

Identity Data Schemas for the AAF

The auEduPerson Working Group

Rodney McDuff

(UQ, AAF Project Architect)

Patty McMillan

(UQ, MAPS Project Manager)

- The Australian Access Federation (AAF).
 - What's it about?
- The auEduPerson Working Group.
 - Who the heck are they?
- The Tasks.
 - Common Attribute and Schema Policy.
 - Profiling the eduPerson schema for the AAF.
 - Creating an auEduPerson Schema for the AAF.
- Progress so far.

The Australian Access Federation



- Trust Federation for the Australasian Higher Education and Research sector
 - Identity Providers (IdP) and Service Providers (SP)
 - each following common agreed policies and practices.
- SP provides content and applications which individuals and groups within the community desire to use.
- IdP provides to SP:
 - trusted IdM and authN services.
 - information (ie attributes) concerning these individuals.
 - so that the SP can make an informed authR decision
 - Levels of Assurance (LoAs) regarding these claims.



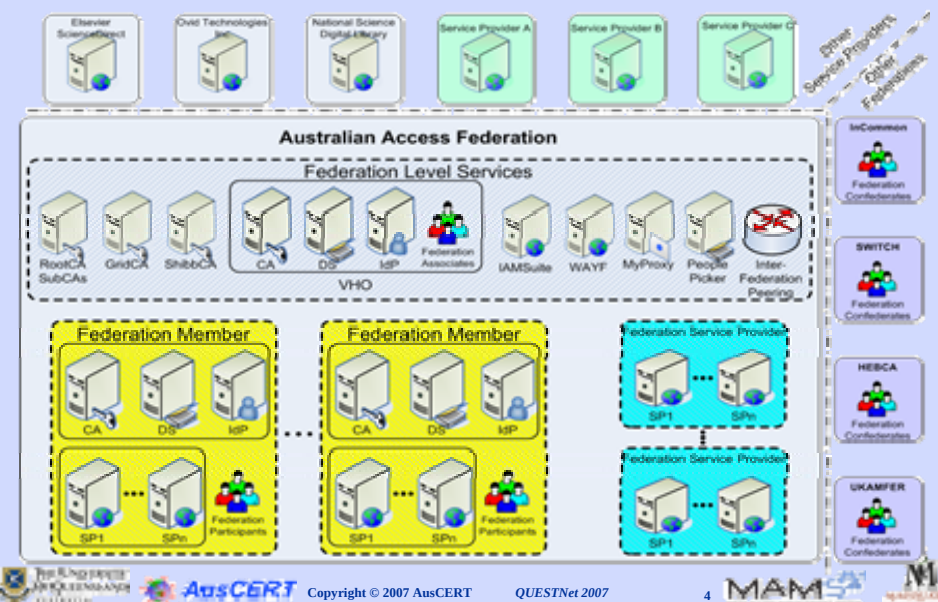
Copyright © 2007 AusCERT

QUESTNet 2007

3



The Australian Access Federation



Copyright © 2007 AusCERT

QUESTNet 2007

4



The Australian Access Federation



- DEST funded project \$4.7M
- Partners:
 - The University of Queensland
 - AusCERT
 - MELCOE, Macquarie University
- Progeny of:
 - eSecurity Framework Project. (DEST, SII, Merri round)
 - MAMS Project (DEST, SII, Frodo round)
 - CAUDIT PKI Project (DCITA, GrangeNet)
- Steering Committee:

• Nick Tate, Chair (<i>The University of Queensland</i>) • James Dalziel (<i>Macquarie University</i>) • Margot Bell (<i>DEST</i>) • Peter Nicholson (<i>DEST</i>) • Rhys Francis (<i>NCRIS</i>)	• Michael Dupe' (<i>AGIMO</i>) • Richard Northam (<i>CAUDIT</i>) • Viviani Paz (<i>AusCERT, AAF Project Manager</i>) • Alan Bevan (<i>The Le@rning Federation</i>) • Maxine Brodie (<i>CAUL</i>)
--	--

The auEduPerson Working Group



- The auEduPerson reports to the AAF Steering Committee
- Tasked with drafting and recommending data attribute schemas for use within the AAF
 - Based on community requirements
 - Interoperability with other national and international federations.
- Patty McMillan (Chair), UQ and MAPS Project
- Peter Austin, WALAP
- David Bannon, VPAC
- Neil James, New Zealand SCIT
- Rodney McDuff, UQ
- Viviani Paz, AusCERT
- Alex Reid, AARNet
- Leon Troeth, Monash
- Lyle Winton, PILIN and eFramework Projects
- Neil Witheridge, MAMS Project
- John Zornig, UQ
- Victoriano Girault, University of Malaga and TF-EMC2
- John Paschoud, London School of Economics
- Ian Young, UK Federation

The Tasks.



- Requirement: All actors in AAF to have a common understanding of:
 - the semantics of the attributes.
 - the semantics and syntax of the value(s) of an attribute.
 - Attribute/value pairs provide an AAF common language.
 - SPs trust IdP's vocabulary is same as its own.
 - AAF can assist in providing this LoA by requiring common policy amongst IdPs.
- Common Attribute and Schema Policy.
- Profiling eduPerson for use with the AAF.
- Creating an auEduPerson Identity schema.
- Requirement: Need all stakeholders to have input.
 - Policies must be community consensus.
 - But how to communicate to *all* stakeholders?
 - Surveys targeting different community groups.



Copyright © 2007 AusCERT

QUESTNet 2007

7



Common Attribute and Schema Policy



- Problem: SP needs to know which attributes are available to base authR decision.
 - Should (at least) be consistent across IdPs in AAF.
- Common Identity schemas are:
 - Person, organizationPerson, inetOrgPerson and eduPerson
- Solution: auEduPerson WG recommends policy which defines required, recommended and optional attribute sets from these schemas.
 - Communication plan to ensure community is consulted and has input into recommendation.
- Complication: Attribute may exist but not released.
 - Attribute Release Policies (ARP) can be defined at each IdP for each federation and each SP.
 - If an IdP doesn't release an attribute, user pressure may encourage IdP to define per-SP ARP.
 - But at least the attribute is there to be released.



Copyright © 2007 AusCERT

QUESTNet 2007

8



Profiling eduPerson for the AAF



- Problem: Aspects of eduPerson are intentionally left very vague. Example:
 - eduPersonAffiliation. Attempt to specify the relationship that a person has to their institution. Controlled vocabulary is
 - faculty
 - student
 - staff
 - alum
 - member. (*Intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community*)
 - affiliate. (*Intended to apply to people with whom the university has dealings, but to whom no general set of "community membership" privileges are extended*)
 - employee



Copyright © 2007 AusCERT

QUESTNet 2007

9



Profiling eduPerson for the AAF



- Moreover eduPerson spec states:
 - “Each institution decides the criteria for membership in each affiliation classification”.
 - “A reasonable person should find the listed relationships commonsensical”.
 - In reality there would be 38+ conflicting criteria in AAF.
- Solution: auEduPerson WG recommends policy to define a common AAF approach to eduPersonAffiliation.
 - Based on community consultation and input.
- Issue: 7 buckets are unlikely to fit all affiliations the AAF community may wish to express.
 - May require an auEduPerson version of affiliation.
 - Still need to sort out eduPersonAffiliation for inter-federation needs.



Copyright © 2007 AusCERT

QUESTNet 2007

10



Creating an auEduPerson Schema for the AAF



- Many international HE & R communities have investigated their need for an extended identity schema. Example attributes:
 - usPerson
 - accessibilityProfile: Base64 encoded [XML](#) from IMS AccessForAll schema
 - authnLoa: Transport (NIST 800-63 based) LoA to SP.
 - <http://www.cio.gov/eauthentication/uspersion/authnloa#nist-sp-800-63-{1,2,3,4}>
 - citizenship: ISO3166 Country codes
 - UKEdPerson. Both XML and LDAP schemas.
 - UKEdPersonCategory: Ref. HESA codes and "Central Categories for AuthR".
 - <http://www.hesa.ac.uk/manuals/03026/fe011.htm#01>
 - » Grade Structure: Lecturer
 - http://www.angel.ac.uk/SECURE/UKEdPerson/UKEdPerson_schema.pdf#consortium#http://www.uklibrariesplus.ac.uk/
 - » Member of the UK Libraries Plus consortium
 - swissEduPerson
 - swissEduPersonStudyBranch{1,2,3}: From [catalog](#) of study branches by Swiss University Information System of the Swiss Federal Statistical Office
 - swissEduPersonStudyLevel: Level of student in Study Branch
 - swissEduPersonStaffCategory: 1xx=Teaching, 2xx=Research, 3xx=Admin, etc



Copyright © 2007 AusCERT

QUESTNet 2007

11



Creating an auEduPerson Schema for the AAF



- Problem: Does the Australian Higher Education and Research sector need an extended identity schema?
- Solution: Well, ask the community.
 - Step 1: Create simple use case template.
 - Step 2: auEduPerson WG authors a series of candidate use cases.
 - Step 3: Invite community to author their own candidate use cases based on template and candidate use cases from step 2.
 - Step 4: Collate and redact responses.
 - Step 5: Survey community to determine which use cases to include.
 - Step 6: Create auEduPerson schema.
- Issue: How to get input from all groups with the community?



Copyright © 2007 AusCERT

QUESTNet 2007

12



The Tasks. Progress so far.



- Common Attribute and Schema Policy.
 - Draft CASP developed.
 - Created CASP survey instrument to seek community input.
 - Survey sent on 18/6/07 to CAUDIT members to give to their technical directory manager.
- Profiling eduPerson for use with the AAF.
 - Draft semantics of eduPersonAffiliation controlled vocabulary in progress.
- Creating an auEduPerson Identity schema
 - Developed use case template.
 - Developing initial set of candidate use cases.



Copyright © 2007 AusCERT

QUESTNet 2007

13

