



**australian access
federation**

Report to the AAF Steering Committee

Regarding the recommendations of the auEduPerson Working Group

29 February 2008

Table of contents

1 - EXECUTIVE SUMMARY	3
2 - INTRODUCTION.....	5
2.1 - WORKING GROUP TERMS OF REFERENCE.....	5
2.2 - WORKING GROUP COMPOSITION	5
2.3 - PROCESS FOR DRAFTING ATTRIBUTE RECOMMENDATIONS	5
3 - KEY ISSUES AND VIEWS	8
3.1 - ATTRIBUTE GROUPINGS	8
3.2 - INCLUSION OF AUEDUPERSONPERSISTENTID	9
3.3 - INCLUSION OF DISPLAYNAME IN THE CORE ATTRIBUTE SET	10
3.4 - INCLUSION OF LOA ATTRIBUTES	11
3.5 - USE OF SCHAC ATTRIBUTES	11
3.6 - FORM OF EDUPERSONTARGETEDID	11
4 - CHANGES TO THE DRAFT DOCUMENT IN RESPONSE TO COMMUNITY COMMENTS	13

1 - Executive summary

The auEduPerson Working Group was formed by the AAF Steering Committee in March 2007 in order to draft and recommend data schemas to be used with the AAF, especially an identity data schema. The working group comprises fifteen members and international participants from the higher education and research sector.

The working group has produced a document, *Attribute recommendations for AAF participants*, that is now submitted for the AAF Steering Committee to review. The process for producing this document included:

- Analysing AAF use cases
- Reviewing attribute recommendations published by other federations
- Surveying potential identity providers regarding their ability to assert common attributes
- Publishing a draft version of the document for community consultation
- Reviewing comments received from the community

Considerable agreement has been reached within the auEduPerson Working Group on the document. The working group recommends:

1. That the document *Attribute recommendations for AAF participants* be adopted.
2. That, notwithstanding the concerns raised by some members of the team, the *Attribute recommendations for AAF participants* as they are stated in the document be adopted, since the overwhelming majority of the working group support them.
3. That further review and development work be undertaken as set out in sections 1.1 and 5 of *Attribute recommendations for AAF participants*, including a six-monthly review process during 2008 and 2009.

Although there has been very good consensus within the working group on the document, there have been a number of issues which have generated discussion and on which the views of the working group members are not unanimous. These are flagged and described in this report for the benefit of the Steering Committee. These issues are:

- *The number of attribute groupings to include in the document and their definitions*
The working group has recommended two groupings: core and recommended. Other attributes from standard schemas are also listed in an appendix. The MAMS team disagrees with this decision and would like the document to focus only on core attributes.
- *Whether to include the new attribute auEduPersonPersistentID*
The working group has recommended this attribute to meet requirements for ARCS and ANDS use cases. The MAMS team has requested additional time to document alternative solutions involving existing attributes to see whether these would be suitable.
- *Whether to include displayName in the core attribute set*
The working group has recommended this as a core attribute, to be released in conjunction with auEduPersonPersistentID for named (non-anonymous) access and as the preferred attribute to use when a service provider requires a user's name. The MAMS team would like to see this attribute moved from the core to the recommended set.
- *Whether to include of Levels of Assurance attributes*
The working group has agreed to include these attributes to carry levels of assurance information. The MAMS team has requested that they be removed until details related to levels of assurance are resolved.
- *Whether to use attributes from the international SCHAC extension to eduPerson*

The working group has recommended that in the interest of international interoperability, attributes from this pan-European extension to eduPerson be used where possible rather than creating new attributes. The MAMS team and other groups question whether sufficient use cases exist for including them.

- *Whether to mention the newer form of eduPersonTargetedID*

The working group has recommended that both the older form and the newer form of this attribute be mentioned in the document, consistent with the eduPerson specification. The MAMS team has requested that mention of the newer format be removed to prevent confusion.

Changes to the 3 Dec 2007 draft in response to community comments have also been listed for information. Use cases provided by ARCS and ANDS have been provided as separate attachments.

2 - Introduction

2.1 - Working group terms of reference

The auEduPerson Working Group was formed by the AAF Steering Committee in March 2007. The working group has the following terms of reference:

1. To formulate a methodology for gathering and analysing requirements for data schemas for the AAF, especially an identity data schema. This methodology should consider requirements from the following groups: service providers, identity providers, end-users (researchers, tertiary instructors, students, and administrators), and other stakeholders.
2. To gather and analyse requirements from the groups mentioned above. Assistance from outside the core working group may be required for creating survey instruments, executing surveys, and analysing survey data.
3. Based on the above analysis, to draft and recommend data schemas to be used with the AAF, that align with user requirements and interoperate with other key federations. Assistance from outside the core working group may be required for creating the data schemas.

2.2 - Working group composition

The working group reports to the AAF Steering Committee and comprises the following members and international contributors:

- Patricia McMillan (Chair), The University of Queensland
- Peter Austin, Edith Cowan University
- David Bannon, Victorian Partnership for Advanced Computing (VPAC)
- Anthony Beitz, Monash University
- Victoriano Giralt, University of Málaga, Spain
- Neil James, The University of Otago, New Zealand
- Rodney McDuff, The University of Queensland
- John Paschoud, London School of Economics, UK
- Viviani Paz, AusCERT
- Alex Reid, AARNet
- Leon Troeth, Monash University
- Lyle Winton, The University of Melbourne
- Neil Witheridge, Macquarie University
- Ian Young, The University of Edinburgh, UK
- John Zornig, The University of Queensland

2.3 - Process for drafting attribute recommendations

The working group met regularly between March and November 2007, usually fortnightly, to draft attribute recommendations for the AAF. Most meetings were via teleconference but were occasionally face-to-face when important stages in the work were reached. The working group

analysed AAF use cases, reviewed attribute recommendations published by other federations, and conducted preliminary community consultation.

On 3 December 2007 the working group published a document titled *Attribute recommendations for AAF participants: A draft whitepaper for community consultation*. The document was posted to the AAF website, and the following groups and mailing lists were advised. The deadline for submission of comments was given as 25 January 2008.

- AAF Reference Group
- CAUDIT
- CAUL
- Members of ARCS
- AAF Identity Managers mailing list
- aaf-announce mailing list
- eresearch-announce mailing list
- middle-I mailing list
- New Zealand Crown Research institutions and National Library
- TERENA TF-EMC2 mailing list

Comments were received from the following organisations. The comments were reviewed by the working group during February, and a number of changes to the draft document were agreed.

- ANDS
- ARCS
- Canterbury University (New Zealand)
- CSIRO
- FUNet (Finland)
- James Cook University
- LaTrobe University
- MAMS
- New Zealand Ministry of Education
- Queensland University of Technology
- Swami (Sweden)
- University of Melbourne
- University of Sydney
- University of South Australia
- University of Western Sydney

The updated document is now presented to the AAF Steering Committee for review as the recommendations of the auEduPerson Working Group.

The auEduPerson Working Group recommends:

1. That the document *Attribute recommendations for AAF participants* be adopted.
2. That, notwithstanding the concerns raised by some members of the team, the Attribute recommendations for AAF participants as they are stated in the document be adopted, since the overwhelming majority of the working group support them.
3. That further review and development work be undertaken as set out in sections 1.1 and 5 of Attribute recommendations for AAF participants, including a six-monthly review process during 2008 and 2009.

3 - Key issues and views

Although there has been very good consensus within the working group on the document, there have been a number of issues which have generated considerable discussion and on which the views of the working group members are not unanimous. These are flagged and described here for the benefit of the Steering Committee.

3.1 - Attribute groupings

The attribute recommendations document contains attributes from the following schemas: person, organizationalPerson, inetOrgPerson, eduPerson, schac, and auEduPerson. The draft document published on 3 December 2007 separated these attributes into three groupings – core, recommended, and optional, based on expectations regarding the type and frequency of use within the AAF.

The groupings and their definitions have been questioned by the MAMS team. The following is an excerpt from the comments submitted by the MAMS team to the working group.

This document introduces three categories of attributes, which results in unnecessary complexity and uncertainty about what needs to be implemented by organisations that may find it challenging to conduct this work. It would be preferable to have only two categories of attributes – a genuine core group that are essential to participation in the federation, and then a non-core group for everything else.

The key point is that for organisations that may find it challenging to join the AAF, it should be simple and clear what the mandatory requirements are (core only), and no further obligation beyond these. It is recommended that the current core group remain core (taking into account the comments below), and then that the "Recommended" category label be removed, and all non-core attributes be described in a single category of "Optional" (the word "Recommended" should not be used for this second group of attributes to avoid confusion about whether it is expected of AAF participants or not).

Note that the working group does not recommend that the list of *Core* attributes be mandatory for Identity Providers to join the AAF. Rather, *Core* attributes are those Identity Providers should be able to assert in order to be capable of interoperating at a basic level with most Service Providers.

The working group discussed this issue during their meeting on 1 Feb 2008. They agreed to retain the *Recommended* category label but to rename *Optional* to *Other* attributes, to put the *Other* attributes in an appendix rather than in the main body of the document, and to shorten the descriptions of these attributes. Arguments in favour of this decision were:

- The attributes in the *Recommended* grouping are different from the *Other* attributes because the former set are based on known use cases. Therefore it is important to distinguish these as a separate group of attributes.
- It is useful to continue to list the *Other* attributes, even though there are currently no known use cases for them within the AAF, for the following reasons:
 - Completeness – it shows that the working group has considered all of the attributes from these schemas and does not leave unexplained gaps.
 - Convenience – it provides in a single document a list of the attributes from these schemas, meaning members do not have to look up several different specifications to see what attributes are available.

- For new use cases, it encourages members to use existing attributes from recommended schemas, rather than inventing new attributes.
- Feedback received from the community has not indicated that identity providers are concerned about the complexity or uncertain regarding what needs to be implemented. In addition to the draft attribute recommendations document circulated 3 Dec 2007, identity providers were also surveyed via CAUDIT in June 2007 regarding their ability to assert attributes in the core and recommended groupings.

Agreement with this decision was not unanimous within the working group.

3.2 - Inclusion of auEduPersonPersistentID

There has been considerable discussion around the attribute *auEduPersonPersistentID*. This attribute was designed to meet the requirements of the Grid community in interoperating with the AAF. ARCS and ANDS have also identified additional use cases where it or something like it will be needed. (See attachments.)

The need for this attribute has been questioned by the MAMS team. The following is an excerpt from the comments submitted by the MAMS team to the working group:

Based on the specific requirement for the Grid, the only requirement is that there is an identifier that is globally unique and common across SPs.

Existing attributes (e.g. ePPN, mail) satisfy these requirements either by themselves or in combination with other attributes. Re-using existing attributes is favoured from an IdP administration perspective.

There is a danger in mis-perception of this attribute as privacy-preserving due to its opaqueness, whereas the opposite is the case (it is a global personal identifier).

auEduPersonPersistentID provides no new benefits hence it is recommended that it should be removed completely.

The MAMS team have requested additional time to document alternative solutions to the ARCS and ANDS use cases and to meet with representatives from ARCS and ANDS to see if an alternative would be suitable. One such meeting was organised by MAMS and held on Friday 15 Feb 2008 with no suitable alternative found; however the latest versions of the ARCS and ANDS use cases were only circulated on Thu 14 Feb and Fri 15 Feb.

Two other groups (University of Sydney and University of South Australia) asked the working group to clarify the intent of this attribute.

The working group discussed this attribute at their teleconference on 18 Feb 2008. It was agreed with very strong consensus to retain *auEduPersonPersistentID* in the document; however this decision was not unanimous, with one working group member not in agreement.

Arguments in favour of retaining the attribute were:

- The attribute is a simple and robust way to meet requirements of use cases that are fundamental to the purpose of the AAF. The solution has the support of both ARCS and ANDS.
- The attribute need not be assigned to all users; only to users (usually researchers) who want to access particular services (such as ARCS and ANDS).
- The attribute need not be released to all service providers; only to those with a genuine requirement.

- When a user changes identity provider, the attribute need only be portable if the user requests to retain it.
- The privacy risk is that service providers to whom the attribute is released could potentially collude to build a picture of an individual's service usage patterns or attributes. In the context of the AAF, and the intended user group for this attribute, this may not represent a major issue. The attribute is not intended for cases where anonymous access can be used.

The latest version of the attribute recommendations document has an updated description for `auEduPersonPersistentID` that attempts to clarify the intent of the attribute and to make it clear that it is not a privacy-preserving identifier.

The working group also agreed to put the attribute in the core set. This decision was unanimous with the proviso that the definition of core as currently in the document is retained.

The name of the attribute has been somewhat problematic, as it tends to generate discussion on whether the attribute is more persistent than other attributes, and whether persistence is the right property to highlight in the attribute. Other suggestions have been:

- `auEduPersonResearchID` (to highlight its intended use)
- `auEduPersonNonTargetedID` (to contrast it with `eduPersonTargetedID`)
- `auEduPersonUniqueID`
- `auEduPersonGridID`

None of these names has firm consensus within the working group.

3.3 - Inclusion of `displayName` in the core attribute set

The need to include `displayName` in the core attribute set was questioned by the MAMS team and generated some discussion. The following is an excerpt from the comments submitted by the MAMS team to the working group:

As defined, `displayName` is not intended to be other than a GUI nicety. It cannot be used as an identifier as uniqueness and persistence is not guaranteed. In addition, the assumption of a check on its reasonableness by Directory administrators may introduce a large administrative burden for little gain.

As not releasing `displayName` should not impact access to services, just how 'user friendly' the GUI appears, and the fact that `displayName` may be readily mapped from another attribute e.g. `cn`, it is suggested that it should be "recommended" rather than "core".

The working group agreed to keep `displayName` in the core attribute set for the following reasons:

- It is intended to be released in conjunction with `auEduPersonPersistentID` for named (non-anonymous) authentications.
- The working group is recommending this attribute as the preferred attribute to use any time a service provider has a requirement for the user's name.

The working group has updated the description of `displayName` to clarify the intent of the attribute.

3.4 - Inclusion of LOA attributes

The MAMS team has questioned the inclusion of the attributes *auEduPersonAuthenticationLOA* and *auEduPersonIdentityLOA*, intended to express levels of assurance information. The following is an excerpt from the comments submitted by the MAMS team to the working group:

The topic of LoA, including these two attributes, is currently under discussion in the LoA working group.

A document has been created based on this discussion and is yet to be finalised. The concerns raised by the MAMS team in this document should be resolved before any further steps are taken on these attributes, or alternatively, these attributes should be removed completely.

The working group agreed to update the description of these attributes to focus on the intent of the attributes rather than on implementation details. The latest version of the document reflects this change.

It is expected that further development of these and other attributes will take place as the AAF progresses and periodic reviews are undertaken. They are included now to make it clear that use cases do exist for them and that they have been considered, even though some details (eg in implementation) may need to be refined.

3.5 - Use of SCHAC attributes

The inclusion of SCHAC as a recommended schema has been questioned by the MAMS team and by two other groups (University of Western Sydney and University of South Australia). The following is an excerpt from the comments submitted to the working group by the MAMS team:

There are not sufficient use-cases for the use of SCHAC schema, hence it is recommended that they be removed from this document.

SCHAC is an initiative of the pan-European TERENA organisation to promote the coordination of attributes for higher education. It is an extension to the *eduPerson* schema and was developed as an alternative to creating multiple overlapping national extensions. It is gradually evolving into an international defacto standard.

The working group has agreed that in the interest of international interoperability, it is preferable to use a SCHAC attribute where possible rather than to create a new auEduPerson attribute. Some of these attributes respond to known AAF use cases. These include *schacGender*, *schacUserPresenceID*, and *schacPersonalTitle*. The other SCHAC attributes are listed for completeness and for consideration as use cases for the AAF evolve.

3.6 - Form of eduPersonTargetedID

There has been discussion over the recommended form of *eduPersonTargetedID*. The document discussed two forms of the attribute, consistent with the *eduPerson* specification.

The MAMS team has questioned mention of the newer form, which is not currently in use within the MAMS testbed federation. The following is an excerpt from the comments submitted by the MAMS team to the working group:

The description of the OID format unnecessarily confuses the description of *eduPersonTargetedID*, hence reference to it should be removed.

The "description" should focus on *eduPersonTargetedID* as an opaque, IdP unique value, with a different value released to different SPs to satisfy privacy requirements. *eduPersonTargetedID* is required to

be scoped in order that the SP may use eduPersonTargetedID as a Federation-unique identifier.

"Usage notes" should say something like: In order to construct an eduPersonTargetedID value for a specific SP, an IdP unique, random string (satisfying AAF defined format constraints) is generated and stored in a database (with primary-key including user identifier and SP ProviderID) and this value is thereafter read from the database for use as the eduPersonTargetedID value for a specific user for a specific SP.

Hence it's only necessary to describe eduPersonTargetedID "format" as a scoped attribute with value being an opaque, unique IdP user identifier, and provide an example with format <opaque, IdP unique identifier>@<valid IdP scope> e.g.

7eak0QQIEhygtPXtpgmu5l5hRnY@mq.edu.au

The working group has agreed to retain mention of both formats because it is possible (and increasingly likely in future) that some Service Providers may begin to request it. Mentioning it in the document allows Identity Providers to be aware of this eventuality.

4 - Changes to the draft document in response to community comments

The changes made to the 3 December 2007 draft in response to a review of community comments are as follows. These changes were agreed by the working group during meetings on 1 Feb, 8 Feb, and 18 Feb 2008.

- C01 Update description of LOA attributes to clarify intent and such that they refer to a separate document for technical configuration and implementation details.
- C02 Rename Optional attributes to Other attributes; shorten descriptions and move to appendix.
- C03 Put schacGender and schacUserPresenceID in the Recommended set. Review Other set to see if there are other attributes related to known use cases that should be moved to the Recommended set.
- C04 Write a paragraph describing the intent of the Other attribute set.
- C05 Update description of eduPersonTargetedID. The updated version should reflect genuine agreement between MAMS and UQ teams. It should focus on the intent and high-level usage information about the attribute and should refer to a separate document for technical configuration details.
- C06 Add a "Notes on privacy" field to each attribute. Where the document currently provides privacy notes in the "Notes on usage" field, this should be moved to the new field. Where the document currently does not address privacy, the field should contain the words "Nothing specified."
- C07 Write notes on academic software licensing to add to the usage notes for eduPersonAffiliation.
- C08 Add information about ongoing document review process to front of document.
- C09 Include the word non-targeted in the description of auEduPersonPersistentID and define in glossary.
- C10 Update the Future directions section to include student/course-related attributes (including possibly ASCED level and age of consent indicator), process for proposing other values for auEduPersonAffiliation, notes on schacPersonalUniqueID.
- C11 Move schacPersonalUniqueID to Other attribute set.
- C12 Update usage notes on schacPersonalUniqueCode to point out that this attribute may be useful in providing local services.
- C13 Add a paragraph to the auEduPerson LDAP schema describing the history of the schema.
- C14 Clarify usage notes on displayName, as questions have been raised about where it may come from and why it should not be self-asserted.
- C15 Add usage notes on the userCertificate attribute, to the effect that it is for applications where a user certificate is required, such as encrypted email.

- C16 Add a paragraph at the front of the document noting that what is in the IdPs directory for a particular attribute does not have to be what is sent.
- C17 Add to the explanation of the classifications used in the document, including an appendix with the original definitions and a note that unused classifications are there as placeholders that may contain recommended attributes in future.
- C18 Simplify scoping explanation.
- C19 Change the sentence regarding outsourcing identity provision so that it states arrangements "will be" spelt out in Federation policy, rather than that they "are".
- C20 Move auEduPersonPersistentID to the core attribute set and update the description of the attribute to reflect discussion on 18 Feb meeting.
- C21 Move eduPersonPrincipalName to recommended attribute set.