IDENTITY AND THE CLOUD: PREPARING YOUR CAMPUS

October 12, 2010 EDUCAUSE Annual Conference

Your Speakers Today

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

Hi from all of us!

Agenda Today

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

- 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, Flicker, …)

Details and Examples of Clouds

<table>
<thead>
<tr>
<th>Cloud Market Type</th>
<th>Type of Offering</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-as-a-Service</td>
<td>2) High internal application websites</td>
<td>Amazon EC2, Google App Engine</td>
</tr>
<tr>
<td></td>
<td>3) Web-based email, salesforce</td>
<td>Salesforce.com, Gmail</td>
</tr>
<tr>
<td></td>
<td>4) Cloud-based office productivity</td>
<td>Microsoft Office 365, Google Apps</td>
</tr>
<tr>
<td></td>
<td>5) Client apps that connect to services in the cloud</td>
<td>Salesforce.com, Google Apps</td>
</tr>
<tr>
<td>App-Container-as-a-Service</td>
<td>1) Mobile app container services for deployment</td>
<td>Amazon ElastiCache, Google App Engine</td>
</tr>
<tr>
<td></td>
<td>2) Cloud software services that can be used to create new services, as in a napkin</td>
<td>Salesforce.com, Google Apps</td>
</tr>
<tr>
<td>Platform-as-a-Service</td>
<td>1) Development-platform-as-a-service</td>
<td>Microsoft Visual Studio Online, Google App Engine</td>
</tr>
<tr>
<td></td>
<td>2) Production-platform-as-a-service</td>
<td>Amazon EC2, Microsoft Azure</td>
</tr>
<tr>
<td>Infrastructure-as-a-Service</td>
<td>1) Virtual services</td>
<td>Amazon EC2, Microsoft Azure</td>
</tr>
<tr>
<td></td>
<td>2) Web services</td>
<td>Amazon EC2, Microsoft Azure</td>
</tr>
<tr>
<td>Physical Infrastructure</td>
<td>1) Software as a Service</td>
<td>Amazon EC2, Microsoft Azure</td>
</tr>
<tr>
<td></td>
<td>2) Cloud storage</td>
<td>Amazon S3, Google Cloud Storage</td>
</tr>
<tr>
<td></td>
<td>3) Cloud database</td>
<td>Amazon RDS, Google Cloud Database</td>
</tr>
</tbody>
</table>

The Role of Cloud in Campus IT

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

Not exactly....
The New IT

- 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

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

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?

- Tedious user registration at all resources
- Unreliable and outdated user data at resources
- Different login process at each resource
- Many different passwords
- Identity provider may need to support multiple custom authentication methods and/or be asked for access to its identity database
The Problem

- 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

- 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

- 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
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

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

- 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

1. Authentication: single-sign-on at home institution
2. Federation-based trust exchange to verify partners and locations
3. Authorization: Privacy-preserving exchange of agreed upon attributes
4. If attributes are acceptable to resource policy, access is granted!

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?
Case Study Discussions

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

Getting Started (and Next Steps)

How Do I Start?

- It’s not hard
  - Identify your business case
  - SAML2-implementation Identity provider
  - eduPerson schema
  - Participant Operating Practices
  - InCommon Agreement
Federated Services: Four Areas

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

Library Services
- Ares (Atlas Systems)
- Aeion (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

- Absorb Learning Management System
- Cengage Learning eLMS (e-academy)
- Activity Insight (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

- National Student Clearinghouse Student Self-Service
- e2Campus by Omnilert – (emergency planning)
- EnergyCAP (facilities)
- CourseLeaf (leepfrog Technologies) (catalog development)
- Burton Group (IT Research)
- Lynda.com (professional development courses)
- Interfase - CSO Research (career center software)
- AlcoholEdu
- 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

- EDUCAUSE
- Internet2
How Do I Start?

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

A Few SAML 2 Implementations

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

InCommon Affiliate Program

- 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?

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

eduPerson Schema

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

How Do I Start?

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

- 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?

- It's not hard
  - Identify your business case
  - SAML2-implementation
  - Identity provider
  - eduPerson schema
  - Participant Operating Practices
  - InCommon Agreement and fee
    - [www.incommon.org/docs/policies/participationagreement.pdf](http://www.incommon.org/docs/policies/participationagreement.pdf)

InCommon Certificate Service

- 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

- 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?

- 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