Overview

The Life Cycles and Affiliations Group (LCAG) was tasked with identifying affiliations the affiliations currently being used at the University and any that could be envisioned. We also discussed the life cycle of affiliations.

Our process included reviewing the affiliations used by various Penn State\(^1\) systems as well as those used at other Universities\(^2\) and Internet2\(^3\). The list we developed was based on those considerations as well as the internal discussions of the group.

This product should not be viewed as either definitive or prescriptive by those who begin implementing IAM 2.0. The product should be used as a way to illustrate the concepts we developed and, perhaps, as a starting point for design discussions which should be discarded if deliberations suggest.

For our purposes, an affiliation identifies where an individual “.touches” the University -- affiliations provide context for electronic interactions with the University (that is, an individual is accessing electronic services provided by our University that require authentication however basic). An individual must have an electronic identity that is trusted by the University for an affiliation to be assigned.

We use the term “individual” inclusively; it includes software applications that require a “user account” to access electronic resources; for example, a web application that connects to a backend database without passing the credentials of the human user accessing the web application.

Electronic identities need not be issued by Penn State; however, use of non-PSU issued identities would require an approval or vetting process that is not discussed in this paper.

Our considerations of life cycle (that is the assignment, maintenance, deactivation and reactivation of affiliations) involved two distinct but related efforts. We sought to identify the current life cycle while also developing practices that ought to enhance the overall process.

The balance of this paper is divided into two sections. The first addresses affiliations \textit{per se} and the second the life cycle of affiliations.

Affiliations

1. Current state.
   a. Application of our working definition of affiliation to the current Penn State environment demonstrates that we have been using the concept of affiliation for many years. Unfortunately, we have not managed the assignment and use of affiliations so we have several, non-integrated, sources for affiliations throughout the University. These include CIDR, CACTUS and other systems.

---

\(^1\) Including CIDR, CACTUS, Auxiliary and Business Services “non-standard” affiliations.
\(^2\) Virginia Tech and Stanford University.
\(^3\) Internet2 EduPerson Specification (200312).
b. The creation of affiliations has been, in many cases, *ad hoc*. This has resulted in blending of identity and affiliation\(^4\); blending of affiliation and role\(^5\); blending of affiliation and unit\(^6\); blending of affiliation and access control parameters\(^7\); and the proliferation of available affiliations where some have very few or no members assigned.

2. Proposal for affiliation management.
      i. There should be as few affiliates as possible.
      ii. Affiliates serve as a first-layer for access control decision making. When considering whether or not to create a new affiliate category the essential question is: “Does this contemplated affiliation embody substantially different access than existing affiliations.” If it does not, then a new affiliation should not be created. There may be political considerations that override this rule of thumb.
      iii. Affiliations should be based on types of relationships with the University; they should not be defined by the specific University organizational element involved. The organizational element should be defined in a given affiliation’s attributes.
      iv. The provisioning of affiliates needs to balance flexibility (so users don’t resort to local creation application specific affiliations) with identity assurance and security. If the system implemented is not sufficient flexible or responsive units will, in order to get their work done, develop local systems that will probably be isolated and insufficiently secure.
      v. A process for the creation of new affiliation types needs to be established.
         1. Authority to create new affiliation types should be tightly controlled.
         2. Individuals who create new affiliation types should have the ability to assign allowable roles.
         3. Individuals who create new affiliation types should have the ability to assign allowable attributes. The creation of new attribute types and allowable values probably would not be the responsibility of this/these individual(s).
   b. Operating concepts. It is possible that affiliation management could work just like role management. In a sense affiliations are root roles, where:
      i. An individual can have multiple affiliations.
      ii. Affiliations may have attributes based on defined vocabularies.
      iii. Roles may be assigned to individuals based on and associated with the affiliation(s) they are assigned. That is, affiliation type constrains the roles which may be assigned to the individual.
      iv. Assignment of affiliations (and attributes) will be audited.
      v. Affiliations are not deleted but deactivated. Affiliations may be reactivated.
      vi. Whenever practicable, the assignment of affiliations should be associated with existing processes and should occur automatically when the parent transaction

---

\(^4\) For example, ACCESS ACCOUNT FOR <first name> <last name> (<company name>)
\(^5\) For example, DEVELOPMENT AND ALUMNI RELATIONS
\(^6\) For example, ADJUNCT FACULTY IN THE FRENCH DEPARTMENT
\(^7\) For example, <name> JUNE 13 THROUGH JULY 3 2004
is finalized. For instance, when a person is hired as a new employee, the affiliation of “staff” should be automatically assigned along with the attribute of home administrative unit and any others which are known.

c. LCAG developed a list of potential affiliations with example attributes (see attachment 1). This is provided to illustrate LCAG’s thinking and is by no means meant to be prescriptive. For instance, the several types of faculty (unmodified, applicant, or visiting) or staff (unmodified, applicant, furloughed, visiting) might be consolidated into single faculty or staff affiliations with attributes used to differentiate access.

d. During LCAG’s discussions we posited several affiliations that were later rejected. Most of these and the reasons for removal were recorded (see attachment 2).

Lifecycle

1. Current state.
   a. For the most part, the life cycle processes currently employed center around the issuance of identities and affiliations. The process, or rather processes, is uncoordinated, require the person receiving credentials to repeatedly interact with different Penn State units, and can take too long.
   b. The “Simple New Employee Process Flow (attachment 3) describes the process flow used to issue credentials to a new Penn State employee.
      i. These processes can take up to six weeks and prevent the conduct of business.
   c. The processes are organized along organizational lines and do not take into account the perspective/needs of users. These stovepipes developed over time and reflect the structures and processes that developed before computerization.
   d. Because the process can take so long workarounds have been developed. This results in “out of band” issuance of affiliations and affiliations that are not coordinated.
   e. There is limited auditing.
   f. Special cases, which are not uncommon, (such as parents of chronically ill children requiring periodic access) are handled by exception.

2. Proposal for life cycle management.
      i. Departmental boundaries should be bridged. Departmental responsibilities need not be merged but they need to be made transparent from the user’s perspective, the user being the person who is being credentialed.
      ii. Coordinating processes. For instance, a Penn State Access Account ID (or its future equivalent) could be issued at the time the Penn State ID is issued.
      iii. Provisioning of affiliations and attributes should be done automatically when ever practicable.
      iv. Management of affiliations (including inactivation and reactivation) may be distributed to authorized units/users.
   b. Operating concepts.
      i. The assignment of affiliations to users have two states:
         1. Active
2. Inactive
   ii. Once inactivated, an affiliation can be reactivated.
   iii. Auditing. Penn State Access Account IDs, assignment of affiliations with attributes (and roles) should be managed centrally. This includes auditing of affiliations and attributes, among others:
       1. Date-time of assignment; relevant data; user making the change.
       2. Date-time of deactivation; relevant data; user making the change.
       3. Date-time of reactivation; relevant data; user making the change.
       4. Date-time of any change; relevant data; user making the change.
   iv. Data Retention. Data retention, archiving and deletion schedules and policies should be developed and implemented.

3. Notional Life Cycles. For some user types there may be a natural progression from affiliation type to affiliation type where the former may be deactivated as the latter is assigned. See “Typical Transitions in Student-University Affiliations” (attachment 4).