IAM

Problems with managing identities and access of University “Guests”

Agenda

- IAM Background / Goals / Status
- Problem with managing “guests” accounts
- Possible solutions

IAM Project Success Factors

- Establishing one University credential
- Requiring single sign-on for all campus and UA technologies
- Providing the self-service functionality
- Protecting the privacy of University community members
- Understanding and managing risk to the University data environment
- Establishing stronger and longer relationships with University community members
  - Retaining one's identity for life
- Providing a central authentication system

IAM Project Components

- SiteMinder Authentication
  - Deployed at UIUC (replaced Bluestem)
- Single ID & Password
  - Phased deployment over next year
- In Planning

    Identity Provisioning and Administration

  - Federation / InCommon Silver
  - Access auditing , compliance control, reporting

Problem

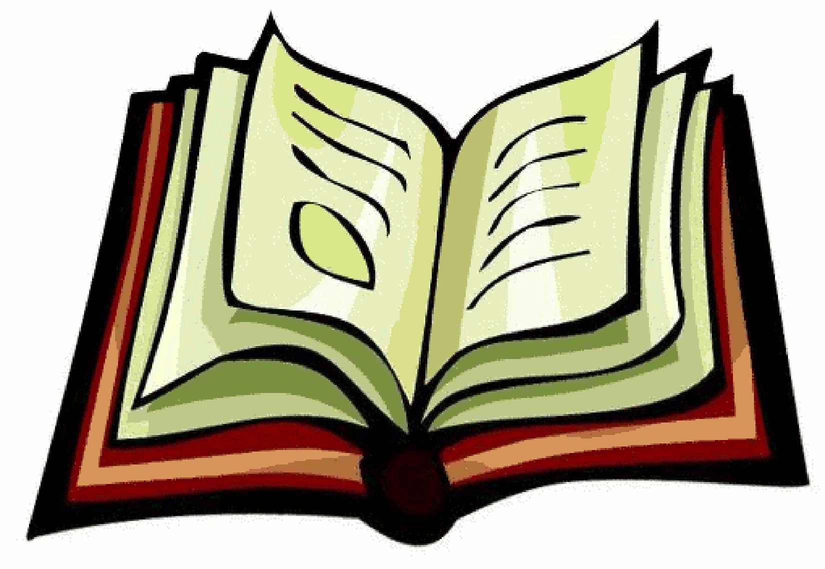
- There are 1000's of NetIDs at UIUC that are created yearly using non-standard methods
  - Additional IT work
  - Delayed Access
    - Tarnished Reputation
  - Potential Security Concerns
  - University Policy Violations

Interviewed IT Pros at UIUC

- Pain points for managing guests
- What services / access do the guests need?
- What would the ideal “to – be” process?

- ACES (Agriculture)
- ATLAS
- Beckman
- CITL (OCE)
- DIA
- Education
- Engineering
- FAA
- F & S
- GS-LIS
- Illini Union
- Law
- Staff Human Resources
- Swanlund

Guest Faculty “As-Is” User Story



As-is Guest Faculty – User Story

Joe is a professor at the University of Illinois and is attending a conference and meets Xiao from the University of Beijing. It turns out they are working on very similar research projects. Joe Invites Xiao to Champaign for a couple week visit where they can work on their research together. Joe needs to provide digital access to Xiao to the data and systems that contain his research. Here are the current steps that is followed:

As-IS guest faculty cont. (2)

- Xiao arrives on campus, and Joe realized that Xiao needs digital access to University systems to proceed with the research.
- Joe contacts his department IT representative Bob and informs him that Xiao is here and needs access to the research data (time passes)
- IT Bob creates a netID for Xiao in the department’s OU of the campus Active Directory (AD)
- IT Bob sets a password for Xiao and tells Joe the password (time passes)
- IT Bob adds Xiao’s netID to Box which provides access to Joe’s research
- Joe gives Xiao his netID and password (time passes)

As –IS Guest Faculty (3) cont.

- Xiao needs access to Wifi so that he can get onto the network
- Joe sends Xiao to IT Bob, and Bob refers Xiao to the Cites Guest wi-fi page and tells Xiao that Joe has to fill this out for him
- Xiao goes back to Joe
- Joe signs up Xiao for 30 day guest wi-fi access
- Joe and Xiao start working on the research

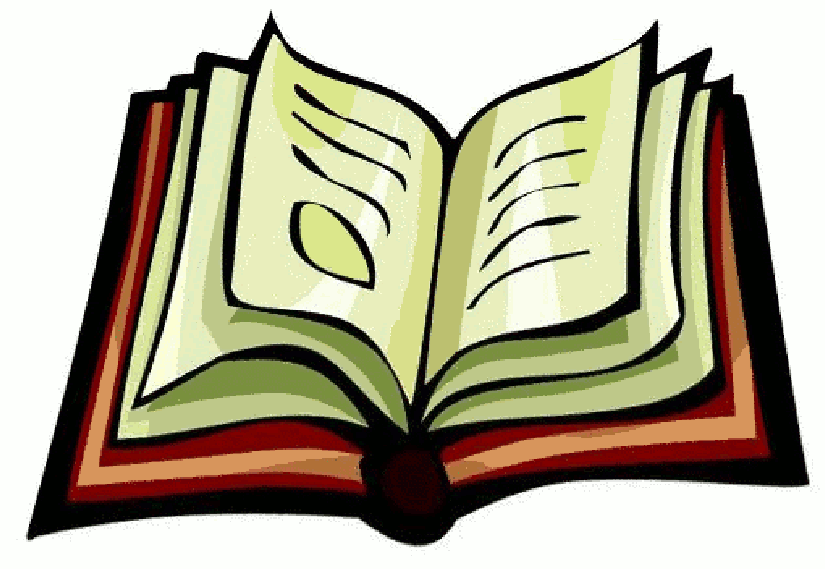
As-IS guest faculty cont. (4)

- The next day, Xiao comes into work and tries to log in, but realizes that he has forgotten his password. Xiao tells Joe.
- Joe calls IT Bob.   Bob goes into the Active Directory and resets Xiao's password and then writes the new password on a yellow post-it and gives it to Joe.
- Joe gives the new password to Xaio and says, "don't forget it this time".
- Xaio puts the post-it on the computer screen so that he won't lose it.

As-IS guest faculty cont. (5)

- The joint research effort has been completed, and Xiao goes back to Beijing
- Unfortunately, Joe forgets to tell IT Bob that Xiao has left, and therefore access for Xiao doesn’t get terminated.

On-Line Class “As-Is” User Story



As – IS On line class

Mike’s dairy certification is going to expire in 2 days and he needs to take the on-line class “How to milk a cow” provided by Vet-Med to complete his recertification

- Mike creates a local ID for himself via the VetMed online registration system, enrolls in the course and pays via credit card
- IT Jim creates NetID in Vet-Med OU for Mike (time passes)
- IT Jim tells CITES to add Mike’s netID to Compass (time passes)
- IT Jim “enrolls” Mike in class in Compass (time passes)
- Someone in Vet Med sends email to Mike his netID, password, and web link to start course.

As-is Online Class cont.

- Mike receives his account information 4 days after enrolling and therefore, his certification has expired☹
- Mike takes the “how to milk a cow” class anyway and completes it in 1 day.
- Unfortunately, no one tells IT Jim that Mike has finished the course so no action is taken on Mike’s account.

Problem Summary

Summary of “Guest” types that need NetIDs

- On-line Class
- Volunteers
- On-site Class or Seminar
- Guest Faculty / Grad Student
- Graduated Grad student extended access
  - Temporary access to finish research
  - “permanent” access to services
- Faculty
  - Access Prior to their start date
  - Access after leaving university
- Extra help
- Vendors

Basic services needed

- WiFi
- Blackboard / Compass
- Box
- Email
- Lync
- Facility Access
- Access to individual department resources

How are these NetIDs created now?

- NetIDs created in department OUs in campus directories
- Departments manage their own ADs/LDAPs
  - manual, slow, claiming, resetting passwords, non-reuse of IDs, access termination
- 0% Appointment
  - Triggers other processes not needed
- Request UIN to get NetID
  - Long Paper form, takes days
- Guest WiFi
  - not persistent
- Accounts are created on local servers

To – Be Future State

The solution……..

- Easy to use, self service, immediate way to create “guest” netIDs and provision access to commonly used services
  - User’s Name, User’s Email
  - Duration access is needed
  - Checklist of resources needed by user
    - ❑Box
    - ❑Blackboard
    - ❑Exchange
    - ❑Lync
    - ❑WiFi

Levels of “Assurance” vs. affiliation

- Self Register, online class – No Vetting
- Sponsored Guest, visiting faculty – Trust the sponsor
- Student – Vet via application process
- Employee / Faculty – Show ID
- Med Center
- Vendor

- Apply different security policies
  - Different password strength & expiration rules
  - Multi factor authentication

Different ways to initiate guest netID creation

- Sponsor completes Guest request form
- User Self Registration
- Batch / .xls
- Programmatic Interface (API)
- Approval(s) where needed

Identity for life

- For each type of guest, determine if identity should be kept forever
  - Maybe use OpenID (or google IDs and passwords) for lower assurance IDs.
  - Use IDs from guest’s home institution (Federation)
- User keeps netID
  - Can be reused across different guest types
  - Guests (e.g. early faculty) can migrate to “real” faculty
  - Student / employee can use their NetIDs to access certain guest services (e.g. continuing education courses)
- Access to systems “auto terminated” when
  - Reaches expiration date
  - Trigger (e.g. course completion)

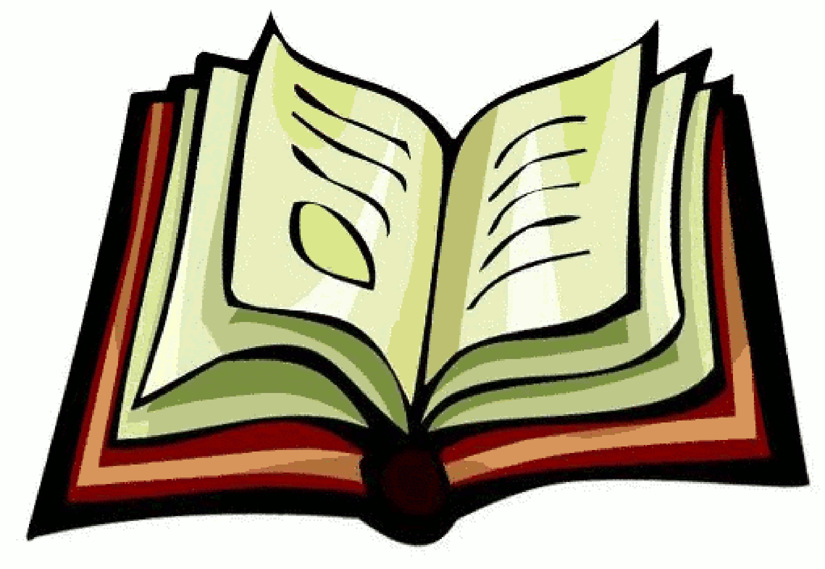
ID Claiming / Password Setting

- NetID is created
- Email sent to user with NetID and tokenized Link
- User clicks on link and sends user to page to
  - Set password
  - Set password reset options (email, SMS)

Possible Future Users of this

- AG Extensions
- Student Applicants
- Student Camps
- Housing

Guest Faculty To-Be User Story



To – Be Guest Faculty

- Joe goes to the University’s “add sponsored user” website and creates guest netID for Xiao.
  - Joe enters Xiao’s name and email address
  - Joe clicks on the check-boxes for those services Xiao will need: e.g. WiFi and Box,
  - Joe enters the two weeks as the amount of time that Xiao should have access
  - Joe hits “Submit”
- Because Joe has permission to create sponsored users accounts, a netID created for Xiao immediately

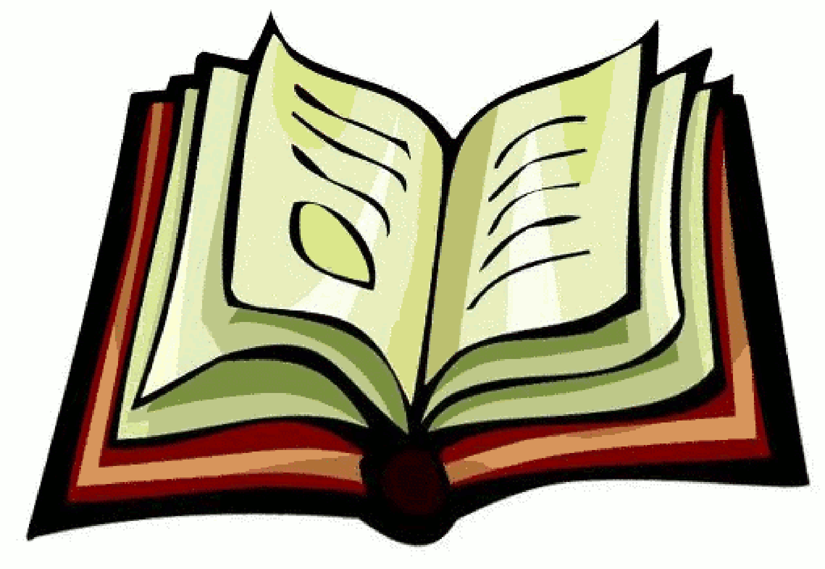
To-Be Faculty Cont. (2)

- An automated email is sent to Xiao’s email address which contains his netID and a tokenized link which will send Xiao to the University’s Password Registration page.
- Xiao is directed to create a password per the University’s password guidelines
- Xiao sets his password reset options (SMS and email)
- Xiao can now productively and securely work with Joe on their research

To-Be Faculty (3) cont.

- Two weeks has passed, the joint research has been completed and Xiao goes back to Beijing
- The IAM system ‘auto – terminates’ access for Xiao in Box and WiFi, and lock’s Xiao’s AD account

On-line Class To-Be User Story



To Be On-line Class

Mike’s dairy certification is going to expire in 2 days and he needs to take the on-line class “How to milk a cow” provided by Vet-Med to complete his recertification

- Mike enters his name and email address to the VetMed online registration system, enrolls in the course and pays via credit card
- Because Mike was a former U of I student, he already had a netID so none was created.
- Mike gets an email informing him of his old netID with a tokenized link to reset his password.
- Mike’s account is auto added to Compass (blackboard) giving him access

To Be On-line Class

- Mike is “enrolled” in the class in blackboard
- Mike may begin taking the course minutes after he enrolled.
- Mike logs into blackboard using his netID & password and completes the course in 1 day and is able to renew his certification.
- A notification is sent to the IAM system that Mike completed the course and his account and access to blackboard get locked.

Next Steps

Next Steps

- Continue to gather needs from more departments, UIC, UIS, Med Center, etc.
- Develop As-IS and To-Be user stories & functional requirements for each type of “guest”
- Work with tech team to architect the solution
- Continue to review requirements with
  - with departments to see if meets needs
  - Review with stakeholders
- Build it!!