Library Services

Library services, databases and academic content providers still use IP addresses (and often IPv4 only) for mapping "users" (network addresses, really) to contracts. There is little we can do today to change this other than to engage with every publisher on the planet to request and help them with integrating identity federation technology. All content providers are encouraged to (and in many cases already do) base authorization of individuals accessing their resources on attributes (i.e., data about the subject or her institution) transmitted via identity federation protocols (today SAML 2).

In most cases the only information required by a content provider will be an attribute detailing whether an individual is covered by an existing contract. (Sometimes an identifier unique to the subject will also be required and will allow the service provider to add personalized services, e.g. storing of search results or documents).
The absence of such authorization data in a response from the issuer (the Identity Provider) of course means that according to the issuer the subject requesting access is not entitled to the resource.

> The service provider needs to actually check for those attributes and deny access if the agreed-upon attribute value has not been provided in the response. There is no other way for an institution to signal whether an individual should be entitled to a resource or not. *Authentication at an academic institution does not mean the subject is necessarily authorized to access licensed resources on behalf of that institution*.

The eduPerson specification has defined the generic attribute eduPersonEntitlement to communicate entitlements, permissions or rights between entities. For the specific case of library services MACE-Dir has then defined a standard eduPersonEntitlement *attribute value* (see below for details). This is the only attribute (other than maybe a unique identifier) library services will generally need, as such no more data should be sent from the Identity Provider:

`common-lib-terms` Entitlement

Here's the current common-lib-terms specification.

"Friendly" attribute name	Formal SAML2 attribute name (on-the-wire)	Attribute value string
eduPersonEntitlement	`urn:oid:1.3.6.1.4.1.5923.1.1.1.7`	`urn:mace:dir:entitlement:common-lib-terms`

The `NameFormat` (what format is the formal attribute name in) is always "`urn:oasis:names:tc:SAML:2.0:attrname-format:uri`". For legacy services still using the SAML1.x protocol the formal attribute name is "`urn:mace:dir:attribute-def:eduPersonEntitlement`" (instead of urn:oid: 1.3.6.1.4.1.5923.1.1.1.7). See https://eduid.at/entities/sp and "mouse-over" the requested attribute's name to find out its formal name for a given service, if in doubt.

Shibboleth IDP Configuration

To add support for this SAML attribute to your Shibboleth IDP 3.x you'll need to adapt the configuration files `attribute-resolver.xml` (to generate the attribute) and `attribute-filter.xml` (to release the attribute).

Define the attribute

See our IDP 3 Attribute resolution documentation for a simple example of how to generate and assign the common-lib-terms entitlement based on eduPersonAffiliation values.

Release the attribute

The most explicit way of releasing this attribute (value) is by listing all relevant (to you) library service providers by name, i.e., referencing their entityID. See https://eduid.at/entities/sp (or https://eduid.at/entities/sp/interfed for Interfederation particpants) for a current list of Service Providers, their entityID and Requested Attributes. (For SPs known via Interfederation any Requested Attributes are managed and accounted for by their respective Home Federation, not by ACOnet. Also note that not all uses of `eduPersonEntitlement` you'll encouter are specific to *this* attribute value, i.e., specific to library services.)

> ⚠ Even though we try to keep the rules on this page up-to-date and fully functional, they are meant as **examples** that will likely also include services your institution does not have a contract/subscription with (or might be missing ones you do). No problems should result from including more services here than you have access to, though, as these services require contracts (and usually payment) in order to provide access, so sending the right SAML attributes is a necessary pre-condition but not sufficient alone.

Release eduPersonEntitlement by enumerating SPs

```
<AttributeFilterPolicy id="CommonLibTerms">
    <PolicyRequirementRule xsi:type="OR">
        <Rule xsi:type="Requester" value="https://test-sp.aco.net/shibboleth" />
        <Rule xsi:type="Requester" value="https://ieeexplore.ieee.org/shibboleth-sp" />
        <Rule xsi:type="Requester" value="http://shibboleth.ebscohost.com" />
        <Rule xsi:type="Requester" value="https://dl.acm.org/shibboleth" />
        <Rule xsi:type="Requester" value="https://sp.tshhosting.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://www.content-select.com/simplesaml/module.php/saml/sp/metadata.
php/preselect.media-sp" />
        <Rule xsi:type="Requester" value="https://www.emeraldinsight.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://sdauth.sciencedirect.com/" />
        <Rule xsi:type="Requester" value="https://www.tandfonline.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://fsso.springer.com" />
        <Rule xsi:type="Requester" value="https://shibboleth.genios.de/shibboleth" />
        <Rule xsi:type="Requester" value="https://shibboleth.statista.com" />
        <Rule xsi:type="Requester" value="https://www.hanser-elibrary.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://shibboleth.ovid.com/entity" />
        <Rule xsi:type="Requester" value="https://prd.thieme.de/shibboleth-sp" />
        <Rule xsi:type="Requester" value="https://elibrary.chbeck.de/Shibboleth.sso" />
        <Rule xsi:type="Requester" value="https://elibrary.vahlen.de/Shibboleth.sso" />
        <Rule xsi:type="Requester" value="https://www.nomos-elibrary.de/Shibboleth.sso" />
        <Rule xsi:type="Requester" value="https://iam.atypon.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://portal.zedhia.at/saml" />
        <Rule xsi:type="Requester" value="https://sp.eblib.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://login.intelliconnect.inta.cch.com/" />
        <Rule xsi:type="Requester" value="https://shibbolethsp.jstor.org/shibboleth" />
    </PolicyRequirementRule>
    <AttributeRule attributeID="eduPersonEntitlement">
        <PermitValueRule xsi:type="Value" value="urn:mace:dir:entitlement:common-lib-terms" />
    </AttributeRule>
</AttributeFilterPolicy>
```

And another *example* specific to those library SPs that do *not* support the standard "common-lib-terms" entitlement and instead rely on eduPersonScopedAffiliation values. What affiliation *values* (student, faculty, staff, member, etc.) should be entitled to access licensed resources in each case cannot be known a priori – usually each institution's librarians need to decide and can configure authorized affiliation values in a self-service web interface provided by the publisher/e-resource provider. If in doubt ask the service provider and/or discuss with the eduID.at community.

We'd prefer the number of library services using eduPerson(Scoped)Affiliation to be zero, since using the "common-lib-terms" eduPersonEntitlement is advantageous for eveyone involved: the SP, the IDP and the federation operator (or federation operators, globally). So the services listed below are where we (as an academic community) failed to communicate those benefits cleary and consistently (or it just fell on deaf ears) – with the exception of a handful of SPs that treat different populations differently and therefore *require* affiliation attributes.

Release eduPersonScopedAffiliation by enumerating SPs that don't support entitlements

```
<AttributeFilterPolicy id="LibrarySPsScopedAffiliation">
    <PolicyRequirementRule xsi:type="OR">
        <Rule xsi:type="Requester" value="https://shibboleth.cambridge.org/shibboleth-sp" />
        <Rule xsi:type="Requester" value="https://shibboleth.highwire.org/entity/secure-sp" />
        <Rule xsi:type="Requester" value="https://secure.nature.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://secure.palgrave-journals.com/shibboleth" />
        <Rule xsi:type="Requester" value="https://ticket.iop.org/shibboleth" />
        <Rule xsi:type="Requester" value="https://shib.rsc.org/shibboleth" />
        <Rule xsi:type="Requester" value="https://sp.emerald.com/sp" />
        <Rule xsi:type="Requester" value="https://cas.manz.at/shibboleth" />
        <Rule xsi:type="Requester" value="https://lindeonline.at/shibboleth" />
        <Rule xsi:type="Requester" value="https://shib.lexisnexis.com" />
    </PolicyRequirementRule>
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="OR">
            <Rule xsi:type="Value" value="student"  ignoreCase="true" />
            <Rule xsi:type="Value" value="staff"    ignoreCase="true" />
            <Rule xsi:type="Value" value="faculty"  ignoreCase="true" />
            <Rule xsi:type="Value" value="employee" ignoreCase="true" />
            <Rule xsi:type="Value" value="member"   ignoreCase="true" />
        </PermitValueRule>
    </AttributeRule>
</AttributeFilterPolicy>
```

Better approaches

Clearly having a Service Category defined for Library Services would help managing the release policies in a more consistent and less implementation-specific way. Discussion about that is currently ongoing and ACOnet is contributing to further developments in that space. As always, please discuss and share examples with the community.