# Attributes

Tuakiri attributes are based on the attributes used  by AAF (for more information, visit our Attributes Documentation). Detailed information about these attributes can be found in the auEduPerson Definition and Attribute Vocabulary document.

Tuakiri Identity Providers need to collect or generate core attributes about their end users. When an end user tries to access a service via the federation, the Service Provider may request some or all of these attributes about the end user from the Identity Provider. With end user permission, the Identity Provider may release the attributes to the Service Provider.

The attributes are used by the Service Provider to make authorisation decisions and to manage the user's experience with the service. Service Providers should consider which attributes they need in order to provide the service effectively and only request those attributes that are needed. The list of core attributes may evolve over time in response to the needs of Tuakiri members.

This page provides background information on how to map Tuakiri/AAF attributes to your own Identity Management System (IdMS). For detailed instructions, refer to Installing a Shibboleth 3.x IdP.

## Attributes Overview

- Attributes are classified as Core, Recommended, or Optional.
- The attribute set is based on multiple formal attribute specifications:
    - Basic LDAP schema (person)
    - eduPerson – additional attributes useful for academic environment
    - auEduPerson – additional extensions developed by CAUDIT
    - schac - SCHema for ACademia
- The IdP can pull some attributes directly from the IdMS (LDAP, AD):
    - Core attributes: displayName, mail, cn
    - Recommended: givenName, sn
- Some attributes are hashes calculated on the fly
    - Core: eduPersonTargetedID, auEduPersonSharedToken (SharedToken should be stored back in the IdMS or a DB)
- Some attributes have to be synthesized from existing IdMS information
    - eduPersonPrincipalName: <uid> + '@' + 'domain.ac.nz'
    - eduPersonAffiliation: using a scriptlet:

```
IF isStaff==TRUE THEN 'staff'
```

- Some attributes may have to be added to the identity management system (e.g, eduPersonEntitlement, eduPersonAssurance)

## Attribute Matrix

| Attribute Name (on IdP) | Attritbute Name (on SP) | Required? | Typical source |
|---|---|---|---|
| commonName | cn | Core | LDAP ("cn" or "displayName") |
| displayName | displayName | Core | LDAP ("displayName") |
| email | mail | Core | LDAP ("mail") |
| givenName | givenName | Recommended | LDAP ("givenName") |
| surname | sn | Recommended | LDAP ("sn") |
| eduPersonTargetedID | persistent-id | Core | Hash-on-the-fly |
| auEduPersonSharedToken | auEduPersonSharedToken | Core | Hash-with-write-back |
| eduPersonPrincipalName | eppn | Recommended | LDAP + rename + add Scope |
| eduPersonAffiliation | unscoped-affiliation | Core | Scripted definition |
| eduPersonScopedAffiliation | affiliation | Core | Take eduPersonAffiliation + rename + add Scope |
| eduPersonPrimaryAffiliation | primary-affiliation | Recommended | Scripted definition |
| homeOrganization | schacHomeOrganization | Recommended | static - "institution.domain.ac.nz" |
| homeOrganizationType | schacHomeOrganizationType | Recommended | static - "urn:mace:terena.org:schac:homeOrganizationType:int:university" |
| organizationName | o | Core | static - "University of Your University" |
| eduPersonEntitlement | entitlement | Core | LDAP (if available)/Static/Scripted. Most relevant value: `urn:mace:dir:entitlement:common-lib-terms` |
| eduPersonAssurance | assurance | Core | LDAP (if available or synthesized from other available information) |

| | | | |
|---|---|---|---|
| Legal Name (auEduPersonLegalName) | auEduPersonLegalName | Optional | LDAP (if available) |
| Business postal address (postalAddress) | postalAddress | Optional | LDAP (if available) |
| Business phone number (telephoneNumber) | telephoneNumber | Optional | LDAP (if available) |
| Mobile phone number (mobileNumber) | mobile | Optional | LDAP (if available) |
| organizationalUnit | ou | Optional | LDAP ("ou" or other if available) |
| auEduPersonAffiliation | auEduPersonAffiliation | Optional | Scripted definition (if underlying information available in LDAP) |
| eduPersonOrcid | eduPersonOrcid | Optional | LDAP (if available) |