Social2SAML: Accepting Social Identities for InCommon Federated Services

Wednesday, December 12, 2012 – 3 p.m. ET

Catherine Zabrisky, Brown University
Michael Gettes, Carnegie Mellon University
Jim Basney, National Center for Supercomputing Applications
Paul Caskey, University of Texas System
Steve Carmody, Brown University

Thank you to InCommon Affiliates for helping to make IAM Online possible.
We’re all building a global identity services network

- Campus IAM
- Identity Federations
- Tools and practices development
- Standards
- International Coordination
- Community support and development
Layers of Campus IAM

Identities
- Registries of who/what, identifiers, attributes, system integration

Credentials and authentication
- Internal, external
- Linked to identity

Access management
- Roles, rules, entitlement, affiliation, groups, privileges, policy, authority, delegation
We’re used to working with identities vetted and issued by other campuses.

Increasingly there is interest in working with people from outside of Higher Ed.

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
Today’s Speakers

Catherine Zabriskie
   Director, Academic Technology Services, Brown University

Michael Gettes
   Assistant Director, Identity Services, Carnegie Mellon University

Jim Basney
   Senior Research Scientist, National Center for Supercomputing Applications (operator of CILogon)

Paul Caskey
   Chief Technology Officer, University of Texas System
Agenda

• How are campuses/services planning to use Social Identities?

• Introduction to the pilot Social-to-SAML Gateway
Unmet need

Easy way to provide access to course tools to individuals outside of the immediate Brown community.
Use Cases

- Online courses to pre-college students.
- Online communities engaging program participants using Brown course tools.
- Open online courses such as MOOCs.
- Brown instructors invite guest instructors to join a course.
- Non-Brown students audit Brown courses.
- Cross-listed courses across multi-institutions share Brown course tools.
Communities of Users

- Pre-college
- Adult learners
- Non-Brown undergraduates
- Professionals
- Instructors
- Faculty
- Artists
- Anyone
Functional requirements

- Non-Brown affiliates **easily self-enroll**;
- **On-going access** - not limited to semester or year;
- Administrator or instructor **easily invites participants**;
- **Integration with our group management solution.**
Participant identifies social credential → Social to SAML Gateway → Course spaces within Tools

Participant logs in with social credential

Access Course Tools

Registration
Criteria- Social to SAML Gateway

- Users have **no long-term relationship to Brown**.
- Users have **no physical presence** at Brown.
- May or **may not be associated with a higher-ed institution**.
- Use requires **no need to validate the individual’s identity**.
- **No credit or grades offered**.
- Value to leveraging group management tool to manage access to a broader set of services.
Issues with this approach

- Requires participants to have a social account.
- Participants of institutions using google may be confused.
- Participant must register in addition to accessing – may be confusing.
- Not as easy as self enrollment at tool level.
Status

- Confirming business practice and technical process.
- Spring semester, 2013 - in place for pilot use
Tartan-ConnectID
(social2saml gateway)

Identity Services Team
Carnegie Mellon University
December, 2012
First App(s)

• My Plaid Student
  – Parents to access Student Invoices
  – go live was July, 2011
  – Later... Bill Pay, Class schedule, Grades, etc.
    • Sep 2011 – 500 users, no marketing to students
    • Dec 2012 – 1426 users, about 20 reported probs

• A generic invitation service for collaborators on projects (wikis and such)
  – identity.andrew.cmu.edu/tartan-connectid-invite
  – sp-prod.andrew.cmu.edu (test application)
Interesting Features

• OpenID (+ Others) Gateway to SAML/InCommon
• Invitation only, by CMU community.
• Tartan-ConnectIDs added to local IdM.
  – Will allow for Groups/Permissions mgmt later.
• Spent reasonable time on legal concerns
• Tartan-ConnectID IdP is in InCommon now.
Implementation

• SOAP services exposed to app.
• Need simpler RESTful interfaces going forward; If use cases warrant. Now interested in Caskey’s solution
• Apps should never show username

https://me.yahoo.com/a/gDwvIn03stsPlIo3YPUGMeIa2THCy#62d2f@affiliates.cmu.edu
Tartan-ConnectId User Flow

A Social 2 SAML Gateway
For Carnegie Mellon University
July 2012
Authenticated invite

Welcome to Tartan-ConnectID

Tartan-ConnectID allows you to invite people from outside the Carnegie Mellon University community to use certain services inside CMU and even around the higher education community. A service is Tartan-ConnectID enabled if the service has been registered into the InCommon Federation. Most CMU services, if protected by Web Login, will be registered into InCommon. If you are unsure whether or not the service you want to invite people to use will work with Tartan-ConnectID, please contact those responsible for the service.

By filling in the requested information below you will be sending an invitation to the email addresses you provide. The invitation will appear to come from you. A standard message is included in the invitation but you can also add some additional text to the invitation. We do not allow you to add HTML to the invitation. The people you invite will have 7 days to respond to the invitation. Problems processing the invitation are usually resolved by re-inviting people.

You may enter up to 10 email addresses separated by commas.

Email address(es):

gottes@gmail.com

testing

Personal message:
(max 500 chars)

493 characters left

Send Invitation

Need Help?
Authenticated invite response

Your invitations have been sent to the following email addresses:

- gettes@gmail.com
Michael Gettes has invited you to register with Carnegie Mellon University’s Tartan-ConnectID service. Tartan-ConnectID allows you to access secured websites at CMU where you have been granted access. You will register using an account from one of the supported Third Party Identity Providers.

* * * * Personal Message from Michael Gettes

testing

* * * * * * * * * * * * * * * * * * * * * * * * * * *

Click on this link to complete the registration process (or copy and paste it to your browser):
https://identity.andrew.cmu.edu/idmAccountLogin/index.action?upname=423180785721717

Your invitation will expire on Aug. 05, 2012. If your invitation expires, please ask Michael Gettes to request a new invitation for you to register with Tartan-ConnectID.

We have posted Frequently Asked Questions about Tartan-ConnectID at

For questions about the registration and log-in process for Tartan-ConnectID, follow the link in this message or call the Computing Services Help Center at 412-268-4357.
Invitee beginning registration

Carnegie Mellon University

Michael Gettes has invited you to access the Tartan-ConnectID website at Carnegie Mellon University. In order to access this website, you must first register with Carnegie Mellon’s Tartan-ConnectID service. The service will allow you to access certain secure websites using an account with Third-Party Identity Providers such as Google, Yahoo, and AOL. Your registration with the Tartan-ConnectID service is conditioned on your acceptance of and compliance with the following terms and conditions.

Terms and Conditions for Tartan-ConnectID Service:

By clicking “Accept” below, you acknowledge that you received an email invitation to register for the Carnegie Mellon University Tartan-ConnectID service from Michael Gettes at gettes@andrew.cmu.edu (“Email Invitation”). You further acknowledge that you are the intended recipient of the Email Invitation and that you are an authorized user of the email account to which the Email Invitation was sent.

When registering for Tartan-ConnectID you will be asked to identify a Third-Party Identity Provider (e.g. Google, Yahoo, AOL, etc.) whose username,

I acknowledge that I have read, understand, and agree to the above terms and conditions.

Accept
Select IdP (we are not proud of this)
Standard Google Login

You are signing in to Identity.andrew.cmu.edu with your Google Account getles@gmail.com

Sign in  Cancel

You can always change your Google Account approval settings. Identity.andrew.cmu.edu is not owned, operated, or controlled by Google or its owners. Learn more
Back from Social IdP – User prompt
Thank you for completing your registration.

A confirmation email has been sent to you containing the URL below. Please retain the email for future reference. You can now access Tartan-ConnectID. You do not need to complete this registration the next time you wish to access Tartan-ConnectID. If another person at Carnegie Mellon declares a relationship to you, you will receive another invitation email and will be asked to confirm that relationship as well.

Tartan-ConnectID can be accessed at the following URL:

https://identity.andrew.cmu.edu/connectID-bake/?
TartanConnectIdTestApp:Google

Please Bookmark the above URL for future reference.
Welcome to Tartan-ConnectID. Your registration was successful!

*** DO NOT DELETE! Please save this email for future log-ins and reference. ***

This link will take you to the Tartan-ConnectID Service page:
https://identity.andrew.cmu.edu/connectID-bako/?TartanConnectIDTestApp1Google

Please:
1. Bookmark the above page for future use, and
2. Remember your log-in information for the provider you used.

We have posted Frequently Asked Questions about Tartan-ConnectID at
https://identity.andrew.cmu.edu/DS/discovery_help.html

For questions regarding the Tartan-ConnectID log-in process, contact the
Computing Services Help Center at 412-268-4387 or adviso@andrew.cmu.edu.

For questions regarding the service you are trying to access, please contact
the provider of the service or the person who invited you.
Recently you sent an invitation to gettes@gmail.com to establish a Tartan-ConnectID. The invitee has now completed the registration process, and is able to use their Tartan-ConnectID to access services at Carnegie Mellon University and other institutions of higher education. You may now wish to authorize this person to have access to certain data or electronic resources you control. The identity information of the person invited and registered is noted below.

***** CAUTION *****

As the Internet continues to have fundamental security concerns, knowing who has responded to your invitation or granted access to data and resources is an ongoing challenge. It is your responsibility to take steps to contact this person and verify they are the person you intended to allow access. You may be providing access to sensitive records belonging to you, Carnegie Mellon University, or to someone else and the responsibility of this authorization remains with you. There are a variety of methods you could use to verify that you are providing access to the right person - from calling this individual, to having a face-to-face interaction. You should use any communication methods appropriate to your situation.

If you are unsure of the true identity of the invitation information shown below then you should remove any authorizations and access you have given to this identity, and not assign any additional authorizations or access. If you feel there is a compromise of this account, contact the intended individual and also contact the Help Center by email to advisor@andrew.cmu.edu or call 412-268-4957.

Email invitation sent to: gettes@gmail.com
Registered First Name: Michael
Registered Last Name: Gettes (Google)
Registered Email: gettes@gmail.com
Registered ID: https://www.google.com/accounts/o8/id?id=Al:0Xm_0eGL50aUFw-n7yNlJVC-fvq1TU8affiitae-emu.edu
IAM Online – Social Identities

Jim Basney
jbasney@ncsa.uiuc.edu

This material is based upon work supported by the National Science Foundation under grant number 0943633 and by the Department of Energy under award number DE-SC0008597. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government or any agency thereof.
CILogon Project Goal

• Enable campus logon to CyberInfrastructure (CI)
  – Use researchers’ existing security credentials at their home institution
  – Ease credential management for researchers and CI providers
CILogon Service
(https://cilogon.org)

• Delivers certificates to desktop, browser, and portals
• Available certificate lifetimes: from 1 hour to 13 months
• Supports InCommon and OpenID authentication
• See also:
  http://www.cilogon.org/faq
  http://www.cilogon.org/news
  http://ca.cilogon.org
Why OpenID?

• Support users w/o institutional logins
  – Home institution not (yet) in InCommon federation
  – Home institution not (yet) releasing attributes to CILogon

• Use existing Google ID rather than signing up for new ProtectNetwork ID

• US ICAM LOA 1 certified OpenID providers
  – Google, PayPal, and VeriSign
  http://openidentityexchange.org/certified-providers
DataONE Users - Home Institutions (Jan 2012)

- Institutions: 309
- InCommon Members: 105
- Working with CIlogon: 35

Catch-all IdP is needed!
Google IDs are popular!

CIlogon Users Per Identity Provider (December 2012)

- Google (34%)
- University of Chicago (12%)
- ProtectNetwork (7%)
- UCSD (4%)
- UIUC (3%)
- PayPal (1%)
- Verisign
Thanks!

For more information:

www.cilogon.org

info@cilogon.org
New Social2SAML Gateway Pilot!

• What is it?

• How does it work?

• How is it used?

• Moving forward....
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
QUESTIONS?

THANK YOU!
Evaluation
Please complete the evaluation of today’s IAM Online: http://www.surveymonkey.com/s/IAMOnline_December_2012

Next IAM Online – January 16, 2013 (1 pm ET)
National Strategy for Trusted Identities in Cyberspace (NSTIC):
Privacy Infrastructure with Common Attributes
www.incommon.org/iamonline

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