

Google, Facebook, and Twitter, oh my!

Can Social Identities Make Your Life Easier?

John Krienke, InCommon/Internet2

David Langenberg, University of Chicago

Dedra Chamberlin, Cirrus Identity

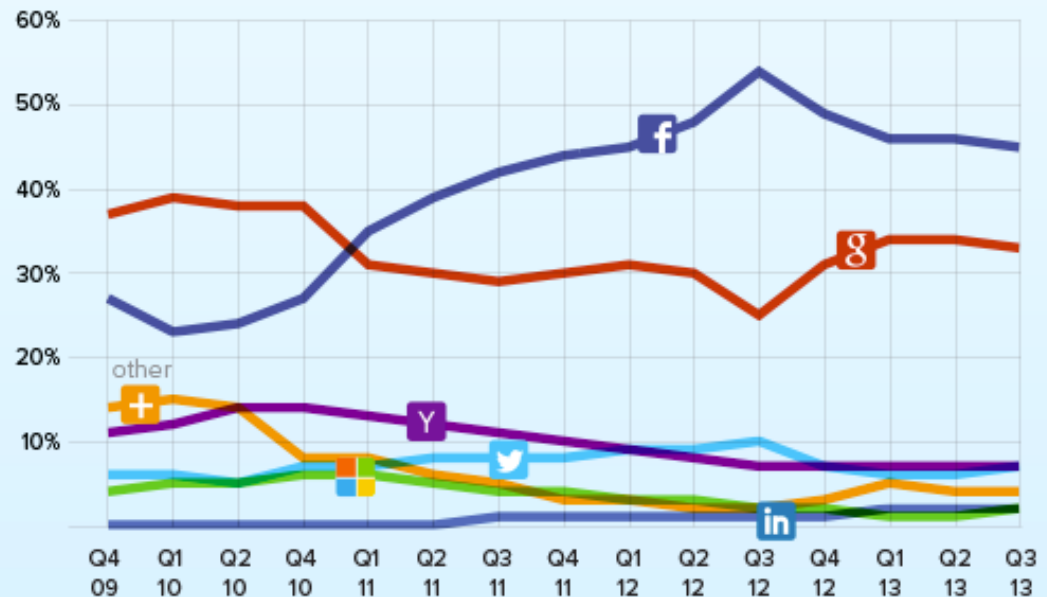
Going Social in 60 minutes:

1. 10' What, Why, Who
2. 10' Univ Chicago Use Case and Local Gateway
3. 15' Brown Use Cases and Cirrus Identity PoC
4. 05' Open issues & Getting involved
5. 20' Discussion

Social Identity for Campus Resources

What is a social identity? An external authN credential + an identifier...

- 87% of consumers are aware of social login, and more than half have tried it. (janrain)



Quarterly Social Login Trends

janrain

What are the driving campus use cases?

Low assurance, 'arms-length' relationships:

- Parents
- Highschool Students
- Continuing Ed, MOOCs
- Applicants
- Research partners
- Visiting professors, lecturers from non-federated organizations
- Alumni, conference guests, non-university guest others ...



THE UNIVERSITY OF
CHICAGO

Visiting Committee Directory

- Composed of alumni, the public, and faculty
- Serves as advisors of the Trustees
- Mix of credentialed and non/credentialed populations
- Committee members are considered to be VIPs



Visiting Committees and Councils

Committee Membership

- [Directory Search](#)

RELATED LINKS

- [Board of Trustees](#)
- [Office of the President](#)
- [Office of the Secretary of the University](#)
- [Divisions and Schools](#)

Secure Directory - beta

Please log in below to use the directory. If you do not have a CNetID, you may log in with an account you already have with Google, Yahoo, or Facebook. *Please note that the social media account you choose should use an email address we have on file.* If you have any trouble logging in, please contact us at weberror@uchicago.edu.

Login with CNetID / UCHADID

Or log in using an existing account below*:



Facebook



Google



Login with Yahoo

* *Please note that the account you choose should use an email address we have on file.*

Need Help?

- *I have an account above, but it's not linked to an email address on file.*
 - [Contact us](#) and give us the email address we're missing and we will add it to your record.
- *I'd like to create an account above, but I don't know what email address you have on file for me.*
 - [Contact us](#) and we'll let you know what email address we have on file for you.



THE UNIVERSITY OF
CHICAGO

Visiting Committee AuthZ

- Using email address as the user identifier
- User must exist in the Alumni Database with that email address
- Limits social choices to only those who provide email, but allows user to switch amongst providers so long as email is consistent
- Reaction of Committee Members has been emphatically positive



THE UNIVERSITY OF
CHICAGO

Social Gateway Setup

- . Based on SimpleSamlPHP
- . Google
- . Facebook
- . Yahoo
- . Linked-In



THE UNIVERSITY OF
CHICAGO

The Sales Process

“Hi IDM, I have a new app and we need to get NetIDs for all these new individuals from the general public”



THE UNIVERSITY OF
CHICAGO

The Sales Process

“Umm, ok, what services do they need?”

“Just authentication ... but we also need to allow this group of staff & students into the application.”



THE UNIVERSITY OF
CHICAGO

<https://openid.uchicago.edu>

IT Services

Information Technology Services



THE UNIVERSITY OF
CHICAGO

Authentication Test

This is an example web application. It demonstrates the ability to authenticate using Facebook, Google, or Chicago credentials over Shibboleth. Website implementers only need to install the Shibboleth Service Provider and they are able to use any of the below protocols (after a brief talk with Identity & Access Management).

 Login with Facebook

Login with 

Login with Linked-In

Login with Yahoo

Login with CNetID / UCHADID

Login with Marine Biological Lab Credentials

Results from Facebook

IT Services

Information Technology Services



THE UNIVERSITY OF
CHICAGO

Authentication Test

Information sent back:

Key	Value
CN	
givenName	David
sn	Langenberg
displayName	
eduPersonPrincipalName	AItOawl79CrVTixGRbh8VIYUe3LCiOSXZrL6R2c@google.com
mail	langedb@gmail.com

[Logout](#)

Results from Google

IT Services

Information Technology Services



THE UNIVERSITY OF
CHICAGO

Authentication Test

Information sent back:

Key	Value
CN	
givenName	David
sn	Langenberg
displayName	
eduPersonPrincipalName	AItOawl79CrVTixGRbh8VIYUe3LCIOSXZrL6R2c@google.com
mail	langedb@gmail.com

[Logout](#)

Results from Yahoo

IT Services

Information Technology Services



THE UNIVERSITY OF
CHICAGO

Authentication Test

Information sent back:

Key	Value
CN	
givenName	
sn	
displayName	David Langenberg
eduPersonPrincipalName	langedb@yahoo.com
mail	langedb@yahoo.com

[Logout](#)

Results from Linked-In

IT Services

Information Technology Services



THE UNIVERSITY OF
CHICAGO

Authentication Test

Information sent back:

Key	Value
CN	
givenName	David
sn	Langenberg
displayName	
eduPersonPrincipalName	QK-bHZXEdh@linkedin.com
mail	

[Logout](#)

Please send any comments,
corrections, or suggestions to:
itm@uchicago.edu.

6045 S. Kenwood Ave.
Chicago, IL 60637

© 2012, [The University of Chicago; IT
Services](#)

Brown University: *Language Consortium*



BROWN

- Distance learning for the delivery of less commonly taught languages
- Students from consortium schools participate in Brown classes
- Access to course tools as a student



Brown University: *Continuing Education*



BROWN

- *Summer@Brown* Instructor Training and community development
- Summer institute for researchers: *Public Health Bio Statistics and Applied Data Analysis*



BROWN

Brown University:

Criteria for use of social identity

Users

- no long-term relationship to Brown.
- no physical presence at Brown.
- may not be associated with a higher-Ed institution.

Use case requires no need to institutionally validate the individual's identity.

No credit or grades offered

Brown University:

Dean of the College: UFunds



BROWN

- UFunds resulted from a College-wide effort to consolidate disparate systems for funding opportunities.
- The system has evolved to support generic application processes.
- Most applications require some type of endorsement or recommendation.
- Our current approach is to email the non-Brown recommenders with token-based URL specific to the recommendation.

Brown University: UFunds Proof-of-Concept

Demonstration Video

Brown University:

Questions resulting from POC



BROWN

- Should non-institutional identities be managed on a per-application basis or in aggregate by the institution?
- Which identity providers should be allowed and with what levels of assurance?
- How do we manage the proliferation of discovery services across the institution to ensure consistent user experience?



cirrus identity

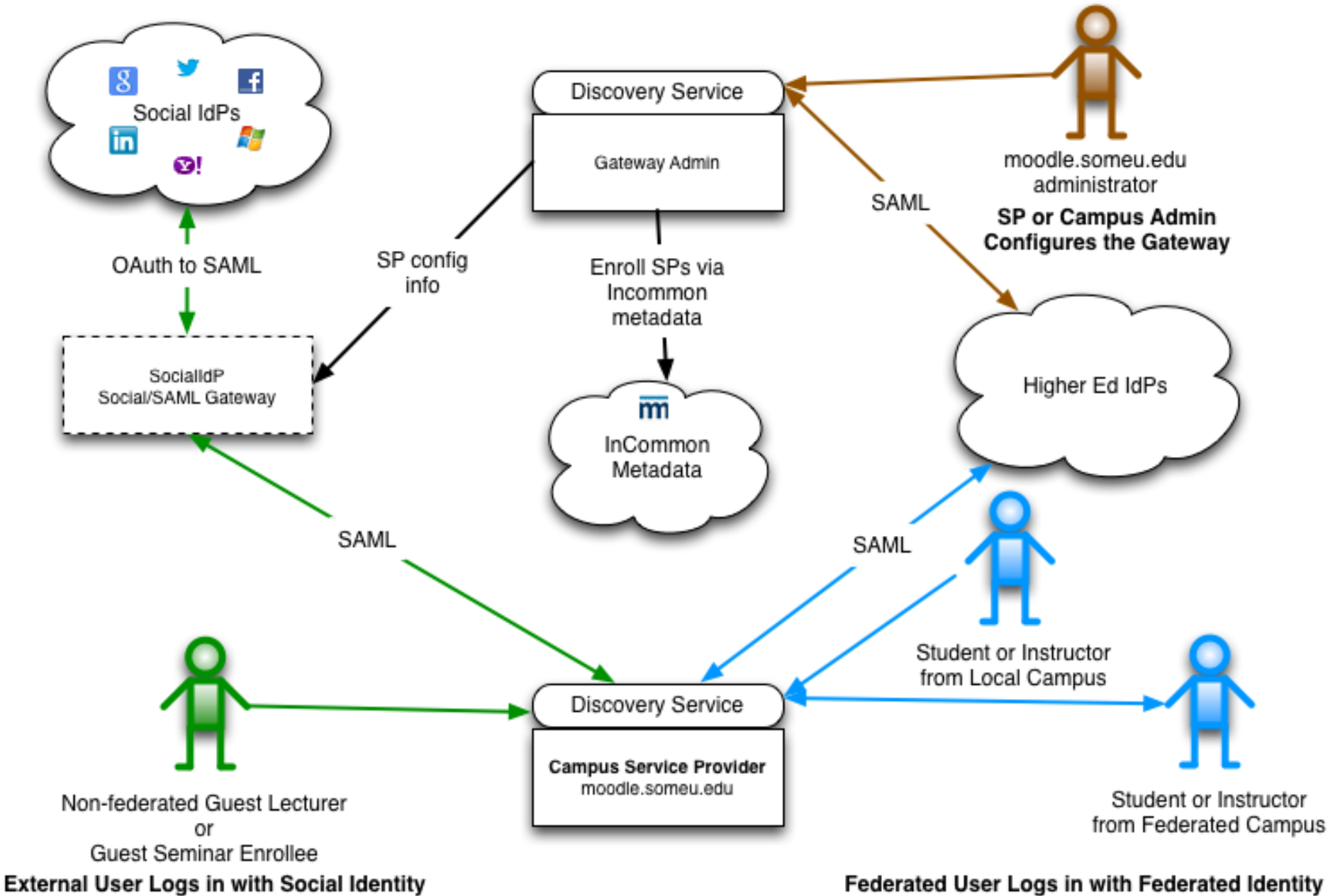
Dedra Chamberlin

Co-Founder and CEO

Cirrus Identity

Shared Gateway Overview

Social-to-SAML Gateway Overview
Cirrus Identity, Inc. - May 2013



The Gateway Admin App

Gateway Admin Login

Select Identity Provider

Pick from a list

[Search for provider](#)

Choose your identity provider from the list below.

Select Identity Provider

Select



Sign in with your Google Account



dedra@cirrusidentity.com

••••••••

Sign in

[Need help?](#)

[Create an account](#)

One Google Account for everything Google



**SocialIdP Gateway Admin** ▾

This app would like to:



View your email address



View basic information about your account



SocialIdP Gateway Admin and Google will use this information in accordance with their respective terms of service and privacy policies.

Cancel

Accept

Gateway Admin

cirrusidentity.com

Welcome to **SocialIdP Gateway Admin** tool. This system allows you to configure your Service Providers to use various OAuth identity providers like Facebook and Twitter, and OpenID identity providers like Google and Yahoo!.

The service providers you are authorized to configure are listed below.

My Service Providers

- [nose11.local/shibboleth](#)
- [apps-test.socialidp.com/shibboleth](#)

Don't see the entityID for one of your service providers? Please contact your organization contact and ask that your SP be enabled.

Manage

cirrusidentity.com[Organization Profile](#)[Admins](#)[Service Providers](#)[Social Providers](#)[Discovery Service](#)

Organization Profile

General information about this organization is listed below, including who is able to administer this organization.

General

Organization Name ⓘ

Support Email ⓘ

Organization URL ⓘ

Admins

Global Admins ⓘ

Chamberlin, Dedra
Rockwell, Lucas
Tegebo, Ian

Manage [cirrusidentity.com](#)

Organization Profile
Admins
Service Providers
Social Providers
Discovery Service

Admins

The admins listed on this page can be set as an Organization Admin (in the Organization section) or as an SP Admin (in the Service Providers section).

New Admin

First Name



Last Name

Email

ePPN

Create

Existing Admins

First Name	Last Name	Email	ePPN	
Dedra	Chamberlin	dedra@cirrusidentity.com	dedra@cirrusidentity.com	
Lucas	Rockwell	lucas@cirrusidentity.com	lucas@cirrusidentity.com	

Manage cirrusidentity.com

Organization Profile
Admins
Service Providers
Social Providers
Discovery Service

Service Providers

The Service Providers listed below have been associated with your organization.

New Service Provider

Entity ID


https://sp.mfa-proxy.com/idp/module.php/saml/sp/metadata.php/default-s...

Admins

Chamberlin, Dedra
Rockwell, Lucas
Tegebo, Ian

Create

Existing Service Providers

Entity ID	Admins	Edit
http://nose11.local/shibboleth		

Manage

[cirrusidentity.com](#)[Organization Profile](#)[Admins](#)[Service Providers](#)**Social Providers**[Discovery Service](#)

Social Providers

The Social Providers listed below are available in the SocialIdP Gateway. Please select which providers you would like to make available to your organization.

Providers

- ☒ Facebook
- ☒ Google
- ☒ LinkedIn
- ☒ Twitter
- ☒ Windows Live

Warning: If you disable a Social Provider that was previously enabled, it will prevent Service Provider Admins from being able to interact with that provider.

[Save](#)[Cancel](#)

Manage [cirrusidentity.com](#)

Organization Profile
Admins
Service Providers
Social Providers
Discovery Service

Discovery Service

The information listed below is for the Discovery Service UI. The default is usually good for most organizations, but you can change the wording if you like. Click on the "Preview" button to view what your changes will look like (you can view the preview without saving).

Discovery Service UI Elements

Heading ⓘ

Select Identity Provider

Preview

Select Tab Label ⓘ

Pick from a list

Select Tab Help ⓘ

Choose your identity provider from the list below.

Search Tab Label ⓘ

Search for provider

Gateway Admin

[nose11.local/shibboleth](#)

Welcome to SocialIDP Gateway. You can use this page to configure your Service Providers to use various OAuth identity providers like Facebook and Twitter, and OpenID identity providers like Google and Yahoo!.

The service providers you are authorized to configure are listed below.

My Service Providers

- [nose11.local/shibboleth](#)
- [apps-test.socialidp.com/shibboleth](#)

Don't see the entityID for one of your service providers? Please contact your organization contact and ask that your SP be enabled.

Manage

 nose11.local/shibboleth[Service Provider Profile](#)[Discovery Service](#)[Facebook](#)[Google](#)[LinkedIn](#)[Twitter](#)[Windows Live](#)

Service Provider Profile

The information below is a general overview of this service provider.

General

Description ⓘ

Some Cool App

Support Email ⓘ

biensen@someu.edu

Save

Cancel

Manage nose11.local/shibboleth

- Service Provider Profile
- Discovery Service

- Facebook
- Google
- LinkedIn
- Twitter
- Windows Live

Discovery Service

The configuration below is for your discovery service for this service provider. As the admin for this service provider, you can set which social providers and which IdPs (both social and those from various federations) you want listed.

Social Providers

- ☐ Facebook
- ☒ Google
- ☐ LinkedIn
- ☐ Twitter
- ☐ Windows Live

Federations

- | | | | |
|--|--|--|--|
| <input type="checkbox"/> Ad Hoc | <input type="radio"/> All Providers | <input type="radio"/> Custom Configuration | |
| <input checked="" type="checkbox"/> InCommon | <input checked="" type="radio"/> All Providers | <input type="radio"/> Custom Configuration | |
| <input type="checkbox"/> Éducation-Recherche | <input type="radio"/> All Providers | <input type="radio"/> Custom Configuration | |
| <input type="checkbox"/> SIR | <input type="radio"/> All Providers | <input type="radio"/> Custom Configuration | |
| <input type="checkbox"/> SWITCH | <input type="radio"/> All Providers | <input type="radio"/> Custom Configuration | |

Sort Option

- ☒ **Grouped, Social Providers at Top** — Sorted as groups, with the IdPs for each federation in their own group, and with Social Providers in their own group at the **top** of the list.
- ☐ **Grouped, Social Providers at Bottom** — Sorted as groups, with the IdPs for each federation in their own group, and with Social Providers in their own group at the **bottom** of the list.
- ☐ **Alphabetical Group** — Social Providers in their own group, but listed alphabetically with the other federations as groups, e.g., first InCommon, then Social Providers, then UK Federation, etc.
- ☐ **Alphabetical List** — Social Providers mixed in with all of the other IdPs, i.e., no groups, just a long list of IdPs.



Application Settings

Application Return Location

/gwadmin/auth/login

This is the location where users should be sent after your SP software has authenticated the user. It is best to put the full URL, including protocol and hostname, e.g., <https://someapp.someu.edu/some/path>.

Type

- ☒ **Stand-alone** — Choose this option if you will redirect users to a stand-alone page that contains the discovery service. 
- ☐ **Embedded** — Choose this option if you want to embed the discovery service in your application via an iframe. 

Click on the wrench icon to get the code for your login page.

Manage

 nose11.local/shibboleth[Service Provider Profile](#)[Discovery Service](#)[Facebook](#)[Google](#)[LinkedIn](#)[Twitter](#)[Windows Live](#)

Twitter

[Configure](#)[API Setup Guide](#)[Attribute Map](#)

API Key

API Secret

Click into the API Secret text box to view the secret.

Instruction for setting up your **API Key** and **API Secret** are listed in the **API Setup Guide** tab.

EPPN Configuration

- ☒ **None** — Select this if you are not going to use EPPN.
- ☐ **Unique ID Scoped to twitter.com** — This is the unique ID for the user at this provider, scoped to the domain of the provider (twitter.com). For instance, <username>@twitter.com.

Note: Once you configure a provider here, make sure you enable the provider in the **Discovery Service** section.

[Save](#)[Cancel](#)

[Service Provider Profile](#)[Discovery Service](#)[Facebook](#)**Google**[LinkedIn](#)[Twitter](#)[Windows Live](#)

Google

Configure[API Setup Guide](#)[Attribute Map](#)

API Key

API Secret

Click into the API Secret text box to view the secret.

Instruction for setting up your **API Key** and **API Secret** are listed in the **API Setup Guide** tab.

EPPN Configuration

- ☒ **None** — Select this if you are not going to use EPPN.
- ☐ **Unique ID Scoped to google.com** — This is the unique ID for the user at this provider, scoped to the domain of the provider (google.com). For instance, <username>@google.com.
- ☐ **Email** — The email address of the user as returned by the social provider.
- ☐ **Email Scoped to google.com** — The email address of the user, but scoped to the domain of the service provider. For instance, someuser@gmail.com would become someuser+gmail.com@google.com for a Google email address (note, Google hosts many email domains, not just gmail.com, hence this option).
- ☐ **Email Scoped to cirrusidentity.com** — The email address of the user, but scoped to the domain of your organization. For instance, someuser@gmail.com would become someuser+gmail.com@cirrusidentity.com for a Google email address.


The Discovery Service

Discovery Service List


Gateway Admin


Gateway Admin Login


Select Identity Provider

 Facebook


 Google

 Allegheny College


 American University

 Ames Laboratory

 Amherst College

 Argonne National Laboratory

 Arizona State University

 Auburn University

 Azusa Pacific University

Enter Identity Provider Name

Show all Providers


Discovery Service Search - “State”

Gateway Admin

Gateway Admin Login

Select Identity Provider

 Arizona State University

 Ball State University

 Boise State University

 California Polytechnic State University-San Luis Obispo

 California State Polytechnic University, Pomona

 California State University, Bakersfield

 California State University, Channel Islands

 California State University, Chico

 California State University, Dominguez Hills

 California State University, East Bay

state|










Show all Providers

Discovery Service Search - “Lab”

Gateway Admin

Gateway Admin Login

Select Identity Provider

-  Ames Laboratory 
-  Argonne National Laboratory
-  Brookhaven National Laboratory
-  LIGO Scientific Collaboration
-  Lawrence Berkeley National Laboratory
-  Marine Biological Laboratory
-  Moss Landing Marine Laboratories
-  University of Alabama at Birmingham
-  University of Alabama, The

lab

Show all Providers

Key Design Considerations

- Gateway is a useful evil
- Connect Service Provider and Social Identity Provider
 - Each SP agrees to Social IdP terms and conditions
 - Social Idp API call limits set per SP, not per campus
 - SP choice on identifier assertion
 - Always allow choices that facilitate portability
- Allow use at campus level or individual department/SP
- Flexible Metadata, Scoping, and Discovery Options

Future Community Contributions

- Prioritizing code completion and optimization
- Likely future community contributions:
 - SSP Google Open ID Connect authN handler
 - Discovery Service components
 - Documentation on lessons learned

Cirrus Identity November Trial

- Brown University
- Carnegie Mellon University
- Penn State
- University of Maryland, Baltimore County
- Colorado State

For More Info:

<http://cirrusidentity.com>

Social to SAML: Next for You

- Join Social Working Group (since 2011)
 - spaces.internet2.edu/display/socialid
 - many campuses involved in sharing common requirements, current practices
 - create best practices
- Trial period for Cirrus social-to-SAML gateway
 - cirrusidentity.com
- InCommon services in development
 - Basic solution: 100% coverage
 - Advanced solutions: discovery, invitation, beginning service validation

Seeding Questions & Issues

- Assurance of Identity: Are all social identities created equal?
- Attributes: What do you get? Are they standard?
- Gateway Issues: Is it a bottleneck? How does it change?
- Privacy: Do we protect privacy of Nouns (PII) and Verbs (transactions)?
- What are we giving up -- Surveillance, Correlations?
- Usability: How does a user know which identity to use when? What about account linking/merging?
- Policy and Technology: Are you comfortable relying on external identities, something we in HE ask our corporate partners to do with our own identities?

Parting thought:

A couple of months in the laboratory can save a couple of hours in the library.

-Frank H. Westheimer, chemistry professor

A couple of months on campus can save a couple of hours in a working group.

THANK YOU

John Krienke

jcwk@internet2.edu

David Langenberg

davel@uchicago.edu

Dedra Chamberlin

dedra@cirrusidentity.com

Seeding Questions & Issues (Detail)

- Assurance of Identity: Are social identities created equal?
 - Identity Proofing
 - Credential Management: issuance, storage, transit, revocation, reassignment
 - Token strength: Passwords, multiple factors
- Attributes
 - Standards & schema
 - Translation
 - Persistence
 - Permanence
- Gateway Issues
 - Licensing terms for use
 - Capacity
 - Resilience for for change
- Privacy
 - Personal information: the nouns
 - Personal transactions: the verbs
 - Correlation
- Usability
 - Discovery (discovery.refeds.org)
 - Invitation
 - Account linking
 - Permission & Consent
- Policy and Technology: Tables are turned: Control and Reliance on External Identities