Accepting Social Identities: Integration With SAML and Deployment

Wednesday, February 13, 2013 – 3 p.m. ET

Steve Carmody, Brown University
Paul Caskey, University of Texas System
Dedra Chamberlin
Renee Shuey, Penn State, Host and Moderator

Thank you to InCommon Affiliates for helping to make IAM Online possible.
Why the Interest in Social Identities?

• We’re used to working with identities vetted and issued by other campuses
• But, we already work with people from outside those communities
  • Applicants
  • Parents
  • Continuing Ed/MOOCs
• Other areas now showing interest in working with people from outside of Higher Ed
  • Courses – additional speakers from the community
  • Research – partners at campuses that are not Shibboleth-enabled
Why the Interest in Social Identities?

- All of those people have identities at one of the social/personal providers
  - Google, Yahoo, FaceBook, etc
- In some circumstances, this approach may be preferable to issuing campus identities to those people
- However, there is NO guarantee about who is using a social account
Federated Identity Concept

Institution A

Institution B

Shared Courses
Adding Social Identities

Institution A

Institution B

Social-to-SAML Gateway

Google

Yahoo

Shared Courses

2/13/13
Agenda

• The pilot Social-to-SAML Gateway (Paul Caskey)

• Brown’s experience with the gateway and plans for social identity (Steve Carmody)

• An open-source approach and the potential for a hosted gateway (Dedra Chamberlin and Lucas Rockwell)
Social2SAML: What Is It?

• Web-based authentication gateway ([FAQ][1])

• Translates authentication responses from popular “social” ID services into regular SAML 2 assertions (consumable by Shibboleth)

• Allows downstream applications which only understand SAML (most versions of Shibboleth), to easily utilize external services without changing the operating environment

• Designed to be as simple and transparent as possible
Social2SAML: How Does It Work?

• Looks like an IdP to your SP. Looks like a single “SP/app” to external services.

• Consumes InCommon metadata (so your SP may already be trusted by the gateway).

• It is *not* in the InCommon metadata (so your SP will need to add appropriate metadata for the gateway [2] to its config)

• Runs a slightly customized version of SimpleSAMLPHP [3]
Social2SAML: How Does It Work? (cont)

- “Per-service” versus “Multi-Auth” logical IdPs?
- Works with these services:
  - Google
  - LinkedIn
  - WindowsLive
  - VeriSign
  - PayPal
  - Facebook
  - Twitter
  - Yahoo
Social2SAML: How Does It Work? (cont)

• Mapped Attributes (if released by service/user)
  – givenName
  – sn
  – mail
  – uid

• Generated Attributes
  – eduPersonPrincipalName
  – eduPersonTargetedID (as a SAML 2 NameID)
  – displayName

• Details here: [2]
Social2SAML: How Is It Used?

• Works great for guest authentication!
• Typical use is “pick-and-choose” among the external services and then include the different logical IdPs’ metadata in your SP’s metadata config.
• Links for metadata – both multi-auth and individual services are found here: [2]
• Even more powerful when combined with invitation capabilities (Grouper, CO-Manage)
Social2SAML: Moving Forward...

• Pilot ends at the end of May 2013!

• Join the discussion ([here][4])
  - What would a service like this from InCommon look like?
  - Would it have invitation/registration capabilities?
  - How seamless and transparent can it be?
  - How should certain attributes be treated (identifiers, namely)?

• Give Feedback ([here][5])
Links

• [1] https://spaces.internet2.edu/display/socialid/Social-to-SAML+Gateway+FAQ


A Social-to-SAML Pilot at Brown

Steve Carmody
February 13, 2013
Goal

- Familiarize ourselves with the concepts
- Learn about the deploy and manage process
  - Reconfigure a test SP to use the Gateway
- Write down what we learned
- Evaluate the results
Implementation Steps

• Found in FAQ
  – https://spaces.internet2.edu/x/GAAEAg

• https://spaces.internet2.edu/display/socialid/Social-to-SAML+Gateway+FAQ - Social-to-SAMLGatewayFAQ-HowcanIusetheGatewaywithmyapplication%3F
Implementation Steps

• Install the Shibboleth SP or use an existing deployment.
  – https://wiki.shibboleth.net/confluence/display/SHIB2/Installation

• Install the Discovery Service component bundled with the SP.
  – No executables; just javascript and CSS
  – https://wiki.shibboleth.net/confluence/display/SHIB2/DSInstall

• Make sure the SP is a member of the InCommon Federation, adding it to InCommon metadata if necessary. (This is because the Gateway consumes InCommon metadata.) https://incommon.org/
Implementation Steps

• Choose which social providers you want to use. (A list of supported social providers is given on the Social-to-SAML Gateway Demo page.)
  – https://samlgwtasth.eotislab.com/servDetails.html

• Configure the SP to load metadata for the chosen social providers. (Metadata files are linked on the Social-to-SAML Gateway Demo page.)
  – <!-- load metadata for social-saml GW -->
    – <MetadataProvider type="XML" file="/path/social-all.xml"
      – legacyOrgNames="true" >

• Configure the SP (and possibly the application) to consume the attributes provided by the chosen social providers. (In particular, some social providers assert long, opaque identifiers.)
Try the Demo Yourself!

- https://grouperdemo.internet2.edu/
What Did We Learn?

- Incredibly easy to deploy and configure - Thank you Paul!
- It’s a new experience for people used to using Social Accounts
- Also used with MACE Grouper - support for external groups
  - Social Providers don’t release enough info to pre-populate the Registration page
Issues

• Consent screen at Social Providers asks user to release attributes to the Gateway, not the SP
• Each Social Provider provides different attributes
• Many applications prefer an invitation service (e.g., MACE Grouper includes one)
  – Should this be part of a central service?
• Should a locally run Gateway instance integrate with the local Person Registry, and register different providers/accounts for each person
Another OpenSource Social2SAML Gateway

Dedra Chamberlin
How is New Gateway Different?

• SP configured directly with Social IdP
• Provides more clarity to users when electing to release attributes
• Ensures that one SP experiencing high volume does not adversely affect other SPs
Hypothetical Example:

Student Billing System used by Students and Parents
Student Requests Access

- Canvas
- Confluence
- Alresco
- Student Billing
- Admissions
- Parking

Discovery

Social2SAML Gateway

Campus IdP

Social2SAML Gateway

- Google
- Yahoo
- LinkedIn
- Twitter
- Facebook
Re-Direct to Campus IdP
Parent Requests Access

Canvas  Confluence  Alresco  Student Billing  Admissions  Parking

Discovery

Social2SAML Gateway

Campus IdP

Google  Yahoo  LinkedIn  Twitter  Facebook
Re-Direct to Social2SAML Gateway

Pilot Gateway Attribute Release

Canvas
Confluence
Alresco
Student Billing
Discovery
Admissions
Parking

Social2SAML Gateway

Google
Yahoo
LinkedIn
Twitter
Facebook

Campus IdP
Re-Direct to Social2SAML Gateway
New Gateway Attribute Release
Mock Moodle Integration

1. Google using global gateway model
2. Twitter using Service Provider specific model
Global Gateway
Configured with Google

Canvas
Confluence
Moodle
Student Billing
Admissions
Parking

Social2SAML Gateway

Campus IdP

Google
Yahoo
LinkedIn
Twitter
Facebook
Accounts

Samigwteet.theotislab.com is asking for some information from your Google Account. To see and approve the request, sign in. Learn more

Sign in

Email

Password

Sign in Stay signed in

Can't access your account?
SP Specific Gateway
Configured with Twitter
You can use your Twitter account to sign in to other sites and services. By signing in here, you can use UNC Moodle Demo without sharing your Twitter password.

Authorize SomeU Moodle Demo to use your account?

This application will be able to:
- Read Tweets from your timeline.
- See who you follow.

Username or email
Password

[ ] Remember me · [link] Forgot password?

[Sign In] [Cancel]

This application will not be able to:
- Follow new people.
- Update your profile.
- Post Tweets for you.
- Access your direct messages.
- See your Twitter password.

SomeU Moodle Demo
moodle.someu.edu
SomeU Moodle Demo for the SocialIdP Gateway
Social IdP Rate Limits

API limits applied to each SP independently
Bills are Due!

Canvas  Confluence  Alresco  Student Billing  Admissions  Parking

Social2SAML Gateway  Campus IdP

Google  Yahoo  LinkedIn  Twitter  Facebook
Multiple AuthN Requests in Short Time Window

Canvas  Confluence  Alresco  Student Billing  Admissions  Parking

Discovery

SAML

Social2SAML Gateway

Campus IdP

Google  Yahoo  LinkedIn  Twitter  Facebook
Social IdP blocks all authN Requests to Gateway

Canvas    Confluence    Alfresco    Student Billing
          Discovery
          SAML

Social2SAML Gateway

Campus IdP

Google    Yahoo    LinkedIn    Twitter    Facebook

39
Social IdP blocks authN Requests to Single SP

Canvas Confluence Alresco

Student Billing

Admissions Parking

Canvas Confluence Alresco Student Billing Admissions Parking

Social2SAML Gateway

Campus IdP

Google Yahoo LinkedIn Twitter Facebook

Discovery SAML
New Guest Logs in to Different SP

Canvas  Confluence  Alresco  Student Billing  Admissions  Parking

Discovery  Discovery

SAML  Social2SAML Gateway

Google  Yahoo  LinkedIn  Twitter  Facebook

Campus IdP
Rate-Limit for First SP Doesn’t Impact the Second
Service Provider Configuration Tool
Delegated Admin for Config Management Tool

- Configuration management tool leverages InCommon metadata
- Admins log in with institutional identity
- SAML assertion includes email address
- Only users with email addresses associated with SPs in metadata allowed to configure SPs
Social IdPs

SocialIdP

Social/SAML Gateway

OAuth to SAML

SAML

SP config info

SocialIdP Management App

AuthZ admins via InCommon metadata

InCommon

Metadata

Discovery Service

moodle.someu.edu

SP config info

moodle.someu.edu administrator

Higher Ed IdPs

SAML

Discovery Service

moodle.someu.edu

moodle.someu.edu administrator

Guest Lecturer

or

Guest Seminar Enrollee

Student

or

Instructor
Configuring the SP

- SP administrators must enter Oauth Key and secret generated by Social IdP
- Configuration management tool includes Social IdP to MACE Dir attribute mapping
Login

Choose your IdP and log in.

Choose
Login

Choose your IdP and log in.

Select Provider

Higher Ed Providers

- Case Western Reserve University
- Clemson University
- Dartmouth College
- Duke University
- InCommon Operations
Manage moodle.someu.edu/shibboleth-sp

Google (OAuth2)

Configure  Attribute Map  Logs

OAuth Key and Secret

Key  OAuth Key
Secret  OAuth Secret

Enable

In order to use this Identity Provider with SocialIdP, it must be enabled.

Enable this SP?  

Save  Reset
Manage moodle.someu.edu/shibboleth-sp

Overview
- AOL
- Facebook
- Google (OpenID2)
- Google (OAuth2)
- Linkedin
- Twitter
- Windows Live

Twitter

Configure  Attribute Map  Logs

OAuth Key and Secret

Key  k2B9jV7VjPlPfIThaJ0aF
Secret  R1jyvFBzk74KL1vzosgJNKzAf35z8G3Qo1E

Enable

In order to use this Identity Provider with SocialIdP, it must be enabled.

Enable this SP?  ✔

Save  Reset
### Google (OpenID2)

<table>
<thead>
<tr>
<th>Google Attribute</th>
<th>SAML/MACE Dir Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://axschema.org/namePerson/first">http://axschema.org/namePerson/first</a></td>
<td>givenName</td>
</tr>
<tr>
<td><a href="http://axschema.org/namePerson/last">http://axschema.org/namePerson/last</a></td>
<td>sn</td>
</tr>
<tr>
<td><a href="http://axschema.org/contact/email">http://axschema.org/contact/email</a></td>
<td>mail</td>
</tr>
<tr>
<td>openid</td>
<td>eduPersonPrincipalName</td>
</tr>
</tbody>
</table>
## Attribute Map

<table>
<thead>
<tr>
<th>Twitter Attribute</th>
<th>SAML/MACE Dir Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>twitter_screen_n_realm</td>
<td>eduPersonPrincipalName</td>
</tr>
<tr>
<td>twitter_targetedID</td>
<td>eduPersonTargetedID</td>
</tr>
<tr>
<td>twitter.name</td>
<td>displayName</td>
</tr>
<tr>
<td>twitter.screen_name</td>
<td>uid</td>
</tr>
</tbody>
</table>
What’s Missing?
Invitation/Registration Service

• Most SPs don’t want to allow anyone with a Google or Twitter identity to log in
• Who can “invite” or “register” guests?
• Where do registered guests land in campus IDMS? Registry? LDAP? Grouper?
• How important is account linking?
  – More than one social ID to one person
  – Social ID(s) to an institutional ID
Concerns

• Google integration options – OpenID? OAuth? Complexity varies greatly

• Campus-specific gateways-a better option than Central Higher Ed gateway
  – OpenID requires integration with realm
  – Attribute mapping standards
  – Create identities to use elsewhere on campus
  – As a rule, tie the gateway as close to the SP as possible
What Next?

• How to help campuses deploy gateway services?
  – Make new Social2SAML gateway code available
  – Provide a supported gateway service campuses can run locally
  – Provide managed, cloud-hosted gateway services campuses can subscribe to
  – Provide a tool that can easily configure simpleSAMLphp to run alongside any Shib integrated Service Provider to operate as a gateway

• We’re seeking pilot campuses or Service Providers to explore all of the above
If you’d like to:

• Help define requirements for an invitation service
• Play with the new gateway code when it’s ready
• Learn more about possible options for how this gateway might be offered as a service

Email:

socialidentity <socialidentity@internet2.edu>
Evaluation
Please complete the evaluation of today’s IAM Online: http://www.surveymonkey.com/s/IAMOnline_February_2013

Next IAM Online – March 13, 2013 (3 pm ET)
Three Campus Case Studies of Managing Access with Grouper
• Carnegie Mellon University
• University of Montreal
• University of Wisconsin-Madison

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.

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