Council of Australian University Directors of Information Technology

auEduPerson Definition and Attribute Vocabulary

2 Sep 2009

Table of contents

1 - Introduction

This document provides the definitions for the auEduPerson schema and the attribute vocabulary from auEduPerson and other schemas endorsed by CAUDIT through the CAUDIT Standing Committee on Technical Standards. It aims to establish a common language for the exchange of identity data amongst CAUDIT organisations and affiliated organisations and service providers.

1.1 - Ongoing input and review

Attribute needs may change over time as the use of federated authentication and distributed resource sharing evolves. The CAUDIT Standing Committee on Technical Standards will review and update this document periodically. If you would like to submit comments for the next document review, please send them to the chair of the auEduPerson Working Group, patricia.mcmillan@uq.edu.au. We welcome all comments and feedback from the Australian and international research and higher education community.

1.2 - Considerations in exchanging identity attributes

Access federations provide a framework for trust between identity providers, who manage identity information for users at their institution, and service providers, who manage services or resources to which users want to gain access. A common attribute framework is an important aspect of trust in an access federation.

- The service provider trusts that user information provided by the identity provider is accurate according to agreed definitions of information elements.
- The identity provider trusts that the service provider will handle user information in an agreed manner, especially to prevent unauthorised disclosure.

The user information provided by the identity provider is used by the service provider to make decisions on whether the user is authorised to access the service functionality and resources. This user information may include:

- Authentication information, such as who the identity provider is, the method of authentication, and the level of assurance.
- Attribute information, a set of user attributes according to one or more defined attribute schemas.

In addition to using attributes for authorisation, service providers may also use attributes for purposes such as:

- Personalisation and contact.
- Transaction logging, record keeping, and traceability.
- Population of resource metadata (e.g. ownership of created artifacts).

1.3 - Security, privacy, and data protection

In establishing policies around attribute exchange, it is important to be aware of security, privacy, and data protection principles. For a particular application, consider whether it is necessary to exchange information that identifies individuals, or whether it is possible to provide the service to users who have authenticated to an identity provider but who otherwise remain anonymous to the service provider. To assist in these decisions, notes on privacy have been included for each attribute in the vocabulary.

Revealing some attribute values can also be a security risk. Examples include *uid* and *eduPersonOrgDN*. Caution should be used if including these in an attribute exchange policy.

2 - Attribute overview

The following table lists an attribute vocabulary for exchanging identity information. Further information on the definitions and usage of the attributes is contained in later sections of this document.

2.1 - Guide to the table headings

Attribute: The name of the attribute.

Schema: The name of the schema from which the attribute comes. Attributes come from the following schemas:

- eduPerson [eduPerson]
- person [RFC 4517, RFC 4519]
- organizationalPerson [RFC 4517, RFC 4519]
- inetOrgPerson [RFC 2798]
- schac [SCHAC]
- auEduPerson (See Appendix in this document)

Classification: Category of the attribute, giving a general indication of how it is intended to be used. The categories listed below have been collected from the NSF Middleware Initiative Higher-Education Person survey [NMI]. The categories are as follows and are described in Appendix B of this document.

- Personal characteristics
- Contact / Location information
- Student information
- Employee information
- Linkage identifiers / Foreign keys
- Entry metadata / Administration information
- Security attributes and keys
- Confidentiality / Attribute release (visibility)
- Authorisation, entitlements
- Group-related attributes
- Other attributes

2.2 - Standard attribute vocabulary for exchanging identity information

Attribute	Schema	Classification
auEduPersonAffiliation	auEduPerson	Personal characteristics
auEduPersonLegalName	auEduPerson	Personal characteristics
auEduPersonSharedToken	auEduPerson	Linkage identifiers/Foreign keys
eduPersonAffiliation	eduPerson	Personal characteristics
eduPersonAssurance	eduPerson	Security attributes and keys
cn	person	Personal characteristics
displayName	inetOrgPerson	Personal characteristics

Attribute	Schema	Classification
eduPersonEntitlement	eduPerson	Authorisation, entitlements
eduPersonPrimaryAffiliation	eduPerson	Personal characteristics
eduPersonPrincipalName	eduPerson	Linkage identifiers/Foreign keys
eduPersonScopedAffiliation	eduPerson	Personal characteristics
eduPersonTargetedID	eduPerson	Linkage identifiers/Foreign keys
givenName	inetOrgPerson	Personal characteristics
mail	inetOrgPerson	Contact/location information
mobile	inetOrgPerson	Contact/location information
o	inetOrgPerson	Contact/location information
postalAddress	organizationalPerson	Contact/location information
preferredLanguage	inetOrgPerson	Personal characteristics
schacGender	schac	Personal characteristics
schacPersonalTitle	schac	Personal characteristics
schacPersonalUniqueCode	schac	Linkage identifiers/Foreign keys
schacUserPresenceID	schac	Contact/location information
sn	person	Personal characteristics
telephoneNumber	person	Contact/location information
userCertificate	inetOrgPerson	Security attributes and keys
userSMIMECertificate	inetOrgPerson	Security attributes and keys

2.3 - Other attributes

The schema from which the above attributes have been selected, also contain a number of other attributes. They are listed in Appendix A. Sufficient use cases have not yet been identified for including these in the standard vocabulary for exchanging identity information. However, organisations may find these or attributes from other schemas useful locally within their institution.

In the interests of interoperability, an attribute in the set above will usually be a better choice for exchanging identity information. However, CAUDIT will periodically review the vocabulary as new use cases arise and if necessary promote attributes to the list, or where no suitable attribute exists, define a new auEduPerson attribute. As such, this document is expected to evolve over time to meet the changing needs of the sector.

3 - Attribute meta-information and notation

For all attributes, the following meta-information is defined.

Description	A short description and semantic meaning of the attribute
Format	Format of the attribute, with permissible values if there is a controlled vocabulary
Classification	The attributes listed in this document are designed to contain information specifically about people. It is helpful to consider this information within broad categories. The categories used below have been collected from the NSF Middleware Initiative Higher-Education Person survey [NMI]. • Personal characteristics • Contact / Location information • Student information • Employee information • Linkage identifiers / Foreign keys • Entry metadata / Administration information • Security attributes and keys • Confidentiality / Attribute release (visibility) • Authorisation, entitlements • Group-related attributes • Other attributes Attributes are classified into a category to give a general indication of how they are normally used. For some categories, CAUDIT has not yet recommended any attributes. These categories are listed as placeholders in the eventuality that use cases requiring these types of attributes are identified in future. A description of each category from the NSF Middleware Initiative Higher-Education Person survey [NMI] is given in Appendix B of this document.
Origin/ObjectClass	The standard from which the attribute originates
OID	Object identifier
SAML attribute name	The name of the attribute in a SAML assertion. Usually within the urn:mace:*:attribute-defs or urn:oid URN name space.
LDAP syntax	The LDAP syntax of an attribute, see [RFC 4517]
Number of values	Single or Multiple
Example values	Example values in the LDIF format, see [RFC 2849]
Notes on usage	Additional notes or advice on using the attribute in the context of exchanging identity information.
Notes on privacy	Usage information specifically related to user privacy. If no specific issues have been identified, this field will say “Nothing specified;” however please note that user privacy should be considered in the release of any attribute.

4 - Attribute definitions

4.1 - auEduPersonAffiliation

Description	Specifies a person's relationship to the institution in broad categories but with a finer-grained set of permissible values than *eduPersonAffiliation*.
Format	This attribute will have a controlled vocabulary. The following values are indicative of possible use cases: • undergraduate-student • honours-student • postgraduate-coursework-student • postgraduate-research-student • nonaward-student • prospective-student • visiting-student • visiting-staff • honorary-staff • contractor
Classification	Personal characteristics
Origin/ObjectClass	auEduPerson
OID	auEduPersonAttributeARC.1
SAML attribute name	urn:oid:auEduPersonAttributeARC.1
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	auEduPersonAffiliation: postgraduate-research-student
Notes on usage	Should be used in favour of the deprecated *auEduPersonSubType* where authorisation is based on broad categories but a finer grain is needed than is available under *eduPersonAffiliation*. *auEduPersonAffiliation* is not a replacement for *eduPersonAffiliation* and is not meant as an exhaustive vocabulary. Values will be added to the vocabulary only in response to community requirements.
Notes on privacy	See privacy notes for *eduPersonAffiliation*.

4.2 - auEduPersonLegalName

Description	The user's legal name, as per their passport, birth certificate, or other legal document.

Format	Free string
Classification	Personal characteristics
Origin/ObjectClass	auEduPerson
OID	auEduPersonAttributeARC.2
SAML attribute name	urn:oid:auEduPersonAttributeARC.2
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	single
Example values	auEduPersonLegalName: Mary Francis Xavier
Notes on usage	A service provider may require the user's legal name either because of some legal requirement prior to service provision or because the service provider must match the legal name with data from an outside source.
Notes on privacy	Due to the sensitivity of this data, an identity provider may desire a bilateral agreement in order to be willing to reveal a user's legal name to a particular relying party. For privacy reasons the user should be aware of the release of this attribute and possibly have a veto capability.

4.3 - auEduPersonSharedToken

Description	A unique identifier enabling federation spanning services such as Grid and Repositories. Values of the identifier are generated using a set formula. The value has the following qualities: *unique;* *opaque*; *non-targeted*; *persistent*; *resolvable* (only by an IdP that has supplied it); *not re-assignable*; *not mutable* (refreshing the value is equivalent to creating a new identity); *permitted to be displayed* (Note: the value is somewhat display friendly, and may be appended to the *displayName* with a separating space, and used as a unique display name to be included in PKI Certificate DNs and as a resource ownership label, e.g. John Citizen ZsiAvfxa0BXULgcz7QXknbGtfxk); and *portable*.
Format	27 character PEM "Base 64 Encoding with URL and Filename Safe Alphabet" encoded string from a 160-bit SHA1 hash of a globally unique

	string. Padding character, '=', is removed from the value. Reference: http://tools.ietf.org/html/rfc4648#page-7
Classification	Linkage identifiers/Foreign keys
Origin/ObjectClass	auEduPerson
OID	auEduPersonAttributeARC.5
SAML attribute name	urn:oid:auEduPersonAttributeARC.5
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Single
Example values	ZsiAvfxa0BXULgcz7QXknbGtfxk
Notes on usage	Service providers participating in federation spanning services may use *auEduPersonSharedToken* to uniquely identify users to other systems or to map to and from identities in PKI certificates used in grid authentication. Other attributes (e.g. *displayName*, identity provider Id, etc) may be used together with *auEduPersonSharedToken* as a transparent description of a particular person at a point in time. This can be implemented to enable interoperability of both SAML and PKI based systems with services such as data and compute grids. The user's *displayName* and identity provider may change over time, but it is possible to implement mechanisms for the *auEduPersonSharedToken* to remain the same.
Notes on privacy	*auEduPersonSharedToken* is not a privacy preserving identifier and should not be used where services are intended to be provided anonymously. Although *auEduPersonSharedToken* is an opaque value, as it may be released with the *displayName* it cannot be relied upon to preserve anonymity.

4.4 - cn

Description	An individual's common name, typically their full name.
Format	Free string
Classification	Personal characteristics
Origin/ObjectClass	person [RFC 4517, RFC 4519]
OID	2.5.4.3
SAML attribute name	urn:mace:dir:attribute-def:cn
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	Mary Francis Xavier

Notes on usage	*cn* is a mandatory attribute of the person LDAP object class. However note that the way it is populated within an organisation's directory often varies considerably.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity.

4.5 - displayName

Description	Preferred name of a person to be used when displaying entries.
Format	Free string
Classification	Personal characteristics
Origin/ObjectClass	inetOrgPerson [RFC 2798]
OID	2.16.840.1.113730.3.1.241
SAML attribute name	urn:mace:dir:attribute-def:displayname
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Single
Example values	displayName: Jack Dougherty
Notes on usage	Where a relying party has a requirement for a user's name, the *displayName* is the preferred attribute to request. An identity provider may source the value to return as *displayName* from any appropriate internal attributes. For example, *givenName* + " " + *surname*; or *cn*. *displayName* is not necessarily a user's legal name and may contain their usual or preferred name. Relying parties should note this value is not guaranteed to be either unique or persistent. It is not recommended to be used as a unique key or for authorisation.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity.

4.6 - eduPersonAffiliation

Description	Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).
Format	This attribute has a controlled vocabulary. Only these values are allowed:

Value	**Meaning**
faculty	Academic or research staff
student	Undergraduate or postgraduate student
staff	All staff

	<table><tr><td>employee</td><td>Employee other than staff, e.g. contractor</td></tr><tr><td>member</td><td>Comprises all the categories named above, plus other members with normal institutional privileges, such as honorary staff or visiting scholar</td></tr><tr><td>affiliate</td><td>Relationship with the institution short of full member</td></tr><tr><td>alum</td><td>Alumnus/alumna (graduate)</td></tr><tr><td>library-walk-in</td><td>A person physically present in the library</td></tr></table>
Classification	Personal characteristics
Origin/ObjectClass	eduPerson [eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.1
SAML attribute name	urn:mace:dir:attribute-def:eduPersonAffiliation
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	eduPersonAffiliation: faculty
Notes on usage	This attribute, like *eduPersonScopedAffiliation*, enables an organisation to assert its relationship with the user. This addresses the common case where a resource is provided on a site licence basis, and the only access requirement is that the user is a *bona fide* member of the organisation, or a specific school or faculty within it. If there is a value in *eduPersonPrimaryAffiliation*, that value should be stored here as well. This attribute may appear suitable for controlling access to, for example, an academic licensed commercial software package. However, this is usually not the case; such licenses have greater constraints than just eduPersonAffiliation=faculty. In most cases an academic user must also agree to use the application for only academic purposes and perhaps accept obligations such as acknowledging the owners or reporting results in a particular way.
Notes on privacy	*eduPersonAffiliation* should be used when the service provider does not need confirmation of the security domain of the user. Service providers who do need the security domain information should ask for *eduPersonScopedAffiliation* instead. Several values of *eduPersonAffiliation* are regarded as being "contained" within other values: for example, the student value is contained within member. It is recommended that identity providers have the ability either to maintain these multiple values for a given individual, or otherwise provide the ability to release either value as appropriate for a particular relying party. For example, although some relying parties might require the release of the more specific student value, a different relying party that only requires the less specific member value should only be sent the less specific value. Releasing student in this case gives the relying party more information about the user than is required, raising privacy and data

	protection concerns. Despite the recommendation above that identity providers should be conservative in what they send, relying parties are recommended to be liberal in what they accept. For example, a relying party requiring member affiliation should also accept student, staff, etc. as alternatives.

4.7 - eduPersonAssurance

Description	Set of URIs that assert compliance with specific standards for identity assurance. This multi-valued attribute represents identity assurance profiles (IAPs), which are the set of standards that are met by an identity assertion, based on the identity provider's identity management processes, the type of authentication credential used, the strength of its binding, etc. Those establishing values for this attribute should provide documentation explaining the semantics of the values. As a multi-valued attribute, relying parties may receive multiple values and should ignore unrecognized values. The driving force behind the definition of this attribute is to enable applications to understand the various strengths of different identity management systems and authentication events and the processes and procedures governing their operation and to be able to assess whether or not a given transaction meets the requirements for access.
Format	A URN that resolves to the definition of the value used.
Classification	Security attributes and keys
Origin/ObjectClass	eduPerson
OID	1.3.6.1.4.1.5923.1.1.1.11
SAML attribute name	urn:oid:1.3.6.1.4.1.5923.1.1.1.11
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	multiple
Example values	eduPersonAssurance: urn:mace:caudit.edu.au:iap:id:1 eduPersonAssurance: urn:mace:caudit.edu.au:iap:id:2
Notes on usage	There are different aspects to the concept of assurance, including the strength of assurance in the user's identity and the strength of the method used to authenticate the user. In a SAML federation, it is possible to use two attributes to differentiate these concepts. The *AuthenticationMethod* attribute that is part of the SAML transaction can assert the strength of the authentication method used in the transaction, and the *eduPersonAssurance* attribute can assert the level of assurance in the user's identity. The SAML *AuthenticationMethod* attribute is not listed as part of this document's attribute vocabulary because it is not an attribute about the user and is not stored in an organisation's LDAP directory – it is

	related to the authentication transaction. Section 5 of this document provides a standard vocabulary to express both of these concepts – the strength of assurance in the user's identity and the strength of the method used to authenticate the user. The CAUDIT URN namespace shown in the examples above contains the definitions of the values in the standard vocabulary. Applications using this vocabulary may choose to use the CAUDIT URNs directly or may create their own URN namespace with the value definitions.
Notes on privacy	Because a particular assurance value may be associated with a small number of persons at an organisation, it may be prudent to remove assurance information from data when performing anonymisation or deidentification.

4.8 - eduPersonEntitlement

Description	URI (either URN or URL) that indicates a set of rights to specific resources.
Format	URIs only, i.e. a URL or URN, see [RFC 3986]
Classification	Authorisation, entitlements
Origin/ObjectClass	eduPerson [eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.7
SAML attribute name	urn:mace:dir:attribute-def:eduPersonEntitlement
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	eduPersonEntitlement: urn:mace:washington.edu:confocalMicroscope eduPersonEntitlement: http://publisher.example.com/contract/GL123
Notes on usage	The meaning of a given value of *eduPersonEntitlement* is normally defined by a service provider. In the case of a value using the "http" scheme, it is recommended that the value resolve to a document giving the definition of the value. Having defined the meaning of the attribute value, the service provider then invites some or all identity providers to express that value for those users who satisfy the definition. In this way the service provider can delegate to the identity provider some or all of the responsibility for authorisation of access to a particular resource. Typically, this attribute is used to assert entitlements over and above those enjoyed by other members of the organisation; for example, "Entitled to access the restricted material present in the Med123 resource". In this case, the service provider trusts the organisation to verify that the user satisfies the (arbitrarily complex) authorisation conditions associated with the entitlement. This may involve an additional licence clause, where the organisation undertakes to assign the *eduPersonEntitlement* values

	according to agreed criteria.
Notes on privacy	Because a particular value of *eduPersonEntitlement* often represents an entitlement to access a specific resource, Identity Providers should be capable of associating any number of entitlements with an individual user. However, such entitlements may represent personal or even sensitive personal data about the individual. It is therefore important to control the release of individual values of *eduPersonEntitlement* closely, so that only Service Providers with a legitimate need for any given value of *eduPersonEntitlement* will have that value released to them. For example, values defined by a particular Service Provider should normally only be released back to that same Service Provider.

4.9 - eduPersonPrimaryAffiliation

Description	Specifies the person's PRIMARY relationship to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).
Format	This attribute has a controlled vocabulary. Permissible values are *faculty*, *student*, *staff*, *alum*, *member*, *affiliate*, *employee*, and *library-walk-in*. See the core attribute *eduPersonScopedAffiliation* for guidance on these values.
Classification	Personal characteristics
Origin/ObjectClass	eduPerson [eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.5
SAML attribute name	Urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Single
Example values	eduPersonPrimaryAffiliation: student
Notes on usage	Think of this as the affiliation one might put on the name tag if this person were to attend a general institutional social gathering. Note that the single-valued *eduPersonPrimaryAffiliation* attribute assigns each person in the directory into one and only one category of affiliation. The assertion of a primary affiliation is context-dependent; therefore this attribute is less useful than *eduPersonScopedAffiliation* or *eduPersonAffiliation*.
Notes on privacy	See privacy notes for *eduPersonAffiliation*.

4.10 - eduPersonPrincipalName

Description	The "NetID" of the person for the purposes of inter-institutional authentication.
Format	The attribute is structured as a scoped attribute, with the form *local-name@security-domain*. The *security-domain* component has the same

	semantics as the corresponding component in *eduPersonScopedAffiliation*. The *local-name* is guaranteed to be unique within the context of the security-domain.
Classification	Linkage identifiers/Foreign keys
Origin/ObjectClass	eduPerson [eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.6
SAML attribute name	urn:mace:dir:attribute-def:eduPersonPrincipalName [Legacy Name and Syntax using the Structured Encoding rules] urn:oid:1.3.6.1.4.1.5923.1.1.1.6 [Uses Simple Encoding rules that are more compatible with vendor products]
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Single
Example values	eduPersonPrincipalName: xxyz1234@ecu.edu.au
Notes on usage	This attribute is used where a persistent user identifier, consistent across different services, is required. Note that although it may appear to be an email address, it is not an email address. It is recommended that a value of *eduPersonPrincipalName* previously associated with one individual should never be reassigned to another individual. However, as in the case of *eduPersonTargetedID*, users and relying parties should be aware that identity providers may not always be able to guarantee to present the same value of *eduPersonPrincipalName*.
Notes on privacy	If the local-name portion of this attribute is not opaque, this attribute should not be used in transactions where it is desirable to maintain user anonymity. It is recommended that the *eduPersonPrincipalName* not contain either the user's single sign-on identifier, as this represents a security vulnerability.

4.11 - eduPersonScopedAffiliation

Description	Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc.
Format	The attribute is structured as a scoped attribute, with the form *affiliation@security-domain*, where affiliation is one of a number of prescribed categories of user. Only these values are allowed to the left of the "@" sign: faculty, student, staff, employee, member, affiliate, alum, library walk-in. These are defined below. The values to the right of the "@" sign should indicate a security domain.

Value	Meaning
faculty	Academic or research staff
student	Undergraduate or postgraduate student

	<table><tr><td>staff</td><td>All staff</td></tr><tr><td>employee</td><td>Employee other than staff, e.g. contractor</td></tr><tr><td>member</td><td>Comprises all the categories named above, plus other members with normal institutional privileges, such as honorary staff or visiting scholar</td></tr><tr><td>affiliate</td><td>Relationship with the institution short of full member</td></tr><tr><td>alum</td><td>Alumnus/alumna (graduate)</td></tr><tr><td>library-walk-in</td><td>A person physically present in the library</td></tr></table>
Classification	Personal characteristics
Origin/ObjectClass	eduPerson [eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.9
SAML attribute name	urn:mace:dir:attribute-def:eduPersonScopedAffiliation [Legacy Name and Syntax using the Structured Encoding rules] urn:oid:1.3.6.1.4.1.5923.1.1.1.9 [Uses Simple Encoding rules that are more compatible with vendor products]
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	eduPersonScopedAffiliation: faculty@cs.berkeley.edu
Notes on usage	This attribute enables an organisation to assert its relationship with the user. This addresses the common case where a resource is provided on a site licence basis, and the only access requirement is that the user is a *bona fide* member of the organisation, or a specific school or faculty within it. This attribute may appear suitable for controlling access to, for example, an academic licensed commercial software package. However, this is usually not the case; such licenses have greater constraints than just eduPersonAffiliation=faculty. In most cases an academic user must also agree to use the application for only academic purposes and perhaps accept obligations such as acknowledging the owners or reporting results in a particular way.
Notes on privacy	See privacy notes for *eduPersonAffiliation*.

4.12 - eduPersonTargetedID

Description	A persistent, non-reassigned, privacy-preserving identifier for a user shared between an identity provider and service provider. An identity provider uses the appropriate value of this attribute when communicating with a particular service provider or group of service providers, and does not reveal that value to any other service provider except in limited circumstances. *Persistence: eduPersonTargetedID* does not require a specific lifetime, but

	the association should be maintained longer than a single user interaction and long enough to be useful as a key for a particular service that is consuming it. *Privacy:* This attribute is designed to preserve the user's privacy and inhibit the ability of multiple unrelated services from correlating user activity by comparing values. It is therefore required to be opaque. *Uniqueness:* A value of this attribute is intended only for consumption by a specific audience of applications (often a single one). Values of this attribute therefore must be unique within the namespace of the identity provider and the namespace of the service provider(s) for whom the value is created. The value is "qualified" by these two namespaces and need not be unique outside them. Logically, the attribute value is made up of the triple of an identifier, the identity provider, and the service provider(s). *Reassignment:* A distinguishing feature of this attribute is that it prohibits reassignment. Since the values are opaque, there is no meaning attached to any particular value beyond its identification of the user. Therefore particular values created by an identity provider must not be reassigned such that the same value given to a particular Service Provider refers to two different users at different points in time.
Format	The *eduPersonTargetedID* value is an opaque string of no more than 256 characters. Note: Common implementations yield a hash in base64 encoding with a length of 28 characters. CAUDIT recommends the value does not exceed this length. The value may be communicated to service providers in either of two forms at the service provider's request. The form in common use within the Shibboleth community has the attribute name *urn:mace:dir:attribute-def:eduPersonTargetedID* and comprises the opaque string value scoped with the identity provider's security domain. These strings are separated by the "@" symbol. A newer form, more compatible with commercial SAML implementations has the attribute name *urn:oid:1.3.6.1.4.1.5923.1.1.1.10* and this new form comprises the entity name of the identity provider, the entity name of the service provider, and the opaque string value. These strings are separated by "!" symbols. This form is advocated by Internet2 and may overtake the other form in due course.
Classification	Linkage identifiers/Foreign keys
Origin/ObjectClass	eduPerson [eduPerson]
OID	1.3.6.1.4.1.5923.1.1.1.10
SAML attribute name	urn:mace:dir:attribute-def:eduPersonTargetedID [Legacy Name and Syntax using the Structured Encoding rules] urn:oid:1.3.6.1.4.1.5923.1.1.1.10 [Uses Simple Encoding rules that are more compatible with vendor products]
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]

Number of values	Multiple
Example values	SAML2 encoding example: (Note:The following is a single string) urn:mace:federation.org.au:testfed:mq.edu.au! urn:mace:federation.org.au:testfed:level-2:wiki.esecurity.edu.au! 7eak0QQIEhygtPXtpgmu5l5hRnY Legacy encoding example: 7eak0QQIEhygtPXtpgmu5l5hRnY
Notes on usage	If a service provider is presented only with the affiliation of an anonymous subject, as provided by *eduPersonScopedAffiliation*, it cannot provide service personalisation or usage monitoring across sessions. These capabilities are enabled by the *eduPersonTargetedID* attribute, which provides a persistent user pseudonym, distinct for each service provider. A service provider may use *eduPersonTargetedID* to support aspects of its service that depend on recognising the same user from session to session. The most common use is to enable service personalisation, to record user preferences such as stored search expressions across user sessions. A secondary use is to enable tracking of user activity, to make it easier to detect systematic downloading of content or other suspected breaches of licence conditions. The attribute enables an organisation to provide a persistent, opaque, user identifier to a service provider. For each user, the identity provider presents a different value of *eduPersonTargetedID* to each service provider to which the attribute is released. The eduPerson specification requires that a value of *eduPersonTargetedID* once assigned to a user for a given service provider shall never be reassigned to another user. Users and service providers should note, however, that not all identity providers may be able to guarantee that a user will always present the same value of *eduPersonTargetedID*; indeed, identity providers may offer their users the ability to generate new values of *eduPersonTargetedID* if they feel their privacy has been compromised. identity providers and users should note that changing a user's *eduPersonTargetedID* for a particular service provider may break the relationship with that service provider.
Notes on privacy	*eduPersonTargetedID* is intended to be a privacy-preserving attribute.

4.13 - mail

Description	Email address
Format	Preferred address for the "to:" field of email to be sent to this person.
Classification	Contact/location information
Origin/ObjectClass	inetOrgPerson [RFC 2798]
OID	0.9.2342.19200300.100.1.3

SAML attribute name	urn:mace:dir:attribute-def:mail
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	dumbledore@hsww.edu
Notes on usage	Mail address should only be used when the service provider needs to communicate with the end user. It should not be used as an identifier and should not be relied upon to be persistent.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity. Privacy considerations should be observed when making a decision about releasing this attribute, as it provides user contact information.

4.14 - mobile

Description	Specifies a mobile telephone number associated with a person
Format	Attribute values should follow the agreed format for international telephone numbers: i.e., "+61 405 891 645"
Classification	Contact/location information
Origin/ObjectClass	inetOrgPerson [RFC 2798]
OID	0.9.2342.19200300.100.1.41
SAML attribute name	urn:mace:dir:attribute-def:mobile
LDAP syntax	TelephoneNumber [1.3.6.1.4.1.1466.115.121.1.50]
Number of values	Multiple
Example values	mobile: +61 405 891 645
Notes on usage	Useful for Service Provider support issues.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity. Privacy considerations should be observed when making a decision about releasing this attribute, as it provides user contact information.

4.15 - o

Description	Standard name of the top-level organization (institution) with which this person is associated.
Format	Free string
Classification	Contact/location information

Origin/ObjectClass	inetOrgPerson [RFC 2798]
OID	2.5.4.10
SAML attribute name	urn:mace:dir:attribute-def:o
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	o: The University of Queensland
Notes on usage	Likely only one value.
Notes on privacy	Nothing specified.

4.16 - postalAddress

Description	Campus or office address of the individual
Format	Free string
Classification	Contact/location information
Origin/ObjectClass	organizationalPerson [RFC 2256, RFC 4519]
OID	2.5.4.16
SAML attribute name	urn:mace:dir:attribute-def:postalAddress
LDAP syntax	PostalAddress [1.3.6.1.4.1.1466.115.121.1.41]
Number of values	Multiple
Example values	postalAddress: PO Box 333$Sydney, NSW 2001
Notes on usage	Useful for white pages.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity. Privacy considerations should be observed when making a decision about releasing this attribute, as it provides user contact information.

4.17 - preferredLanguage

Description	Preferred written or spoken language for a person
Format	See RFC2068 and ISO 639 for allowable values in this field. Esperanto, for example is EO in ISO 639, and RFC2068 would allow a value of en-US for US English.
Classification	Personal characteristics
Origin/ObjectClass	inetOrgPerson [RFC 2798]

OID	2.16.840.1.113730.3.1.39
SAML attribute name	urn:mace:dir:attribute-def:preferredLanguage
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Single
Example values	preferredLanguage: EO
Notes on usage	Useful if a service is available in more than one language.
Notes on privacy	Nothing specified.

4.18 - schacGender

Description	The state of being male or female. The gender attribute specifies the legal gender of the subject it is associated with.
Format	• 0 Not known • 1 Male • 2 Female • 9 Not specified
Classification	Personal characteristics
Origin/ObjectClass	schacPersonalCharacteristics
OID	1.3.6.1.4.1.25178.1.2.2
SAML attribute name	urn:oid: 1.3.6.1.4.1.25178.1.2.2
LDAP syntax	Integer [1.3.6.1.4.1.1466.115.121.1.27]
Number of values	Single
Example values	schacGender: 2
Notes on usage	May be useful, for example, if access to a collection is based on gender, as with some indigenous collections.
Notes on privacy	Privacy considerations should be observed when making a decision about releasing this attribute, as it is a personal characteristic.

4.19 - schacPersonalTitle

Description	The Personal Title attribute type specifies a personal title or salutation for a person. Examples of personal titles are "Ms", "Dr", "Prof", "Rev", and "Sr".
Format	Free string
Classification	Personal characteristics
Origin/ObjectClass	schacPersonalCharacteristics

OID	1.3.6.1.4.1.25178.1.2.8
SAML attribute name	urn:oid:1.3.6.1.4.1.25178.1.2.8
References	RFC1274 - The COSINE and Internet X.500 Schema, personal title, Section 9.3.30
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Single
Example values	schacPersonalTitle: Prof
Notes on usage	Use in favour of the deprecated attribute *auEduPersonSalutation*. Generally used in combination with a name, such as *displayName*.
Notes on privacy	Privacy considerations should be observed when making a decision about releasing this attribute, as it is a personal characteristic.

4.20 - schacPersonalUniqueCode

Description	Specifies a "unique code" for the subject it is associated with. Its value does not necessarily correspond to any identifier outside the scope of the directories using this schema. This might be Student number, Employee number, ...
Format	This attribute is of the format: *urn:mace:terena.org:schac:personalUniqueCode:<country-code>:<iNSS>* The *<country-code>* must be a valid two-letter ISO 3166 country code identifier or the string "int", and assigned by the TERENA URN Registry for this attribute at http://www.terena.org/registry/terena.org/schac/personalUniqueCode/ *<iNSS>* is a Namespace Specific String as defined in RFC 2141 but case insensitive, from a nationally controlled vocabulary, published through the URI identified at the above mentioned TERENA URN registry.
Classification	Linkage identifiers/Foreign keys
Origin/ObjectClass	schacLinkageIdentifiers [SCHAC]
OID	1.3.6.1.4.1.25178.1.2.14
SAML attribute name	urn:oid:1.3.6.1.4.1.25178.1.2.14
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	Common values: *urn:mace:terena.org:schac:personalUniqueCode:int:studentID:<country-code>:<code>*

	National extensions: *urn:mace:terena.org:schac:personalUniqueCode:fi:tut.fi:hetu:010161-995A* *urn:mace:terena.org:schac:personalUniqueCode:es:uma:estudiante:a3b123c12* *urn:mace:terena.org:schac:personalUniqueCode:se:LIN:87654321*
Notes on usage	This attribute may be useful in providing system linkages within organisations by containing, for example, student number, employee number, etc. Organisations may wish to consider this approach rather than creating separate attributes for each intra-organisational linkage identifier, as this will reduce the potential of conflicts with future inter-organisational linkage identifier attributes. This attribute should also be used in favour of the deprecated attributes *auEduPersonID* and *auEduPersonLibraryBarCodeNumber*.
Notes on privacy	Nothing specified.

4.21 - schacUserPresenceID

Description	To store a set of values related to network presence protocols.
Format	URI
Classification	Contact/location information
Origin/ObjectClass	schacContactLocation
OID	1.3.6.1.4.1.25178.1.2.12
SAML attribute name	urn:oid:1.3.6.1.4.1.25178.1.2.12
References	RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax RFC 3508 - H.323 URL Schema RFC 3261 - SIP: Session Initiation Protocol
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	schacUserPresenceID: xmpp:pepe@im.univx.es schacUserPresenceID: sip:pepe@myweb.com schacUserPresenceID: sip:+34-95-505-6600@univx.es;transport=TCP;user=phone schacUserPresenceID: sips:alice@atlanta.com?subject=project%20x&priority=urgent schacUserPresenceID: h323:pepe@myweb.fi:808;params schacUserPresenceID: skype:pepe.perez

Notes on usage	May be useful within virtual organisations and VO portals.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity. Privacy considerations should be observed when making a decision about releasing this attribute, as it provides user contact information.

4.22 - sn

Description	Surname or family name
Format	This is the X.500 surname attribute, which contains the family name of a person. If the person has a multi-part surname (whether hyphenated or not), store both 1) the whole surname including hyphens if present and 2) each component of a hyphenated surname as a separate value in this multi-valued attribute. That yields the best results for the broadest range of clients doing name searches.
Origin/ObjectClass	person [RFC 2256, RFC 4519]
OID	2.5.4.4
SAML attribute name	urn:mace:dir:attribute-def:sn
LDAP syntax	directoryString [1.3.6.1.4.1.1466.115.121.1.15]
Number of values	Multiple
Example values	sn: Carson sn: Fotherington-Thomas
Notes on usage	*sn* is a mandatory attribute of the person LDAP object class.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity.

4.23 - telephoneNumber

Description	Office or campus phone number of the individual
Format	Attribute values should follow the agreed format for international telephone numbers: i.e., "+44 71 123 4567."
Classification	Contact/location information
Origin/ObjectClass	person [RFC 2256, RFC 4519]
OID	2.5.4.20
SAML attribute name	urn:mace:dir:attribute-def:telephoneNumber
LDAP syntax	TelephoneNumber [1.3.6.1.4.1.1466.115.121.1.50]
Number of values	Multiple

Example values	telephoneNumber: +61 2 9850 1234
Notes on usage	Useful for service provider support issues.
Notes on privacy	This attribute should not be used in transactions where it is desirable to maintain user anonymity. Privacy considerations should be observed when making a decision about releasing this attribute, as it provides user contact information.

4.24 - userCertificate

Description	A user's X.509 certificate
Format	RFC 2256 states that this attribute is to be stored and requested in the binary form, as 'userCertificate;binary.' Note that *userSMIMECertificate* is in binary syntax (1.3.6.1.4.1.1466.115.121.1.5) whereas the *userCertificate* attribute is in certificate syntax (1.3.6.1.4.1.1466.115.121.1.8).
Classification	Security attributes and keys
Origin/ObjectClass	inetOrgPerson [RFC 2798]
OID	2.5.4.36
SAML attribute name	urn:mace:dir:attribute-def:userCertificate
LDAP syntax	Certificate [1.3.6.1.4.1.1466.115.121.1.8]
Number of values	Multiple
Example values	Binary encoded X.509 PKI Certificate
Notes on usage	*userCertificate* is the standard attribute where applications expect to find any X.509 PKI Certificates issued to a user. There are no constraints other than that the certificates are expected to be issued to the user associated with the attribute. Multiple certificates may be stored. Making user certificates available via this attribute may enable functionality such as encrypted email communications to users from service providers.
Notes on privacy	PKI certificates are normally considered to be public documents. But because many certificates contain users' email addresses efforts to prevent "scraping" and other inappropriate access to certificates should be considered.

4.25 - userSMIMECertificate

Description	An X.509 certificate specifically for use in S/MIME applications (see RFCs 2632, 2633 and 2634).
Format	RFC 2798 states that this attribute is to be stored and requested in the binary form, as 'userSMIMECertificate;binary.'

Classification	Security attributes and keys
Origin/ObjectClass	inetOrgPerson [RFC 2798]
OID	2.16.840.1.113730.3.1.40
SAML attribute name	urn:mace:dir:attribute-def:userSMIMECertificate
LDAP syntax	Binary [1.3.6.1.4.1.1466.115.121.1.5]
Number of values	Multiple
Example values	
Notes on usage	An X.509 certificate specifically for use in S/MIME applications. According to RFC 2798, "If available, this attribute is preferred over the *userCertificate* attribute for S/MIME applications."
Notes on privacy	Nothing specified.

5 - Levels of Assurance vocabulary

Assurance is an expression of confidence in the user identities electronically presented to an information system. There are different aspects to the concept of assurance, including the strength of assurance in the user's identity and the strength of the method used to authenticate the user. This section provides a standard vocabulary to express both of these aspects.

The vocabulary is based on and aligns with the NIST Electronic Authentication Guideline [NIST 800-63] which is used by many organisations internationally. For further details on the definitions, please refer to that document. The Liberty Alliance Identity Assurance Framework [Liberty IAF] also provides useful clarifications on the levels. It is in alignment with NIST 800-63 and is sometimes referred to in the definitions below.

Relying parties should complete a risk assessment that maps identified risks to assurance levels in order to determine which levels they require. The Australian National e-Authentication Framework [NeAF] provides useful information on conducting such a risk assessment.

5.1 - Identity

The levels below are intended to be used as a vocabulary for the *eduPersonAssurance* attribute. They can be expressed as the following URNs (or under a different URN namespace if preferred):

- urn:mace:caudit.edu.au:iap:id:1
- urn:mace:caudit.edu.au:iap:id:2
- urn:mace:caudit.edu.au:iap:id:3
- urn:mace:caudit.edu.au:iap:id:4

5.1.1 - Level 1

Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data.

5.1.2 - Level 2

At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. Both in-person and remote registration are permitted.

The required evidence for issuing credentials is as follows. Please refer to the Liberty Alliance Identity Assurance Framework [Liberty IAF] for details on carrying out evidence checks. That document also provides procedures that pertain to applicants with whom the enterprise or service has a previous relationship.

In-person verification

Ensure that the applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

Remote verification

Ensure that the applicant submits the references of and attests to current possession of at least one primary Government Picture ID document, and either a second Government ID or

- an employee or student ID number; or
- a financial account number (e.g., checking account, savings account, loan or credit card); or
- a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document.

Ensure that the applicant provides additional verifiable personal information that at a minimum must include:

- a name that matches the referenced photo-ID;
- date of birth; and
- current address or personal telephone number.

Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.

5.1.3 - Level 3

At this level, identity proofing procedures require verification of identifying materials and information. Both in-person and remote registration are permitted.

Level 3 requires the same evidence for issuing credentials as Level 2; however at this level verification of the documents or references is required. Please refer to the Liberty Alliance Identity Assurance Framework [Liberty IAF] for details on carrying out evidence checks. That document also provides procedures that pertain to applicants with whom the enterprise or service has a previous relationship.

5.1.4 - Level 4

Level 4 is intended to provide the highest practical remote network authentication assurance. Remote verification is not permitted at this level. Identity proofing at Assurance Level 4 requires the physical presence of the applicant in front of the registration officer, who must ensure that the applicant is in possession of:

- a primary Government Picture ID document that bears a photographic image of the holder and either
    - secondary Government Picture ID or an account number issued by a regulated financial institution, or
    - two items confirming name, and address or telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing.

A current biometric (e.g. photograph or fingerprints) of the applicant is recorded to ensure the applicant cannot repudiate application.

Please refer to the Liberty Identity Assurance Framework for details on carrying out evidence checks.

5.2 - Authentication

The levels below are intended to be used as a vocabulary for the *AuthenticationMethod* attribute asserted in a SAML transaction, for example. They are taken directly from the NIST Electronic Authentication Guideline [NIST 800-63]. Please refer to that document for further details on authentication mechanism requirements at each level.

The levels can be expressed as the following URNs (or under a different URN namespace if preferred):

- urn:mace:caudit.edu.au:iap:authn:1
- urn:mace:caudit.edu.au:iap:authn:2
- urn:mace:caudit.edu.au:iap:authn:3
- urn:mace:caudit.edu.au:iap:authn:4

5.2.1 - Level 1

This level allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

5.2.2 - Level 2

Level 2 provides single factor remote network authentication. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

5.2.3 - Level 3

Level 3 provides multi-factor remote network authentication. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens and "one-time password" device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

5.2.4 - Level 4

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed, FIPS 140-2

cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

6 - Future directions

This section describes possible future developments under consideration. Community input on these topics is welcome.

6.1 - eduPersonAffiliation controlled vocabulary

There is considerable international discussion on semantics for the controlled vocabulary elements of *eduPersonAffiliation* and associated attributes. Currently these elements – student, staff, faculty, alum, member, etc. – are left undefined in the eduPerson specification and therefore applications have adopted their own definitions which are not necessarily aligned. As federated access management becomes more widespread, service providers are increasingly working with multiple federations and this lack of alignment is becoming problematic. The guidelines currently provided in this document for the *eduPersonAffiliation* controlled vocabulary may be refined in future as this international discussion progresses.

6.2 - auEduPersonAffiliation controlled vocabulary

Some suggestions have been made regarding additions to the controlled vocabulary of the attribute *auEduPersonAffiliation*. This controlled vocabulary may be reviewed in future.

7 - Glossary

Assert: An attribute is asserted when an Identity Provider sends a statement, the assertion, containing the attribute name and value to a Service Provider.

Attribute: A Name/Value pair which is associated with a particular subject or person.

Attribute Release Policy: A policy, expressed in XML, in the configuration of an Identity Provider which governs which attributes and attribute values may be released in assertions to different Service Providers or groups of Service Providers. At each Identity Provider there may be the site Attribute Release Policy (ARP) and a set of user specific ARPS.

Authentication: Authentication (AuthN) is the process where one entity proves their identity to another entity by use of a previously established credential, such as a username/password or PKI Certificate.

Authorisation: Authorisation (AuthZ) is the process where a Service Provider makes an access control decision about an authenticated entity performing some action on some resource. The AuthZ decision makes use of attributes associated with the authenticated entity.

Authoritative: An Identity Provider asserting an attribute associated with a user is authoritative when that Identity Provider is the original source of the attribute or the attribute is securely retrieved from the source system of record for that attribute. Attributes which are assigned by other parties unrelated to the Identity Provider or supplied by the user are not authoritative when asserted by the Identity Provider.

Identity Provider: An Identity Provider (IdP) is a system component implemented by an entity to authenticate its users and to provide authentication and attribute assertions to Service Providers or Relying Parties.

Identifier: A link to an object be it a person or a thing.

Mutable: The attribute assigned to an object may change.

Non-reassignable: Typically applies to an identifier. Once the attribute is assigned to an object it is never assigned to any other object.

Non-targeted: Typically applies to an identifier. An attribute characteristic where a common attribute value is created for all Service Providers (and released to all Service Providers that the Identity Provider has agreed to provide it to). All Service Providers would receive the same value.

Opaque: The format of the identifier or other attribute contains no embedded semantics or metadata. For example a cryptographic hash or a random number may be used as opaque identifiers.

Persistent: The mapping between the attribute (typically an identifier) and object is valid over some (presumably large) time frame.

Portable: An identifier is portable if the identifier value assigned to a user at a new Identity Provider can be the same as the identifier value that was assigned to them at a previous Identity Provider.

Relying Party: An entity which delegates user authentication and attribute retrieval to an Identity Provider, often by means of a Service Provider.

Resolvable: There is a mechanism defined which allows discovery of information concerning the object by just using the attribute itself.

Schema: A Schema is a formal definition of a set of attributes. It defines the semantics of the attribute and the syntax of the possible values. The schemas used in this specification are LDAP schemas. The LDAP schema is used as a convenient and well understood method for formal attribute specification.

Scope: A component of an attribute value which defines some restriction on the interpretation of the value. Scopes are commonly Security Domains.

Security domain: A value which defines the administration or policy for an object or value. In Shibboleth, security domains are often expressed as DNS domains such as uq.edu.au

Service Provider: A Service Provider (SP) is a system component implemented by an entity to delegate user authentication and attribute retrieval.

Targeted: Typically applies to an identifier. An attribute characteristic where the attribute value is created for a specific Service Provider or group of related Service Providers. Each (defined group of) Service Provider(s) would receive a different value.

Transparent: The format of the identifier or other attribute contains embedded semantics or metadata. For example, an email address is a transparent identifier.

Unique: Within some scope, no other object will have the same identifier or attribute value.

8 - References

[eduPerson] eduPerson Object Class Specification (200806)
http://www.educause.edu/eduperson

[ISO 3166] ISO 3166: Country codes
http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm

[Liberty IAF] Liberty Alliance Identity Assurance Framework 1.1
http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf

[NeAF] National e-Authentication Framework
http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

[NIST 800-63] NIST Special Publication 800-63: Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (Version 1.0.2, April 2006)
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[NMI] Higher-Education Person: A Comparative Analysis of Collaborative Public LDAP Person Object Classes in Higher-Education
http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-higher-ed-person-analysis-latest.htm

[RFC 2256] RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3
http://www.ietf.org/rfc/rfc2256.txt

[RFC 2798] RFC 2798: Definition of the inetOrgPerson LDAP Object Class
http://www.ietf.org/rfc/rfc2798.txt

[RFC 2849] RFC 2849: The LDAP Data Interchange Format (LDIF) – Technical Specification
http://www.ietf.org/rfc/rfc2849.txt

[RFC 3986] RFC 3986: Uniform Resource Identifiers (URI): Generic Syntax
http://www.ietf.org/rfc/rfc3986.txt

[RFC 4517] RFC 4517: Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
http://www.ietf.org/rfc/rfc4517.txt

[RFC 4519] RFC 4517: Lightweight Directory Access Protocol (LDAP): Schema for User Applications
http://www.ietf.org/rfc/rfc4519.txt

[schac] SCHAC Attribute Definitions for Individual Data (Version 1.3.0)
http://www.terena.org/activities/tf-emc2/schac.html

9 - Contributors and acknowledgements

The working group would like to acknowledge the work of international federations and groups in formulating attribute vocabularies and specifications from which this document draws heavily, in particular the UK Access Management Federation for Education and Research, TERENA, MACE-Dir, and SWITCH.

This document has been prepared by the auEduPerson Working Group on behalf of the CAUDIT Standing Committee on Technical Standards. Working group members are:

- Patricia McMillan (Chair), The University of Queensland
- Peter Austin, Edith Cowan University
- David Bannon, VPAC
- Anthony Beitz, Monash University
- Victoriano Giralt, University of Malaga, Spain
- Florian Goessmann, ARCS
- Robin Harrington, The University of Canterbury, New Zealand
- Rodney McDuff, The University of Queensland
- Jim McGovern, ARCS
- Alex Reid, AARNet
- Terence Smith, Queensland University of Technology
- Leon Troeth, Monash University
- Neil Witheridge, ARCS

10 - Document change history

Version 2.1, 2 Sep 2009

- Added levels of assurance vocabulary in Section 5 and updated the details on the *eduPersonAssurance* attribute in Section 4.7 to reflect this.
- Removed individual descriptions of other attributes in Appendix A to make the document a more manageable size.
- Minor modifications to Section 1 – Introduction.
- Updated Section 6 – Future directions.
- Updated Section 9 – Contributors and acknowledgements.
- Updated the auEduPerson schema definitions in Appendix C.

Version 2.0, 8 July 2009

- The document title changed to "auEduPerson definition and attribute vocabulary" and branding updated to reflect its ownership by CAUDIT.
- The document scope changed, with changes throughout the document reflecting this. The current document is an attribute vocabulary standard with usage guidelines for the exchange of identity information. With the new scope, the document is not limited to one specific implementation of attribute exchange (the AAF) but can be applied to many applications. Information and guidelines from previous versions that were specific to the AAF have been removed.
- In section 10, added descriptions for some attributes that were missing them – *description, homePhone, homePostalAddress, seeAlso*.
- Future directions section updated.

Version 1.5, 23 Sep 2008:

- The *auEduPersonSharedToken* was updated to reflect a change in character set and format.
- An example was added of SharedToken appended to DisplayName for use in PKI DN and resource labels.
- Minor edit to *auEduPersonSharedToken* notes on usage.
- Minor edit to *eduPersonTargetedID* description.
- Update Reference to eduPerson schema to reflect new version 200806.
- The LoA attributes were revised to reflect the use of AuthenticationMethod and eduPersonAssurance as the attributes which will transport LoA assurances and the AAF IdentityLoA Vocabulary and AAF AuthenticationLoA Vocabulary were added.
- Removed auEduPersonAuthenticationLoA and auEduPersonIdentityLoA attribute definitions from the auEduPerson Schema definition.
- A description of group and course membership attributes was added to Future directions section.

Version 1.4, 4 Jun 2008:

- The name of the attribute *auEduPersonPersistentID* was changed to *auEduPersonSharedToken* and the description updated.

- Documents describing implementation options for *auEduPersonSharedToken* were added to the References.
- A section on Document change history was added.

Version 1.3, 29 Feb 2008:

- Revised version, based on working group review. This version was accepted by the AAF Steering Committee as the working draft for the federation.

Version 1.2, 20 Feb 2008:

- Substantially revised version, based on community consultation.

Version 1.1, 3 Dec 2007

- Draft submitted for community consultation.

11 - Appendix A: Other attributes

The schemas from which the standard attribute vocabulary has been selected also contain a number of other attributes. These are listed below. Please refer to the source schemas of these attributes for further details. CAUDIT currently has not identified sufficient use cases for including these in the standard vocabulary. Members may find these or attributes from other schemas useful locally within their institution.

In the interests of interoperability, an attribute in the standard vocabulary will usually be a better choice for service providers to request. However, as new use cases arise, CAUDIT will assess community feedback and if necessary promote attributes to the vocabulary, or where no suitable attribute exists, define a new auEduPerson attribute. As such, this document and the attribute lists contained in it are expected to evolve over time to meet the changing needs of the sector.

11.1 - List of other attributes

Attribute	Schema	Brief description
description	person	Contains a human-readable description of the object.
eduPersonNickname	eduPerson	Person's nickname, or the informal name by which they are accustomed to be called.
eduPersonOrgDN	eduPerson	The distinguished name (DN) of the directory entry representing the institution with which the person is associated.
eduPersonOrgUnitDN	eduPerson	The distinguished name(s) (DN) of the directory entries representing the person's Organizational Unit(s).
eduPersonPrimaryOrgUnitDN	eduPerson	The distinguished name (DN) of the directory entry representing the person's primary Organizational Unit(s).
facsimileTelephoneNumber	organizationalPerson	A fax number for the directory entry.
homePhone	inetOrgPerson	Specifies a home telephone number associated with a person.
homePostalAddress	inetOrgPerson	Home address. OrgPerson has a PostalAddress that complements this attribute.
initials	inetOrgPerson	Contains the initials of some or all of an individual’s names, but not the surname(s).
jpegPhoto	inetOrgPerson	Used to store one or more images of a person using the JPEG File Interchange Format [JFIF].
l	organizationalPerson	Locality name. According to RFC 2256,

Attribute	Schema	Brief description
		"This attribute contains the name of a locality, such as a city, county or other geographic region (localityName)." X.520(2000) reads: "The Locality Name attribute type specifies a locality. When used as a component of a directory name, it identifies a geographical area or locality in which the named object is physically located or with which it is associated in some other important way."
labeledURI	inetOrgPerson	Commonly a URL for a web site associated with this person.
manager	inetOrgPerson	This attribute carries the DN of the manager of the person represented in this entry.
ou	organizationalPerson	Organizational unit(s). When used as a component of a directory name it identifies an organizational unit with which the named object is affiliated.
pager	inetOrgPerson	Specifies a pager telephone number for an individual.
postOfficeBox	organizationalPerson	Specifies the Postal Office Box by which the object will receive physical postal delivery. If present, the attribute value is part of the object's postal address.
postalCode	organizationalPerson	Specifies the postal code of the named object. If this attribute value is present, it will be part of the object's postal address.
schacCountryOfCitizenship	schac	Specifies the (claimed) countries of citizenship for the subject it is associated with.
schacCountryOfResidence	schac	Specifies the (claimed) country of residence for the subject it is associated with.
schacDateOfBirth	schac	The date of birth for the subject it is associated with.
schacExpiryDate	schac	The date from which the set of data is to be considered invalid (specifically, in what refers to rights and entitlements). This date applies to the entry as a whole.
schacHomeOrganization	schac	Specifies a person´s home organization

Attribute	Schema	Brief description
		using the domain name of the organization.
schacHomeOrganizationType	schac	Type of home organization.
schacMotherTongue	schac	Is the language a person learns first. Correspondingly, the person is called a native speaker of the language. Usually a child learns the basics of their first language from their family.
schacPersonalPosition	schac	The Personal Position attribute type specifies a personal position inside an institution.
schacPersonalUniqueID	schac	Specifies a "legal unique identifier" for the subject it is associated with.
schacPlaceOfBirth	schac	Specifies the place of birth for the subject it is associated with.
schacSn1	schac	First surname of a person ("the surname" in international terms). schacSn1 would contain whatever values the described person thinks they should contain. Splitting shall be done by humans. That means that, when filling a SCHAC-based description that allows the use of schacSn1 and schacSn2, the administrators must ask for 1st surname and 2nd surname (if applicable) as well as they do for givenName, surname, etc.
schacSn2	schac	Second surname of a person (how this is assigned is a local matter). schacSn2 would contain whatever values the described person thinks they should contain. Splitting shall be done by humans. That means that, when filling a SCHAC-based description that allows the use of schacSn1 and schacSn2, the administrators must ask for 1st surname and 2nd surname (if applicable) as well as they do for givenName, surname, etc.
schacUserPrivateAttribute	schac	Used to model privacy requirements, as expressed by the user and/or the organizational policies. The values are intended to be attribute type names and apply to the attribute and any subtypes of it for a given entity. In respect to data exchange, it applies to

Attribute	Schema	Brief description
		the expression of privacy requirements.
schacUserStatus	schac	Used to store a set of statuses of a person as a user of services. An example where this may be useful is for sessional staff who may not be currently employed but who still retain access to a range of services.
seeAlso	person	The distinguished name of another directory entry. From RFC 4519: The 'seeAlso' attribute type contains the distinguished names of objects that are related to the subject object. Each related object name is one value of this multi-valued attribute."
st	organizationalPerson	Abbreviation for state or province name.
street	organizationalPerson	Contains the physical address of the object to which the entry corresponds, such as an address for package delivery (streetAddress).
title	organizationalPerson	Specifies the designated position or function of the object within an organization.
uid	inetOrgPerson	Specifies a computer system login name.

11.2 - Appendix B: Attribute classifications

The attributes listed in this document are designed to contain information specifically about people. It is helpful to consider this information within broad categories. The ten categories listed below have been collected from the NSF Middleware Initiative Higher-Education Person survey [NMI]. This appendix gives the description of each category from the NMI document.

Attributes are classified into a category to give a general indication of how they are normally used. For some categories, CAUDIT has not yet recommended any attributes. These categories are listed as placeholders in the eventuality that use cases requiring these types of attributes are identified in future.

- **Personal characteristics**

  Personal characteristics describe the individual person represented by the entry. Name and favorite drink are attributes that would be considered personal characteristics.

- **Contact / Location information**

  Higher education's established history of openness and collaboration gives rise to the use of institutional directories as a primary means of locating and contacting potential collaborators and other persons-of-interest at peer institutions.

- **Student information**

  Student information includes attributes that have relevance to the student role, such as curriculum, major, and degree.

- **Employee information**

  Employee information includes attributes that have relevance to the employee role, such as position, office hours, and job title.

- **Linkage identifiers / Foreign keys**

  Linkage attributes are those identifiers used to link a directory entry with records in external data stores or other directory entries. The use of linkage identifiers can obviate the need to synchronize data elements between systems of record and the enterprise directory. Linkage attributes are also used in the implementation of metadirectory services.

- **Entry metadata / Administration information**

  Entry metadata attributes are used to contain information about the entry itself, often its status, birth, and death. Such attributes can be critical to metadirectory processing. While the object classes discussed here were designed to accommodate person entries, metadata attributes can also be useful with non-person entry types such as groups. In such cases the metadata attributes may be best defined in an auxiliary object class independent of the person object class.

- **Security attributes and keys**

  Security attributes are used to assist in authentication-related activities such as password self-reset. Security attributes that contain sensitive data such as passwords should be carefully protected, highly restricted, and probably encrypted using a one-way hash algorithm such as MD5 or SHA1 so that in the event that the directory server is compromised in an attack the attribute values are not useful to an attacker.

- **Confidentiality / Attribute release (visibility)**

  Often person lookup, termed "white pages", is the first institutional service reliant upon an LDAP directory. Even if an LDAP directory is designed to support multiple applications, it is common practice for the directory to be accessible via LDAP and LDAPS queries and return limited information to institution members and other interested parties around the globe.

While there are risks to allowing direct LDAP protocol access to an institutional directory, such as directory harvesting or crawling (a technical term meaning to browse the directory content) to obtain email addresses, allowing LDAP access can simplify integration with LDAP-enabled products and reduce application integration time, as well as allowing institutional members the freedom to utilize many LDAP-enabled utilities and applications that are freely available.

Confidentiality attributes are commonly used to indicate whether an entry is visible publicly, visible only to affiliates of the institution, or not visible at all. In some cases only specific attributes, such as phone, address, and email address, are restricted, in other cases all attributes are restricted.

Confidentiality attributes may be provided to applications so that the applications can determine under what circumstances to display the attributes. Confidentiality attributes may also be used internally by the directory DSA to restrict the information returned by the server to LDAP queries, this can be done through directory access controls. DSA's vary in their access control capabilities.

Access control information is used to define the accessibility of directory entries and attributes. Each DSA implements access controls in its own fashion and syntax. In X.500 these are referred to as Access Control Information. LDAP DSA's may refer to them as access control lists (ACL's) or access control instructions (ACI's) or by other names. (Generally ACL's are stored in a DSA configuration file, but not within the directory itself, whereas ACI's are entries within the directory DIT.) Membership in a group may give a person or account the privileges necessary to see entries and attributes. Privileges may also be based on what type of authentication is used or what IP address the query is initiated from. The entries and attributes returned can be filtered so that only entries or attributes that meet certain criteria are returned. Confidentiality attributes can be used to dynamically customize and personalize the filters that are applied so that queries retrieve only the information that is allowed, which may vary from person to person.

There is nothing in the LDAP protocol itself to categorize or define restrictions, it is left to the directory architect to structure the access controls, define attributes that describe confidentiality preferences, and determine how those attributes are best populated and propagated to ensure that personal confidentiality and privacy is maintained.

Directory architects are encouraged to review their governmental privacy regulations and their institutional interpretation of those regulations. Not doing so can result in the inappropriate release of private information via the directory, which can seriously undermine institutional acceptance of the directory service.

- **Authorisation, entitlements**

  Authorization for services is generally implemented in LDAP directories either through the use of entry attributes or group memberships. Applications such as Shibboleth (see <http://shibboleth.internet2.edu/>) can make use of entitlement attributes in an entry to provide authorization information to requesting services.

- **Group-related attributes**

  Directory groups are often used to provide authorization to entries and attributes, as well as to restrict or provide access to services. There are benefits to having group memberships described in members' entries as well as in a group entry. Because not all DSA's provide this functionality (Microsoft Active Directory and Novell eDirectory do) local attributes are often defined to meet organizational needs.

- **Other attributes**

  Additional non-standard attributes that did not fit well into the primary categories, but may be of general interest.

12 - Appendix C: LDAP Schema for auEduPerson

The following is the proposed the auEduPerson schema. The schema can also be found at https://wiki.caudit.edu.au/confluence/display/aafaueduperson/LDAP+Schema+Definitions.

```
#------------------------------------------------------------------------
#
# auEduPerson  v: 20090820
#
# auEduPerson schema
#
# The first draft of the auEduPerson schema was produced by
# WALAP (Western Australian Libraries Authentication Project) in 2002-09-27
# to provide an authentication infrastructure to assist the Western
# Australian University Libraries in the continuing development of
# access to online resources. This document defined two objectclasses;
# auEduPerson and auEduUnit; registered in the AARNet OID namespace.
# See <http://walap.curtin.edu.au/docs/walap_schema_1_0.ldif>
#
# In March 2007 the Australian Access Federation Steering Committee approved
# the creation of a working group to determine the need for identity attributes
# and schemas for the Australasian Higher Education and Research sector which
# would extend the WALAP work. Consequently representatives of the WALAP project
# were invited to join the new working group.
#
# During the deliberations of the auEduPerson WG it was decided to deprecated
# most of the attribute definitions in the WALAP auEduPerson objectclass
# and define attributes and schema that were more representative of the whole
# Australasian Higher Education and Research sector.
#
# New attributes added to the auEduPerson schema are registered under the
# AAF OID namespace (1.3.6.1.4.1.27856) whilst the auEduPerson objectclass itself
# remains registered in the AARNet OID namespace. The auEduUnit objectclass and
# related attributes remain intact were considered, at the time, out of the
# scope of the auEduPerson WG.
#
# The latest version of this document is avaliable at
# http://?????
#
#------------------------------------------------------------------------
#
# 20020907 - Initial Release.
# 20071106 - Re-released.
# 20090514 - Moved jurisdiction from AAF to CAUDIT. OID ARC remaining the same.
# 20090820 - DEPRECATED auEduPersonAuthenticationLOA and auEduPersonIdentityLOA
in
#            lieu of of the eduPersonAssurance attribute in the eduPerson schema.
# 20090820 - RENAMED the auEduPersonPersistentID attribute to
#            auEduPersonSharedToken with the same OID.

objectIdentifier CAUDITARC                                  1.3.6.1.4.1.27856
objectIdentifier AARNetARC                                  1.3.6.1.4.1.8852

objectIdentifier auEduPersonARC                      CAUDITARC:1
objectIdentifier auEduPersonObjectClassARC     auEduPersonARC:1
objectIdentifier auEduPersonAttributeARC       auEduPersonARC:2

objectIdentifier WALAPAttributeARC                   AARNetARC:4.1.1
objectIdentifier WALAPObjectClassARC           AARNetARC:4.1.2


#------------------------------------------------------------------------
# Orginal WALAP auEduPerson Attributes
```

```
#-----------------------------------------------------------------------

#
# auEduPersonSalutation [DEPRECATED] Use schacPersonalTitle
#
# Descrip: Attribute type salutation is derived from attribute type title
#          which is specified in RFC 2256 and X.520.
#
#  Format: Possible values include "Ms", "Mr", "Dr" and "Prof".
#
# Example: auEduPersonSalutation: Mr
#
attributetype ( WALAPAttributeARC:0
   NAME                                        'auEduPersonSalutation'
   SUP                                         title
   SINGLE-VALUE)

#
# auEduPersonPreferredGivenName [DEPRECATED]
#
# Descrip: Attribute type auEduPersonPreferredGivenName is derived from
#          attribute type givenName as defined in RFC 2256 and X.520.
#
#  Format: A typical value may be "John".
#
# Example: auEduPersonPreferredGivenName: Johnny
#
attributetype ( WALAPAttributeARC:1
   NAME                                        'auEduPersonPreferredGivenName'
   SUP                                         givenName )

#
# auEduPersonPreferredSurname [DEPRECATED]
#
# Descrip: Attribute type auEduPersonPreferredSurname is derived from
#          attribute type sn as defined in RFC 2256.
#
#  Format: A value could be "Smith"
#
# Example: auEduPersonPreferredSurname: Smith
#
attributetype ( WALAPAttributeARC:2
   NAME                                        'auEduPersonPreferredSurname'
   SUP                                         sn )

#
# auEduPersonExpiryDate [DEPRECATED]
#
# Descrip: Attribute type auEduPersonExpiryDate is used to store the date
#          when the entry expires. It is a single-valued attribute
#
#  Format: The date format used is ISO 8601, which specifies a date as
#          YYYY-MMDD. For example the twenty-second day in May in the year
#          2008 is represented as, 2008-05-22
#
# Example: auEduPersonExpiryDate: 2008-05-22
#
attributetype ( WALAPAttributeARC:3
   NAME                                        'auEduPersonExpiryDate'
   EQUALITY caseIgnoreMatch
   SYNTAX                                      '1.3.6.1.4.1.1466.115.121.1.15'
   SINGLE-VALUE)

#
```

```
# auEduPersonID [DEPRECATED]
#
# Descrip: Attribute type auEduPersonID is derived from attribute type
#          employeeNumber as defined for object class inetOrgPerson in
#          RFC 2798. This attribute is used to store a numeric or an
#          alphanumeric identifier assigned to a person, such as student
#          or staff identification number. It is a single-valued attribute.
#          The value of auEduPersonID has to be unique across a university.
#
#  Format: An example value is "856302"
#
# Example: auEduPersonID: 856302
#
attributetype ( WALAPAttributeARC:4
   NAME                                          'auEduPersonID'
   SUP                                           employeeNumber )

#
# auEduPersonType [DEPRECATED]
#
# Descrip: Attribute type auEduPersonType is derived from attribute type
#          employeeType as defined for object class inetOrgPerson in
#          RFC 2798. The attribute is used to identify the person's
#          relationship to the university. Values may be, "student",
#          "staff" or "others". The directory server will accept any other
#          value, but for the purpose of the WALAP-ISP project, the
#          participating universities have agreed to use only one of the
#          three values given above. The attribute is single-valued
#
#  Format:
#
# Example: auEduPersonType: student
#
attributetype ( WALAPAttributeARC:5
   NAME                                          'auEduPersonType'
   SUP                                           employeeType
   SINGLE-VALUE)

#
# auEduPersonSubType [DEPRECATED] Use auEduPersonAffiliation
#
# Descrip: Attribute type auEduPersonSubType is derived from attribute
#          type employeeType as defined for object class inetOrgPerson in
#          RFC 2798. Together with attribute auEduPersonType the attribute
#          is used to describe the type of a person. Values may be
#          "undergrad", "postgrad", "alumni" etc., but any value is
#          accepted.
#
#  Format:
#
# Example: auEduPersonSubType: postgrad
#
attributetype ( WALAPAttributeARC:6
   NAME                                          'auEduPersonSubType'
   SUP                                           employeeType )

#
# auEduPersonEmailAddress [DEPRECATED]
#
# Descrip: Attribute type auEduPersonEmailAddress is derived from attribute
#          type mail, which is specified in object class inetOrgPerson in
#          RFC 2798. A possible value may look like "Smith@ecu.edu.au".
#
#  Format:
```

```
#
# Example: auEduPersonEmailAddress: jsmith@ecu.edu.au
#
attributetype ( WALAPAttributeARC:7
   NAME                                          'auEduPersonEmailAddress'
   SUP                                           mail )

#
# auEduPersonLibraryBarCodeNumber [DEPRECATED]
#
# Descrip: Attribute type auEduPersonLibraryBarCodeNumber is used to hold
#          an alphanumeric string used for identifying borrowers in the
#          library information systems.
#
#  Format:
#
# Example: auEduPersonLibraryBarCodeNumber: 892727
#
attributetype ( WALAPAttributeARC:8
   NAME                                          'auEduPersonLibraryBarCodeNumber'
   EQUALITY caseIgnoreMatch
   SYNTAX                                        '1.3.6.1.4.1.1466.115.121.1.15')

#
# auEduPersonLibraryPIN [DEPRECATED]
#
# Descrip: Attribute type auEduPersonLibraryPIN stores an identification
#          number used for library information systems.
#
#  Format:
#
# Example: auEduPersonLibraryPIN: 7392
#
attributetype ( WALAPAttributeARC:9
   NAME                                          'auEduPersonLibraryPIN'
   EQUALITY caseIgnoreMatch
   SYNTAX                                        '1.3.6.1.4.1.1466.115.121.1.15')

#
# auEduPersonActiveUnit [DEPRECATED]
#
# Descrip: Attribute type auEduPersonActiveUnit is derived from attribute
#          type member as given in RFC 2256 and X.500. It is of syntax,
#          "Distinguished Name" and is used to hold dn of the units in
#          the units sub tree according to the person's current active
#          enrolment.
#
#  Format:
#
# Example: auEduPersonActiveUnit: cn=POL3101, ou=units, o=ecu, c=au
#          auEduPersonActiveUnit: cn=PHR3105, ou=units, o=ecu, c=au
#          auEduPersonActiveUnit: cn=HST4582, ou=units, o=ecu, c=au
#
attributetype ( WALAPAttributeARC:10
   NAME                                          'auEduPersonActiveUnit'
   SUP                                           member )


#-----------------------------------------------------------------------
# Orginal WALAP auEduUnit Attributes
#-----------------------------------------------------------------------

#
# auEduUnitCode
```

```
#
# Descrip: Attribute type auEduUnitCode is derived from attribute type
#          name, which is specified in RFC 2256 and X.500. It is defined as
#          a single-valued attribute. An example value is "POL3101".
#          Object class auEduUnit declares auEduUnitCode as a mandatory
#          attribute. Its value is used to name an entry of object class
#          auEduUnit. A unit's entry in the WALAP Directory of object class
#          auEduUnit is named with the cn (common name) attribute. The
#          value used for cn is the value of auEduUnitCode.
#          The value of auEduUnitCode has to be unique across a university.
#
#  Format:
#
# Example: auEduUnitCode: POL3101
#
attributetype ( WALAPAttributeARC:11
   NAME                                          'auEduUnitCode'
   SUP                                           name
   SINGLE-VALUE)

#
# auEduUnitName
#
# Descrip: Attribute type auEduUnitName is derived from attribute type
#          name, which is specified in RFC 2256 and X.500. Attribute
#          auEduUnitName holds some descriptive information about the
#          unit, such as the title "Politics and Government for
#          beginners and politicians".
#
#  Format:
#
# Example: auEduUnitName: "Politics and Government for beginners and
#                          politicians"
#
attributetype ( WALAPAttributeARC:12
   NAME                                          'auEduUnitName'
   SUP                                           name )

#
# auEduUnitActiveMember
#
# Descrip: Attribute type auEduUnitActiveMember is derived from attribute
#          type member, which is specified in RFC 2256 and X.500. Its
#          syntax is "Distinguished Name" and it holds the dn of a person
#          actively enrolled in this unit.
#
#  Format:
#
# Example: auEduUnitActiveMember: cn=67181, ou=people, o=ecu, c=au
#
attributetype ( WALAPAttributeARC:13
   NAME                                          'auEduUnitActiveMember'
   SUP member )

#-----------------------------------------------------------------------
# New auEduPerson Attributes
#-----------------------------------------------------------------------

#
# auEduPersonAffiliation
#
# Descrip: Specifies a person's relationship to the institution in broad
#          categories but with a finer-grained set of permissible values
#          than eduPersonAffiliation.
```

```
#
#  Format: This attribute has a controlled vocabulary. The following values
#          are permissible:
#               * undergraduate-student
#               * honours-student
#               * postgraduate-coursework-student
#               * postgraduate-research-student
#               * nonaward-student
#               * prospective-student
#               * visiting-student
#               * visiting-staff
#               * emeritus-staff
#               * contractor
#               * physically-present
#
# Example: auEduPersonAffiliation: postgradate-research-student
#
attributetype ( auEduPersonAttributeARC:1
    NAME 'auEduPersonAffiliation'
    DESC ''
    EQUALITY caseIgnoreMatch
    ORDERING caseIgnoreOrderingMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

#
# auEduPersonLegalName
#
# Descrip: A Service Provider may requires the user's Legal Name either because
of some
#          legal requirement prior to service provision or because the Service
Provider
#          must match the Legal Name with data from a source outside the
Federation
#          Identity Provider.
#
#  Format:
#
# Example:
#
attributetype ( auEduPersonAttributeARC:2
    NAME 'auEduPersonLegalName'
    DESC ''
    SINGLE-VALUE
    EQUALITY caseIgnoreMatch
    ORDERING caseIgnoreOrderingMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

#
# auEduPersonAuthenticationLOA [DEPRECATED]
#
# Descrip: Provides a measure of the strength of the authentication act of the
user
#          so as to allow a Service Provider auxiliary information on which to
judge
#          access rights. See AAF Authentication Management Policy for more
information.
#
# Two schemes for attribute values are under consideration
#
#  Format: URN scheme. Permissible values for the attribute under this scheme
are:
#               * urn:mace:aaf.edu.au:iap:authN:level1
```

```
#               * urn:mace:aaf.edu.au:iap:authN:level2
#               * urn:mace:aaf.edu.au:iap:authN:level3
#               * urn:mace:aaf.edu.au:iap:authN:level4
#  Format: OID scheme. Permissible values for the attribute under this scheme
are:
#               * auEduPersonAttributeARC:3.1
#               * auEduPersonAttributeARC:3.2
#               * auEduPersonAttributeARC:3.3
#               * auEduPersonAttributeARC:3.4
#
# Example: auEduPersonAuthenticationLOA: urn:mace:aaf.edu.au:iap:authN:level1
#
attributetype ( auEduPersonAttributeARC:3
    NAME 'auEduPersonAuthenticationLOA'
    DESC ''
    SINGLE-VALUE
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

#
# auEduPersonIdentityLOA [DEPRECATED]
#
# Descrip: Provides a measure of the strength of the Identity Management Process
of
#          the user  so as to allow a Service Provider auxiliary information on
which
#          to judge access rights. See AAF Identity Management Policy for more
information.
#
#  Format: URN scheme. Permissible values for the attribute under this scheme
are:
#               * urn:mace:aaf.edu.au:iap:ID:level1
#               * urn:mace:aaf.edu.au:iap:ID:level2
#               * urn:mace:aaf.edu.au:iap:ID:level3
#               * urn:mace:aaf.edu.au:iap:ID:level4
#  Format: OID scheme. Permissible values for the attribute under this scheme
are:
#               * auEduPersonAttributeARC:4.1
#               * auEduPersonAttributeARC:4.2
#               * auEduPersonAttributeARC:4.3
#               * auEduPersonAttributeARC:4.4
##
# Example: auEduPersonIdentityLOA: urn:mace:aaf.edu.au:iap:ID:level3
#
attributetype ( auEduPersonAttributeARC:4
    NAME 'auEduPersonIdentityLOA'
    DESC ''
    SINGLE-VALUE
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

#
# auEduPersonSharedToken
#
# Descrip: An opaque identifier which is unique, not reassignable, and persistent
across
#          different Service Providers.
#
#  Format: free string
#
# Example: auEduPersonSharedToken: 7eak0QQIEhygtPXtpgmu5l5hRnY
#
attributetype ( auEduPersonAttributeARC:5
    NAME 'auEduPersonSharedToken'
```

```
    DESC ''
    SINGLE-VALUE
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

#---------------------------------------------------------------------
# ObjectClasses
#---------------------------------------------------------------------

objectclass ( WALAPObjectClassARC:0
     NAME                                       'auEduPerson'
     SUP                                        inetOrgPerson
     AUXILIARY
     MAY ( auEduPersonID $
           auEduPersonSalutation $
           auEduPersonPreferredGivenName $
           auEduPersonPreferredSurname $
           auEduPersonExpiryDate $
           auEduPersonType $
           auEduPersonSubType $
           auEduPersonEmailAddress $
           auEduPersonLibraryBarCodeNumber $
           auEduPersonLibraryPIN $
           auEduPersonActiveUnit $
                     member $
           auEduPersonAffiliation $
           auEduPersonLegalName $
           auEduPersonAuthenticationLOA $
           auEduPersonIdentityLOA $
                     auEduPersonSharedToken )
            )

objectclass ( WALAPObjectClassARC:1
     NAME                                       'auEduUnit'
     SUP                                        top
     STRUCTURAL
     MUST ( cn $ auEduUnitCode )
     MAY (auEduUnitName $ auEduUnitActiveMember )
     )

#---------------------------------------------------------------------
# End of auEduPerson schema
#---------------------------------------------------------------------
```