High-level Overview of UCTrust Entity Services

Note: Further work on this topic was done and a more complete technical proposal put together by the UCTrust SP Integration Workgroup.

DRAFT

~~Attachment (Added 4/20/2015): Federated Authentication Data Release Approval Processes v0.3.docx, this same proposal cast as a document for non-technical audiences.~~

New attachment version (added 5/10/2016): Federated Authentication Data Release Approval Processes v0.9.docx, an updated version of this proposal intended for ITLC review.

Table of Contents

Introduction

This document provides a high-level overview of the tentatively named UCTrust Entity Services ("Entity Services"). The role of Entity Services is to manage entity details in the federation. As of this time, the "entity details" to manage are entity attributes added to IdP's and SP's in InCommon metadata. By adding entity attributes to InCommon metadata, UCTrust gains securely managed and distributed metadata that reliably identifies UCTrust member entities. The hoped-for first benefit UCTrust obtains through the addition of identifying entity attributes are pre-defined attribute release bundles - that is, bundles of attributes that IdP's are pre-configured to release to identified SP's. (More on entity attributes.)

Entity Services (and Process)

UCTrust has typically been a group of identity managers from the member institutions. And while we commiserated on identity management issues, we did not typically provide any centralized services for the membership. However, the processes required to vet and manage entity attributes necessitates the creation of an operational group within UCTrust - the creation of a service. There may be more than one service as time goes on, but this initial service is the management of entity details.

At this stage, after discussions with InCommon, InCommon has agreed in principle to implement a mechanism whereby UCTrust, as an organization, can manage the availability of UCTrust-controlled entity attributes to UCTrust entities. We haven't yet discussed technical implementation details. The general process would be for UCTrust to propose the addition of an attribute to an entity belonging to a site (i.e., one of the UCTrust members.) The InCommon Site Admin for that UCTrust member would then log in to the InCommon Site Admin tool and approve the addition of the attribute to the entity. Presumably, UCTrust will be able to request that an attribute be removed without the approval step; that aspect of the process has not yet been discussed.

Eric Goodman has mocked up the flow in the attached document, "UCTrust SP Approval.pdf". Page 2 covers this process:

1. An aspiring UCTrust SP identifies the bundle of attributes it would like to obtain.
2. The SP owner documents how it meets the usage criteria of the bundle.
3. The SP owner's UCTrust campus rep reviews the proposal, and when satisfied, submits it to the UCTrust governance committee.
4. If approved, UCTrust submits the request for the attribute to be added to the entity and notifies the UCTrust rep (who, if a different person, will have to contact the local InCommon Site Admin) to approve the attribute. *NOTE: the actual technical mechanism used to convey "UCTrust approval" may differ from this depending on whether this specific functionality will be supported by InCommon.*

This is still an early stage in developing this process, so we don't yet have details to propose regarding all of the above steps and what they mean. We're hoping to suss some of those things out through discussion.

(The above is an SP-centric view. We will probably also want to added attributes to IdP's that have committed to support specific categories. This will make filtering of discovery service listings much easier.)

Entity Categories

The entity attributes themselves are name-value pairs. SP's have an attribute named "http://macedir.org/entity-category", while IdP's have an attribute named "http://macedir.org/entity-category-support". We have currently proposed using "http://uctrust.universityofcalifornia.edu/category/<category>" as the values. (Whether to use universityofcalifornia.edu, which is what we have used for existing UCTrust attribute naming, or ucop.edu, was discussed, with no real technical barriers to either solution.)

At this stage, we need to understand what these categories should be. What is the best way to categorize SP's in UCTrust to most effectively map attribute bundles to them? Some ideas:

- faculty-staff-basic
  - mail
  - displayName
  - ePPN/ePTID
  - givenName
  - sn
- faculty-staff-enhanced
  - +UCNetID
  - +<some other identifier going around>
  - +<some critical UCPath attribute>
- student-basic
  - mail
  - displayName
  - givenName
  - sn
  - ePPN
- student-enhanced
  - ?
- student-enrollment
  - ?
- student-academic
  - ?
- all-basic
  - Same as other basics, but for all

Maybe this is too many? Too few? Some of these seem likely to be easier than others.

Requirements from the Campuses

Prior to any implementation, the UCTrust governance process will require high-level approval. But then, it will likely come down to the individual campuses working with their data stewards to approve delegation to UCTrust to make determinations about applications. No doubt this will be easier for some bundles than for others.

After implementation, it is up to the campuses to keep the state of their entities up-to-date.

Ongoing Central Resources

UCTrust will need to provide some central, operational resources.

- Governance committee, to review proposals as they come in
- Review processes, to check in on existing entities and whether they still meet the assertions
- Whatever the resource is for submitting attributes proposals to InCommon

UCTrust SP Approval.pdf