OpenID Connect claims in SURFconext

When you connect to SURFconext you can use **OpenID Connect** or **SAML** as a protocol to authenticate a user using SURFconext. Different standards result in different protocols and in their turn tend to use a jargon specific to that standard. This is also the case with OpenID Connect and SAML. This page depicts how to translate the commonly used SAML attributes to OpenID Connect claims and vice versa.

OpenID Connect Claims and SAML attributes

Most services require extra information about the authenticated user, such as a 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: The access token has a lifetime, which is by default configured at 1 hour. After the lifetime of the access token has expired, it's no longer possible to retrieve the claims.

An extensive list of SAML attributes together with their details and properties can be found on our support page about attributes. 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.

User identifiers

The user's identity is transmitted in the form of the NameID element by an IdP. Every IdP must supply this, but for privacy reasons SURFconext will generate a new one, which is duplicated in the **subject**.

To identify a user the relying party can use the subject. This subject is made available in the "sub" claim. In SAML this is called the NameID. This subject is guaranteed to be stable for a fixed user, except in the case of transient identifiers. SURFconext will generate a subject for each new user. It is unique for the user and specific to the relying party, so RP's cannot correlate their received subject's between each other. There are two types:

- `persistent`
  A persistent subject contains a unique string identifying the user for this RP and is persisting over multiple sessions.
- `transient`
  A transient subject contains a unique string identifying the user for this RP during the session. If the user logs in again, a new transient subject will be generated.

Remark

The subject, when set to persistent, is unlikely to change and very privacy aware but can change when service providers or identity provider make critical changes. This can cause user profiles for services to be lost. The subject is generated using the **uid**, **schacHome Organization**, the **Client id** of **the relying party** together with a secret that uses a SHA algorithm. Institutions or services that are in production and change one of these attributes, will cause a new subject to be generated by SURFconext when doing so. This can cause loss of access to profiles at services. We will notify identity providers and relying parties when we see a change in one of these claims to prevent user data being lost.

The following table describes the translation from OpenID Connect Claims to SAML attributes.

OpenID Connect Claim	SAML Attribute	Description of attribute
sub		OpenID Subject (not available as SAML attribute)
given_name	urn:mace:dir:attribute-def:givenName	Given name
family_name	urn:mace:dir:attribute-def:sn	Surname
name	urn:mace:dir:attribute-def:cn	Common name (e.g. Prof.dr. John Doe)
nickname	urn:mace:dir:attribute-def:displayName	Display name (e.g. Prof.dr. Jane Doe)

preferred_username	urn:mace:dir:attribute-def:displayName	Display name (e.g. Prof.dr. Jane Doe)
locale	urn:mace:dir:attribute-def:preferredLanguage	Preferred language (e.g. nl, en)
email	urn:mace:dir:attribute-def:mail	Email address
email_verified		Boolean, always "true" when an email address is provided
ou	urn:mace:dir:attribute-def:ou	Organizational Unit
schac_home_organization	urn:mace:terena.org:attribute-def:schacHomeOrganization	Organization (e.g. university.nl)
schac_home_organization_type	urn:mace:terena.org:attribute-def:schacHomeOrganizationType	Organization type (e.g. educationInstitution, universityHospital)
eduperson_affiliation	urn:mace:dir:attribute-def:eduPersonAffiliation	Affiliation (student, employee, etc)
eduperson_scoped_affiliation	urn:mace:dir:attribute-def:eduPersonScopedAffiliation	Scoped affiliation (e.g. student@uniharderwijk.nl, faculty@uniharderwijk.nl)
uids	urn:mace:dir:attribute-def:uid	UID (unique code for a person that is used as the login name within the institution)
schac_personal_unique_code	urn:schac:attribute-def:schacPersonalUniqueCode	Personal code (e.g. student number)
eduperson_principal_name	urn:mace:dir:attribute-def:eduPersonPrincipalName	EduPersonPrincipleName (This is a scoped identifier. e.g. piet@studenthartingcollege.nl)
eduperson_entitlement	urn:mace:dir:attribute-def:eduPersonEntitlement	eduPersonEntitlement (e.g. urn:x-surfnet:surf.nl:surfdrive:quota:100)
edumember_is_member_of	urn:mace:dir:attribute-def:isMemberOf	isMemberOf
eduperson_orcid	urn:mace:dir:attribute-def:eduPersonOrcid	eduPersonOrcid
eckid	urn:mace:surf.nl:attribute-def:eckid	eckid
surf-crm-id	urn:mace:surf.nl:attribute-def:surf-crm-id	surf-crm-id
-	nlEduPersonOrgUnit	Deprecated and unavailable in both OIDC and SAML
-	nlEduPersonStudyBranch	Deprecated and unavailable in both OIDC and SAML
-	nlStudielinkNummer	Deprecated and unavailable in both OIDC and SAML