# Summary of REFEDS Debate

## Notes from REFEDS debate on attribute release, consent and assurance

Below I have attempted to summarise the wide-ranging discussion on attribute release, consent and assurance from the REEFDS mailing list (June / July 2011). Full records of the archive can be found here.

To subscribe to the mailing list click here.

## 1. CONSENT

- How do gain consent on consent?
- Is there a notable difference between release of personal data via email, vs release of data from an IdP?
- Addressing attribute release based on consent vs. attribute release based on necessity.
- Federation by federation model of consent with country-specific legal advice needed?
- eduGAIN Data protection good practice profile relies on IdPs having a consent module in place.
- Updating consent information on the REFEDs wiki.
- Are we using the wrong terminology? Consent vs informing?
- What role does the MD spec have to play here?
- Wide deployment dependent on simplistic models. Have often do I have to say I am aware data is being passed?

## 2. ATTRIBUTE PROFILE URLS

- Can we create attribute profile URLs / URIs for SPs, in line with the current RENATER approach.
- How do we ensure that these profiles are adopted by IdPs (assumes mandating is not possible)?
- What groups are we serving here? Academic publishers, e-science use cases…what else?
- What support information do we have for e-science use cases – what role will the EU AAA for e-Science study play and how are we influencing?
- Importance of the affiliation statement within various user groups.
- Working with the CLARIN use case.

## 3. PRIVACY RISK

- What is the value story as well as what is the risk profile? Should we be creating ‘impact categories’ and should we be categorising data field.
- Role of the MDUI spec solution: <mdui:PrivacyStatementURL> - how do we work with SPs to provide this information?
- The Andrew Cormack data field category list:
  - Attributes that do not identify a unique user (e.g. ePSA);
  - Indirect identifiers designed for privacy (e.g. ePTID);
  - Indirect identifiers not designed for privacy (e.g. IP address);
  - Direct identifiers (e.g. name, address);
  - E-mail address & fax number;
  - Location information (e.g. mobile phone cell);
  - Sensitive personal data (health, race, religion, etc.).

## 4. ASSURANCE

- The cost question. Even self-auditing has significant costs associated with it.
- Role of REFEDs / federations as auditors.
- Issue of relatively mature deployments grappling with complex use cases (like informed consent) vs newer entrants starting from simple cases (light weight single sign on, user delegation among protected resources under their own control) and then backing into the more complex issues (privacy, back channel exchanges, data minimization, LOAs, etc.).
- Dynamic attribute release consent in openid / UMA / OAuth because they are newer and less enterprise focused – can SAML meet these requirements?
- Should LOA be on a per-credential basis?

- Managing multiple LOAs within the same directory structure as a requirement.
- What is the ‘below LOA 1’ definition?
- What can we learn from the IGTF membership / auditing processes?
- End-to-end security and LOA1 as a barrier for IdPs.
- Issues of SPs that ‘require’ LOA2, but currently use non-federated processes below this barrier.

## 5. LINKS

- Rzemek Jaroszewski's presentation from TNC2011, slide 4 recommended.
- M04-04.
- CERN ‘federated identity system for scientific collaborations’ workshop.
- Computer weekly on claims-based assurance
- OpenID Connect.
- Current OAuth 2.0 draft.
- 800-63.
- Eric Sachs, OIX GSA Certification.
- Unintett self-asserted IT Security Policy.
- ERUIM analysis of UK vs NIST LOA.
- Privacy Risk for Access Management - Andrew Cormack
- Explaining Attribute Release - Andrew Cormack