Return to Advance CAMP wiki

Advance CAMP Wednesday, Sept. 28, 2016

10:20am-11:10am

Tuttle Room

# accounts for individuals w multiple roles

CONVENER: Kerry Havens - University of Colorado Boulder

MAIN SCRIBE: Pregash Devasagayam

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 17
Craig Baker - Clemson
Pregash Devasagayam - University of Colorado Boulder

## DISCUSSION:

Comment from Chris Bongaarts (stuck in another session): Our security folks have recently proposed this as a mechanism to work around data classification issues (if we give people separate accounts for “staff” and “student” roles, they might be more likely to store their stuff in appropriate places for their role, so we can preserve access or revoke access when they transition out of the role more easily). My personal opinion is that users will end up putting all their stuff in one account because they are lazy (or more charitably, too busy to be switching accounts all the time).

Clemson - made transition a few years ago with a concept of a primary ID with multiple ac

- If you are an employee, you are an employee first (except for student employees)
- 2 email systems tied to a top level email handle (@clemson.edu can go to g.clemson.edu, exchange.clemson.edu or both)

- Only employees have access to provision an exchange inbox, anyone can have g.clemson.edu

Michigan - one id for student and faculty
- Student use mail forwarding to personal mailbox
- Multiple IDs for the hospital
    - Level 1 and level 2 accounts
    - On different mail server (whereas rest of the campus on google.)

University of Missouri - 1 identity tied to emplid
- Student email in o365 and employee in on-premise exchange
- Can have two mail boxes but only one primary address
- Idea: different tenants (domain names)
    - Clemson does a top level

University of Utah - 3 major roles, employees (including student employees), affiliates, students
- Single unique id account, which then can propagate to various accounts or access logic based on risk level.

Multiple accounts, same password. Helps with data segregation issues.

Login with employee/faculty account, belongs to department - student account belongs to student

In Utah, what you start with is your primary mail service, so student start with google, that will be their primary account
- How do you handle mixed roles and separation from that employee role.
- For the scenario where an employee leaves employment but remains a student, the employee mailbox is decoupled from the user and attached to the department.

Move to an access driven policy implementation, taking value away from the account in and of itself.

Broad problem with affiliations that are much more extensive then just employee/student/faculty

Wisconsin allows for ad hoc account creation to for
- Multiple accounts fall apart in a more expanded scheme
- Demographic based linking

One account with multiple business roles with effective dates on the roles
- Keeps a hierarchy on employee-faculty-student
- Complete transparency that on the effective dates the account is subjected to the policies governing the highest role.

How do you handle the public directory?
- Let end user control.

- Problem with multiple accounts is that they show up twice in GAL or google directory
- Request based process to enter in

ACTIVITIES GOING FORWARD / NEXT STEPS: