UCTrust Standard Attributes and SAML OIDs

It is essential that UCTrust participants support and use common definitions for certain basic identity attributes. The formal specification of identity management attributes for use within UCTrust, ucEduPerson, is an augmentation of the eduPerson attributes that are used by InCommon. Additional elements may be added from time to time but the definition and meaning of existing attributes is not expected to change.

Participants need not be able to assert all attributes but when they do assert an attribute from that schema the meaning of that attribute must match the definition provided in the specification.

UCTrust: Supported Identity Attributes

The attributes that all participants should be able to recognize is identified in the table below. Note that no attributes are universally available for all users at all locations through UCTrust SSO. These attributes have been selected because most or all locations have agreed to support them (or are considering supporting them) as commonly available to applications authenticating through UCTrust services.

The table below lists UCTrust's locally-defined extensions to the InCommon Federated attribute set.

Attribute (Friendly-ish name)	URN	Source	UCTrust Support	Encoding	Format	Value	Description	Last Update
UCnetID	urn:oid:2.16.840.1.113916.1.1.4.1	UCTrust	Current		Ten Digit number	Single	UCnetID, as assigned by UC's Universitywide Demographics Database. The UCnetID is an integer that uniquely identifies a single member of the UC community. This integer is transmitted between UCOP and the campuses in the form of a ten-character field with the digits representing the UCnetID left justified within the field. Note that the number of digits in the UCnetID may be increased in the future.	
UCTrustAssurance	urn:oid:2.16.840.1.113916.1.1.5	UCTrust	Current, but likely inconsistent			Multi	UCTrust Assurance. This multivalued attribute defines the UCTrust assurance associated with a particular SAML-2 assertion. Values for this attribute are of the form urn:mace:universityofcalifornia.edu:ucidentity:attributes:assurance:*	
UC Campus Employee ID (PPS ID)	urn:oid:2.16.840.1.113916.1.1.6	UCTrust	Legacy	SAMLxScopedString	9 digit number with campus scope	Single	UC Campus Employee ID. This single-valued attribute contains the nine-digit employee ID (including leading zeros), as defined by the Campus' Payroll /Personnel System (PPS) and issued by this IdP's campus. Scoped/qualified by the campus's top domain name [1] provided to InCommon. For example, 012345678@ucla.edu would be the value for the employee with PPS ID 012345678 at UCLA. *Note, existence of this value does NOT imply an individual is a current employee of the campus. Use eduPersonAffiliation, eduPersonPrimaryAffiliation or eduPersonScopedAffiliation to identify employees.*	

UCTrust Short Campus ID	urn:oid:2.16.840.1.113916.1.1.7	UCTrust	Deprecated			***Single***	To facilitate a migration to long identifiers, UCTrustCampusIDShort, will be available for a limited transition period, no more than five years. It will not exceed 12 characters in length, it will contain only alphanumeric characters, and its persistence will not be greater than five years.
							
							• It will be scoped in a non-standard way. The format will be two characters to designate the UC location, followed by no more than 10 alphanumeric characters assigned by that location. For example, "RI1234567890" could designate Jane Doe at UC Riverside. The following are the two-character location codes:
							  ◦ BE - UC Berkeley
							  ◦ DA - UC Davis
							  ◦ IR - UC Irvine
							  ◦ LA - UC Los Angeles
							  ◦ ME - UC Merced
							  ◦ RI - UC Riverside
							  ◦ SD - UC San Diego
							  ◦ SF - UC San Francisco
							  ◦ SB - UC Santa Barbara
							  ◦ SC - UC Santa Cruz
							  ◦ OP - UC Office of the President
							  ◦ LB - Lawrence Berkeley National Labs
							• It will not be reassigned to more than one person by the same campus within the five-year lifetime of the identifier.
							• Duplicate identifiers for an individual should be rare from a single campus, but are allowed.
							• Duplicates will occur for people who are assigned UCTrustCampusIDShort's by multiple campuses.
							• UCTrustCampusIDShort will be deprecated on or before July 1, 2012. If at any time before that date there are no current applications that need UCTrustCampusIDShort to operate, the UCTrust Work Group may choose to deprecate it sooner.	

~~UCPathEmplid~~	~~urn:oid:2.16.840.1.113916.1.1.8~~	UCTrust	Retired				*This attribute was removed following UCTrust decision to map UCPathEmplid to the existing "inetOrgPerson:employeeNumber" value.*	

UCPathEmplid (released as inetOrgPerson: employeeNumber)	urn:oid:2.16.840.1.113730.3.1.3	UCTrust (reuse of inetOrgPerson)	Current	SAMLxString	8 digit number	Single	UCPath Emplid, a value assigned by the UCPath HR system. This single valued attribute contains the 8 character employee id (including leading zeros) used to uniquely identify individuals stored in the UCPath system. These mostly consist of employees, but also include some contractor, volunteer and similar type affiliates. Note that this OID is part of the inetOrgPerson defintion (specifically, it represents inetOrgperson::employeeNumber). The UCTrust-specific use of this OID is to define that it will contain the UCPath Emplid. *Note, existence of this value does NOT imply an individual is a current or past employee of the University. Use eduPersonAffiliation, eduPersonPrimaryAffiliation or eduPersonScopedAffiliation to identify employees.*	
UC Campus Student System ID (proposed)	urn:oid:2.16.840.1.113916.1.1.9	UCTrust	???	SAMLxScopedString	(max) 36 alpha-numeric characters plus campus scope	Single	UC Campus Student System ID. This single-valued attribute contains the individual's local student system ID as defined by the appropriate campus' Student Information System and issued by this IdP's campus, qualified by the campus's top domain name provided to InCommon. For example, 0111111@ucsc.edu would be the value for the person with the student system ID of 0111111 at UCSC. (While this example is only numeric, the identifier is allowed to be alpha-numeric). Identifier lengths are not consistent across campuses, but a maximum identifier length of 36, not counting the campus scope[1], has been agreed to. *Note, existence of this value does NOT imply an individual is a current or past student of the campus. Use eduPersonAffiliation, eduPersonPrimaryAffiliation or eduPersonScopedAffiliation to identify student affiliations.*	
eduPersonPrincipleName (aka ePPN)	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	eduPerson	Current	SAMLxScopedString		Single	*Definition* A scoped identifier for a person. Basically, a common globally-unique SSO ID for the person associated with their campus. It will take the form "*user@scope*" where '*user*' is a location-assigned username and the "*scope*" is the campus' internet domain (e.g., *campus.edu*).	
eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	eduPerson	Current Inconsistent	SAMLxString	Constrained Values	Multi	*Definition* Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary). *Permissible values* faculty, student, staff, alum, member, affiliate, employee, library-walk-in Note: UCTrust members vary significantly in how these values are derived, making this value of limited value beyond as an informational/display element.	
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	eduPerson	Current Inconsistent	SAMLxScopedString	Constrained Values	Multi	This value is the same as eduPersonAffiliation, but with a scope ("@campus.edu") appended to each value. E.g., "faculty@berkeley.edu" instead of "faculty".	
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	eduPerson	Deprecated Inconsistent	NameID Format	Triplet of data, some opaque	Single	*Definition* A persistent, non-reassigned, opaque identifier for a principal (user) that is also unique to the service being accessed (typically to a specific entityID). As an opaque identifier that is frequently generated "on the fly" during user login, the value is not easily human readable, or a value that users will know. See eduPerson schema definition. Note that the spec for this attribute has evolved some over time, and as a result, UC locations implement the attribute slightly differently. This can on occasion cause processing difficulties for SPs receiving and processing TargetedID values.	
eduPersonUniqueID	urn:oid:1.3.6.1.4.1.5923.1.1.1.13	eduPerson	Emerging				Intended as a more stable value to replace the need for ePPN. Should be opaque (e.g., not name based). See eduPerson schema definition.	
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	eduPerson	Not supported				Used to send information about what permissions a user should have within a source system. Only appropriate for cases where the IdP should directly control the user's access in a system. See eduPerson schema definition.	
eduPersonOrcid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16	eduPerson, orcid	Proposed				*Definition* ORCID iDs are persistent digital identifiers for individual researchers. Their primary purpose is to unambiguously and definitively link them with their scholarly work products (even as the researchers may change institutions). ORCID iDs are assigned, managed and maintained by the ORCID organization.	
subject-id	urn:oasis:names:tc:SAML:profiles:subject-id	oasis/saml, InCommon	Emerging				New ID added to the SAML standards definition. Largely the same as eduPersonUniqueID, but is also case insensitive (to avoid potential case colliding edge cases).	

pairwise-id	urn:oasis:names:tc:SAML:attribute:pairwise-id	oasis/saml, InCommon	Emerging				New ID added to the SAML standards definition. Intended to replace eduPersonTargetedID and similar constructs with a standard value.	
givenName (FirstName)	urn:oid:2.5.4.42	eduPerson, person (LDAP objectclass)	Current				Contains the "First Name" of the individual. As campuses implement support of the Gender Recognition and Lived Name policy (https://policy.ucop.edu/doc/2700693/GRLN), this will be expected to the user's Lived Name information.	
sn (LastName)	urn:oid:2.5.4.4	eduPerson, person (LDAP objectclass)	Current				Contains the "Last Name" of the individual. As campuses implement support of the Gender Recognition and Lived Name policy (https://policy.ucop.edu/doc/2700693/GRLN), this will be expected to the user's Lived Name information.	
cn (FullName)	urn:oid:2.5.4.3	eduPerson, person (LDAP objectclass)	Current				Contains the "Full Name" of the individual. As campuses implement support of the Gender Recognition and Lived Name policy (https://policy.ucop.edu/doc/2700693/GRLN), this will be expected to the user's Lived Name information. *Multi-valuedness?*	
displayName	urn:oid:2.16.840.1.113730.3.1.241	eduPerson, inetOrgPerson	Current				Contains the "Display Name" of the individual. Originally this was intended to allow the user to personalize the display of their full name. (Including nicknames, displaying or suppressing middle names, etc.) *Within UCTrust, it is largely synonymous with the cn value.* As campuses implement support of the Gender Recognition and Lived Name policy (https://policy.ucop.edu/doc/2700693/GRLN), this will be expected to the user's Lived Name information.	
mail	urn:oid:0.9.2342.19200300.100.1.3	eduPerson, X.500 LDAP Schema	Current				A user's email address as tracked in the UCTrust Location's SSO/IAM system. Note, this value is not necessarily assigned by the location; in many cases it is just a collected value. It is not guaranteed to be in any specific format or have any particular domain (e.g., it might not be xxxx@campus.edu). Be warned that this value is not generally a good choice for a userID, both because it is not stable - it may change or be reassigned to a different user over time - and because of the lack of controls around managing it - it is frequently self-reported by the user. Many SaaS services treat email address as a Unique ID, but be warned of the concerns above before using it in this manner.	
telephoneNumber	urn:oid:2.5.4.20	eduPerson, person (LDAP objectclass)	Proposed				Some UCTrust locations make phone numbers available as profile information through this attribute. However, what phone number this is (personal, office, reception, etc.) varies. Many users will not have a value available.	
title	urn:oid:2.5.4.12	inetOrgPerson	Proposed				Some UCTrust locations make a job title available via this attribute. What values are contained will vary, and do not necessarily match any specific "official" value (e.g., may not match any specific UCPath Job-related field). It may be self-reported. This is a text value that is generally only suitable for display purposes.	
manager	urn:oid:0.9.2342.19200300.100.1.10	inetOrgPerson	Proposed					
company	urn:oid:1.2.840.113556.1.2.146	inetOrgPerson	Proposed					
eduPersonOrgDN								
department	urn:oid:1.2.840.113556.1.2.141	inetOrgPerson	Proposed				Some UCTrust locations make a job title available via this attribute. What values are contained will vary, and do not necessarily match any specific "official" value (e.g., may not match any specific UCPath Job or Department related field). It may be self-reported. This is a text value that is generally only suitable for display purposes.	
eduPersonOrgUnitDN								

These attributes are formally described for LDAP servers as the ucEduPerson object class.

[1] For data element sizing purposes, the longest UC top level domain likely to be used as a "scope" value is "universityofcalifornia.edu" (26 characters, 27 counting the "@" sign).