InCommon Grows Up

www.incommon.org

Kevin M. Morooney
Vice Provost for Information Technology
Penn State
2010 Chair, InCommon

Jack Suess
Vice Provost for Information Technology
UMBC
2010 Vice Chair, InCommon
How we’ll use the time

• InCommon...
  – ...101 & Background
  – ...Community
  – ...On campus
  – ...Beyond campus
  – ...The Futures Report - Our blueprint
  – ...Hot topics
Who is here?
The InCommon Basic Value Propositions (v1.0)

• For the campus: InCommon enables campuses to leverage their identity management systems to allow the use of one set of credentials to access multiple resources.

• For the provider: Online service providers no longer need to maintain user accounts. Identity providers manage the levels of their users' privacy and information exchange.

• For everyone: InCommon uses SAML-based authentication and authorization systems (such as Shibboleth®) to enable scalable, trusted collaborations among its community of participants.
...another way to say it....
InCommon Federation Value Proposition
(v1.1)

Provides the trust framework for access to online resources

- Single sign-on with higher education credentials
- Enhanced security with fewer data spills
- Privacy – release of only those attributes necessary
- Access – Service provider makes decision based on attributes
- Scalable – Once implemented, federated access relatively simple to extend
...another way to say it....
Before Federation

- Destinations
- Many Managed Accounts
- Multiple ID’s

After Federation

- One Home Account
- Single ID
InCommon Community
InCommon Participants Year-by-Year

- 2004: 10
- 2005: 10
- 2006: 30
- 2007: 50
- 2008: 80
- 2009: 180
- 2010 (Apr): 220
Growth of InCommon

InCommon Participants

Number of Participants

- 2004
- 2005
- 2006
- 2007
- 2008
- 2009
- Dec-10
Principle
50M Elvis fans can’t be wrong
Absolute Software, Inc.
Apple - iTunes U
Atlas Systems, Inc.
BioOne, Inc.
Blatant Media Corporation
Burton Group
Cengage Learning, Inc.
Colorado Alliance of Research Libraries
Davie County Schools
Digital Measures
e-academy, Inc.
e2Campus by Omnilert, LLC
Ebook Library - EBL
EBSCO Publishing
EDUCAUSE
Elsevier
EnergyCAP, Inc.
Houston Academy of Medicine - Texas Medical Center
Identit-e
Internet2
JSTOR
Kuali Foundation
Learn.com
Leepfrog Technologies, Inc.
lynda.com
MCNC
Microsoft
National Student Clearinghouse
NC Live
NG Web Solutions
North Carolina Department of Public Instruction
OCLC
OhioLink - The Ohio Library & Information Network
Outside The Classroom
PeopleAdmin, Inc.
ProQuest LLC
ProtectNetwork
Qualtrics
RefWorks, LLC
Rockingham County Schools
Safari Books Online
Students Only Inc.
SumTotal Systems Inc.
Symplicity Corporation
The H.W. Wilson Company
Thomson Reuters
Travel Solutions, Inc.
Trondent Development Corp.
Turnitin
University of Texas Health Science Center At Tyler
UniversityTickets
WebAssign
Argonne National Laboratory
Energy Sciences Network (ESNet)
Lawrence Berkeley National Laboratory
Moss Landing Marine Laboratories
National Institutes of Health
National Science Foundation
TeraGrid
InCommon Leadership-Steering Committee

- Steve Cawley, University of Minnesota – Treasurer
- Joel Cooper, Carleton College – Secretary
- Mark Crase, California State University
- Chris Holmes, Baylor University
- Ken Klingenstein, Internet2 (ex officio)
- Tracy Mitrano, Cornell University
- Kevin Morooney, Penn State – Chair
- John O'Keefe, Lafayette College
- Stephanie Reel, Johns Hopkins University
- Jack Suess, University of Maryland, Baltimore County – Vice-Chair
- Chris Shillum, Elsevier
- Shel Waggener, UC Berkeley
- Advisers:
  - Renee Frost, Internet2, University of Michigan
  - Rodney Petersen, EDUCAUSE (ex officio)
  - David Wasley, retired, UCOP
InCommon Leadership-Technical Advisory Committee

- RL "Bob" Morgan, University of Washington – Co-Chair
- Renee Shuey, Penn State – Co-Chair
- Tom Barton, University of Chicago
- Jim Basney, Teragrid
- Scott Cantor, The Ohio State University
- Steven Carmody, Brown University
- Paul Caskey, University of Texas System
- Michael Gettes, Massachusetts Institute of Technology
- Keith Hazelton, University of Wisconsin - Madison
- Ken Klingenstein, InCommon Steering Committee
- Mike LaHaye, Internet2
- David Walker, University of California Davis
- David Wasley, retired, UCOP
InCommon is Community Driven

- evangelize new vendors
- analyze service opportunities
- develop technical strategies
- do interoperability testing, etc.
InCommon learning opportunities

IAM Online

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

IAM Online is a new monthly series delivering interactive education on Identity and Access Management (IAM), including federated identity management essentials, advanced issues in IAM, and hot topics from the EDUCAUSE Identity and Access Management Working Group. Experts will provide overviews, answer questions and lead discussions.

IAM Online includes three types of presentations/discussions:

- **Federated Identity Management Essentials** - Learn how you can leverage your existing identity management infrastructure to provide single sign-on access to resources both on- and off-campus.
- **Advanced Issues in Identity Access and Management** - Community developers and experts will provide information and lead discussions about emerging technical, architectural and other topics involved with the deployment of identity and access management.
- **Hot Topics and Current Issues in Identity and Access Management** - The leadership of the EDUCAUSE Identity and Access Management Working Group will probe hot topics and current issues gleaned from questions posed to the Identity Management Discussion Group, federal policy developments affecting identity and privacy, and other higher education and industry initiatives.

To Participate

We will use Adobe Connect for slide sharing and to post questions via the chat function. A conference call bridge will be available for those not near a computer.

Adobe Connect: http://internet2.acrobat.com/iam-online

Dial-in numbers:

+1-734-615-7474 Preferred (from any phone where long distance has no add'l cost over local or 800 calling)

+1-866-411-0013 (US/Canada Only and only if above 734- number costs user more than 800/866 calls; this number costs Internet2 substantially more than above 734 number and should be avoided if possible)

IAM Online - Thursday, April 8, 2010

Federated Identity Essentials: Making Federation Happen

Download the slides here.
The archived session is here.

This session will demonstrate how schools of all sizes can get started with InCommon and federated identity management. Our speakers will identify the specific policy and technical steps that lead to successfully joining InCommon and leveraging your identity management system for use with resource providers.

Guest Speakers:

John O’Keefe, director of academic technology and network services at Lafayette College and member of the InCommon Steering Committee.

Joel Cooper, director of information technology services at Carleton College and member of the InCommon Steering Committee.
InCommon learning opportunities

InCommon Online Forum

The InCommon Online Forum provides an opportunity for policy and technical discussions with the InCommon Steering Committee, the InCommon Technical Advisory Committee and InCommon’s collaboration groups.

If you are looking for the IAM Online educational sessions, please go here.

Archived Sessions

March 30 - InCommon Steering Chat

View the archived Adobe Connect session
Slides from the presentation

Session overview: Topics included: InCommon Update; extending your federated services.

February 25, 2010 - InCommon Technical Advisory Committee Discussion

View the archived Adobe Connect session
Slides from the presentation

Session overview: Topics included: SAML 2 profiles/support, University of Michigan’s uApprove implementation, InCommon technical priorities.

For more information about the InCommon Online Forum, contact Dean Woodbeck (woodbeck@internet2.edu)

This page last updated April 1, 2010

Email any questions to: incommon-admin@incommonfederation.org
© Copyright 2010 InCommon, LLC. All Rights Reserved. InCommon is operated by Internet2.
InCommon learning opportunities

InCommon Forum, "InCommon Grows Up" Available via Web
Not attending the Internet2 Spring Member Meeting? Two InCommon sessions - the InCommon Forum and InCommon Grows Up - will be available via the web. See the details here.

Federate! Internet2 Spring Member Meeting
InCommon participants and identity management enthusiasts will find a program chock full of sessions from InCommon, IdM and Middleware:
- See the complete InCommon/Middleware schedule.
- See the poster sessions, scroll down the page to check out the federated logon to NSF.
- An InCommon Forum and InCommon 101 are also planned (both are included with the InCommon/Middleware schedule).

Make your plans to join us April 26-28 in Arlington, Virginia.

InCommon CAMP Program Unveiled
The program for the 2010 InCommon CAMP: Exploring and Supporting Federated Identity Management, is now available on the CAMP website. Whether you are considering - or already supporting - federated identity management, you'll find something at CAMP.

Advance CAMP Focuses on Identity Services
InCommon On Campus
InCommon: Federating as Horizontal and Vertical Integration
Horizontal Integration
Multiple services all over campus

- Libraries
- Registrar
- Research office
- Faculty (course management)
- Career center
- Students (iTunes U, discount services)
InCommon Beyond Campus
Vertical Integration
Multiple services in one area (library)

- Atlas Systems
- BioOne
- EBSCO
- Elsevier
- JSTOR
- OCLC
- OhioLink
- RefWorks
- Thomson Reuters
- H.W. Wilson

etc., etc.
R&E Federations

- Substantial deployments in many countries, including UK, Norway, Switzerland, Sweden, Japan, Australia, France, Denmark, Finland, Spain, Germany, Netherlands, etc. Coverage in a number of countries is now 100%.
- Uses include roaming access, grid credentials, digital content access, wiki controls
The InCommon Futures Task Force Report

Our blueprint for the future
The Task Force

Amy Philipson, Pacific NW Gigapop, (Internet2 AMSAC)
Chris Shillum, Elsevier, (InCommon Steering)
Clair Goldsmith, UT System, (InCommon Steering)
  Cliff Lynch, CNI, (Internet2 RAC)
Doug Van Houweling, Internet2 CEO
Jack Suess, UMBC, (InCommon Steering, Internet2 AMSAC)
  John Krienke, Internet2, InCommon
Ken Klingenstein, Internet2, U Colorado, (InCommon Steering)
  Kevin Morooney, Penn State, (InCommon Steering)
Lois Brooks, Stanford, (InCommon Steering)
  Richard Katz, EDUCAUSE
Rosio Alvarez, Lawrence Berkeley Labs, (Internet2 RAC)
  Ray Ford, U Montana, (Internet2 AMSAC)
RL 'Bob' Morgan, U Washington, (MACE, InCommon TAC --
  Technical Advisory Committee)
  Rick Summerhill, Internet2 CTO
Sally Jackson, U Illinois, (Internet2 AMSAC)
What they were asked to do

- Task Force launched and charged, January 2009
- Final report submitted to Internet2 board, July 2009
The Recommendations

- Structure
- Governance
- Membership
- Specifics
Structure

- Trust services platform
  - Increase offerings
  - Become financially self-sufficient
- A foundation
  - endeavor to become a place or coordinating point for R&D, development of I2MI and like efforts
Governance

• Set a path towards financial independence

• Establish a Board of Directors to whom the Executive Director of InCommon reports
Membership

• Continue to focus on U.S. higher education

• Actively pursue technical and political relationships with U.S. federal government (notably NSF, NIH, DoE), state-based federations and consortiums, companies and organizations that provide services to education
Specific Recommendations

- Q2 2010, mission and funding plan
- Secure Internet2’s continued support for 3 years
- Internet2 to fund additional positions
- Internet2 continues to provide admin services
- Internet2 commitment to drive InCommon membership to 75% of Internet2 membership
Specific Recommendations

- InCommon to continue to analyze and plan for new trust services
- InCommon, with additional support, to develop training and promotional programs
- InCommon, with additional support, to develop formal outreach programs
- Bronze and Silver profiles to be released at spring I2MM
- Develop new, tiered pricing plan by 2011
InCommon Hot Topics
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold
• Personal privacy management: uApprove, SWITCHaai
• Interfederation
• It’s all about the attributes
• Internet of Things
• Trust, Identity, and the Internet
• Certificate Service
Shaping activities, new directions

• **Level of Assurance: Bronze, Silver, Gold**
• Personal privacy management: uApprove, SWITCHaai
• Interfederation
• It’s all about the attributes
• Internet of Things
• Trust, Identity, and the Internet
• Certificate Service
InCommon LOA (Level of Assurance)

• InCommon – today’s federation
• Bronze (LOA 1) - A campus researcher uses their campus account to access an NIH clinical trial wiki
• Silver (LOA 2) – A sponsored research accountant uses their secure campus account to modify documents on NSF Fastlane
• Gold (LOA 3) - A campus security officer could use their local two factor authentication to participate in a Teragrid security incident
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold

• **Personal privacy management:** uApprove, SWITCHaai

• Interfederation

• It’s all about the attributes

• Internet of Things

• Trust, Identity, and the Internet

• Certificate Service
This is the Digital ID Card to be sent to 'https://aai-demo.switch.ch':

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td>SWITCHaai</td>
</tr>
<tr>
<td>Given name</td>
<td>Demouser</td>
</tr>
<tr>
<td>Unique ID</td>
<td><a href="mailto:234567@example.org">234567@example.org</a></td>
</tr>
<tr>
<td>User ID</td>
<td>demouser</td>
</tr>
<tr>
<td>Home organization</td>
<td>example.org</td>
</tr>
<tr>
<td>Home organization type</td>
<td>other</td>
</tr>
<tr>
<td>Affiliation</td>
<td>staff</td>
</tr>
<tr>
<td>Entitlement</td>
<td><a href="http://example.org/res/99999">http://example.org/res/99999</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://publisher-xy.com/e-journals">http://publisher-xy.com/e-journals</a></td>
</tr>
</tbody>
</table>

- Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.
The following personal information will be shared with the IT Service Provider you are attempting to access, collab.cic.net.

**Digital ID Card**

<table>
<thead>
<tr>
<th>First Name</th>
<th>Luke</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>Tracy</td>
</tr>
<tr>
<td>Full Name</td>
<td>Luke W-B Tracy</td>
</tr>
<tr>
<td>Your e-mail address</td>
<td><a href="mailto:ltracy@umich.edu">ltracy@umich.edu</a></td>
</tr>
<tr>
<td>University Affiliation</td>
<td>staff</td>
</tr>
<tr>
<td></td>
<td>member</td>
</tr>
</tbody>
</table>

By clicking 'Confirm', you agree to adhere to the conditions of use on the site to which you are going, in addition to the Information Technology Policies at U-M.

For help using collab.cic.net, use the contact information on that site. If you cannot access the site at all, contact shibboleth@umich.edu for assistance.
You did not agree to send your Digital ID Card to "collab.cic.net". Therefore, you will not be able to access "collab.cic.net". In order to cancel the login process, please close your web browser.
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold
• Personal privacy management: uApprove, SWITCHaai
• **Interfederation**
  • It’s all about the attributes
  • Internet of Things
  • Trust, Identity, and the Internet
• Certificate Service
Interfederation

• Connecting autonomous federations
• Critical for global scaling, accommodating state and local federations, integration across sectors
• Has technical, financial and policy dimensions
• Elegant technical solution being developed in the eduGAIN project of Geant
• Policy activities in Kalmar2 Union, Geant, Kantara, Terena
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold
• Personal privacy management: uApprove, SWITCHaai
• Interfederation
• It’s all about the attributes
• Internet of Things
• Trust, Identity, and the Internet
• Certificate Service
The Attribute Ecosystem

• Authentication is very important, but identity is just one of many attributes
• And attributes provide scalable access control, privacy, customization, linked identities, federated roles and more
• We now have our first transport mechanisms to move attributes around – SAML and federations
• There will be many sources of attributes, many consumers of attributes, query languages and other transport mechanisms
Federated Identity, Attributes and Access Control

• For the last ten years we’ve been promoting federated identity
• But the real agenda was to manage access control…
• And the scalable, privacy-preserving way to do access control is attributes
• And group membership is a necessary and sufficient attribute for access control
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold
• Personal privacy management: uApprove, SWITCHaai
• Interfederation
• It’s all about the attributes
• **Internet of Things**
• Trust, Identity, and the Internet
• Certificate Service
The Internet of things

• We have built the Internet of computers and now the Internet of people and identity; next is things.
• Federation is a powerful model – it provides a degree of local freedom but a scalable infrastructure; with interfederation it can reach Internet scale.
• Devices need to have identity, attributes, access control privileges, etc that tend to federate and also need to interact with identity federation.
• Next generation Internet work has many types of federations of circuits, of firewalls, of routers, etc.
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold
• Personal privacy management: uApprove, SWITCHaai
• Interfederation
• It’s all about the attributes
• Internet of Things
• Trust, Identity, and the Internet
• Certificate Service
Trust, Identity and the Internet

• The Internet was built for friendly behavior; that is not the current situation
• ISOC initiative to introduce trust and identity-leveraged capabilities to many RFC’s and protocols
• First target area is DKIM; subsequent targets include SIP and firewall traversal (trust-mediated transparency)
• FCC - Broadband Strategy
• FTC - National Strategy for Secure Online Transactions
Shaping activities, new directions

• Level of Assurance: Bronze, Silver, Gold
• Personal privacy management: uApprove, SWITCHaai
• Interfederation
• It’s all about the attributes
• Internet of Things
• Trust, Identity, and the Internet
• Certificate Service
InCommon

• Certificate Service