InCommon®

IAM Online

EDUCAUSE Identity and Access Management Working Group

Thursday, October 14, 2010 – 4 p.m. EDT / 1 p.m. PDT

IAM Online

EDUCAUSE Identity & Access Management Working Group Update Featuring EDUCAUSE's Implementation of Federated Identity Management

IAM ONLINE IS BROUGHT TO YOU BY INCOMMON, IN COOPERATION WITH INTERNET2 AND THE EDUCAUSE IDENTITY AND ACCESS MANAGEMENT WORKING GROUP

EDUCAUSE Identity & Access Management Working Group Initiatives

- Charge to IAM project teams
- IAM online sessions in collaboration with InCommon and Internet2
- Identified one key deliverable for each project team
- Met regularly to keep the conversation going
- List currently has 1,180 subscribers
- Averaging 65 posts a month
- Topics range from technical to policy

Awareness & Advocacy

- **Purpose:**
  - Help CIOs and IT leaders understand the strategic importance of IAM for their enterprise
  - Discuss and identify ways to inform/educate CIO's and IT leaders, helping them become mindful of IAM and knowledgeable of key aspects of IAM and effective advocates for it at their institutions
- **Featured Project:** IAM communications plan for CIO's
- **Project Description:** Toolkit for CIO's as they work to roll out IAM on their campus.
  - IAM Primer (What is it, why it's important, roles/responsibilities, governance)
  - CIO IAM Resource Kit
- **Contact:** Matthew Dalton (daltonm@ohio.edu)

Outreach & Coordination

- **Purpose:** Identify and engage one or more key professional communities to advocate, integrate, and facilitate interoperable IAM
- **Featured Project:** Association of College & University Auditors
- **Project Description:**
  - Add IdM section to ACUA's Risk Dictionary to enable auditors to build IdM-appropriate assessment programs
  - Create & disseminate value proposition materials for IdM, Federated IdM, and InCommon's Identity Assurance program (Silver)
  - Help InCommon align Identity Assurance program with campus assessment practices
- **Contact:** Tom Barton (tbarton@uchicago.edu)

IAM Tools & Effective Practices

- **Purpose:** The IAM Tools & Effective Practices Working Group is focused on establishing a set of resources for IAM Architects to use in implementing a cohesive program on their respective campuses. Individual projects and events will support this effort and may focus on the revision of existing documents or processes as well as the creation of new resources or tools.
- **Featured Project:** Two efforts – (1) Solicit and publish peer input on solutions to current IAM challenges or "Hot Topics"; (2) Link to new or existing resources for each topic highlighted.
- **Project Description:**
  - Survey IDM listserv (members and recent list "threads") to identify current areas of IAM interest or concern to "spotlight" during the coming year
  - Develop a web site to present content in an organized and useful way
  - Tag current resources after reviewing for currency and relevancy
- **Contact:** Mark Scheible (mark_scheible@ncsu.edu)

EDUCAUSE'S IMPLEMENTATION OF FEDERATED IDM AND INCOMMON

Matthew Pasiewicz, Manager of Web Development, EDUCAUSE
Craig Hancock, Senior Programmer/Analyst, EDUCAUSE

http://www.educause.edu/idp_setup

VERY APPRECIATIVE

We're very grateful for the hard work of

Craig Hancock & **Mehmet Alkanlar**

who helped bring our support for InCommon to life.

The community has been great and very supportive.

Special Thanks To:

The University of Chicago
Colorado State University
The Johns Hopkins University
University of Alaska

Lafayette College
The University of Washington
The Ohio State University
Brown University

BACKGROUND INFORMATION

- **65 Staff** – We're smaller than many of your IT departments
- **More than 2,200 member organizations**
  - Domestic & International Users
  - Universities, Corporations, Associations, etc.
- **User base of 110,000 +**
- **Most logins at point of need**
  - Destination site, but high percentage of content is freely available
  - Some content/services password protected (CoreData, ECAR, etc)

GETTING STARTED/OBSERVATIONS

- Better Security & Greater Trust
- Better Customer Service
  - no password calls/emails
  - streamlined setup
- Lower Operational Overhead
- Great Community == Lots of Help

InCommon is an organization poised for rapid expansion!

EDUCAUSE/INCOMMON STATUS

- Large majority of site “shib enabled” since May
- .EDU Administration is great candidate, but hard
- More services likely next year

TARGETED/PERSISTENT IDS

I heart disambiguous identifiers.

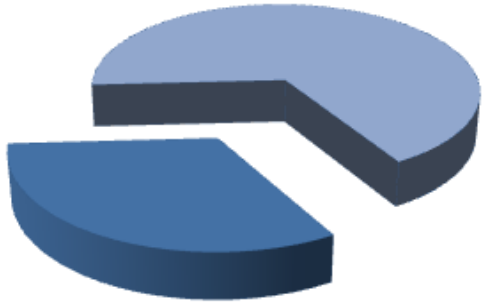
Reduces confusion by letting SPs know that an EPPN has changed or been reused.

More secure/less margin for error/lower TCO

EDUCAUSE/INCOMMON STATUS

154 InCommon IdPs

Based on Federation Metadata from 10/12/2010



33% Already Setup

We're ready for more!

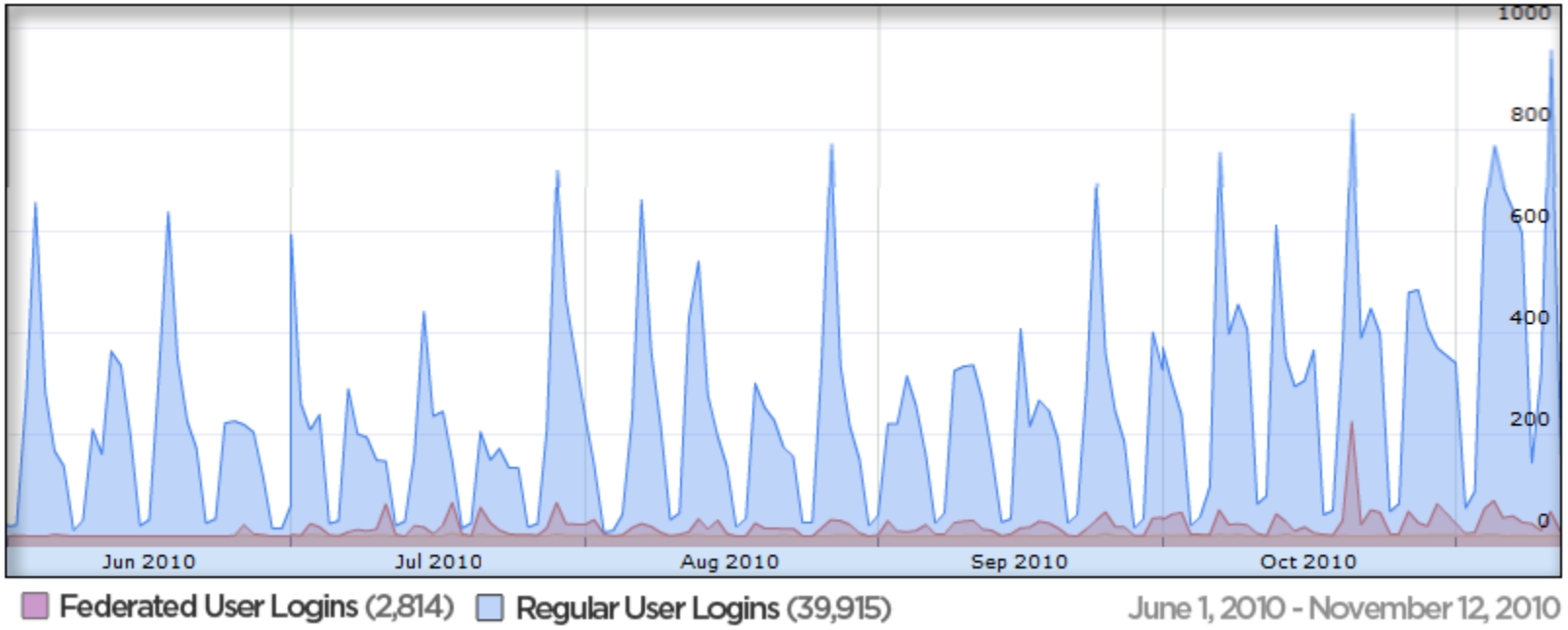
52 IdPs (61 organizations) have used our self service setup system.

More than 1,300 users have logged almost 3,000 times.

Roughly 500 new-to-EDUCAUSE users created!

ALL LOGIN ACTIVITY

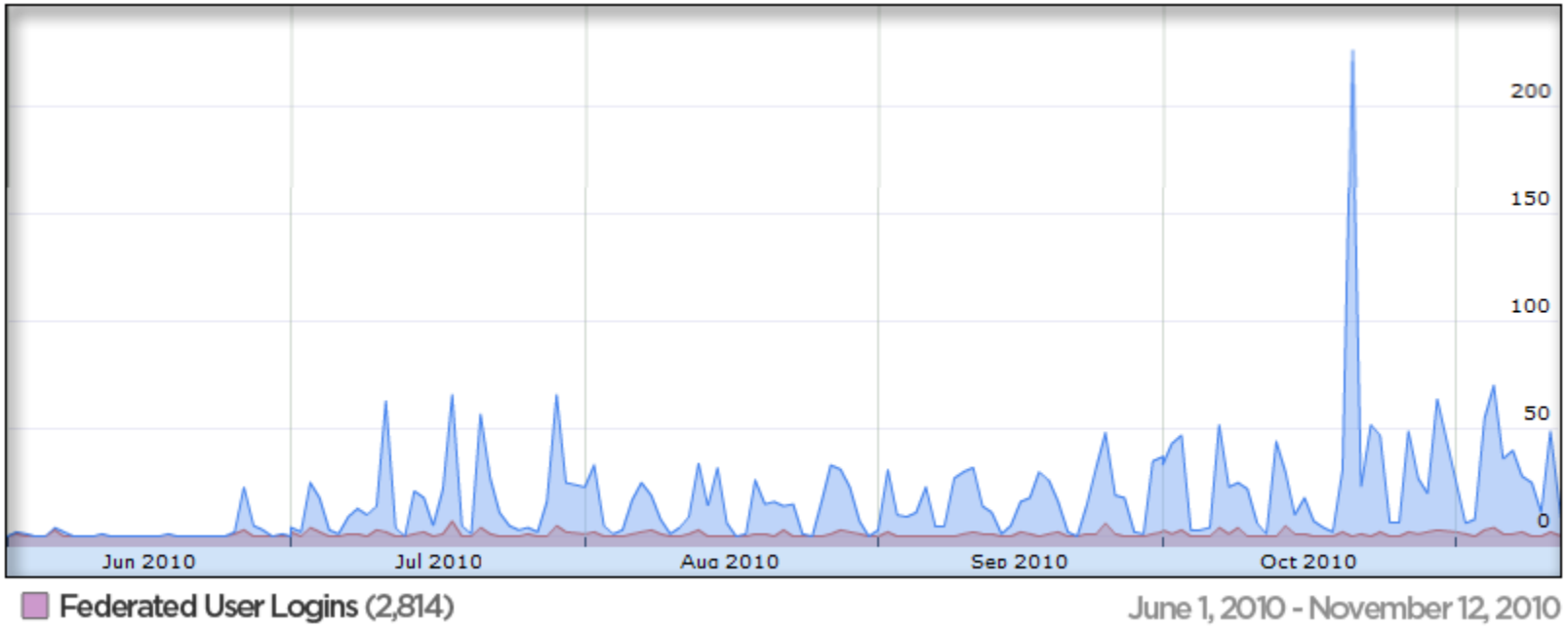
Almost 40,000 Logins Processed



Still a long way to go

FEDERATED LOGIN ACTIVITY

Almost 3,000 Logins Processed



Slow, steady growth with nice jump timed with a E10 registration mailing

SUPPORTING TECHNOLOGIES

- Drupal Shib Auth
  - http://drupal.org/project/shib_auth
  - NIIF (Hungarian Research and Education Network)
  - Modified extensively, but good starting point
- SWITCHwayf PHP
  - http://www.switch.ch/aai/support/tools/wayf.html
  - BSD licensed WAYF/DS implementation from Switzerland
- Shibboleth
  - You don't really need that URL, do ya?

LESSONS LEARNED

- Testing is HARD, but community is great
- SLO (single log out) remains a tough issue
- Fingers crossed for metadata expansion
  - No standardized “keys” for “entities”
  - IPEDS Unit ID is on our wishlist
- Some IdPs exposing both SAML 1 and 2 attributes

BIG QUESTIONS

- How to handle the initial (IdP) setup process
- What do we do with existing users (aka – How do we handle the boarding process)
- How do we handle support issues

OPEN QUESTIONS

- Where should we go next?
  - Enable other services – a matter of timing.
  - Pursue other federations/inter-federation support?

- Should we require login thru institutional IdP?

  No EDUCAUSE managed user/pass allowed?

NEXT STEPS

- Refine the setup process
- Continue monitoring use
- Encourage adoption
- Monitor risks
- Expand to other EDUCAUSE services

EDUCAUSE

UNCOMMON THINKING
FOR THE COMMON GOOD

THANK YOU

http://www.educause.edu/idp_setup

matt@educause.edu

ATTRIBUTE REQUIREMENTS

Requested Attributes

ATTRIBUTE	OPTION A	OPTION B (NameID with Format)
persistentID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

Required Attributes

ATTRIBUTE	SAML 1	SAML 2
eppn	urn:mace:dir:attribute-def:eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
sn	urn:mace:dir:attribute-def:sn	urn:oid:2.5.4.4
givenName	urn:mace:dir:attribute-def:givenName	urn:oid:2.5.4.42
mail	urn:mace:dir:attribute-def:mail	urn:oid:0.9.2342.19200300.100.1.3
affiliation *	urn:mace:dir:attribute-def:eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9

•Please note, only persons with the Member@ scoped affiliation will be authorized to access the portfiolio of services available to your institution.

Optional Attributes

ATTRIBUTE	SAML 1	SAML 2
nickname	urn:mace:dir:attribute-def:eduPersonNickname	urn:oid:1.3.6.1.4.1.5923.1.1.1.2
title	urn:mace:dir:attribute-def:title	urn:oid:2.5.4.12
cn	urn:mace:dir:attribute-def:cn	urn:oid:2.5.4.3
displayName	urn:mace:dir:attribute-def:displayName	urn:oid:2.16.840.1.113730.3.1.241
primaryAffiliation	urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.5
street	urn:mace:dir:attribute-def:street	urn:oid:2.5.4.9
st	urn:mace:dir:attribute-def:st	urn:oid:2.5.4.8
l	urn:mace:dir:attribute-def:l	urn:oid:2.5.4.7
postalCode	urn:mace:dir:attribute-def:postalCode	urn:oid:2.5.4.17
telephoneNumber	urn:mace:dir:attribute-def:telephoneNumber	urn:oid:2.5.4.20

Call to Action

- Join Identity Management Discussion Group
  Website: www.educause.edu/cg/idm
- Volunteer for the Working Group of a Project Team
  E-mail: idm@educause.edu
- For more information, visit www.educause.edu/iam
- Contacts:

  Chris Duffy (CDuffy@peirce.edu)
  Valerie Vogel (vvogel@educause.edu)
  Rodney Petersen (rpetersen@educause.edu)

InCommon®

Survey

Please complete the survey about today's IAM Online:
http://www.surveymonkey.com/s/NW95LSN

Internet2 Fall Member Meeting

Federation track, Middleware track http://bit.ly/d8pTQG
November 1-5, 2010 – Atlanta, Georgia – events.internet2.edu/2010/fall-mm/

Day CAMP:

Getting Started with the InCommon Federation
November 4-5, 2010 – Atlanta, Georgia – www.incommon.org/camp

Shibboleth Workshop Series – Lafayette College (Easton, PA)

November 9, 2010 – Identity Provider
November 10, 2010 – Service Provider
www.incommon.org/educate/shibboleth

InCommon®

Survey

Please complete the survey about today's IAM Online:
http://www.surveymonkey.com/s/NW95LSN

Next IAM Online www.incommon.org/iamonline

November 11, 2010 – Federated Provisioning and Google Groups
Speakers will describe work on federated provisioning with an emphasis on provisioning groups with Google.

Thank you to InCommon Affiliates for helping to make IAM Online possible.

UNICON® aegisUSA™ Microsoft gluu

Brought to you by InCommon, in cooperation with Internet2
and the EDUCAUSE Identity and Access Management Working Group