OpenIDP

ACOnet operates the ACOnet OpenIDP, a self-service SAML Identity Provider for members and guests of ACOnet participants, with the entityID (i.e., globally unique name) of `https://openidp.aco.net/saml`. This service is open to everyone needing to access federated resources from eduID.at members who is lacking credentials at a SAML IDP known to the relevant service.

Registration of an ACOnet OpenIDP account only provides a means to authenticate. Use of this service does not imply access to any specific resource or service, as this remains solely the service owner's responsibility. Also, service owners are reminded that successful authentication at *any* (inter-)federated SAML IDP does not necessarily equate successful authorization. Always protect your resources with proper access rules based on attributes provided (such as `eduPersonScopedAffiliation`) unless your service is in fact open to everyone and everything that can self-register an account and authenticate.

The prime purpose of the ACOnet OpenIDP is to allow eduID.at Service Providers to offer their resource to their whole intended community, whether or not all members of that community are affiliated with an institution that operates a SAML Identity Provider within eduID.at. This obviates the need for service owners to also implement local or alternative authentication methods within their resource (which usually lead to password management and "password /username/email address forgotten" support issues at the service), in addition to federated access via SAML. As such the ACOnet OpenIDP is part of the eduID.at Metadata, together with all other Identity Providers within eduID.at.

Attributes sent by the ACOnet OpenIDP

Subjects may enter any profile data they want during the account registration phase, so *relying on any of the data provided should only be done with caution*!

The only piece of data which is verified in some sense is the **email address**, which will be used during account generation, so it must be deliverable and accessible to the subject registering the account – *at least at the time of the account creation.*

The following attributes will be issued by the OpenIDP to any Service Provider known to it (i.e., all eduID.at Service Providers):

Friendly name	Formal attribute name	Description
givenName	`urn:oid:2.5.4.42`	First name
sn	`urn:oid:2.5.4.4`	Last name
displayName	`urn:oid:2.16.840.1.113730.3.1.241`	"Firstname Lastname" (without the quotes)
mail	`urn:oid:0.9.2342.19200300.100.1.3`	The email address used for verification emails during account creation
eduPersonPrincipalName	`urn:oid:1.3.6.1.4.1.5923.1.1.1.6`	Always of the form `[a-z0-9]{7}@openidp.aco.net`, i.e. seven (random) lower-case characters and/or digits + "`@openidp.aco.net`". The string is "random" only during account creation; after that the created eduPersonPrincipalName value will not change for a given registration. Also, eduPersonPrincipalName values will not be re-used or re-assigned from one person to another at the OpenIDP.
~~eduPersonEntitlement~~	`urn:oid:1.3.6.1.4.1.5923.1.1.1.7`	~~For application owners the OpenIDP allows the provisioning of entitlement values via a proprietary API. E.g. after the u:book support team (see below) has verified someone's identity and eligibility ("studentness") status, they are able to store that fact in an entitlement specific to their services, e.g. `https://guests.ubook.at` to express the fact that someone should be entitled to use the services u:book brokers.~~ ~~ACOnet currently has no plans to expand use of this API, so this should be considered a legacy service.~~

Services known to accept ACOnet OpenIDP identities

If you have an account at a eduID.at member institution *always* use your institutional account instead of registering a new one at the OpenIDP. Save yourself the additional registration step, creating and remembering Yet Another password, etc. An OpenIDP account will not give you any additional rights or permissions. If you already have registered an OpenIDP account unnecessarily please contact the owners of the services you used it with (not ACOnet, who cannot help here) and ask them to transfer your user data to your institutional account.

These services are known to externalize their guest credentials management to the ACOnet OpenIDP, so they don't have to manage, keep secure and support passwords themselfs:

- ~~USI Wien Kursanmeldung~~: ~~The University Sports Institute (USI) at Vienna University implements online registration for its many sports courses via eduID.at. Since not all Austrian institutions whose members are eligible for USI courses currently participate in ACOnet or eduID.at subjects from such institutions can register an account at OpenIDP once, and use that for online registration at USI as long as desired.~~
- ~~u:book is a federated service by University of Vienna allowing members of participating academic institutions in Austria to buy things and services at participating online stores.~~
- ~~Training Courses by the Computer Center and Human Resources Development departments at the University of Vienna. Some of these courses are open to the general public and so need a method to authenticate people outside the eduID.at membership (or even outside the ACOnet constituency) in order to register for courses online. Authorization in these cases usually happens by payment of the course fee, so (self-asserted) attributes or identity vetting are not an issue.~~