About eduPerson attributes

Since most federations around the world are aimed at the education and research communities, the eduPerson schema is prevalent when it comes to attribute names. Here's what all the attributes are and what they mean. The three highlighted ones are the main ones used in most federations.

SAML attribute (SAML 2)	What is it?	Typical value where relevant	'Friendly' name
`urn:oid:1.3.6.1.4.1.5923.1.1.1.1`	Not generally used in the OpenAthens federation. The role part of 'scopedAffiliation' of the user.	`member`	`eduPersonAffiliation`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.2`	Not generally used in the OpenAthens federation. A persons nickname or preferred form of address.	`bob`	`eduPersonNickname`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.3`	Not used in the OpenAthens federation. Little reason to use in any federation. The DN of the directory entry of the user's organisation.	`DN=directory, CN=organisation, CN=org`	`eduPersonOrgDN`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.4`	Not used in the OpenAthens federation. Little reason to use in any federation. The DN of the directory entry of the user's organisation unit.	`OU=campus, DN=directory, CN=organisation, CN=org`	`eduPersonOrgUnitDN`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.5`	Not generally used in the OpenAthens federation. A version of eduPersonAffiliation limited to a single value.	`organisation.org`	`eduPersonPrimaryAffiliation`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.6`	Occasionally used in the OpenAthens federation. The UPN of the user. Resembles an Email, but is unlikely to be an actual email. If you release this, OpenAthens will add your scope, so make sure you only populate the 'string' part of this.	`string@organisation.org`	`eduPersonPrincipalName`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.7`	**The 'Entitlement' value for a user. This one is *technically* in common usage, but few service providers ask for it.** **Is used to do more granular groupings than roles - e.g. if a library service could not afford to buy access for all 20,000 students, but could for the 150 Geology staff and students, they might arrange with the publisher to pass an entitlement value for just the geologists.** **Set these on permission sets.**	**`geology`**	**`eduPersonEntitlement`**
`urn:oid:1.3.6.1.4.1.5923.1.1.1.8`	Not used in the OpenAthens federation. Little reason to use in any federation. Essentially the same as eduPersonOrgUnitDN and just as useful.		`eduPersonPrimaryOrgUnitDN`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.9`	**The 'scopedAffiliation' of the user. A two part identifier consisting of a role and a federation_scope.** **Since most federations are academic, roles are typically one or more of: *member, staff, student, faculty, alum, library-walk-in, affiliate, employee*.** **The federation scope is the organisation identifier and can identify sub-organisations too - e.g. a group of hospitals might have a root federation scope of `eng.nhs.uk`, but an individual hospital might have the scope of `holbycity.eng.nhs.uk`. This facilitates activities such as selling access to the whole group by authorising on `*.eng.nhs.uk`, or supplying specific OUs in the group.** **Set these on permission sets.** **Users can have multiple values assigned.**	**`member@organisation.org`** **`staff@organisation.org`**	**`eduPersonScopedAffiliation`**
`urn:oid:1.3.6.1.4.1.5923.1.1.1.10`	**The 'targetedID' of the user. An opaque user ID that is provided by default for any OpenAthens federation user, and is in general use in all major federations.** **It is persistent for a user so long as federation entityIDs do not change, however each publisher sees a different value.** **If OpenAthens gets a SAML1 request the returned attribute is scoped, but not for SAML 2.**	**`3d6qquvckr9vcauasrp3g13rur`**	**`eduPersonTargetedID`**

`urn:oid:1.3.6.1.4.1.5923.1.1.1.11`	Not generally used in the OpenAthens federation.
	
	Set of URIs that assert compliance with specific standards for identity assurance.
	
	These days entity categories are more likely to be used (See: https://wiki.refeds.org/display/ENT/Entity-Categories+Home).
		`http://blah.organisation.org/compliance/1`
		
		`http://blah.organisation.org/compliance/2`
		
		`http://blah.federation.net/agreement`
			`eduPersonAssurance`

`urn:oid:1.3.6.1.4.1.5923.1.1.1.12`	Not generally used in the OpenAthens federation.
	
	Multi-valued set of previous eduPersonPrincipalNames the user may have had.
		`somthing@organisation.org`
		
		`another@organisation.org`
			`eduPersonPrincipalNamePrior`

`urn:oid:1.3.6.1.4.1.5923.1.1.1.13`	Not generally used in the OpenAthens federation. A persistent user identifier expected to be unique within a single federation. Very unlikely to ever come up.	`oifh845oi8sd85o87a4hi8ai4ai8ah.federation`	`eduPersonUniqueId`
`urn:oid:1.3.6.1.4.1.5923.1.1.1.14`	Could be used in the OpenAthens federation ORCID iDs are persistent digital identifiers for individual researchers. Their primary purpose is to unambiguously and definitively link them with their scholarly work products. ORCID iDs are assigned, managed and maintained by the ORC ID organisation: http://orcid.org/	`http://orcid.org/1234-5678-1234-5678`	`eduPersonOrcid`

Whilst only the SAML 2 attributes are listed (SAML 2 superseded SAML 1 in 2005) a SAML 1 request from a publisher will get a SAML 1 response in the relevant namespace (e.g. `urn:mace:attribute-def:edupersonTargetedID`)