

# auEduPerson and Other schemas

## *Attribute recommendations for AAF participants*

19 Aug 2008

Patricia McMillan  
The University of Queensland  
patricia.mcmillan@uq.edu.au



Australian Government  
Department of Innovation, Industry, Science and Research



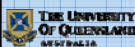
australian access  
federation

## auEduPerson Working Group



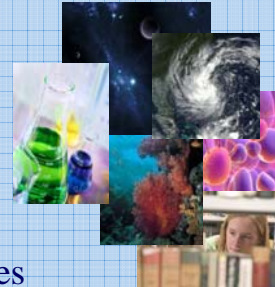
australian access  
federation

- Formed by AAF Steering Committee, March 2007
- 15 members from Australia, New Zealand, UK, Spain
- Analysed AAF use cases
- Reviewed other federations' policies on attributes
- Wide community consultation
- Latest version of recommendations at <http://www.aaf.edu.au/documentation>



## Some AAF use cases

- Research data and facilities
- Institutional repositories
- Cross-institutional course delivery
- Collaboration tools and shared services
- Scholarly and information resource licensing
- Trusted electronic communications



## Schemas used with AAF

- person
- organizationalPerson
- inetOrgPerson
- eduPerson
  - International defacto standard for attributes in higher education defined by Internet2/EDUCAUSE taskforce
- schac
  - European higher education schema defined by TERENA
- auEduPerson
  - New schema to fill important gaps
  - Identifiers and levels of assurance

## Core attributes for AAF

- auEduPersonSharedToken
  - Unique identifier enabling federation spanning services
- eduPersonAffiliation
- eduPersonEntitlement
- eduPersonScopedAffiliation
- eduPersonTargetedID
  - Privacy preserving identifier
- displayName
- mail

## Recommended attributes for AAF

- auEduPersonAffiliation
- auEPAAuthenticationLOA
- auEduPersonIdentityLOA
- auEduPersonLegalName
- cn
- eduPersonPrimaryAffiliation
- eduPersonPrincipalName
- givenName
- mobile
- o
- postalAddress
- preferredLanguage
- schacGender
- schacPersonalTitle
- schacPersonalUniqueCode
- schacUserPresenceID
- sn
- telephoneNumber
- userCertificate
- userSMIMECertificate

## Do I need to know who you are?

- AAF supports anonymous, authenticated access
  - Sometimes it's not important to know who you are
  - e.g. access institution's subscription to Elsevier
- AAF supports identified access
  - Sometimes it's very important to know who you are
  - Scientific instrumentation, e.g. Synchrotron
  - Accessing one's own data objects in data grid
  - Viewing sensitive data, e.g. medical linkage

## Identifiers used with the AAF

- When I do need to know who you are
- PKI user certificate
  - Requires passing 100 points test
  - Two types: digital and crypto token
  - AusCERT provides root Certificate Authority (CA)
- Attributes asserted in SAML (Shibboleth) transaction
  - eduPersonTargetedID
  - auEduPersonSharedToken

## eduPersonTargetedID

- From eduPerson international de facto std schema
- Different value for each combination of
  - User, Identity provider, and Service provider
- Privacy-preserving
  - Because each Service gets a different ID for a user
- Difficult to do linkage across services (e.g. Grids)
- Difficult to link objects and services to a user over time
  - Because users move around

## auEduPersonSharedToken

- Part of new auEduPerson schema
- Unique, opaque value for each user
- Non-targeted
  - Each Service gets the same ID for a user
- Portable (at user's option)
  - When a user changes organisations
- Enables linkage across services (e.g. Grids)
- Enables linkage of objects and services to users over time

## Working group reconvening

- Important to update with new developments and new use cases
- Fine-tuning auEduPersonSharedToken format
- New version of eduPerson specification
  - New attribute eduPersonAssurance
- Consider new uses cases involving a GroupID or CourseID



## Questions?



[www.aaf.edu.au](http://www.aaf.edu.au)  
[aaf@aaf.edu.au](mailto:aaf@aaf.edu.au)