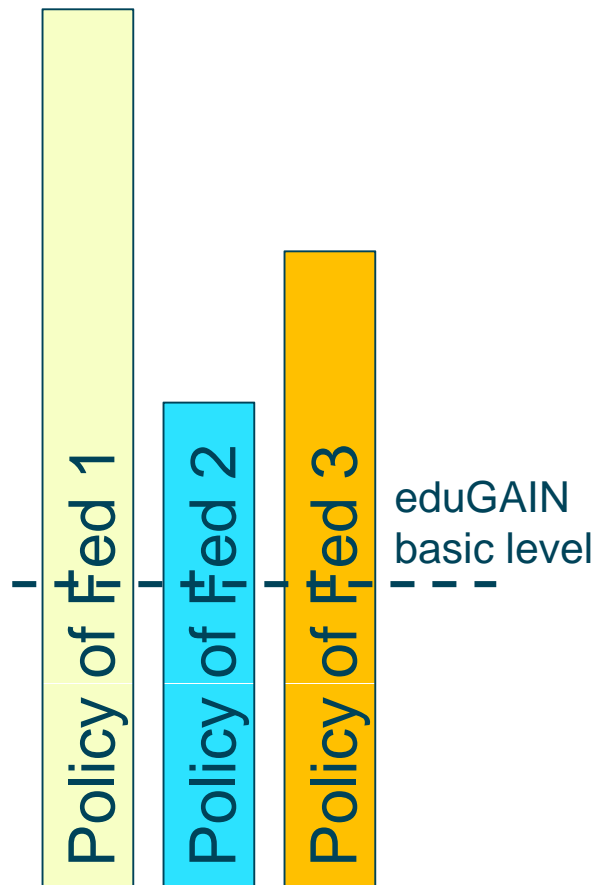
- SP needs to trust the IdP
 - **LoA:** quality of identities and authentication are as agreed
 - **Schema:** attributes and their semantics are as agreed
- IdP needs to trust the SP
 - **Privacy:** That the SP does not infringe the privacy laws
- Everyone needs to trust the federation operator
 - **Security:** Operations are done securely
 - **Rules:** Operations follow the federation rules
- These issues are covered in the federation policy (agreement)

- No federation policy => no federation
 - c.f. PEER, a pure SAML metadata delivery service

Starting point for the eduGAIN service

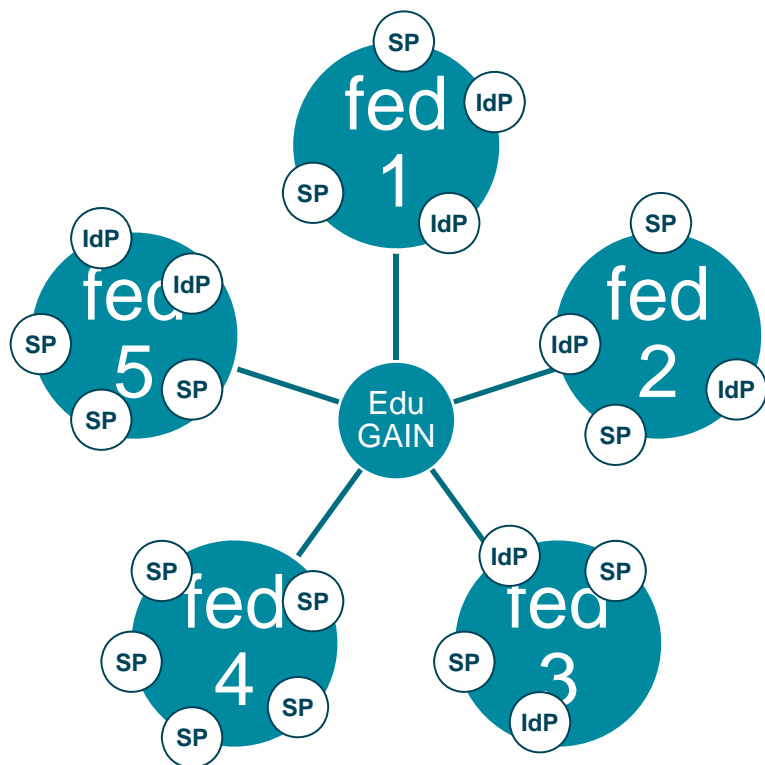


- **Heterogeneous** national federations
 - Sectors covered: universities, research institutions, schools...
 - Level of Assurance (LoA): reliability of identities/authentication
 - Attributes. Recommended attributes. Semantics (ePAffiliation)
 - Privacy mechanisms: attribute release policies, consent modules
 - Incident handling mechanisms
 - Liability, indemnification, other typical contractual issues
- eduGAIN didn't want to make the national federations to change policies
 - Would have caused too much trouble/hassle for the federations



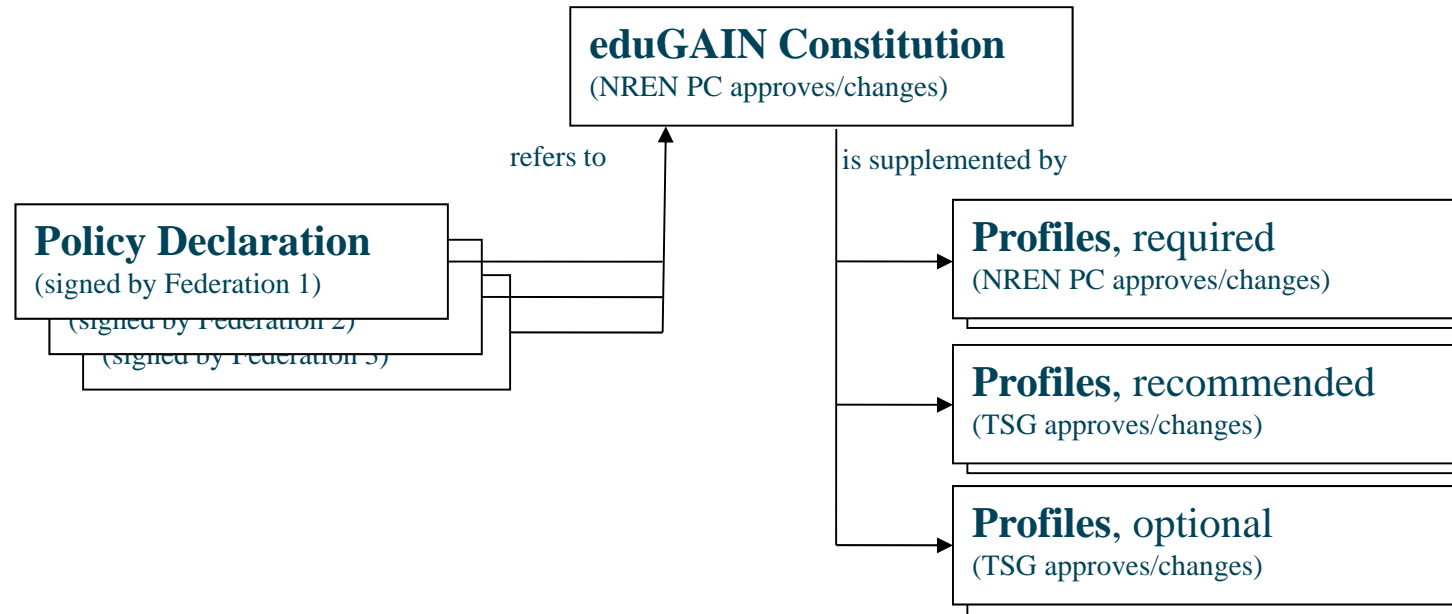
- Keep the bar low for federations to join
- Don't exclude anyone
- Keep the basic level of trust low
- Introduce optional profiles for higher levels of trust
 - Data protection
 - Level of Assurance

And the result was



- Interfederation, not confederation
- eduGAIN is mostly a metadata exchange service
- IdPs and SPs are bound only by their national federation's policy
- Any complaints about an IdP or SP will be covered locally in its home federation
- Side effect: Provider in fed 1 doesn't necessarily trust provider in fed 2
⇒ opt-in needed by Entities

1. "Uplink": Entity opts in for being exposed to eduGAIN
 2. "Downlink": Each peer Entity decides if it wants to on-board the metadata of an entity that has been exposed to eduGAIN
- IdP needs to consider the privacy risks of releasing Personal Data to foreign SPs
 - SP needs to consider LoA and attribute semantics of foreign IdPs
 - Everyone needs to consider if they are happy with the peer Provider's federation agreement



1. Policy Declaration
2. Constitution
3. Metadata Terms of Access and Use

Profiles:

4. Metadata profile (MUST)
5. WebSSO profile (MAY)
6. Attribute profile (SHOULD)
7. Data protection good practice profile (MAY)

See also:

Introduction to the eduGAIN policy framework

1. eduGAIN Declaration

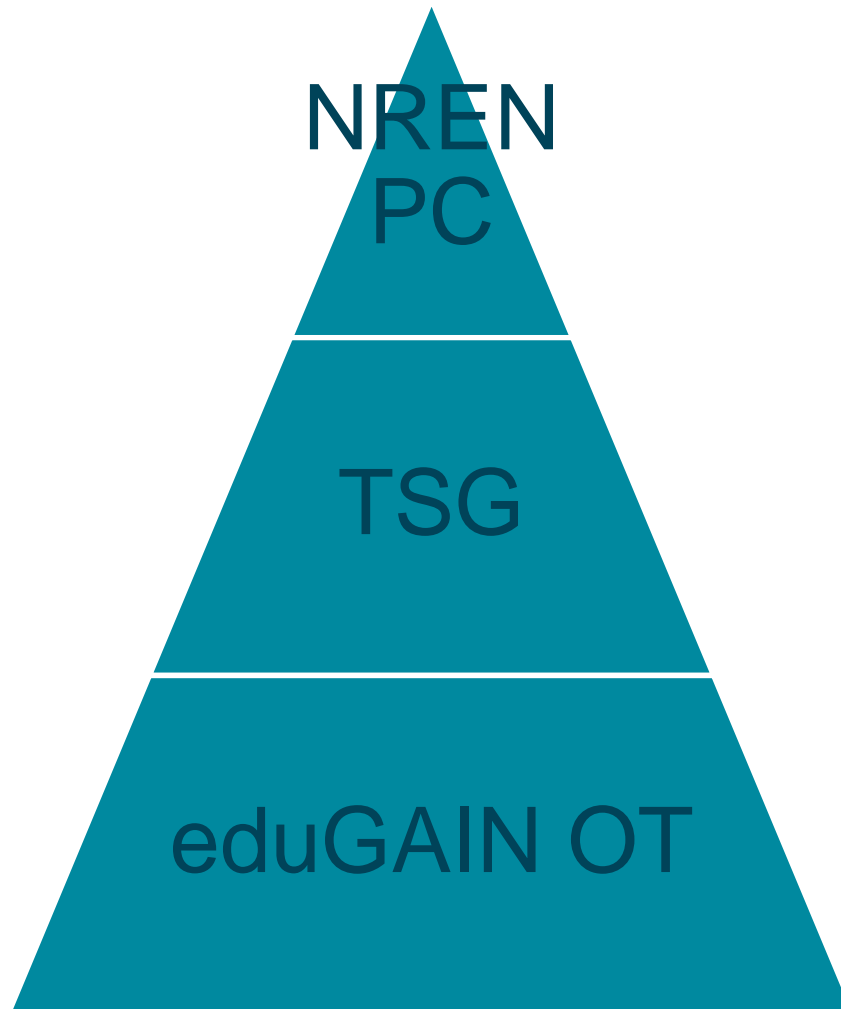


- Cannot be changed later
- Two pages of text
- Joining federation signs and presents to Operational Team (OT)
- Unilateral agreement, no countersigning
- Essential issues of the policy
 - Metadata exchange
 - Entities are bound by their local federation policies only
 - No new legal rights or obligations for Entities (e.g. liabilities)

2. Constitution



- Goal of eduGAIN
 - "to support NREN constituency by interfederation service"
- Bodies
 - NREN PC, GEANT EXEC, Technical steering group, OT
- Requirements and process for joining
- Policy violation
- Branding and trademarks
- Quality of identities and attributes
 - dispute resolution for user identities, freshness of attributes
- Audits for Entities and federations and eduGAIN Operations Team



Mandatory issues
Very long term documents
(policy)

Recommendations and documents
changing more frequently
(technical)

Daily issues and very changing
documents

3. Metadata Terms of Use



```
<!--  
  Use of this metadata is subject to the Terms of Use at  
  http://www.edugain.org/policy/metadata-tou\_1\_0.txt  
-->
```

- URL Attached to all published eduGAIN metadata
- "license" agreement of the metadata file
- Secondary; participant federations' policies override this
- "use at your own risk"

4. SAML2 Metadata profile (MUST)



- MUST: <mdrpi:PublicationInfo>
 - MUST: publisher
 - MUST: <mdrpi:UsagePolicy> with a link to Metadata ToU
 - SHOULD: creationInstant or publicationID
- <md:EntityDescriptor> elements
 - MUST: <md:ContactPerson> with contactType="technical"
 - *MUST: <md:EmailAddress>*
 - MUST: <mdrpi:RegistrationInfo>
 - *MUST: registrationAuthority*
 - *SHOULD: registrationInstant, <mdrpi:RegistrationPolicy>*
 - SHOULD: <md:Organization> with English and native values:
 - *<md:OrganizationName>, <md:OrganizationDisplayName>, <md:OrganizationURL>*

4. SAML2 Metadata profile (c'd)



- If <md:EntityDescriptor> contains <md:IDPSSODescriptor> or <md:AttributeAuthorityDescriptor> or <md:SPSSODescriptor>
 - SHOULD: <mdui:DisplayName> and <mdui:Description> in English and native language(s)
- If <md:EntityDescriptor> contains <md:SPSSODescriptor>
 - MAY:<md:AttributeConsumingService>
- Aggregated <md:EntityDescriptor>
 - SHOULD: <mdrpi:PublicationPath>
- MUST: Conformance to SAML V2.0 Metadata Interoperability Profile

5. WebSSO profile (OPTIONAL)



”Currently, the only allowed SAML 2.0 protocol profile to be used for Web Single Sign-on in eduGAIN is saml2int (ver 0.2) ”

6. Attribute profile (SHOULD)



- RECOMMENDED attributes: displayName, common name, mail, eduPerson(Scoped)Affiliation), schacHomeOrganization and schacHomeOrganizationType
 - At least one schacHomeOrganizationType SHOULD be from *urn:mace:terena.org:schac:homeOrganizationType:int*
- MUST: eP(S)A vocabulary: member, faculty, student, alum, affiliate, library-walk-in
 - Semantics as defined by REFEDS comparison ver 0.13
- SAML2 persistent ID is RECOMMENDED as the unique ID

Introduction to the eduGAIN service



- eduGAIN provides the means for entities to exchange information – but what gets exchanged is the up to the exchangers
- Opt-In for entities within federations!
- The eduGAIN interfederation service is targeting federations
- Federations target IdPs and SPs!

Challenges and lessons from the eduGAIN interfederation service?



- The technology is now in place to use, today
- Connect federations, the value of the network grows with more participants
- Universities (IdPs) and SPs needs to opt in for interfederation – BUT..
- What is the Return Of Investment (ROI) for a university in joining the eduGAIN interfederation service?

Challenges for the growth of the eduGAIN interfederation service?



- Discovery in an interfederated environment? “Small” and “large” SP?
- Attribute release from IdP (and AA) – to whom and what?
- What happens if (when!) a SP don't get the expected attributes?
- User experience if (when?) something breaks
- Legal issues and agreements – within, outside and between [EU|US|AUS|JP|your own choice]
- Attributes, attributes and attributes - how to solve release and transfer of attributes in a multinational environment?

- www.edugain.org
- [**eduGAIN service definition and policy**](#)
- **Presentation from TNC2011 on how SWITCH AAI and eduGAIN by Lukas Hämmerle (well worth reading/watching!)**
“Trimming your AAI federation fit for eduGAIN... technically”
Slides available [here](#)
Online presentation [here](#) (starting at around 58 min)
- [**eduGAIN policy**](#)
Recommended reading with regards to the policy:
[Introduction to the eduGAIN Policy Framework](#)
[eduGAIN Constitution](#)
[eduGAIN Declaration](#) (the document a federation sign and publish)
- Contact the eduGAIN OT at edugain-ot@geant.net