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. It comes to no surprise this is 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: SURFconext caches claims at the userinfo endpoint for 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 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.

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

OpenID Connect Claim after 22/11/2019	OpenID Connect Claim before 22/11/2019	SAML Attribute	Description of attribute
sub	sub		OpenID Subject (not available as SAML attribute)
given_name	given_name	urn:mace:dir:attribute-def:givenName	Given name
family_name	family_name	urn:mace:dir:attribute-def:sn	Surname
name	name	urn:mace:dir:attribute-def:cn	Common name (e.g. Prof.dr. John Doe)
nickname	nickname	urn:mace:dir:attribute-def:displayName	Display name (e.g. Prof.dr. Jane Doe)
preferred_username	preferred_username	urn:mace:dir:attribute-def:displayName	Display name (e.g. Prof.dr. Jane Doe)
locale	locale	urn:mace:dir:attribute-def:preferredLanguage	Preferred language (e.g. nl, en)
email	email	urn:mace:dir:attribute-def:mail	Email address
schac_home_organization	schac_home_organization	urn:mace:terena.org:attribute-def:schacHomeOrganization	Organization (e.g. university.nl)
schac_home_organization_type	schac_home_organization_type	urn:mace:terena.org:attribute-def:schacHomeOrganizationType	Organization type (e.g. educationInstitution, universityHospital)
eduperson_affiliations	edu_person_affiliations	urn:mace:dir:attribute-def:eduPersonAffiliation	Affiliation (student, employee, etc)
eduperson_scoped_affiliations	edu_person_scoped_affiliations	urn:mace:dir:attribute-def:eduPersonScopedAffiliation	Scoped affiliation (e.g. student@uniharderwijk.nl, faculty@uniharderwijk.nl)
eduperson_targeted_id	edu_person_targeted_id	urn:mace:dir:attribute-def:eduPersonTargetedID	eduPersonTargetedID (This is a copy of the SURFconext generated NameID)
uids	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	schac_personal_unique_codes	urn:schac:attribute-def:schacPersonalUniqueCode	Personal code (e.g. student number)

eduperson_principal_name	edu_person_principal_name	urn:mace:dir:attribute-def:eduPersonPrincipalName	EduPersonPrincipleName (This is a scoped identifier. e.g. piet@studenthartingcollege.nl)
eduperson_entitlements	edu_person_entitlements	urn:mace:dir:attribute-def:eduPersonEntitlement	eduPersonEntitlement (e.g. urn:x-surfnet:surf.nl:surfdrive:quota:100)
-	-	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