Attribute best practice

You have decided to connect your service to SURFconext. Instead of using a username and password, your service will be dealing with user attributes with SAML or *claims* if you use OpenID Connect. But what attributes or claims should you request?

As a guideline, use:

- As **few** as possible for your service to work properly.
- As **privacy preserving** as possible for your service to work properly.

SURFconext, in line with the European General Data Protection Regulation (GDPR), assumes a *minimum disclosure principle*. In short, this means a service should only process (personal) information that is strictly necessary for providing the service. On this page you will learn more about:

More on Attributes

This page is a mere introduction to attributes in SURFconext. Read our detailed page on attributes to find out more.

Webinar Identifiers

In this webinar (Dutch) we explain the important identifiers available in SURFconext

Identifiers: the best option

From a privacy perspective, the best possible way to make your service work within SURFconext is to use a pseudonymised identifier generated by SURFconext. In SAML, this value can be found in the *NameID* element; in OpenID Connect, it will be in the *sub* claim. The use of this identifier is both privacy aware and robust.

When using this identifier, there are two options: *transient* and *persistent*.

SAML Attributes	OpenID Connect Claims	Explanation
NameID element (transient)	sub claim (transient)	Service Providers who have no need to identify one user from another should use this element. The *transient* NameID/sub claim is an opaque identifier generated by SURFconext. It is impossible to see who is behind it. It also changes every time the user re-authenticates. As a Service Provider, you are therefore unable to see whether it is the same user logging in, or someone else.
NameID element (persistent)	sub claim (persistent)	If you do need to identify returning users, the *persistent* NameID/sub claim is available; a persistent NameID/sub claim is like the transient NameID/sub claim explained above, except that returning users will have the same value each time they return. This attribute is privacy aware and is, of all attributes available, least likely to change for a given user thus a certain and consistent identifier.

Identifiers: the second best option

If your service needs more information, for example if your service needs to be able to recognise different type of users on their first login, we can provide additional identifiers. In order of order of privacy preserving, the following applies:

SAML Attribute	OpenID Connect Claim	Explanation
schacPersonalUniqueCode	schac_personal_unique_codes	This is a number that is often used within internal institution systems and very well suited for uniquely identifying users without affecting their privacy too much. However, currently **only a few institutions provide this attribute**. If you wish to use this attribute, please inform the SURFconext Team; they will ask the institution to provide this attribute.
uid	uids	A uid is unique for an institution, but it is **not unique within SURFconext**. The same uid could be used for different persons in different institutions. Be aware that uid is reusable. This means that when 'John' leaves the university, a second John could be provided with the same uid. This attribute can be useful in the scenario that your services uses the value of the uid from the institution for identification. This attribute gets globally unique when it is combined with the schacHomeOrganization (see below)
eduPersonPrincipalName	edu_person_principal_name	The principal name can be used to uniquely identify a user. Downside is that in most cases, the value gives away a lot of information about the user. Bear in mind that the principal name is reusable.
Mail	email	The email attribute could also be used to identify a user. However, **we strongly advise against it**: an email address can change over time (e.g. after marriage or when someone changes surname). Also, email is reusable. If john@university.edu leaves the university, a second John could be provided with the same email address. Furthermore, the email attribute is multi valued, which means a user can have more than one email address.

Other attributes

Next to identifiers, there are other types of attributes available to discern between different *types* of users without necessarily knowing the exact identity of the user.

SAML Attributes	OpenID Connect Claims	Explanation
eduPersonAffiliation	`edu_person_affiliations`	This attribute can be multi-valued and indicates whether the user logging in is a `student`, `employee`, `faculty`, `prestudent` and/or `affiliate`.
eduPersonEntitlement	edu_person_entitlements	Sometimes the Identity Provider is in charge of managing authorisations, e.g. which user or group is entitled to which roles and rights within a Service Provider. A very handy attribute for managing this is the `eduPersonEntitlement` attribute.
SchacHomeOrganization	`schac_home_organization`	This attribute allows you to discern users from university 'x' from university 'y'. This attribute is extremely handy if you don't need to know who the user is, only which institution the user is from.

Mapping attributes to existing users

If you are connecting an existing service you probably already have a user database. You need attributes which you can map to the information you already have about users. Common options are:

Existing user information	SAML Attributes	OpenID Connect Claims
email	mail	email
username	uid	uids
student number	schacPersonalUniqueCode	`schac_personal_unique_codes`

Minimize authentication attributes

Please consider using as few and privacy friendly attributes for the authentication flow and present the user an option after he/she has authenticated, so has entered your service, to supply you with more profile information, for instance in a user account management panel. We assume, when doing that, you also keep in mind with all laws and regulations, for instance regarding consent.

Read more

For all available attributes and technical details read on on our attributes page in our backgrounds section. The translation from attributes to claims can be found there as well. Remember, **the more attributes you request, less obvious it becomes institutions are willing to connect** to your service. Choose wisely.

Navigate