IAM Online

The Challenges of User Consent

Wednesday, May 11, 2011 – 3 p.m. ET

Tom Barton, University of Chicago
Steve Carmody, Brown University
Russell Beall, University of Southern California
Tom Scavo, InCommon

Please note: you will not hear any audio until the session begins
Why InCommon?

- The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States.

- What this means to me as a user:
  
  *I can use the credentials provided to me by my organization to gain access to systems and services from others in the federation*

- What this means to me as a Service Provider:
  
  *I can outsource user account management to Identity Providers (Higher Eds, National Labs) and implement one authentication interface that supports many customers*
# Current InCommon Participants

A community of more than 5 million end users.

(Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System. Calculated October 2010.)

<table>
<thead>
<tr>
<th>Higher Education Participants (209)</th>
<th>Government and Nonprofit Laboratories, Research Centers, and Agencies (8)</th>
<th>Sponsored Partners (73)</th>
</tr>
</thead>
<tbody>
<tr>
<td>American University</td>
<td>Argonne National Laboratory</td>
<td>Absolute Software, Inc.</td>
</tr>
<tr>
<td>Arizona State University</td>
<td>Energy Sciences Network (ESNet)</td>
<td>ALEKS Corporation</td>
</tr>
<tr>
<td>Augsburg College</td>
<td>Fermi National</td>
<td>Alexander Street Press</td>
</tr>
<tr>
<td>Ball State University</td>
<td></td>
<td>Apple - iTunes U</td>
</tr>
<tr>
<td>Baylor College of Medicine</td>
<td></td>
<td>Atlas Systems, Inc.</td>
</tr>
<tr>
<td>Baylor University</td>
<td></td>
<td>BioOne, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blackboard, Inc.</td>
</tr>
</tbody>
</table>
Federation value proposition: do the math

- Without Federation
  
  \[209 \text{ HEs } \times (78+8) \text{ Service Providers}\]
  
  \[= 17,974\] bilateral custom integration & service agreements

- With Federation
  
  \[(209 \text{ HEs } + 86 \text{ Service Providers}) \times 1 \text{ Federation}\]
  
  \[= 295\] standard integration agreements

*Federations create a place for inter-organizational transactions to happen at scale*
Two impediments to scaling

- Service Providers whose transactions have associated risk
  
  *How can I outsource user account management to Identity Providers and still manage my liability?*
  
  - InCommon’s Identity Assurance program (Silver) mitigates the risk of an authentication error

- Service Providers whose transactions need user attributes
  
  *Do I have to ask 209 Identity Providers to release name, email, and affiliation of their users to me? How?*
  
  - The basis for one approach is the subject of today’s IAM Online
Presenters

• Steve Carmody, Sr. IT Architect, Brown University
• Russ Beall, Director, ITS Enterprise System Development, University of Southern California
• Tom Scavo, Operations Manager, InCommon Federation
Agenda

• Introduction and Context
• Problem Definition
• Proposed Approach
• Demo!
• "Making this happen"
  – Evolve Campus Attribute Release Policy
  – Federation Extend Metadata Management Tool
  – IDP Technology -- Implement User Consent Extension for Shibboleth (uApprove)
• Next Steps
• Wrapup
### Problem Definition

- Continuing the Evolution of Higher Ed/Research Interop

<table>
<thead>
<tr>
<th>Federations</th>
<th>Scaleable Trust and Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>eduPerson</td>
<td>Standard Attributes</td>
</tr>
<tr>
<td>InCommon Silver</td>
<td>Higher Levels of Assurance</td>
</tr>
<tr>
<td>Managing</td>
<td>… Our Next Task…</td>
</tr>
<tr>
<td>Attribute Release</td>
<td></td>
</tr>
</tbody>
</table>
The Original Shibboleth Use Cases (2001 ?)

- Member of campus community accessing licensed resource
  - Anonymity required
- Member of a course accessing remotely controlled resource
  - Anonymity required
- Member of a workgroup accessing controlled resources
  - Controlled by unique identifiers (e.g. name)
- Intra-campus - crossing political boundaries
  - Controlled by unique identifiers (e.g. name)

- Taken individually, each of these situations can be solved in a variety of straightforward ways.
- Taken together, they present the challenge of meeting the user's reasonable expectations for protection of their personal privacy while respecting the content provider’s need for accountability.
Collaboration Use Case

• We now need a scaleable approach to use case 3
  – campuses/users releasing attributes to support the authentication/authorization requirements of collaborative work

• Note… despite widespread rumor..
  • Shibboleth ≠ Anonymous Access
Why is this a Problem?

• Currently, for ALL campuses, the default attribute release policy is “opaque identifier only”.
  – releasing any PII requires manual intervention by the IDP admin
• For every SP site requiring attributes -- a policy must be approved and then implemented
• This approach will work for contractual situations (eg outsourced business systems)
• This approach is overly bureaucratic when the release decision is made by an IDM stakeholder (eg the Registrar)
Why is this a Problem?

• This approach is unworkable in collaboration situations (e.g., researcher accessing a VO site, accessing a site shared among their peers).
• Also unworkable with some vendor sites (especially when there is no contract between the vendor and the campus).
• In these situations, users will use social identities, which are not constrained by default campus policy.

• Goal -- make it easier for users, campuses, and IDP admins to manage the release of attributes beyond the basic opaque identifier, in appropriate situations, consistent with site policy.
Why is This Use Case Important?

• Collaboration among researchers is a core business for Higher Ed
• The campus has a vested interest in having a researcher’s “campus identity” associated with their work
• Some projects (eg Bamboo) will require a campus identity in order to access certain information
Proposed Approach

- The campus establishes global policy
  - Will release certain attributes IF the user approves the release (call this set the "consent policy group")
  - IDP admin implements this policy once
  - This approach is FERPA compliant
- The Federation facilitates SPs using metadata to request certain attributes
  - New metadata management tools
- The first time a user accesses an SP...
  - If the attributes requested by the SP are a subset of the consent policy group, then the user is asked to consent to the release
  - This occurs without any involvement from the IDP admin
Demo!
University of Southern California
uApprove Demo

Russell Beall
Senior Programmer/Analyst
Information Technology Services
University of Southern California
Los Angeles, California, USA
beall@usc.edu
Basics

- Developed by SWITCH – the Swiss Federation
- Two components:
  - Plugin to the Shibboleth IdP
  - Separate webapp to serve consent pages
- Provides:
  - Terms of service for login system
  - User consent for attribute release
  - Blacklist/whitelist for both SPs and attributes
Links

- uApprove:
  - http://www.switch.ch/aai/support/tools/uApprove.html

- USC:
  - http://www.usc.edu

- Russell Beall:
  - beall@usc.edu
Making This Happen

- Evolve Campus Attribute Release Policy
- Federation Extends Metadata Management Tool
- IDP Technology -- User Consent Extension for Shibboleth (uApprove)
• Current ‘standard’ policy
  – By default, Brown will only release a unique opaque identifier to 3rd party service providers. The unique identifier will be different for each service provider accessed by a user.
• A Policy Supporting Collaborative Work
  – Will release certain attributes, in appropriate situations, IF the user approves the release (call this set the "consent policy")
  – Draft Brown Policy
    • For 3rd party Service Providers that are federated with Brown via InCommon, or Brown sites that are not certified by the University Identity & Access Management Steering Committee (UIAMSC), the IdP will release first name, last name, email, university affiliation, and NetID scoped to Brown (e.g. Josiah_Carbury@brown.edu) with the consent of the user. On first access to a particular Service Provider (SP), users are made aware of the attributes that may be disclosed to it, along with their current values, and asked to approve this disclosure. This dialog screen will be repeated any time that the list of attributes or their values being disclosed to a particular SP changes.
• SAML 2 Metadata allows SPs to include RequestedAttribute elements
  – List the attributes the SP requires
• InCommon Metadata Management Tool being Extended to Allow SPs to Enter These Values
Making This Happen - New Federation Tools

- <AttributeConsumingService index="1">
  - <ServiceName xml:lang="en">Internet2-Hosted Federated Wiki</ServiceName>
  - <ServiceDescription xml:lang="en">
      - A shared Wiki service with automatic registration for users who can supply a supported identifier, such as eduPersonPrincipalName or swissEduPersonUniqueID.
  - </ServiceDescription>
  - <RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:mace:dir:attribute-def:eduPersonPrincipalName" NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
  - <RequestedAttribute FriendlyName="mail" Name="urn:mace:dir:attribute-def:mail" NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
  - <RequestedAttribute FriendlyName="displayName" Name="urn:mace:dir:attribute-def:displayName" NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
  - <RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  - <RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  - <RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  - </AttributeConsumingService></SPSSODescriptor>
Making This Happen - New Federation Tools

• Demo -- new InCommon Metadata Management Tool
InCommon Site Admin: InCommon LLC

trscavo@internet2.edu (Logout)

New User Interface Element
* Denotes a required field

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Keywords</td>
<td></td>
</tr>
<tr>
<td>Information URL</td>
<td></td>
</tr>
<tr>
<td>Privacy Statement URL</td>
<td></td>
</tr>
<tr>
<td>Logo URL</td>
<td></td>
</tr>
</tbody>
</table>

Save  | Cancel

Please contact ri-admin@internet2.edu if you have any questions.
• User Consent Extension for Shibboleth (uApprove)
  – Developed by SWITCH (the SWISS Federation)
  – http://www.switch.ch/aai/support/tools/uApprove.html
• Adds “user consent” screens to the IDP flow
• Standard version requires manual configuration of attribute filters
• Includes “Attribute In Attribute Requester's Metadata” Plugin
  – “metadata driven release filter”
  – Allows release to be driven from SP Requested Attribute elements
  – Will only release an attribute if the SPs metadata requests it
  – ?? Role of federation in vetting SP metadata ???
Installing uApprove

• Good documentation!
• Requires a database to store consent data…
• Define new Attribute Filters for “consent policy group” of attributes
An Interesting Idea …

• The French Federation is assigning SPs to categories
  – https://services-federation.renater.fr/liste?action=view_all&type=sp&federation=renater&lang=en

• Their List of Categories
  – e-learning resource
  – groupware service
  – e-documentation (licensed information)
  – software providing
  – business application
  – wi-fi service
  – institutional web site
An Interesting Idea …

• Each category has a “recommended” set of attributes that a campus IDP should release

• A Possible Approach to Managing Release
  – Federation TAGs an SP’s metadata element to indicate its category
  – Campus can configure its IDP to release Attributes X, Y, and X for Category 1 …
Next Steps

- We’re all in this together…
- InCommon has to
  - deploy new metadata management tool
- SPs have to
  - add RequestedAttribute elements to their Federation metadata
  - … perhaps InCommon outreach could “encourage” SPs
- IDPs have to
  - create new global policy
  - deploy uApprove extension in their IDPs
  - train users on what to expect
• Have already joined together in an informal “Inc-Consent Working Group” to share experiences and help on another...
For more information...

• Email to
  – incommon-participants@incommonfederation.org
  – Steven_Carmody@brown.edu
Upcoming Events

Advance CAMP: Identity Services Summit III
www.incommon.org/camp

CAMP: Hot Topics in Identity and Federated Identity Management
June 21-23, 2011 – Columbus, Ohio
www.incommon.org/camp
Survey
Please complete the survey about today’s IAM Online:
http://www.surveymonkey.com/s/829BM2S

Next IAM Online www.incommon.org/iamonline
Wednesday, June 8, 2011 – 3 p.m. EDT
Tentative: InCommon Identity Assurance Profiles

New! IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

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