eduPersonScopedAffiliation

⚠ Take into account the findings from the REFEDS whitepaper on eduPersonAffiliation use on what values to use or avoid, especially in cross-/international contexts and projects/services spanning cultures and/or federations.

Definition

Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc. The values consist of a left and right component separated by an "@" sign. The left component is one of the values from the eduPersonAffiliation controlled vocabulary. This right-hand side syntax of eduPersonScopedAffiliation intentionally matches that used for the right-hand side values for eduPersonPrincipalName. [...] – eduPerson 2020-01

For eduID.at members we recommend the following mapping to eduPerson-standardised values:

- `faculty`: "wissenschaftliches Personal" (see linked Wikipedia article for how that maps to English-language terminology)
- `staff`: "allgemeines Personal" is the complementary antonym to `faculty`, meaning supporting, administrative, non-teaching, non-research personnel. (The terms are antonyms, not that an individual couldn't have both roles.)
  N.B.: `staff` was historically used within eduID.at in the UK sense of "all people who work here". Such use is discouraged nowadays (use `employee` instead, see below).
- `employee`: all personnel, whether faculty or staff. Use this if you cannot differentiate between `faculty` and `staff` within your IDM system or SAML IDP.
- `student`: "Studierende", specifically students in tertiary education (i.e., ISCED levels 5 and above; at earlier levels they are called "Schülerinnen" /"Schüler" in German, akin to UK use of "pupil").
- `member`: applies (and needs to be asserted) if the subject has *any (i.e., at least one) of the above* affiliations – plus possibly other subjects who fit the eduPerson-defined criteria for `member`.
- `alum`: for alumnæ/alumni (former graduates), if available in the same Identity Management system(s) your IDP accesses.
- `affiliate`: only if *none of the above* are applicable but you still need to express some kind of defined relationship with the organisation, i.e. `affiliate` should **not** be assigned if the subject has *any of the above* affiliations. Note that it's perfectly fine to *not assign any affiliation value*, though, so often no value will be sufficient (and is semantically equivalent to "none of the defined values") and therefore preferable over ma(r)king those `affiliate` gratuitously.
- `library-walk-in`: Special case only relevant for IDPs that need to support "patrons" of their public libraries (and where the accessed resources *rely solely on SAML attributes* for authorisation puposes, which is still very rare). That may include subjects with (only) a library card, or subjects physically present in a library location, e.g. based on IP address authentication.
  Don't use this for authorisation to licensed content if the provider can also accept the "common-lib-terms" entitlement instead, c.f. Library Services. And of course you don't need to worry about this at all if accessed resources allow authorisation based on location (IP address ranges), as the physical library location itself will already be sufficient to allow access. Also, if proxies, tunnels or VPNs are in use (to make remote subjects appear to be coming from the local data network) this affiliation – and SAML attributes and WebSSO itself – usually does not matter at all.

Out of those 8 affiliations only a few are common or useful in inter-institiutional (i.e., federated) contexts. All eduID.at IDPs should be able to create at least the following affiliation values for their relevant communities:

- `student`
- `faculty` / `staff` if you can differentiate those (see above for specifics), otherwise use `employee` for "all people who work here".
- `member`

Covering more affiliations certainly will not hurt and maybe you have other (non-federation or not even SAML-related) local use-cases for more values and clear assignment rules for all the different kinds of communities you have to cater for. But there is no need to cover all of the values for some of them to be useful to the services that rely on them.

Examples:

- Our IDP 5 Attribute resolution documentaton shows how to create and populate this attribute.
- In eduID.at the u:book services rely on eduPersonScopedAffiliation (ePSA) for authorization purposes and also offers certain privileges (e.g. payment methods) only to some affiliations
- Some Library Services don't support the standard "common-lib-terms" entitlement and instead authorize subjects based on ePSA. Use only "`member`" with those to keep things simple.
- USI Wien (the University Sports Institute Vienna) uses ePSA for the determination of the price someone has to pay for a course, in combination with an eduPersonEntitlement attribute value (stating that the subject is eligible for student discount based on her age).