# *eduPerson (Scoped)Affiliation*

Identity Management & Federation 2019

# *eduPersonAffiliation*

- “Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).”

eduPerson schema @ https://wiki.refeds.org/pages/viewpage.action?pageId=38895708

# *eduPersonAffiliation*

- “The primary intended purpose of eduPersonAffiliation is to convey broad-category affiliation assertions between members of an identity federation. Given this inter-institutional context, **only values of eduPersonAffiliation with broad consensus in definition and practice will have any practical value**. The list of allowed values in the current version of the object class is certainly incomplete, especially in terms of local institutional use. The editors felt that any additional values should come out of discussions with the stakeholder communities. Any agreed-upon additional values will be included in later versions of eduPerson.”

eduPerson schema

# *ePA vocabulary*

- faculty
- student
- staff
- alum
- member
- affiliate
- employee
- library-walk-in

NB! multi-valued

It is expected that most users will have more than one value for ePA (e.g. member, staff)

eduPerson schema

# *ePA usage comparison*

- Interpretation of ePA vocabulary has differed from federation to federation
- This means that in practice, only a subset of the controlled vocabulary has widespread acceptance/significance

> "Be conservative in what you send,
> be liberal in what you accept"
>
> — *Postel's law*

https://www.terena.org/activities/refeds/docs/ePSAcomparison_0_13.pdf

# *ePA in South Africa*

- In South Africa we've tied the definitions of "student", "faculty", and "staff" to data elements in DHET's HEMIS:
  - "student" → "*enrolled student*"
  - "faculty" → "*instruction/research professional (academic)*"
  - "staff" → "*executive/administrative/managerial professional*" + "*specialised/support professional*" + "*technical + non-professional administration (senior management, administrative & support staff)*"
- This also puts us in rough alignment with global usage

https://safire.ac.za/technical/attributes/edupersonaffiliation/

# ePA nesting/hierarchy

**member**

**employee**

**staff**

*executive/administrative/ managerial professional + specialised/support professional + technical + non-professional administration (senior management, administrative & support staff)*

**faculty**

*instruction/research professional (academic staff)*

*trade/craft + service staff*

**student**

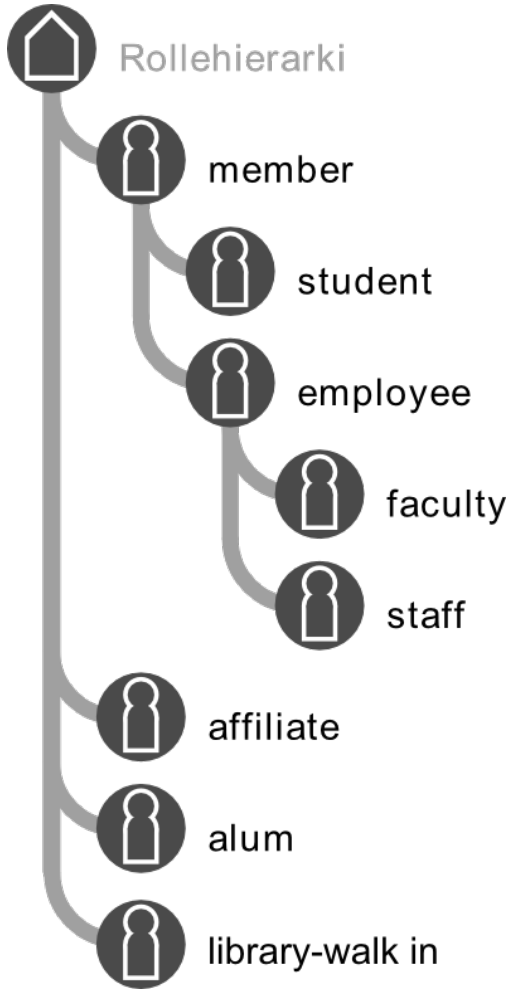
*enrolled students (both undergraduate and postgraduate)*

**faculty**

*postgraduates who are are not employees but nevertheless also fulfil a instruction/research professional (academic) role*

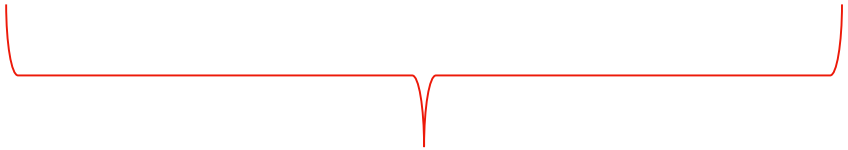
*member in good standing*
*(including e.g emeritus appointments, retired academic staff, visiting lecturers, etc)*

≈



# *What are scopes?*

member@example.ac.za



scope

# *(Scoped) ???*

What are scopes?

# *What are scopes?*

- “For Identity Provider entities, scopes MUST be rooted in the DNS domain name space, expressed in lowercase. Multiple scopes are allowed.”
- “… checks by the Federation Operator for the member’s right to use those domains.”

https://safire.ac.za/safire/policy/mrps/

# Scopes in metadata

```
<?xml version="1.0"?>
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
  entityID="https://idp-01.tenet.ac.za/idp/shibboleth"
>
 <md:IDPSSODescriptor>
    <md:Extensions>
      <shibmd:Scope regexp="false">tenet.ac.za</shibmd:Scope>
    </md:Extensions>
 </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

# *Where are scopes used?*

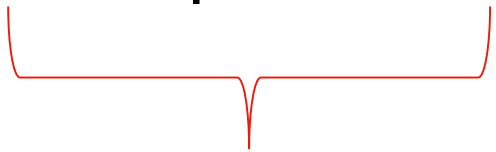
- In SAFIRE, the following attributes are checked for scoping:
  - eduPersonPrincipalName
  - eduPersonScopedAffiliation
  - schacHomeOrganization

  - eduPersonUniqueId

- NB: mail is **NOT** checked for scoping. It is possible to assert e.g. a Gmail address to federation.

# *Complex scoping*

- member@example.ac.za
- employee@example.ac.za
- student@astrobiology.dept.example.ac.za
- faculty@science.faculty.example.ac.za



MUST be rooted in the DNS domain name space

… but does not have to be a valid DNS name

… but MUST be covered by metadata <shibmd:Scope>