

**eduGAIN policy:  
From a can of worms  
Towards a nice family of worms**

REFEDs Rome 21.10.2009

Mikael Linden, CSC

The worm farmer

# GN3 Service Activity 3 Task 3: eduGAIN



- A project that implements the framework to interconnect the various AAI federations in Europe
- Builds on GN2/JRA5 eduGAIN
- Deliverables and milestones
  - 10/2009: use case analysis
  - **4/2010: eduGAIN service definition and policy**
  - 10/2010: service rollout plan
  - 4/2011: pilot phase with five NRENs
- SA3 Activity Leader: Josh Howlett
- SA3T3 Task Leader: Valter Nordh
- SA3T3 policy subtask Leader: Mikael Linden

# Goal of this speak



- **Inform** the community on the policy work that is being carried in GN3/SA3 task 3 "eduGAIN" project
- **Gather** the community's opinion on the policy issues that the federations have in common and can reach a consensus on
  - In the short run (common policy issues right in the beginning)
  - In the long run (transition period to a common policy)
  - By making an optional profile (nobody needs to use the profile but its may ease life for those who use it)
- Please fill in your opinions on the worms (40)
  - On a paper form
  - Or in Surveymonkey: <http://tinyurl.com/yzjqul5>

# 1. Fundamentals: Who can join, how to join?



- **Geographical coverage**
  - EU countries? Countries with adequate level of data protection?
- eduGAIN participants; **which kind of entities may join**
  - national feds only (1..n IdPs, 1..n SPs). What is a national fed? (e.g. CERN)
  - also “SP-feds” (no IdPs but a collection of SPs, e.g. the Clarin community).
  - also individual IdPs and SPs (e.g. from a country without a national fed)
- **IdPs**: higher education and research only?
  - further education, K-12
  - relationship to governments’ authentication services for citizens
- **SPs**: higher education and research only?
  - services not related to research and education (e.g. government services, commercial services e.g. gambling...)
- **Operational requirements** for participants; what a participant must be capable of
  - e.g. provide a helpdesk for IdP&SP admins for sorting out trivial issues
  - e.g. provide mechanism for handling security incidents
- Can a federation or an **IdP opt-out an SP** coming via eduGAIN? How?

## 2. Legal and contractual issues



- **contractual** structure
  - Bilateral agreement (such as eduroam)
  - Unilateral declaration made by the joining federation
- confederation **governance**; who decides and how (majority/consensus)
  - who is eligible to join? Is everyone eligible automatically accepted?
  - confederation peering
  - policy updates
- **jurisdiction**
- **dispute** resolution
- **liability** and indemnification

### 3. Data protection and the Data Protection Directive (DPD)



- Is data protection in or **out of scope** for eduGAIN?
- Is it **allowed** to pass personally identifying information (PII) in eduGAIN?
- Is the SP a data **controller or processor**? (DPD 2 (d), (e))  
Do we expect IdP/SPs to **agree bilaterally** on exchange of PII?
- Sticking to the **purpose of processing** personal data? (DPD 6 1 (b))
- What are **necessary attributes** for an SP? Who decides? Who manages ARPs? (DPD 6 1 (c))
- Criteria for making data processing legitimate (DPD Article 7): **consent or necessity**?
- How to **inform the data subject** (DPD 11)? In which language?
- Releasing personal data to **3<sup>rd</sup> countries** (e.g. to the US)?

Do you want to have optional processes and practices that facilitate exchange of personal data between IdPs and SPs, without expecting them to have bilateral agreements?

# 4. Attributes



- **mandatory attributes**, are there any?
  - having some whose existence the SPs can rely on eases confederated SP's life
- The **unique identifier**
  - ePPN only? Re-assignment of ePPN? Management for ePPN "scope"
  - ePTID only? Policy for persistence of entityIDs for IdPs and SPs
  - either ePPN or ePTID released to each SP? Having just one eases confederated SP's life
  - ePPN is personal data, ePTID depends on jurisdiction
- **semantics** of attributes
  - the attribute for the full name. CN? displayName?
  - attributes for authorization. eduPersonAffiliation and derivatives' semantics
- relationship to the **Schac** activity of Terena

## 5. User experience, branding and intellectual property



- Discovery service **usability** (how end users understand the concept. See JISC Publisher Interface study, chapter 5)
- Tailoring the disco (only showing the IdPs eligible to use the service)
- **Branding** eduGAIN for end users (c.f. JISC Publisher Interface study, conclusions)
- Language issues
- **trademarks and domain names**: who registers and controls them?

## 6. Campus Identity Management quality



- Assurance for **identity** and **authentication**
- Assurance level for **attributes**/Campus Identity management

# 7. Audits



- Are there audit requirements for **eduGAIN operations**?
- Are there audit requirements for **national federations**?
- Are there audit requirements for **IdPs and SP**?
  
- Self-audit, peer-audit, external audit?

## 8. Technical issues



- SAML2 only?
- SAML2 webSSO profiles: SAML2int, Single logout, Attribute Query
- non-web profiles?
- metadata deployment profile. Certificates/PKI vs. public keys in the metadata