External Identities in Higher Ed:
Why and How with Real World Examples

IAM Online
May 13, 2015 - 2 pm EDT

Eric Goodman, UCOP and Chair of InCommon External IDs Workgroup
Erica Lomax and Andy Morgan, Oregon State University
Todd Haddaway, University of Maryland, Baltimore County (UMBC)
Dedra Chamberlin, Cirrus Identity
When should campuses get out of the account management business?

- And just manage access, and maybe 2\textsuperscript{nd} factor when needed?
- Why do we duplicate effort and provide duplicate service – doesn’t everyone have an account in their “real” lives that campuses can just use?
  - Campus SPs mostly did already
  - External SPs are going that way (federation)
- The presenters bring some deep thinking about this
  - Some examples where it makes sense and is easy
  - Some idea of where the dragons are
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Trajectory of Conversation

Social Identities Workgroup (~2011-2013)
- Business Drivers for integrating social identities
- Common Use Cases

External Identities Workgroup (Aug 2014 – Present)
- Implementation Concerns
  - Risks
  - Pros and Cons of different external providers
  - Relationship to internal Net IDs
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
“Arms Length” Customers

- Parents
- Alumni/Donors
- Research Collaborators
- Continuing Ed Students
- Guest Faculty
- Prospective Students
Your IDMS…

- HR
- SIS
- MedCntr

- Registry
- Credentials
- LDAP
- AD
Where Do “Guests” Go?

SOR? →

- HR
  - Guests
- SIS
  - Guests
- MedCntr
  - Guests

Registry

- Credentials
- LDAP
- AD
Where Do “Guests” Go?

Registry? → Guests → Registry

- HR
- SIS
- MedCntr
- Credentials
- LDAP
- AD

Guests
Guests
Guests
Where Do “Guests” Go?

- HR
- SIS
- MedCntr

- Registry?
  - Invitation and Registration
  - Guests
  - Registry

- Credentials
  - Guests
- LDAP
  - Guests
- AD
  - Guests
Where Do “Guests” Go?

- Invitation and Registration
  - Guests
  - AD LDAP Creds
- Registry
  - Credentials
- HR
- SIS
- MedCntr
- LDAP
- AD
Accessing a University Service

Hypothetical University

Welcome to the Alumni Services Portal

Login with your University Account:

Username
Password

Don’t have a university account?
Click here for Guest Accounts
Accessing a University Service

Hypothetical University

Guest Account Access

Already have a guest account? Login here:

Username
Password

Don’t have a guest account? Register here
Forgot your password: Reset password
Accessing a University Service

Hypothetical University

Guest Account Registration

Fill in the fields below to register for a guest account:

- **First Name**
- **Last Name**
- **Email**
- **Password**

[Submit]
Accessing a University Service

Hypothetical University

Guest Account Registration Successful! You will receive an email to activate your account. Once you complete that step, you can log in with your guest account.
Email Verification
Accessing a University Service

Hypothetical University

Guest Account Access

Already have a guest account? Login here:

Username
Password

Don’t have a guest account? Register here
Forgot your password: Reset password
Accessing a University Service

Hypothetical University

Welcome to the Alumni Services Portal

Thanks for being a part of the vibrant University of Fabulous Alumni community! Click the links below to access information, participate in one of our programs, or make a donation!

Calendar of Events

Alumni Mentorship Program

Donate!

Your gift makes all the difference!
One Year Later…
Accessing a University Service

Hypothetical University

Guest Account Access

Already have a guest account? Login here:
Username: [input field]
Password: [input field]

Don’t have a guest account? Register here
Forgot your password: Reset password
Accessing a University Service

Hypothetical University

Guest Account Access

Username and/or password incorrect. Try again or click below to reset your password.

Already have a guest account? Login here:

Username: [Input]
Password: [Input]

Don’t have a guest account? Register here
Forgot your password: Reset password
"Length of Arm"

- Helpdesk Request/Password Reset Frequency
- User Annoyance Factor
- Login Frequency
Accessing a University Service

Hypothetical University

Welcome to the Alumni Services Portal

Login with your University Account:

Username
Password

Don't have (or remember) your University Account info?
Login with:

Google
Facebook
Welcome to the Alumni Services Portal

Thanks for being a part of the vibrant University of Fabulous Alumni community! Click the links below to access information, participate in one of our programs, or make a donation!

Calendar of Events
Alumni Mentorship Program
Donate!

Your gift makes all the difference!
Social Identities
Workgroup – Why?

External Identities
Workgroup – How?
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Categorizing Use Cases

- How broadly will we leverage external identities?
- For short term/guest access, or longer term use cases?
- Is it okay to use external identities to control access to my resource(s)?
External Identity per app vs. at Institution

- Support access to a specific application
  - Every application integrates separately
  - Maintains distinction of services

- Supporting an “institutionally” understood external identity
  - Institutionally trusted external attributes
    - May not be all attributes
  - User Experience with the institution is “as” the external identity
Length and Depth of Association

- Short term, guest-like access
  - More transient access support can simplify implementation
    - Parents
    - Project Support
    - Conference Guests

- Longer term associations
  - Mapping to “real” internal identities adds complexity
    - Alumni
    - Separated Employees
    - Student Prospects
    - External Employees (for VOs)
Risk of Access

- The $64K question!
- The most difficult element to generalize. Varies by:
  - Application needs
  - Access sensitivity
  - External Provider operational practices
  - Expressiveness of protocols
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Technical Approaches

- Implement at application, via “Gateway”, or “seamlessly”
  - Direct Integration Support
    - Protocol translation
    - Attribute mapping
  - Provide Common Institutional View
    - Shared “SP” (Proxy) between institutional apps and external ids
    - Institutional “Identity Linking”
  - Supporting services
    - Externalized Authorization services
    - Invitation services
Evaluating Providers

● Ideally all identities would come with risk measures
  ● Silver/Bronze, NIST LoA, Vectors of Trust, MFA indicators, etc.
  ● Not realistic in today’s environment

● What can app owners/institutions use as Criteria today?
  ● Working Group report provides a list of suggested criteria
For More Information

- External Identities Working Group Draft Report

- External Identities Working Group Wiki Space
  - https://spaces.internet2.edu/display/EXTID
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Parent Access at UMBC

Todd Haddaway
haddaway@umbc.edu
Before…

Dinner table conversations

Report cards sent to parents

High School Graduation
After…

Call your mother, please!
Are you there??

College Life

What classes are you taking?
Grades??
Social Identities at UMBC

- Students use an invitation system to grant or revoke access
- Using Google and Facebook credentials
- Access to information becomes an issue between the student and their parent
- Eliminates a paper system of “permission to view”
Social Identities at UMBC

Parent access walk through
myUMBC Account
UMBC Students, Faculty, and Staff
Username/Email:
hadda1
Password:
**********
Log In  Forgot Your Password?

Guest Access
Special guests that have been granted access

Log In with Facebook
Log In with Google

Important: Usage of UMBC computing resources is governed by the UMBC Policy for Responsible Computing (PDF) and this notice.
**Spotlights** for Monday, April 27, 2015

Pre-Aging?
Hear from Pre-health Professionals about working with Elders

News
Articles that have been sawed most in the past 24 hours

Group Events
Upcoming events in your groups

Transfer Students Teleport to Campus
How to materialize at UMBC and trek forward at warp speed!
Profile Sharing

It's easy to share parts of your profile with others.

1. Click **Share Profile** and specify the person's email and the parts of your profile you want to share.
2. They receive an invitation in their inbox.
3. They click the link in the email and log in with a **myUMBC**, **Google**, or **Facebook** account.
4. They can access your profile through a **People** menu.

**Note:** This information is private, so only share with people that you know and trust.
Share Profile

Type the email address of the person you want to invite to share your profile with.

IMPORTANT: To accept the invite, they must have a UMBC, Google, or Facebook account.

Email: 

Allow access to the following parts of my profile: (you can change this later)

☐ Profile Summary
Some basic info, including UMBC-specific IDs and billing address.

☐ Course Schedule
Currently enrolled courses, as well as courses registered for in the future.

☐ Grade History
A complete history of grades received in all past courses.

Grant Access
Profile Sharing

It's easy to share parts of your profile with others.

1. Click Share Profile and specify the person's email and the parts of your profile you want to share.
2. They receive an invitation in their inbox.
3. They click the link in the email and log in with a myUMBC, Google, or Facebook account.
4. They can access your profile through a People menu.

Note: This information is private, so only share with people that you know and trust.

Share Profile

Pending Invitations

The following people haven't accepted the invite to see your profile:

• todd.haddaway@gmail.com
  View Profile Summary, View Current Classes, View Grade History

Cancel Invitation
Rebecca Haddaway has shared their myUMBC profile with you.

The following info has been shared:

- **Profile Summary**
  Some basic info, including UMBC-specific IDs and billing address.

- **Course Schedule**
  Currently enrolled courses, as well as courses registered for in the future.

- **Grade History**
  A complete history of grades received in all past courses.

To accept this invitation, click the **Accept Invitation** button below and log in with a myUMBC, Google, or Facebook account.

Please Note: You will have access to a student's private, academic information, so please do not share it with others.

---

**Accept Invitation**

**Note:** This info is shared by the individual themselves and they may change or revoke access at any time.

If you experience any problems, please contact our Technical Support Center.
myUMBC Account
UMBC Students, Faculty, and Staff

Username/Email:

Password:

Log In

Forgot Your Password?

Guest Access
Special guests that have been granted access

Log In with Facebook

Log In with Google

These services are only used to log in. No personal info is shared with third parties. Learn more

Important: Usage of UMBC computing resources is governed by the UMBC Policy for Responsible Computing (PDF) and this notice.
Profile Sharing

Profile access granted!

Access granted to Rebecca Haddaway for the following information:
- View Profile Summary
- View Current Classes
- View Grade History

You can see this information under the People menu. View Now
Rebecca Haddaway

Profile Summary

- **campus id**: IH17090
- **username**: hadda1
- **email**: hadda1@umbc.edu
- **billing address**: 10542 Dorchester Way, Woodstock, MD 211631383

Class Schedule

**Fall 2015**

**ENGL 302: Literary Methodologies and Research (Enrolled)**

An introduction to contemporary literary theories and methodologies for English majors in the Literature Track. Students will acquire an understanding of the basic theoretical concepts underlying contemporary approaches to literature. This course will build upon the skills acquired in ENGL 301, and familiarize students with the process of conducting literary research.
Profile Sharing

It's easy to share parts of your profile with others.

1. Click Share Profile and specify the person's email and the parts of your profile you want to share.
2. They receive an invitation in their inbox.
3. They click the link in the email and log in with a myUMBC, Google, or Facebook account.
4. They can access your profile through a People menu.

Note: This information is private, so only share with people that you know and trust.

Shared With

You are sharing your profile with the following people:

- Todd Haddaway (todd.haddaway@gmail.com)
  View Profile Summary, View Current Classes, View Grade History
Update Profile Sharing

Access for Todd Haddaway (todd.haddaway@gmail.com)

☑ Profile Summary
Some basic info, including UMBC-specific IDs and billing address.

☑ Course Schedule
Currently enrolled courses, as well as courses registered for in the future.

☑ Grade History
A complete history of grades received in all past courses.

Update Access  Remove ALL Access
Social Identities at UMBC

What’s next?

• Student finances - View account balance and details
• Financial Aid - View awards and award status
• Advising sessions - View notes taken during
• Applicants and Admits
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Canvas and Noncredit students

Erica Lomax & Andy Morgan
How we got here

• Switching from Blackboard to Canvas
• Noncredit students have local Blackboard accounts
• OSU has no guest account system

Project Influences
• No more local accounts!
  • Poor lifecycle management of local Blackboard accounts
• Must be off Blackboard by January 2016
  • Noncredit would like to be ready for Fall 2015
Existing State - Noncredit

- Self-asserted identities, no vetting
- Registration not in SIS
- Local accounts issued for noncredit services/systems
  - 3rd party registration/enrollment system
  - Blackboard
  - Drupal
- Support overhead for forgotten username/passwords
Our solution

Solution
• Social-to-SAML Gateway (Cirrus Identity)
• Integration at individual service
• No central registry of noncredit identities maintained by IAM
• IAM owns social API keys / secrets

Why social-to-SAML?
• Canvas was already integrated with OSU IdP using SAML
• All services had SAML support
• No time or interest in building guest system
What we learned about Canvas

• No SAML IDP Discovery Protocol support
• Uses separate /login/### URLs for each configured IDP
• We can specify a discovery URL
Keys to executive stakeholder approval

• Partner with everyone to find the solution
  • PACE, IAM, Office of Information Security, Enterprise API Architect, Canvas team
  • Get key support early

• Timeline & Value proposition

• Scope limited to self asserted identities
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Overview

1. Trajectory of the Conversation
2. Why social identities?
3. Categorizing use cases
4. Implementation approaches
5. Real-world example – UMBC parent access to PeopleSoft
6. Real-world example – Oregon State and Canvas
7. Questions and Discussion
8. Closing
Evaluation

Please complete the evaluation of today’s webinar

InCommon Shibboleth Installation Workshops

June 11-12, 2015 – OARnet, Columbus, OH – SOLD OUT

September 17-18, 2015 – DeAnza College, Cupertino, CA

October 19-20, 2015 – University of Texas – Arlington, Arlington, TX

www.incommon.org/shibtraining
Upcoming Events

Upcoming IAM Online webinars

June 10, 2013 - IAM Online - Grouper

www.incommon.org/iamonline

October 4-7 – Technology Exchange, Cleveland, OH

Call for Proposals Closes May 21

https://meetings.internet2.edu/2015-technology-exchange/