# What attributes are relevant for a Service Provider

The data protection directive implies minimum disclosure of attributes. In general, attributes can be divided into three categories: necessary, optional and not relevant.

## Attributes that are necessary for a Service Provider

NECESSARY attributes can be released to the Service Providers.

The Code of Conduct for Service Providers requires that the Service Provider agrees and warrants

- *b) [Purpose limitation] to only process Attributes of the End User that are necessary for enabling access to the service provided by the Service Provider;*
- *c) [Data minimisation] to minimise the Attributes requested from a Home Organisation to those that are adequate, relevant and not excessive for enabling access to the service and, where a number of Attributes could be used to provide access to the service, to use the least intrusive Attributes possible;*

In practice, this can mean that

- access control at the SP requires certain attributes
- providing the service requires a reliable (i.e. not user-provided) identifier to be associated with each on-line account
- the Service Provider software will not function or important functionalities of the service require the attributes
- the service requires that people are able to transfer their existing real-world trust of other members of the collaboration

Examples of NECESSARY attributes

- an attribute (such as, eduPersonAffiliation, eduPersonEntitlement or schacHomeOrganization) indicating the user's permission to use the service
  - if the attribute is not released, the service cannot verify user's authorisation
  - a trusted value provided by the IdP is needed instead of a value self-asserted by the user
- an attribute (such as SAML2 PersistentId) uniquely identifying the end user is necessary to store user's profile in the service
  - a trusted value provided by the IdP is needed. The user cannot self-assert his/her unique identifier
- if there are several alternative unique identifiers available for the service, the least intrusive MUST be used
  - pseudonymous bilateral identifier (SAML2 persistentId) is preferred
  - if there is a legitimate reason to match the same user's accounts between two Service Providers, a more intrusive identifier (such as eduPersonPrincipalName) can be used
- a name attribute (such as cn or DisplayName) is necessary for a wiki or other collaboration platform, if the users know each other in the real life and need to be able to transfer their existing real-world trust of other members of the collaboration
  - if it makes a difference in the collaboration platform to know the person's name, it can be released
  - otherwise, the user may be indicated as "unknown" or user "12345678901"
- email address, if, for the functionality of the service, it is necessary to be able to reach the end user
  - for instance, the service is for applying access to a research database, and once the application is processed, the applicant is informed if the access was denied or grant

## Attributes that are optional for a Service Provider

**Note: Introduction to Code of Conduct proposes to defer support to optional extra attributes to Phase 2.**

Optional attributes belong to category REQUIRING CONSENT and can be released to the Service Provider, if the user consents to it.

An Attribute is categorized as REQUIRING CONSENT if the service can operate without it, but the service will provide some additional service level to the user (or to other users of the site) if the Attribute is provided.

Examples of optional attributes

- for a wiki, the user's email address
  - if the user wants to receive email notifications on updates of certain pages in a wiki service, instead of frequently visiting the wiki
  - alternatively, if the user does not want to receive email, he has the liberty to frequently visit the wiki page
- for a wiki, the name of the user (for instance, to show who has edited a page)
  - if the wiki is not related to a real-world collaboration where people know each other by name and need to tranfer this trust to the wiki

Alternatively, the Service Provider may ask the user to type in the optional attributes by him/herself.

For contrast, the definition of "freely-given" is that it can be withdrawn at any time. If withdrawing consent to disclosing a name breaks the service (as it does for a research collaboration) then consent is the wrong basis. That is exactly the situation where necessity applies.

## Attributes that are not relevant for a Service Provider

The SP can only process attributes that are adequate, relevant and not excessive in relation to the purposes for which the SP processes them. The SP MUST NOT request other attributes from the IdP.