Attributes available to Relying Parties

This document describes the SAML attributes and OIDC claims that are available to relying parties connected to the eduTEAMS Service. Attribute - claims marked as *Mandatory* will always be available to a relying party. Attribute - claims marked as *Optional* will be made available under certain circumstances. For example, some attributes - claims can be available only if the respective attributes - claims are released by the home Identity Provider of the user. Attributes - claims and values marked as *Experimental* might change or removed in the future, so relying parties should not rely on them, but use them only for experimental purposes.

List of Attributes - Claims

eduTEAMS Identifier

Name	eduTEAMS Identifier
Description	User's Community Identifier is an opaque and non-revocable identifier (i.e. it cannot change over time) that follows the syntax of eduPersonUniqueId attribute of eduPerson. It consists of "uniqueID" part and fixed scope "eduteams.org", separated by at sign. The uniqueID part contains up to 64 hexadecimal digits (a-f, 0-9)
SAML Attribute(s)	- 1.3.6.1.4.1.5923.1.1.1.13 (eduPersonUniqueId) - urn:oasis:names:tc:SAML:attribute:subject-id
OIDC claim (s)	sub (public)
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	openid
Origin	eduTEAMS assigns this attribute to a user when they register on the Service
Changes	No
Multiplicity	Single-valued
Availability	Mandatory
Example	28c5353b8bb34984a8bd4169ba94c606@eduteams.org
Notes	eduPerson defines the comparison rule caseIgnoreMatch for eduPersonUniqueID. Relying services are encouraged to validate the scope of this attribute against the values permitted for eduTEAMS. eduTEAMS makes exclusive use of scope eduteams.org". The eduTEAMS identifier and username "test@eduteams.org" are test accounts reserved for testing and monitoring the proper functioning of the eduTEAMS Login. The Relying parties should not authorise it to access any valuable resources.

Display Name

Name	Display Name
Description	User’s name (firstname lastname).
SAML Attribute(s)	urn:oid:2.16.840.1.113730.3.1.241 (displayName)
OIDC claim(s)	name
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	profile
Origin	Entered by the user when they register on eduTEAMS
Changes	Yes
Multiplicity	Single-valued
Availability	Mandatory
Example	Jack Dougherty
Notes	

Given Name

Name	Given Name
Description	Name strings that are the part of a person's name that is not their surname (see RFC4519).
SAML Attribute(s)	urn:oid:2.5.4.42 (givenName)
OIDC claim (s)	given_name
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	profile
Origin	Entered by the user when they register on eduTEAMS
Changes	Yes
Multiplicity	Single-valued
Availability	Mandatory
Example	Jack
Notes	In the specification of urn:oid:2.5.4.42 it is stated that the attribute supports multiple values, but the OIDC claim support only a single value. eduTEAMS will release a single value to both SAML and OIDC relying parties

Family Name

Name	Family Name

Description	Family Name.
SAML Attribute(s)	urn:oid:2.5.4.4 (surname)
OIDC claim (s)	family_name
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	profile
Origin	Entered by the user when they register on eduTEAMS
Changes	Yes
Multiplicity	Single-valued
Availability	Mandatory
Example	Dougherty
Notes	In the specification of urn:oid:2.5.4.4 it is stated that the attribute supports multiple values, but the OIDC claim support only a single value. eduTEAMS will release a single value to both SAML and OIDC relying parties

Email address

Name	Email address
Description	Email address of the user.
SAML Attribute(s)	urn:oid:0.9.2342.19200300.100.1.3 (email)
OIDC claim(s)	email
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	email
Origin	Entered by the user when they register on eduTEAMS. Users have to verify their e-mail address before they are registered on eduTEAMS
Changes	Yes
Multiplicity	Single-valued
Availability	Mandatory
Example	jack.dougherty@example.com
Notes	

Affiliation within Home Organization

Name	Affiliation within Home Organization

Description	One or more home organisations (such as, universities, research institutions or private companies) this user is affiliated with. The syntax and semantics follows eduPersonScopedAffiliation attribute. Following values are recommended for use to the left of the "@" sign: • Faculty The person is a researcher or teacher in their home organisation. The exact interpretation is left to the home organization, but the intention is that the primary focus of the person in their home organisation is in research and/or education. **Note**. This attribute value is for users in the *academic* sector • Industry-researcher The person is a researcher or teacher in their home organisation. The exact interpretation is left to the home organisation, but the intention is that the primary focus of the person in their home organisation is in research and/or education. **Note**. This attribute value is for users in the *private sector*. • Member Member is intended to include faculty, industry-researcher, staff, student and other persons with a full set of basic privileges that go with membership in the home organisation, as defined in eduPerson. In contrast to faculty, among other things, this covers positions with managerial and service focus, such as service management or IT support. • Affiliate The affiliate value indicates that the holder has some definable affiliation to the home organisation NOT captured by any of faculty, industry-researcher, staff, student and/or member. If a person has faculty or industry-researcher affiliation with a certain organisation, they have also the member affiliation. However, that does not apply in a reverse order. Furthermore, those persons who do not qualify to member have an affiliation of affiliate.
SAML Attribute(s)	urn:oid:1.3.6.1.4.1.25178.4.1.11 (voPesonExternalAffiliation)
OIDC claim (s)	voperson_external_affiliation
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	voperson_external_affiliation
Origin	To become a holder of the faculty, industry-researcher or member attribute values in eduTEAMS the user must have either • Performed federated login to eduTEAMS using their home organisation's credentials, during which the home organisation releases the related eduPersonAffiliation or eduPersonScopedAffiliation attribute, or • Be assigned that value manually in eduTEAMS by a dedicated person in their home organisation To become a holder of the affiliate value, the user must either • Use either of the two alternatives above, or • Demonstrate they control an e-mail address that belongs to the home organisation
Changes	Yes
Multiplicity	Multi-valued
Availability	Optional
Example	faculty@helsinki.fi industry-researcher@zeiss.com member@ebi.ac.uk

Notes	The freshness of the attribute values is managed by asking users to refresh the value every 12 months using the procedure described above. eduTEAMS asserts attribute values with different scopes. The Relying services are not supposed to do SAML scope check to this attribute.

Affiliation within eduTEAMS

Name	Affiliation within eduTEAMS
Description	Specifies the person's affiliation within eduTEAMS in broad categories such as student, faculty, staff, alum, etc, as defined in eduPerson schema. Fixed scope “eduteams.org" is used after the @ sign. Default value member@eduteams.org is automatically assigned for each Community ID. eduTEAMSmay later define policies for assigning other values compliant with eduPerson specification.
SAML Attribute(s)	urn:oid:1.3.6.1.4.1.5923.1.1.1.9 (eduPersonScopedAffiliation)
OIDC claim (s)	eduperson_scoped_affiliation
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	eduperson_scoped_affiliation
Origin	Assigned by eduTEAMS
Changes	Yes
Multiplicity	Multi-valued
Availability	Mandatory
Example	member@eduteams.org
Notes	Relying services are encouraged to validate the scope of this attribute against the values permitted for eduTEAMS. eduTEAMS will make exclusive use of scope “eduteams.org”.

Groups

Name	Groups
Description	This attribute describes the groups this user is a member of in eduTEAMS [AARC-G002].
SAML Attribute(s)	urn:oid:1.3.6.1.4.1.5923.1.1.1.7 (eduPersonEntitlement)
OIDC claim(s)	eduperson_entitlement
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	eduperson_entitlement
Origin	Group memberships are managed by VO and group administrators in eduTEAMS.
Changes	Yes

Multiplicity	Multi-valued
Availability	Mandatory
Example	• urn:geant:eduteams.org:service:eduteams:group:eduTEAMS#eduteams.org • urn:geant:eduteams.org:service:eduteams:group:Hollywood#eduteams.org • urn:geant:eduteams.org:service:eduteams:group:Hollywood:writers#eduteams.org • urn:geant:eduteams.org:service:eduteams:group:Hollywood:writers:movies#eduteams.org This is an example of user registered in eduTEAMS, who is member of the Hollywood VO and she in the writers group and the movies movies subgroup within the writers group.
Notes	

Assurance

Name	Assurance
Description	**Assurance of the identity of the user, following REFEDS Assurance Framework (RAF).** Following RAF values are qualified and automatically set for all eduTEAMSidentities: • https://refeds • https://refeds/ID/unique • https://refeds/ID/eppn-unique-no-reassign • https://refeds/IAP/low • https://refeds$/ATP/ePA-1m • https://refeds/ATP/ePA-1d Following RAF values are set if the currently used authentication provider asserts (or otherwise qualifies to) them: • https://refeds/IAP/medium • https://refeds/IAP/high Following compound profiles are asserted if the user qualifies to them - **Experimental** • https://refeds/profile/cappuccino • https://refeds/profile/espresso **Assurange of the identify of the user, following AARC-G021 - Experimental** Users logging-in via non-institutional Identity Providers (e.g. Google, ORCID) will have the following assurance value: • https://aarc-project.eu/policy/authn-assurance/assam **Assurange of the identify of the user, eduTEAMS specific - Experimental** Users logging-in via non-institutional Identity Providers (e.g. Google, ORCID) will have the following assurance values: • https://eduteams.org/assurance/IDP/rs-sirtfi • http://refeds.org/category/research-and-scholarship • https://refeds.org/sirtfi
SAML Attribute(s)	urn:oid:1.3.6.1.4.1.5923.1.1.1.11 (eduPersonAssurance)
OIDC claim(s)	eduperson_assurance
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	eduperson_assurance
Origin	eduTEAMS is the origin for values it has set (see description). The current authentication provider is the origin for the values it asserts (or otherwise qualifies to).
Changes	Yes

Multiplicity	Multi-valued
Availability	Mandatory
Example	• https://refeds • https://refeds/ID/unique • https://refeds/ID/eppn-unique-no-reassign • https://refeds/IAP/low • https://refeds$/ATP/ePA-1m • https://refeds/ATP/ePA-1d
Notes	This attribute defines just the identity assurance. Authentication assurance is described using authentication contexts (SAML authentication context or OIDC acr claim).

ORCID

Name	ORCID
Description	ORCID identifier assigned to this user.
SAML Attribute (s)	urn:oid:1.3.6.1.4.1.5923.1.1.1.16 (eduPersonOrcid)
OIDC claim(s)	eduperson_orcid
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	eduperson_orcid
Origin	This attribute is set automatically when the user has linked their ORCID identifier to their eduTEAMS Identity following the regular identity linking process.
Changes	Yes
Multiplicity	Single-valued
Availability	Optional
Example	https://orcid.org/0000-0002-1825-0097
Notes	

eduTEAMS Username

Name	eduTEAMS Username
Description	The eduTEAMS username is a user selected, human-readable, revocable identifier (i.e. the user can change it). It is intended to be used when a unique identifier needs to be displayed in the user interface (e.g. wikis or Unix accounts). It has the syntax of eduPersonPrincipalName, which consists of “user” part and a fixed scope “eduteams.org”, separated by the @ sign. The user part (syntax derived from Linux accounts) begins with a lowercase letter or an underscore, followed by lower case letters, digits, underscores, or dashes and should between 4 and 16 characters long. The following regular expression applies: (^[a-z0-9_-]{4,16}$) The usernames beginning with an underscore are dedicated to eduTEAMS service IDs. (Experimental)
SAML Attribute(s)	urn:oid:1.3.6.1.4.1.5923.1.1.1.6 (eduPersonPrincipalName)
OIDC claim (s)	eduperson_principal_name

OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	eduperson_principal_name
Origin	Set when a user registers on eduTEAMS
Changes	Yes
Multiplicity	Single-valued
Availability	Mandatory
Example	dougherty@eduteams.org
Notes	Revoked identifiers will not be reassigned. Relying services are encouraged to validate the scope of this attribute against the values permitted for eduTEAMS. eduTEAMS will make exclusive use of scope “eduteams.org”. The eduTEAMS identifier and eduTEAMS username “test@eduteams.org are test accounts reserved for testing and monitoring the proper functioning of the eduTEAMS Login. The Relying parties should not authorise it to access any valuable resources.

SSH Public Key

Name	SSH Public Key - **Experimental**
Description	SSH public key of the user
SAML Attribute(s)	urn:oid:1.3.6.1.4.1.24552.500.1.1.1.13 (sshPublicKey)
OIDC claim(s)	ssh_public_key
OIDC claim location	The claim is available in: ID token Userinfo endpoint Introspection endpoint
OIDC scope	ssh_public_key
Origin	Created and uploaded to eduTEAMS by the user.
Changes	Yes
Multiplicity	Multi-valued
Availability	Optional
Example	ssh-ed25519 AAAAC3NqaC1lZDI1TTE5AAAAIJ4pfKk7hRdUVeMfrKdLYhxdKy92nVPuHDlVVvZMyqeP
Notes	This attribute is not deployed yet