



# **Attribute Specification**

Version 1.0  
(04 April 2012)

# Attribute Specification

## Purpose of this document

In a federation, information about the user is represented in SAML attributes transferred from the Identity Provider to the Service Provider. It is important for both parties to interpret the data in the same way.

Exact definitions of the attributes are maintained in their defining schemas. Within this specification, we use the following schemas:

- *person*, *organizationalPerson* (X.521)
- *inetOrgPerson* (RFC2798)
- *eduPerson* (<http://middleware.internet2.edu/eduperson/>, version 200806)
- *SCHAC* (<http://www.terena.org/activities/tf-emc2/schacreleases.html>, version 1.4.1)
- *niiPerson*, *niiEduPerson* ([NIIFSchema](#))

This Attribute Specification provides an *interpretation* of the defined attributes for their use within the federation. It might be somewhat more specific than the original definition, in order to let the SPs get more specific information about the user.

Beyond the specification, parties may bilaterally agree on any other attributes.

## Use of attributes

### Terms

- An attribute is **implemented**, if the information is available according to the semantics of the specification. Releasing an implemented attribute is simply a policy decision of the IdP.
- An attribute is **released**, when the data is transferred from the IdP to an SP. Not all available information is sent out normally, only the attributes that are relevant for the SP.

### Levels of implementation

- **Mandatory**: every IdP must implement the attribute.
- **Recommended**: it is recommended for every IdP to implement the attribute, however, it is understood that it might be impossible or very complex for certain IdPs
- **Optional**: an IdP may freely implement the attribute, however, the implementation must follow this specification.

### Attribute Requirements of the SP

SPs can indicate attribute requirements among the information provided to [Resource Registry](#). This information also shows up in the federation metadata. From the point of view of the SP, an attribute can be:

- **Required**: the information is a requirement for the proper operation of the SP application  
i.e. `eduPersonPrincipalName` is often required for applications, which are not prepared for handling opaque identifiers.

- **Desired:** the information can add extra functionality to the application or can provide better user experience  
i.e. when `displayName` is transferred, the user is not prompted to supply his or her common name.

# Attributes

## Summary

### Mandatory attributes

eduPersonPrincipalName  
 eduPersonTargetedID  
 eduPersonScopedAffiliation  
 schacHomeOrganizationType

### Recommended attributes

displayName  
 mail  
 eduPersonEntitlement

### Optional attributes

Attributes describing user properties	Attributes describing institutional relationship	Attributes for educational use
sn	ou	niifEduPersonAttendedCourse
givenName	eduPersonOrgUnitDN	niifEduPersonArchiveCourse
preferredLanguage	eduPersonPrimaryOrgUnitDN	niifEduPersonHeldCourse
schacDateOfBirth		niifEduPersonMajor
schacYearOfBirth		niifEduPersonFaculty
schacPersonalTitle		niifEduPersonFacultyDN
niifPersonMothersName		niifEduPersonStudentCategory
niifPersonResidentialAddress		
homePostalAddress		
telephoneNumber		
mobile		
eduPersonNickName		
cn		
jpegPhoto		
labeledUri		

## Persistent user identifiers

For most services, it is necessary to store application-specific data, such as user edits for a wiki page. This data is stored in a database, which is local to the SP, while the key between the user and the database entry is the **persistent user identifier**.

Persistent identifiers can be:

- **computed**: the identifier is generated run-time from one or more attributes of the user (usually by some cryptographic hashing algorithm).
- **stored**: the identifier is stored in the user's digital identity at the IdP, thus it is persistent even when other user information is changed. Uniqueness of the identifier must be preserved.

Identifiers can hold the following properties:

- **persistence**: IdPs must ensure that the identifier does not change during the life-cycle of the user at the institution.
- **non-reassignable**: IdPs must ensure that an identifier of a user will not be reassigned to another user.
- **opacity**: opaque identifiers do not refer to any personal data
- **targeted**: targeted identifiers are different for each SP, thus the SPs are unable to build common user profile without the cooperation of the IdP. Such identifiers are preferred from privacy reasons.

Persistent identifiers can be transferred in SAML attributes or in NameID of a SAML Assertion. Certain SP implementations (such as Shibboleth 2.x) can hide the details of the transfer, and can provide a persistent identifier in REMOTE\_USER header.

## List of attributes

In this specification, only mandatory and recommended attributes are specified. The [Hungarian version of the Attribute Specification](#) contains descriptions of the optional attributes as well. If you have any questions regarding the optional attributes, please contact the Federation Operator.

### eduPersonTargetedID

eduPersonTargetedID	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:eduPersonTargetedID <b>OID:</b> 1.3.6.1.4.1.5923.1.1.1.10
<b>Description</b>	<b>Opaque, targeted, non-reassignable</b> identifier
<b>Implementation level</b>	mandatory  See: <a href="https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPTargetedID">https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPTargetedID</a>
<b>Semantics</b>	An SP must process the received value, it must not forward unparsed XML value to the application. A <b>NameQualifier</b> must be included in the parsed value, which is forwarded to the application. It is (with the <b>NameQualifier</b> values) with an exclamation mark (!).
<b>Allowed values</b>	no stipulation
<b>No. of values</b>	single
<b>Syntax</b>	Must be a SAML2 persistent NameID; the unique identifier part must not be longer than 256 ASCII characters
<b>Asserted by</b>	institution
<b>Example</b>	An IdP sends the attribute on the wire such as:

```
<saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
  NameQualifier="https://idp.example.org/idp/shibboleth"
  SPNameQualifier="https://sp.example.org/shibboleth">
84e411ea-7daa-4a57-bbf6-b5cc52981b73
</saml2:NameID>
```

The application at the SP receives the attribute as the following:

<https://idp.example.org/idp/shibboleth!https://sp.example.org/shibboleth!84e411ea-7daa-4a57-bbf6-b5cc52981b73>

## eduPersonPrincipalName

eduPersonPrincipalName	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:eduPersonPrincipalName <b>OID:</b> 1.3.6.1.4.1.5923.1.1.1.6
<b>Description</b>	<b>Persistent, non-targeted, non-reassignable</b> personal identifier
<b>Implementation level</b>	mandatory  Format: <local_id>@<scope>  where:
<b>Semantics</b>	<ul style="list-style-type: none"> <li>• &lt;local_id&gt;: arbitrary persistent key which unambiguously maps to a person within an institution.</li> <li>• &lt;scope&gt;: local security domain. It must have a format as a DNS domain, and ends with a resolvable domain name, which is possessed by the identity provider institution. (Note: the scope as a whole may not be resolved from DNS.)</li> </ul> <p><b>Note:</b> <b>eduPersonPrincipalName</b> is sensitive personal data, it is often equal to the mail address of the person. It is recommended to use it only within the institution's domain. For federation use, opaque, targeted identifiers are more privacy preserving.</p> <p>eduPersonPrincipalName <b>must not be reassigned</b></p>
<b>Allowed values</b>	no stipulation
<b>No. of values</b>	single
<b>Syntax</b>	Directory String
<b>Asserted by</b>	institution
<b>Example</b>	gipsz.jakab@example.org

## displayName

displayName	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:displayname <b>OID:</b> 2.16.840.1.113730.3.1.241
<b>Description</b>	Display name of the person
<b>Implementation level</b>	recommended
	Full name of the person in a form the user (or his or her institution) probably wants to be shown.
<b>Semantics</b>	For international use, please note that Hungarian names are usually in the form of <i>Surname Givenname</i> , and names often contain accented or other non-ascii characters. But also note that this document does not specify the exact name order.
<b>Allowed values</b>	no stipulation
<b>No. of values</b>	single
<b>Syntax</b>	Directory String
<b>Asserted by</b>	not defined
<b>Example</b>	Gipsz Jakab Aladár

## mail


mail	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:mail <b>OID:</b> 0.9.2342.19200300.100.1.3
<b>Description</b>	Mail address of the person
<b>Implementation level</b>	recommended
	Notification email address of the person. The institution asserts that
<b>Semantics</b>	<ul style="list-style-type: none"><li>• either the address is provided by the institution to the person</li><li>• or the address was provided by the person and the availability and the possession of the mailbox was verified (i.e. by sending a verification email before recording).</li></ul> <p>Transferring unverified values in this attribute is not allowed.</p>
<b>Allowed values</b>	Valid email address
<b>No. of values</b>	multi
<b>Syntax</b>	See also: <a href="#">RFC 2822</a>
<b>Asserted by</b>	institution

**Example** gipsz.jakab@example.org

## eduPersonScopedAffiliation

<b>eduPersonScopedAffiliation</b>	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:eduPersonScopedAffiliation <b>OID:</b> 1.3.6.1.4.1.5923.1.1.1.9
<b>Description</b>	Describes the relationship between the person and the institution
<b>Implementation level</b>	mandatory  <affiliation>@<scope>
<b>Semantics</b>	<ul style="list-style-type: none"><li>• &lt;affiliation&gt;: the following values are permitted<ul style="list-style-type: none"><li>• <i>student</i>: the person is a student at the institution</li><li>• <i>faculty</i>: the person is a member of the teaching or researching staff</li><li>• <i>staff</i>: the person is a member of the non-teaching staff (ie. IT personnel, etc)</li><li>• <i>employee</i>: the person is employed in the institution (not recommended for use between institutions)</li><li>• <i>member</i>: users who get basic set of privileges. In general, users having <i>student</i>, <i>faculty</i> or <i>staff</i> affiliations, should also be given this value.</li><li>• <i>affiliate</i>: the user is recognised by the institution, but no basic privileges should be given.</li><li>• <i>alum</i>: alumni</li><li>• <i>library-walk-in</i>: affiliated to the library only</li></ul></li><li>• &lt;scope&gt;: local security domain. It must have a format as a DNS domain, and ends with a resolvable domain name, which is possessed by the identity provider institution. (Note: the scope as a whole may not be resolved from DNS.)</li></ul> See also: <a href="http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html#eduPersonAffiliation">http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html#eduPersonAffiliation</a>
<b>Allowed values</b>	One of the following: {student,faculty,staff,employee,member,affiliate,alum,library-walk-in}, followed by the <b>scope</b>
<b>No. of values</b>	multi
<b>Syntax</b>	Directory String
<b>Asserted by</b>	institution
<b>Example</b>	<ul style="list-style-type: none"><li>• Learners: <i>student@example.org;member@example.org</i></li><li>• Teachers: <i>faculty@example.org;member@example.org</i></li></ul>

## eduPersonEntitlement

eduPersonEntitlement	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:eduPersonEntitlement <b>OID:</b> 1.3.6.1.4.1.5923.1.1.1.7
<b>Description</b>	URI (either URN or URL) that indicates a set of rights to specific resources.
<b>Implementation level</b>	recommended
<b>Semantics</b>	List of resources what the user is entitled to use at the SP. The trust between the two parties must be established out of band. <b>Note</b>  An IdP should give only the values which are relevant for the SP
<b>Allowed values</b>	no stipulation
<b>No. of values</b>	multi
<b>Syntax</b>	Directory String
<b>Asserted by</b>	institution
<b>Example</b>	urn:geant:niif.hu:niif:entitlement:vhoadmin

## schacHomeOrganizationType

schacHomeOrganizationType	
<b>Name</b>	<b>URI:</b> urn:mace:dir:attribute-def:schacHomeOrganizationType <b>OID:</b> 1.3.6.1.4.1.25178.1.2.10
<b>Description</b>	Type of the Home Organisation
<b>Implementation level</b>	mandatory
<b>Semantics</b>	<ul style="list-style-type: none"><li>• <b>university:</b> universities and colleges</li><li>• <b>nren:</b> National research and educational network</li><li>• <b>library:</b> Libraries</li><li>• <b>vho:</b> Virtual home organisation</li><li>• <b>school:</b> Primary and secondary education</li><li>• <b>business:</b> Industrial or commercial companies</li><li>• <b>other:</b> Other</li><li>• <b>test:</b> The principal is a test account</li></ul>
<b>Allowed values</b>	urn:schac:homeOrganizationType:hu: {university,nren,library,vho,school,business,other,test}
<b>No. of values</b>	single
<b>Syntax</b>	URN
<b>Asserted by</b>	institution
<b>Example</b>	-



