User Identifiers for UCTrust

User Identifiers for UCTrust

(DRAFT - 7/25/2007)

Background

UCTrust supports a variety of identity attributes that can be used by applications as user identifiers, some of which are inherited from InCommon, and some of which are unique to UCTrust. The most notable of these are:

- **eduPersonPrincipleName** - A "scoped" identifier that consists of two parts, a local identifier within the originating institution and an identifier for the institution, for example, John.Smith@ucmerced.edu. eduPersonPrincipleName provides global uniqueness throughout InCommon, but different institutions will assert different values for a person who has affiliations with those multiple institutions, and it is not defined to be persistent over time; it can be reassigned to another person.
- **eduPersonTargetedID** - Also a "scoped" identifier, so it is globally unique throughout InCommon. It is also defined to be persistent over time, so it cannot be reassigned to another person. It enhances privacy, as the value of eduPersonTargetedID is different for different target services. Unfortunately, it is difficult for an application to determine a person's eduPersonTargedID before the person's first session with the application, so it is not usable for applications that require their users to be provisioned before the first session. There has been recent work (see http://staff.washington.edu/fox/notes/tgtid.shtml), though, that could make eduPersonTargetedID useful when provisioning is required by providing an IdP control over its values.
- **uCnetID** - uCnetID is a ten-digit number that is unique throughout UC, and all UC locations will assert the same value for people who have multiple affiliations within UC. It is defined to be persistent over time and cannot be reassigned to another person. In order to assure the same value across all of UC, a person's Social Security Number and date of birth are used to create a new uCnetID, so it is currently valid only for UC employees.

The selection of which of these identifiers should be used for a particular application is shown in the following table. Selection is dependent on the application's requirements for provisioning of users prior to the first session ("Provisioning Required?"), the application's tolerance of duplicate identifiers for the same person ("Duplicates allowed?"), and whether the identifier must be valid for a long time or forever ("Persistence required?").

Provisioning required?	Duplicates allowed?	Persistence required?	Strong match possible?	Recommended Identifier	Example Applications
Y	Y	Y	Y		Kuali, Travel?
Y	Y	Y			HRLMS non-employees
Y	Y		Y	ePPN	
Y	Y			ePPN	
Y		Y	Y	uCnetID	HRLMS employees
Y		Y		Not feasible	
Y			Y	uCnetID	
Y				Not feasible	
	Y	Y	Y	ePTID	
	Y	Y		ePTID	Library services
	Y		Y	ePTID	
	Y			ePTID	
		Y	Y	uCnetID	AYSO
		Y		Not feasible	
			Y	uCnetID	
				Not feasible	

The "Strong match possible?" column specifies whether it is possible to acquire SSN and date of birth from the target user community for the application (in order to assign a uCnetID).

Note that we have no recommended identifier for applications that require provisioning and persistence, and we are starting to see applications that require such identifiers. UC's new system-wide training management system is a good example of such an application.

Applications that Cannot Accomodate Long Identifiers

Other than uCnetID, all of the identifiers mentioned here can be very long. For example, if a UUID, which is typically written as 36 characters, were used for the campus part of the a scoped attribute, then the maximum length of the value of that attribute for UC Berkeley would be 49 characters (36 for the UID, plus 13 for "@berkeley.edu"). This is longer than the maximum length of a user ID for many applications, and eduPersonPrincipleName can be even longer.

Proposal

Implementation of the University of Washington's alternate implementation of eduPersonTargetedID (or waiting for it to become part of the standard Shibboleth distribution) should give us a fairly complete set of identifiers that can be used by applications within UCTrust, except for applications that cannot accomodate long identifiers.

It is strongly recommended that applications be designed or modified to accommodate identifiers of arbitrary length, at least 100 characters. A convenient work-around to accomplish this for an existing application is to add a front-end to the application's normal authentication that maps a UCTrust identifier to the application's native identifier.

Recognizing that migration to long identifiers will not be trivial for many applications, however, a new attribute, 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. uCTrustCampusIDShort will also have the following properties:

- 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 August 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.