OpenID Connect claims in SURFconext (EN)

OpenID Connect Claims and SAML attributes

Most services require extra information about the authenticated user, such as name, email address or affiliation. In OpenID Connect (OIDC), this extra information comes in the form of **claims**, whereas in SAML, claims are called **attributes**. In SURFconext, the user authenticates at his Identity Provider (called *OpenID Provider* in OIDC) - this all happens using SAML. SURFconext translates the incoming SAML attributes to OIDC claims and provides them at the userinfo endpoint for your Service Provider (called *Relying Party* in OIDC) to consume.

> **Please note:** SURFconext only caches the claims at the userinfo endpoint for a limited amount of time: 1 hour (after a successful authentication). If you request claims at the userinfo endpoint after this, the user is required to re-authenticate.

An extensive list of SAML attributes together with their details and properties is located here: Attributes in SURFconext. Those SAML attributes are provided by institutions connected to SURFconext as Identity Provider. You can use any of those attributes in your service (SURFconext translates them to OpenID Connect claims), however you must comply with our data minimisation policy, meaning you are only allowed to receive the bare minimum of attributes strictly needed for you to operate your service.

The following table describes the translation from SAML attributes to OIDC claims:

OIDC claim	Description of SAML attribute
`sub`	OpenID Subject (not available as SAML attribute)
`given_name`	Givenname attribute
`family_name`	Surname attribute
`name`	Common name attribute
nickname	Display name attribute
`preferred_username`	Display name attribute
`locale`	Preferred language attribute
`email`	Email address attribute
`schac_home_organization`	Organization attribute
`schac_home_organization_type`	Organization type attribute
`edu_person_affiliations`	Affiliation attribute
`edu_person_scoped_affiliations`	Scoped affiliation attribute
`edu_person_targeted_id`	eduPersonTargetedID
`uids`	Uid attribute
`schac_personal_unique_codes`	Personal code attribute
`edu_person_principal_name`	EduPersonPrincipleName
`edu_person_entitlements`	eduPersonEntitlement