

AACRAO Tech - July 11, 2008

# OPPORTUNITIES AND EFFICIENCIES:

Supporting Student Services  
with Federated Identity

Nancy Krogh, University of Idaho  
Ann West, EDUCAUSE/Internet2/Michigan Tech

# Topics



- What's Federated Identity?
- What's in it for me?
- What's going on that I should know about?
- What's next for the community and for my campus?

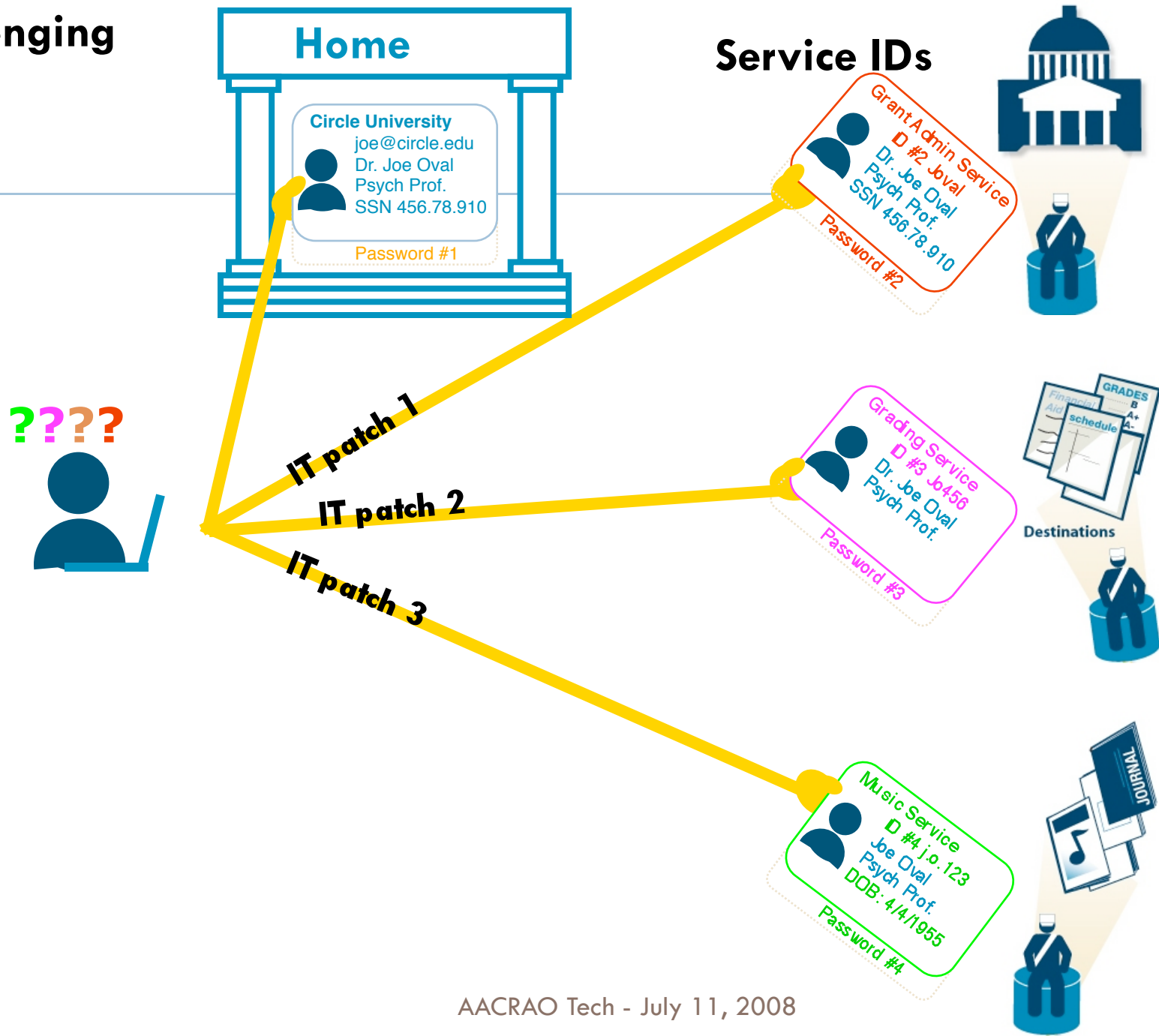
# What's Federated Identity?



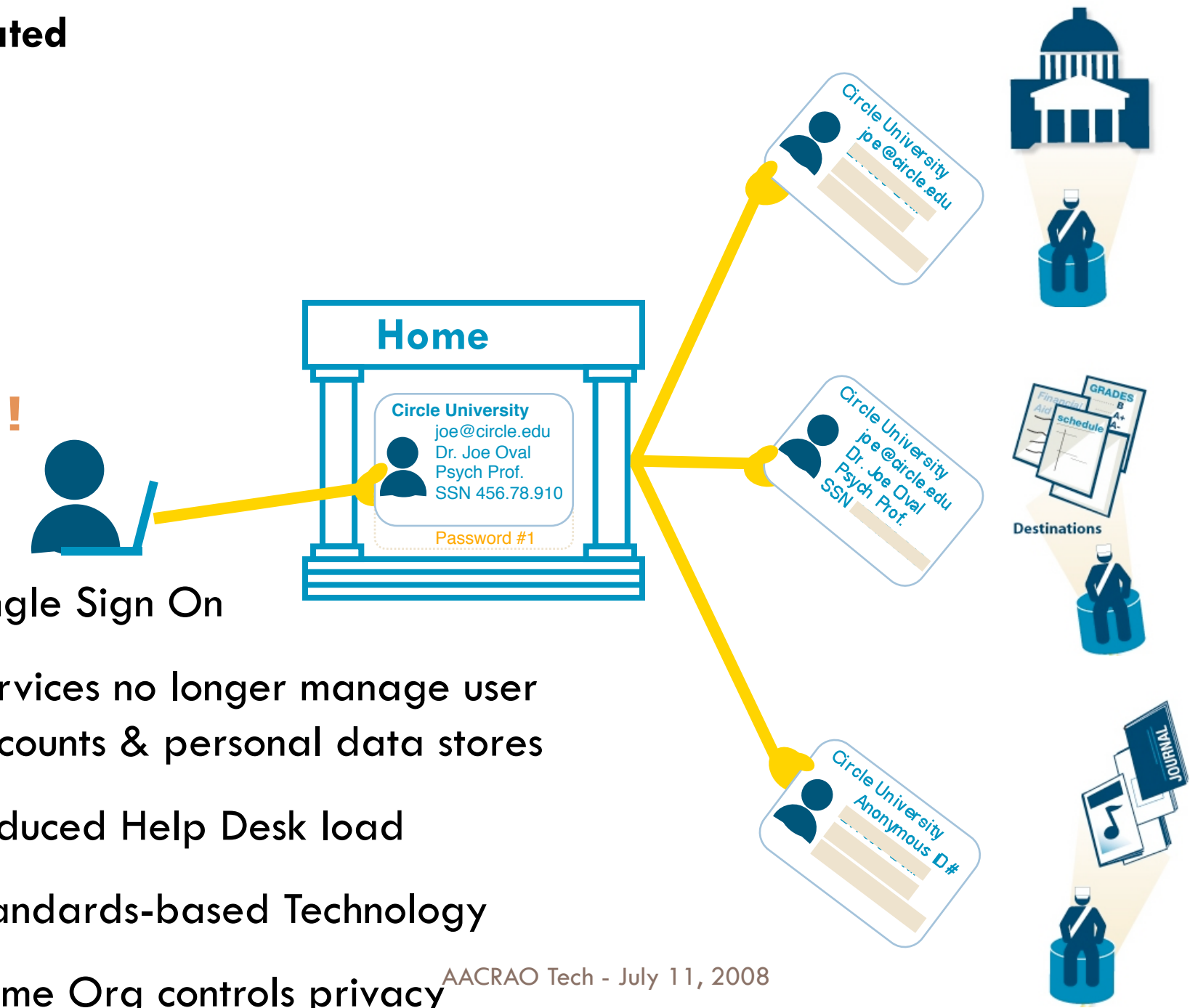
# An After Lunch Bedtime Story...



# Challenging Way



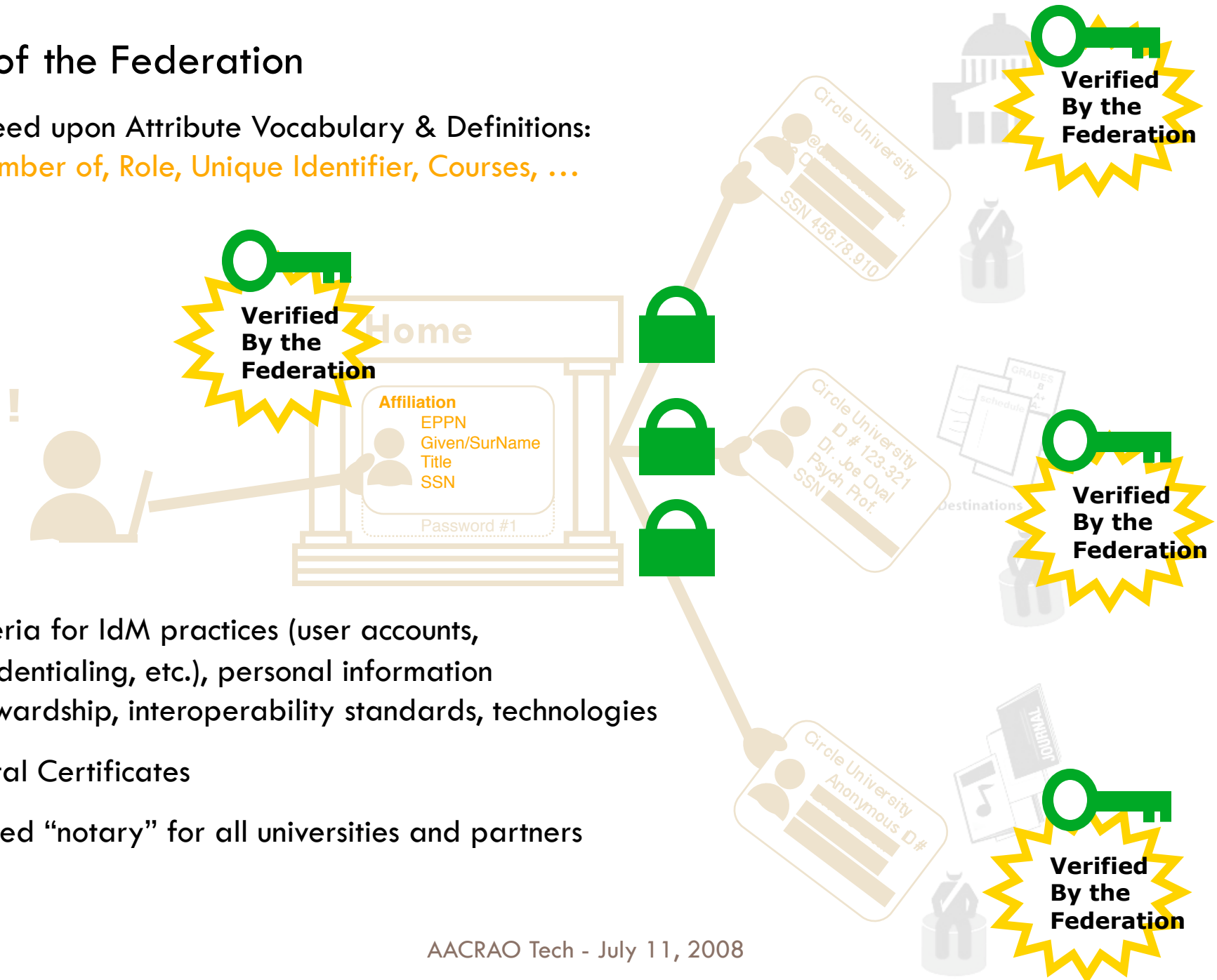
# Federated Way



1. Single Sign On
2. Services no longer manage user accounts & personal data stores
3. Reduced Help Desk load
4. Standards-based Technology
5. Home Org controls privacy

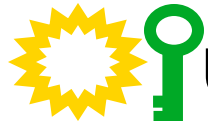
# Role of the Federation

1. Agreed upon Attribute Vocabulary & Definitions:  
*Member of, Role, Unique Identifier, Courses, ...*



2. Criteria for IdM practices (user accounts, credentialing, etc.), personal information stewardship, interoperability standards, technologies
3. Digital Certificates
4. Trusted “notary” for all universities and partners

## federation metadata

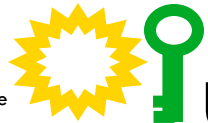


### University A

IdP: name, key, url, contacts, etc.

SP1: name, key, url, contacts, etc.

SP2: name, key, url, contacts, etc.



### University B

IdP: name, key, url, contacts, etc.

SP1: name, key, url, contacts, etc.

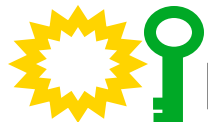
future



### University C

IdP: name, key, url, contacts, etc.

bronze  
LoA



### Partner 1

SP1: name, key, url, contacts, etc.



### Partner 2

SP1: name, key, url, contacts, etc.

silver  
LoA

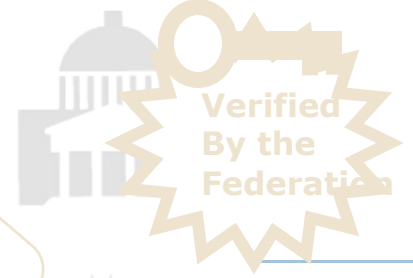


### Partner 3 ...

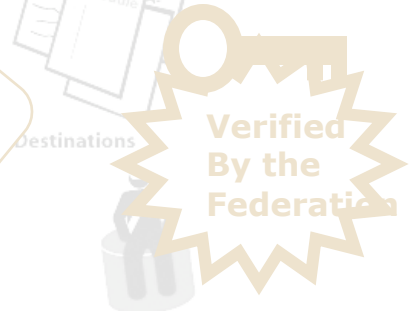
silver  
LoA



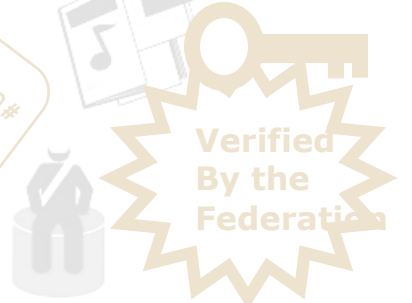
Circle University  
#56.78.910



Circle University  
D # 123-321  
Dr. Joe Oval  
Psych Prof.  
SSN



Circle University  
Anonymous D#



# US Research and Education Federation: www.incommonfederation.org



[Home](#) | [About InCommon](#) | [Join InCommon](#)

- Join InCommon
- InCommon Participants
- InCommon Benefits
- Policies and Practices
- Technical Information
- Frequently Asked Questions
- Administrative Login
- Metadata, WAYF, & CA
- Related Links
- Glossary
- Contact
- About

## InCommon makes sharing protected online resources easier.

InCommon eliminates the need for researchers, students, and educators to maintain multiple, password-protected accounts. Online service providers no longer build and manage account provisioning systems. InCommon uses innovative [Shibboleth®](#) authentication and authorization systems to enable cost-effective, privacy-preserving collaboration among its community of participants.

### The Benefit:

Online service providers make access decisions based on a user's log-in to his or her home organization. Authorized resources stay protected while users have fewer accounts and passwords to juggle. Furthermore, only agreed upon attributes about each user are released. In this way, levels of privacy are always maintained and controlled by the home organization. This "federated identity" system of trust makes it easier on the user, more scalable for resource providers, and takes advantage of identity management infrastructure already in place at universities and partner organizations.

Find out how to join this innovative trust federation:

- [Joining the InCommon Federation](#) (Eligibility Criteria and Process)
- [The InCommon Participation Agreement \[PDF\]](#)
- [The InCommon Fee Schedule](#)
- [Sponsorship Information](#) for Non-U.S. Higher Education organizations

## Case Studies

Read about current InCommon Participants and how they are implementing innovative approaches to federating identity and access management systems.

**\*New\***

Symplicity Student Career Services and Penn State [\[pdf\]](#)



NYU, University of Washington, and DRAM [\[pdf\]](#)



Penn State and WebAssign [\[pdf\]](#)



AACRAO Tech - July 11, 2008

Email any questions to: [incommon-admin@incommonfederation.org](mailto:incommon-admin@incommonfederation.org)  
© Copyright 2007 InCommon, LLC. All Rights Reserved. InCommon is operated by [Internet2](#).  
Participation in InCommon is separate and distinct from membership in Internet2.

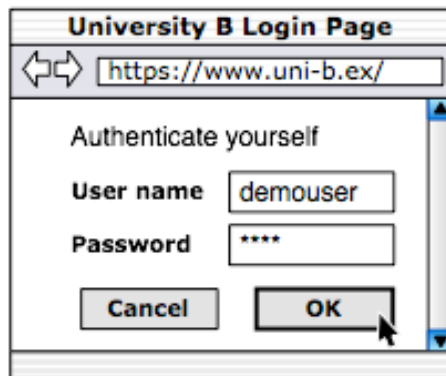
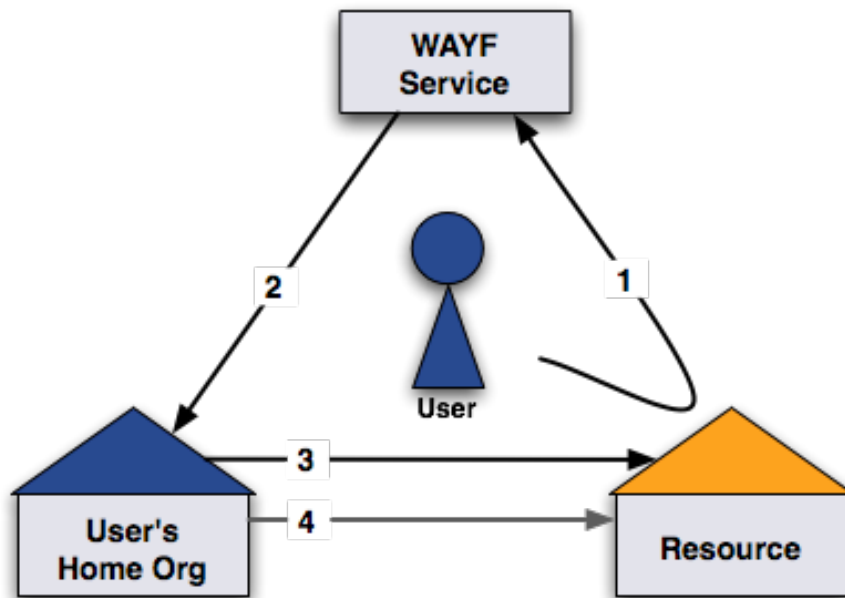
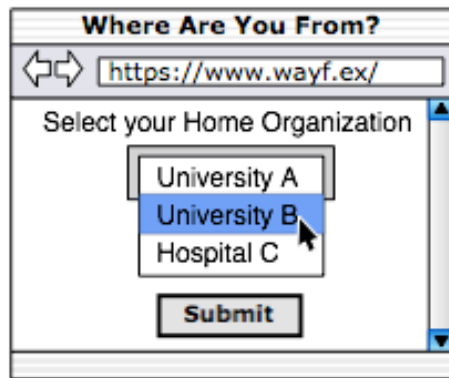
# InCommon Technology



- Security Assertion Markup Language (SAML)
  - ▣ XML-based standard of the OASIS Security Services Technical Committee
  - ▣ Used to exchange authentication and authorization data between an identity provider and a service provider
- Shibboleth Federating Software
  - ▣ On campus single Sign-on to off campus services
  - ▣ Developed by the Internet2 Community
    - [shibboleth.internet2.edu](http://shibboleth.internet2.edu)

# eduPerson Schema

- “**eduPerson** - An LDAP object class authored and promoted by the EDUCAUSE/Internet2 ... to facilitate the development of inter-institutional applications...”
  - ▣ InCommon Glossary at <http://www.incommonfederation.org/>
- Enterprise directory data schema
- Attribute release for authorization



# InCommon Security Profiles



- Based on the Federal levels of assurance
- Emerging standard practices
  - Business and operations
  - Identity registration and proofing
  - Credential issuance and management
  - Digital electronic credential technology
  - Security and management of authentication events
  - Identity information management
  - Identity assertion and content
  - Technical environment

# InCommon Benefit



Federation enables communities to share information about individuals' identity, reducing the overall work required to maintain connections and reduce the friction in cross-community interactions.

Burton Group,

*Federating a Distributed World: Asserting Next-Generation Identity Standards*

# What's in it for me?



# Is identity and access management a current project on your campus?

	<b>Total</b>	<b>Percent</b>
Don't Know	79	22.8%
Under Discussion	75	21.7%
Yes	164	47.4%
No	28	8.1%

*If yes or under discussion, what are the main reasons that your institution is working on an identity and access management project? (Check all that apply.)*

	Total	Percent
Security	189	79.1%
Better ways of giving and removing access to systems	149	62.3%
Better role management	115	48.1%
Better data control	140	58.6%
Better service	116	48.5%
Access to external services	52	21.8%
Service to external partners and affiliated faculty	43	18.0%
Other reasons	10	4.2%

# Other Reasons



- ❑ Student privacy
- ❑ Single sign-on
- ❑ User experience
- ❑ Our auditors and access controls
- ❑ Student expectations
- ❑ Avoid institution liability
- ❑ Faster account provisioning and removal

# Why?



- Federated is a solution for these challenges

# Survey Gaps

<b>How familiar are you with the term "identity management"?</b>	<b>Total</b>	<b>Percent</b>
Not at all	68	19.5%
Have heard the term	65	18.7%
Somewhat familiar	125	35.9%
Very familiar	86	24.7%
Consider myself an expert	4	1.1%

# Survey Gaps

<b>Are you familiar with the term "federated identity"?</b>	<b>Total</b>	<b>Percent</b>
Not at all	227	66%
Have heard the term	52	15%
Somewhat familiar	37	11%
Very familiar	29	8%
Consider myself an expert	1	0%

# *How do you rate your working relationship with your central IT department?*

	<b>Total</b>	<b>Percent</b>
Not working together at all	1	0.3%
Strained communication	23	6.7%
Neutral interaction	13	3.8%
Working relationship	142	41.6%
Very collaborative partnership	162	47.5%

# AACRAO IdM Survey



- ▣ Summary of Results – stay tuned

# What's going on?



AACRAO Tech - July 11, 2008

# AACRAO Identity Management Workshop with Internet2 and EDUCAUSE

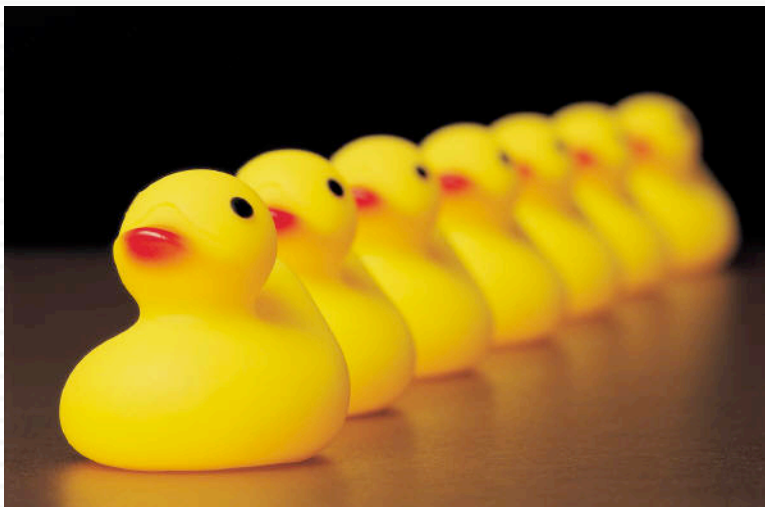
- ▣ Jointly sponsored workshop
- ▣ 90 attendees
- ▣ Themes
  - Governance and working together
  - Identifiers: duplication/distribution
  - Education
  - Security
  - Federated identity, outsourcing, data release
- ▣ Hot topic – stay tuned

# InCommon Federation Student Services group



- IT and Registrar group advancing Federated Identity in the student services
  - Education
  - Share
  - Pilot
  - Review and comment
  - <https://spaces.internet2.edu/display/InCCollaborate/InC-Student>
- Case Studies

# What's next?



# What's next?



- Registrars need to be at the table for successful campus IdM projects
- The registrar community needs to be at the table for higher education federations to work
- How do we bring everyone to the table?

# Getting Started



1. Engage
2. Educate
3. Benchmark
4. Define
5. Ensure
6. Identify

# AACRAO IdM Next Steps?



- Get involved and sign up
  - AACRAO Listserv
  - Practice paper development
  - New opportunities and IdM-related resources
  - Workshops
  - InCommon Student list with your IT partner
- Ideas? Send them to us or to  
Jeff von Munkwitz-Smith

# Parting Thoughts



- Community Trust - Collective responsibility
- Mindset switch
- Local practice to best practice to standard practice
  - Standards are being set now outside registrar community
  - Integrating, not developing practices



# Questions?

AACRAO Tech - July 11, 2008

# Contact Information



- Nancy Krogh

University Registrar

University of Idaho

[nkrogh@uidaho.edu](mailto:nkrogh@uidaho.edu)

- Ann West

Program Manager, Tech Transfer and Outreach

EDUCAUSE/Internet2/Michigan Tech

[awest@educause.edu](mailto:awest@educause.edu) or [awest@internet2.edu](mailto:awest@internet2.edu)