

1

IDENTITY AND THE CLOUD: PREPARING YOUR CAMPUS

October 12, 2010 EDUCAUSE Annual Conference

Your Speakers Today

2

HI from
all of us!

- Tracy Mitrano, Cornell University
- John O'Keefe, Lafayette College
- Justin Sipher, Skidmore College
- Ann West, InCommon/Internet2/
Michigan Tech/Penn State

Agenda Today

3

- Introductions
- Federated Identity Management Concepts
- Interactive Session on Cloud Services
- Break
- Federated Identity Checklist
- Getting Started

Basic Cloud Definitions

4

- A model of computation and data storage based on “pay as you go” access to “unlimited” remote data center capabilities
- A cloud infrastructure provides a framework to manage scalable, reliable, on-demand access to applications
- Cloud services provide the “invisible” backend to many of our mobile applications
- High level of elasticity in consumption
- Historical roots in today’s Internet apps
 - Search, email, social networks
 - File storage (Live Mesh, Mobile Me, Flickr, ...)

Details and Examples of Clouds

5

Cloud Market Types	Types of Offerings	Examples
Software-as-a-Service	<ul style="list-style-type: none"> • Rich Internet application web sites • Application as Web Sites • Collaboration and email • Office Productivity • Client apps that connect to services in the cloud 	<ul style="list-style-type: none"> • Flickr • Myspace.com • Cisco WebEx office • Gmail • IBM Bluehouse
App-components-as-a-Service	<ul style="list-style-type: none"> • APIs for specific service access for integration • Web-based software service than can combine to create new services, as in a mashup 	<ul style="list-style-type: none"> • Amazon Flexible Payments Service and DevPay • Salesforce.com’s AppExchange • Yahoo! Maps API • Google Calendar API • zembly
Platform-as-a-Service	<ul style="list-style-type: none"> • Development-platform-as-a-service • Database • Message Queue • App Services • Blob or object data stores 	<ul style="list-style-type: none"> • Google App Engine and BigTable • Microsoft SQL Server Data Services • Engine Yard • Salesforce.com’s Force.com
Infrastructure-as-a-Service	<ul style="list-style-type: none"> • Virtual servers • Logical disks • VLAN networks • Systems Management 	<ul style="list-style-type: none"> • Akamai • Amazon EC2 • CohesiveFT • Mosso (from Rackpace) • Joyent Accelerators • Nirvanix Storage Delivery Network
Physical Infrastructure	<ul style="list-style-type: none"> • Managed Hosting • Collocation • Internet Service Provider • Unmanaged hosting 	<ul style="list-style-type: none"> • GoDaddy.com • Rackspace • Savvis

Adapted from Forrester Research Taxonomy

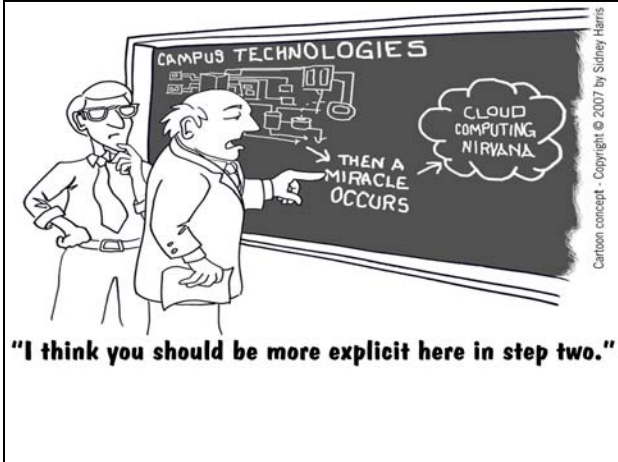
The Role of Cloud in Campus IT

6

- So we will just buy everything from the cloud and won’t need IT, right?



Not exactly....



The New IT


6

- IT is shifting from developing technical solutions to enabling efficient solutions through a mix of sourced technology services.
- How do we do that?
 - Embrace change
 - Streamline adoption
 - Provide integration
 - Facilitate reuse
- While protecting privacy, reducing institutional risk, ensuring continuity, meeting regulatory compliance and high availability requirements.

....And do it all for less \$\$\$.

Identity Management

9



Who are you? (identification)

- Collect personally identifying information to prove you are who you say you are (identity proofing), such as drivers license or passport
- Assign attributes [(name, address, college or university, department, role (faculty, staff, student), major, email address)]

How can you prove it? (authentication)

- Verifying that the person seeking access to a resource is the one previously identified and approved

Key Roles

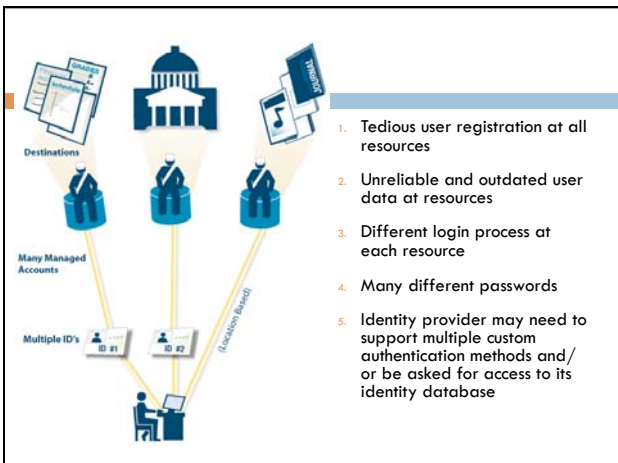
10

Three roles are involved in gaining access to a resource:

1. Subject (i.e. user) – The person identified and the subject of assertions (or claims) about his or her identity.
2. Identity Provider – Typically the college or university that maintains the identity system, identity-proofs the subject and issues a credential. Also provides assertions or claims to the service provider about a subject's identity.
3. Service Provider (sometimes called the relying party) – Owner/provider of the protected resource to which the subject would like to access. Consumes the assertion from the identity provider and makes an authorization decision.

Traditional Two-Party Approach

- The Relying Party (i.e., college/university) must do it all –
 - Identify the employee/student/guest
 - Determine whether person is acceptable for specified purpose
 - Issue a credential (e.g., employee/student ID card, UserID)
 - Establish method to correlate identified individual to the credential – e.g., a picture, a password
 - Authenticate individual for remote access e.g., does picture match?, is password correct?



The Problem

14

- Growing number of applications – on-campus and outsourced or hosted
- All of these service providers must:
 - Verify the identity of students
 - Know who's eligible to access the service
 - Know the student is active and hasn't left school
- How comfortable are you with the security and privacy of the identity data?

The Answer: Federated Identity Management

15

- Federation: An association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.
- All participants in a federation agree on the same policies and procedures related to identity management and the passing of attributes.
- Instead of one-to-one relationships, the federation allows one-to many relationships.

Federated Identity Management

16

- Parties agree to leverage the identity provider's database, rather than creating separate data stores
- Users no longer register with the service provider, using their university credentials for transactions
- Single sign-on convenience for users
- Identity provider does the authentication; service provider does the authorization
- Attributes are the key – maintain privacy and security

The diagram illustrates a central user icon at the bottom, connected to a 'Single ID' box. Above this, a 'One Home Account' box is shown. At the top, three 'Destinations' (represented by icons for a document, a building, and a book) are shown, each with a 'Verified' seal. A list of five benefits is provided to the right of the diagram.

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 and user controls privacy

InCommon Federation

18

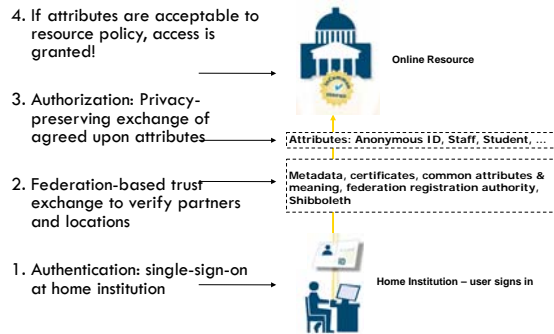
InCommon is the federation for U.S. research and education, providing higher education and their commercial and non-profit partners with a common trust framework for access to online resources.

InCommon Federation Benefits

19

- Convenience – Single sign-on with higher education credentials
- Safety – Enhanced security with fewer data spills
- Privacy – Release of only the minimum information necessary to gain access to resources (via attributes)
- Scalability – Once implemented, federated access relatively simple to extend
- Authentication – Campus does the authentication, maintaining control of user information
- Authorization – Service provider makes access decisions based on attributes

Federated Access in 30 Seconds



How Many Off-campus Applications Do You Have?




Your Current Environment(s)

- What externally hosted applications do you have?
- How do these service providers
 - Verify the identity of your constituents?
 - Know who's eligible to access the service?
 - Know the constituent is active and hasn't left?

How comfortable are you with the security and privacy of the identity data each external partner is storing?

Case Study Discussions



24 Getting Started (and Next Steps)

How Do I Start?

25

- It's not hard
 - ▣ Identify your business case
 - ▣ SAML2-implementation Identity provider
 - ▣ eduPerson schema
 - ▣ Participant Operating Practices
 - ▣ InCommon Agreement

InCommon
Home | About InCommon | Join InCommon

26 **Join InCommon**

- Participants
- IAN Online
- Education and Training
- Affiliates
- Certificate Service
- Policies and Practices
- Technical Information
- Software Guide
- Metadata and WAYF
- Site Administrator Info
- Frequently Asked Questions
- Benefits
- Site Administrator Login
- Collaboration Wiki
- Glossary
- Contact Us
- About

Current InCommon Participants

A community of more than 4.5 million end users.
(Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System, Calculated April 2010.)

Higher Education Participants (180)	Government and Nonprofit Laboratories, Research Centers, and Agencies (7)	Sponsored Partners (66)
American University Arizona State University Augustana College Ballou University Brown University California Institute of Technology California Maritime Academy California Polytechnic State University, San Luis Obispo California State Polytechnic University, Pomona California State University, Bakersfield California State University, Channel Islands	Argonne National Laboratory Energy Sciences Network (ESNet) Lawrence Berkeley National Laboratory Moss Landing Marine Laboratories National Institutes of Health National Science Foundation TeraGrid	Absolute Software, Inc. ALEKS Corporation Alexander Street Press Apple - iTunes U Atlas Systems, Inc. BioOne, Inc. Blattat Media Corporation Burton Group Cambridge University Press Cengage, Inc. Cengage Learning, Inc. Colorado Alliance of Research Libraries CSO Research, Inc. Davie County Schools

27

Federated Services: Four Areas

- Library Resources
- Teaching, Learning and Research
- Campus Support
- Higher Education Support Organizations

28

Library Services

- Ares (Atlas Systems)
- Aeon (Atlas Systems)
- BioOne
- eBook Library
- EBSCO Host
- Science Direct (Elsevier)
- Scopus (Elsevier)
- JSTOR
- RefWorks COS
- Thomson Reuters Web of Science
- WilsonWeb (H.W. Wilson Company)
- First Search (OCLC)
- OhioLINK
- Proquest Classic
- Chadwyck-Healy (ProQuest)
- CSA Illumina (ProQuest)
- Safari Books Online
- Alexander Street Press
- Cambridge University Press
- IEEE
- Serials Solutions

Teaching, Learning and Research

29

- Absorb Learning Management System
- Cengage Learning
- eLMS (e-academy)
- ActivityInsight (Digital Measures)
- CourseResponse (Digital Measures)
- iTunesU (Apple)
- TurnItIn (iParadigms)
- Learn.com
- Dreamspark (Microsoft)
- Sum Total LMS
- WebAssign
- ALEKS
- VoiceThread (collaboration)
- CTSA wiki (National Institutes of Health)

Campus Support

30

- National Student Clearinghouse Student Self-Service
- e2Campus by Omnilert – (emergency planning)
- EnergyCAP (facilities)
- CourseLeaf (Leapfrog Technologies) (catalog development)
- Burton Group (IT Research)
- Lynda.com (professional development courses)
- Interfase - CSO Research (career center software)
- Alcohol.edu
- NextGen Web Solutions (forms, scholarships, student employment)
- PeopleAdmin (human resources)
- Qualtrics Research Suite
- StudentsOnly (student discounts)
- Symplicity (career centers)
- Travel Solutions (travel)
- Trondent Development (travel)
- University Tickets
- ZimRide
- Absolute Software (IT)
- Kuali Foundation
- Cayuse (research)

Organizations

31

- EDUCAUSE
- Internet2

How Do I Start?

32

- It's not hard
 - Identify your business case
 - SAML2-implementation Identity provider
 - eduPerson schema
 - Participant Operating Practices
 - InCommon Agreement

A Few SAML 2 Implementations

33

- Open Source
 - Shibboleth Single Sign-on and Federating Software
 - SimpleSAMLphp
 - Guanxi
- Corporate
 - Oracle Identity Federation
 - Netegrity SiteMinder

InCommon Affiliate Program

34

- Connect campus interested in getting help with corporate partners with federated-related products or services
 - AegisUSA – Federated appliances
 - Gluu – Outsourced Identity Providers
 - Microsoft – Federated consulting
 - Unicon – Shibboleth consulting, support, and integration

How Do I Start?

35

- It's not hard
 - Identify your business case
 - SAML2-implementation Identity provider
 - eduPerson schema
 - Participant Operating Practices
 - InCommon Agreement

eduPerson Schema

36

- Standard for InCommon Attribute Exchange
 - Directory schema
 - Attribute definition
 - middleware.internet2.edu/eduperson/

How Do I Start?

37

- It's not hard
 - Identify your business case
 - SAML2-implementation Identity provider
 - eduPerson schema
 - Participant Operating Practices
 - InCommon Agreement

Participant Operating Practices

38

- Tell others how you manage the creation and use of electronic credentials
- Service Providers care about campus practices
- Emerging standards for higher value services
 - ▣ Financial
 - ▣ Federal Government

How Do I Start?

39

- It's not hard
 - ▣ Identify your business case
 - ▣ SAML2-implementationidentity provider
 - ▣ eduPerson schema
 - ▣ Participant Operating Practices
 - ▣ InCommon Agreement and fee
 - www.incommon.org/docs/policies/participationagreement.pdf

InCommon Certificate Service

40

- Service developed by and for the higher education community. InCommon is a non-profit, community-governed organization – the primary driver is to provide value to the community.
- Unlimited SSL certificates now. Future will include personal certificates (for signing, encryption, code signing and authentication).
- One fixed annual fee.
- One publicly signed certificate source for all campus servers and domains
- Includes all domains owned by the college or university – such as professional organizations or athletic sites (including any .org, .com, .net or others).
- Internet2 members receive a 25 percent discount

Workshops and Training

- IAM Online – Monthly presentations on identity and access management. www.incommon.org/iamonline
- CAMP and Day CAMP – Conferences focused on federated identity and access management. www.incommon.org/camp
 - Day CAMP: Getting Started with the InCommon Federation
November 4/5 Atlanta, GA
- Affiliate Program – Linking higher ed with partners able to help build the necessary underlying infrastructure that supports federated access. www.incommon.org/affiliate
- Shibboleth Workshop Series – Intensive workshops on installation and management of Shibboleth Single Sign-on and Federating Software. www.incommon.org/educate/shibboleth
 - Identity and Service Provider Workshops
November 9/10 at Lafayette College, Easton, PA

EDUCAUSE InCommon Sessions

42

- Wednesday
InCommon Federation Meeting
4:30pm - 6:00pm (Meeting Room 201B/C)
- Thursday
IAM Working Group Community Update
(Educause presentation about joining InCommon/Simulcast as IAM Online)
1:00pm - 1:50pm (Meeting Room 211A)
- The InCommon Federation: What's New in the Community?
4:30pm - 5:20pm (Meeting Room 205B)
- Friday
Getting Started with Federations: Build or Buy?
9:30am - 10:20am (Meeting Room 210D)

Questions?

43

- Tracy Mitrano, Cornell University
tbm3@cornell.edu
- John O'Keefe, Lafayette College
okeefej@lafayette.edu
- Justin Sipher, Skidmore College
jsipher@skidmore.edu
- Ann West, InCommon/Internet2/
Michigan Tech/Penn State
awest@internet2.edu
