Ad-hoc Lists

Problem

Access rules for many applications and services cannot be derived from an authoritative source and must therefore be managed in a more ad hoc fashion. This pattern is characterized by the fact that access is manually managed by individuals or self sign-up, not identified registrars. In some cases, authoritative data exists, but is difficult to feed in to the IdM system. In other cases, membership in an access group is entirely left up to individual users or departments to maintain.

Solution

Ad-hoc, static group lists can be used when there is no good way to dynamically manage membership. Managing the group in a central IdM system allows the group membership to be used for multiple provisioning and access management decisions that would otherwise have to be managed in each application. (Similar to white lists.)

There may be optional content or services that are offered by the institution that require attributes or group membership in order to participate or not. In addition, there may be information about oneself (person attributes within a directory service) that the user may elect to have public or private. In these cases, it is desired that the users manage and control this access and content, since the items described are optional or user preference.

Examples

- At the University of Michigan, access to many systems is dependent upon the successful completion of application-specific training courses or certifications. Course or certification completions are tracked in a variety of isolated side systems that are not easily fed to the IdM system. Static group lists can be created in the IdM system and the individual group membership is either manually managed or periodically synchronized with the appropriate training system according to the requirements of each application.
- The institution maintains a photo directory as part of the main campus email/phone directory. Some users may wish to not have their photos displayed in the public directory. This is an example of an opt-out service where the individual user is maintaining their own membership in a group.
- The campus maintains a portal which can generate a variety of content blocks based on role. While some content may be openly available, it is only pushed out to the individual's portal page if the individual chooses to subscribe to it. Again, the individual user is maintaining their own membership in a group in order to subscribe or unsubscribe from this optional content. This is an example of opt-in.
- Lafayette College has a home grown web application that is currently used to view LDAP information, reset passwords, and perform other basic functions. We are considering adding a module for this to enable basic opt-in and opt-out features as well.

Graphics (click on them to view full size)