

Federated Identity in Research: A US Perspective

Scott Koranda for LIGO and CTSC

University of Wisconsin-Milwaukee

February 3, 2015
LIGO-XXXXXXXXX-v1



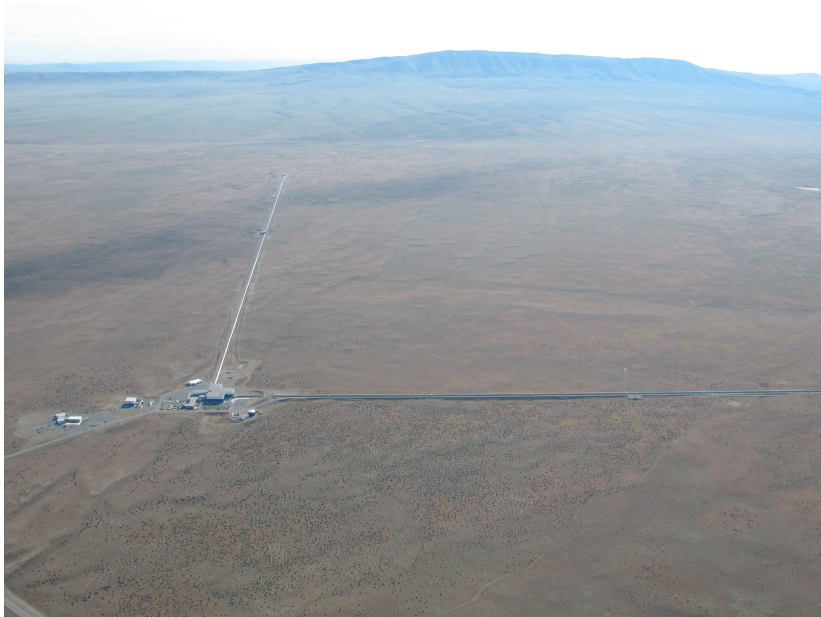


LIGO

LIGO Science Mission

LIGO, the Laser Interferometer Gravitational-wave Observatory, seeks to detect gravitational waves – ripples in the fabric of spacetime. First predicted by Einstein in his theory of general relativity, gravitational waves are produced by exotic events involving black holes, neutron stars and objects perhaps not yet discovered.

LIGO Hanford, WA



LIGO Livingston, LA



LIGO India!



Anticipated to be operational 2020

LIGO Scientific Collaboration

The LIGO Scientific Collaboration (LSC) is a self-governing collaboration seeking to detect gravitational waves, use them to explore the fundamental physics of gravity, and develop gravitational wave observations as a tool of astronomical discovery. The LIGO Scientific Collaboration was founded in 1997 and currently has just over 1000 members from more than 70 institutions worldwide.



LIGO Scientific Collaboration



Broader Gravitational-wave Community

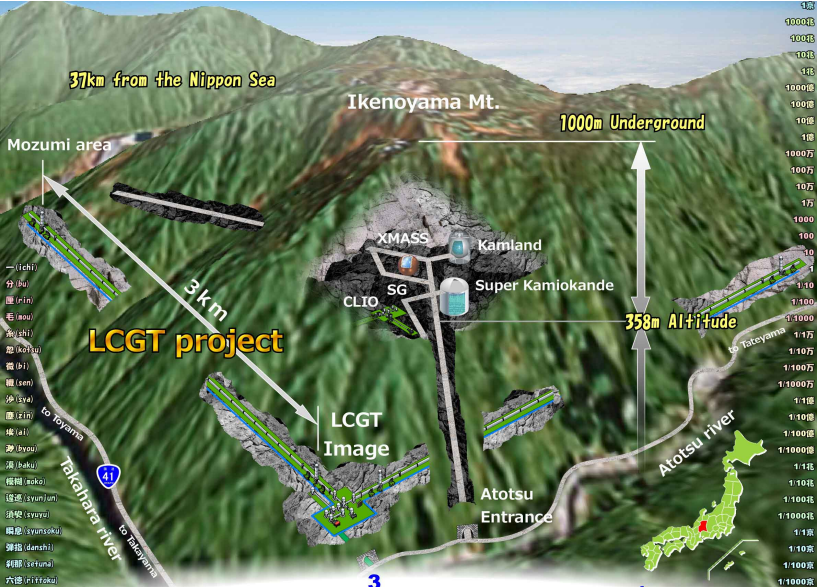
Gravitational-wave community is larger than LIGO...

Virgo Interferometer, Cascina, Italy



Kamioka Gravitational Wave Detector (KAGRA)

previously Large Scale Cryogenic Gravitational Wave Telescope (LCGT)



Broader Multimessenger Astronomy Community



Comprehensive Multimessenger Studies

LIGO
Livinston



LCGT



GEO



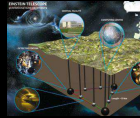
LIGO Hanford



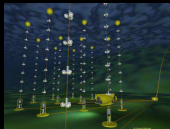
Virgo



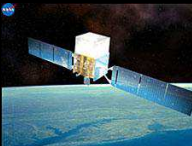
ET



Antares



Fermi



Swift



LVD

QUEST



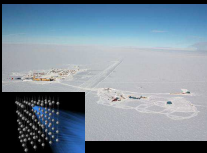
TAROT



Super-K



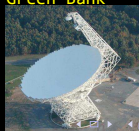
IceCube



Arecibo



Green Bank



LOFAR



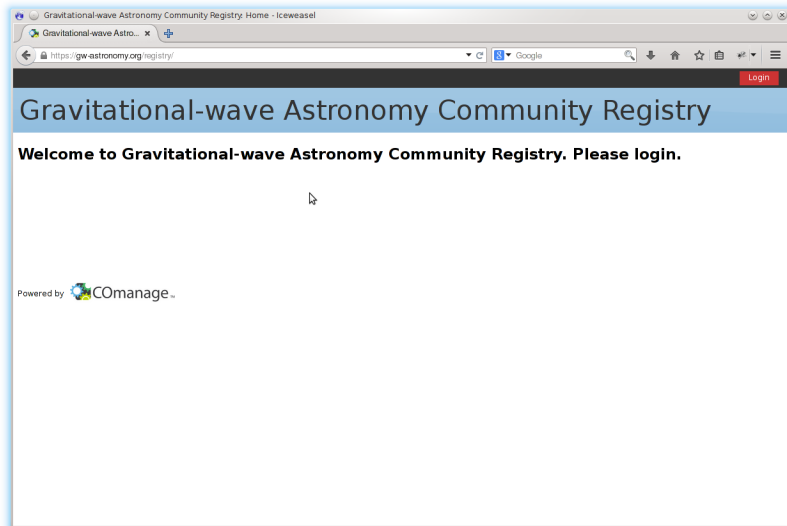
Two Primary Use Cases for Federated Identity

1. Supporting LIGO collaboration itself
2. Streamlining collaboration with broader community

Two Primary Use Cases for Federated Identity

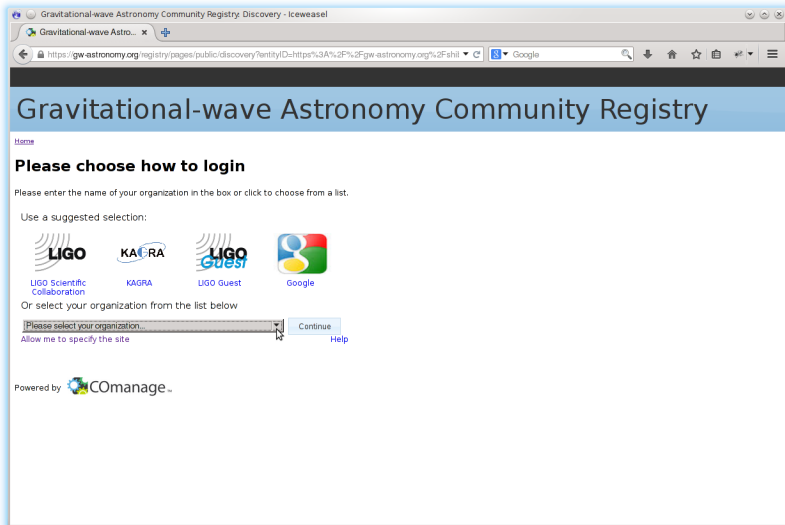
1. Supporting LIGO collaboration itself
2. Streamlining collaboration with broader community

GW Astronomy Registry



The image shows a web browser window displaying the homepage of the Gravitational-wave Astronomy Community Registry. The browser's address bar shows the URL `https://gw-astronomy.org/registry/`. The page features a blue header with the title "Gravitational-wave Astronomy Community Registry" and a red "Login" button in the top right corner. Below the header, a black banner contains the text "Welcome to Gravitational-wave Astronomy Community Registry. Please login." in white. The main content area is white and contains the text "Powered by" followed by the COmanage logo and the text "COmanage". A mouse cursor is visible in the center of the page.

GW Astronomy Registry



The screenshot shows a web browser window with the URL <https://gw-astronomy.org/registry/pages/public/discovery/?entityID=https%3A%2F%2Fgw-astronomy.org%2Fahil>. The page title is "Gravitational-wave Astronomy Community Registry". Below the title, there is a "Home" link and a heading "Please choose how to login". A sub-heading says "Please enter the name of your organization in the box or click to choose from a list." Underneath, it says "Use a suggested selection:" and displays four logos: LIGO Scientific Collaboration, KAGRA, LIGO Guest, and Google. Below the logos, it says "Or select your organization from the list below" and shows a dropdown menu with the text "Please select your organization...". To the right of the dropdown is a "Continue" button and a "Help" link. At the bottom left, it says "Powered by CManage..".


Gravitational-wave Astronomy Community Registry


[Home](#)


Please choose how to login


Please enter the name of your organization in the box or click to choose from a list.

Use a suggested selection:

 **LIGO**
LIGO Scientific
Collaboration

 **KAGRA**
KAGRA


 **LIGO**
Guest

 **Google**
Google

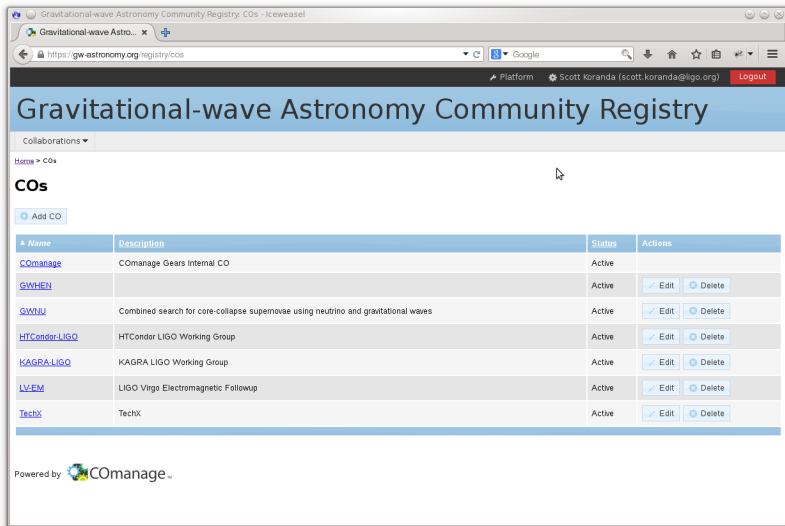
Or select your organization from the list below

[Help](#)

Allow me to specify the site


Powered by  CManage..

GW Astronomy Registry



The screenshot shows a web browser window with the URL <https://gw-astronomy.org/registry/cos>. The page title is "Gravitational-wave Astronomy Community Registry". A navigation bar at the top right shows the user is logged in as "Scott Koranda (scott.koranda@ligo.org)" with a "Logout" button. Below the title, there is a "Collaborations" dropdown menu and a "Home > COs" breadcrumb. The main heading is "COs", followed by an "Add CO" button. A table lists several collaborations, each with a "Name", "Description", "Status", and "Actions" column. The actions column contains "Edit" and "Delete" buttons for each entry.

Name	Description	Status	Actions
COManage	COManage Gears Internal CO	Active	
GWHEN		Active	Edit Delete
GWHLU	Combined search for core-collapse supernovae using neutrino and gravitational waves	Active	Edit Delete
HTCondor-LIGO	HTCondor LIGO Working Group	Active	Edit Delete
KAGRA-LIGO	KAGRA LIGO Working Group	Active	Edit Delete
LVEM	LIGO Virgo Electromagnetic Followup	Active	Edit Delete
TechX	TechX	Active	Edit Delete

Powered by  COManage

Which Federated Identities?

- ▶ Surveyed the 60+ “contact” persons for the MOUs
- ▶ Asked from which university(ies), institution(s), or organization(s) users might come to LIGO services
- ▶ Quick and gracious response from contact persons
- ▶ So far...
 - ▶ 26 countries including Australia, Canada, Chile, China, Germany, UK, Ireland, India, Mexico, Poland, United States
 - ▶ 161 unique institutions
 - ▶ 72 of 161 are US institutions
 - ▶ Many MOUs signed by international VOs

International Federation Challenges

Two (related) primary challenges:

1. Federate in scalable way with global network of IdPs
2. Attribute release by higher education IdPs

Research likelihood and timeline for eduGain via InCommon

- ▶ Jim Basney spun up InCommon TAC Interfederation WG
- ▶ Later chaired by Warren Anderson (LIGO), Paul Caskey (UT)
- ▶ Executive Summary (March 2014)
 1. InCommon should sign the eduGAIN Declaration as soon as possible (Done)
 2. TAC should work with Ops to operationalize eduGAIN over the next six months (Done for LIGO)
 3. TAC should instantiate a new working group with a charter based on the Future Work items (Done)

“New Entities” working group addressing issues

InCommon TAC New Entities Working Group

The InCommon metadata file contains, from a policy perspective, only one kind of entity—those owned and managed by, either directly or indirectly, an InCommon participant. There are proposals currently under review to add entities to metadata that deviate from this established practice:

- ▶ *Operationalizing eduGAIN will add IdPs and SPs that are members of other federations, but not members of InCommon.*
- ▶ *A Social-to-SAML Gateway would rely on external/social identity providers to authenticate users and assert attributes about them (often self-asserted).*
- ▶ *Some Regional Network Operators would like to facilitate InCommon participation by K-12 systems without themselves being directly responsible for the operation of the K-12 entities that would appear in the metadata.*

The appearance of these new types of entities within the InCommon metadata file will create new risk scenarios for current InCommon members.

eduGain and InCommon from LIGO Perspective

- ▶ gw-astronomy.org and 3 related SPs injected into eduGAIN
- ▶ SPs in REFEDs Research & Scholarship (R&S) entity category
- ▶ InCommon (beta) metadata aggregate with eduGAIN IdPs

(Many thanks to Tom Scavo and his team)

Participation somewhat “manual” right now but InCommon close to generalizing and putting it on operationally solid footing

Open question is what if any projects or organizations are not using federated identity for international collaboration because they do not think it is possible through InCommon?

Federated Identity in US

- ▶ 72 US institutions identified for gw-astronomy.org
- ▶ Major R1 universities to small liberal arts colleges
 - ▶ **Size not good indicator of federated identity success**
- ▶ 64 are InCommon members
- ▶ 61 have registered IdPs
- ▶ Primary concern is attribute release—will the IdP release **any** attributes to our SPs?
- ▶ At the very least need ePPN(today)
- ▶ *InCommon participant IdPs under no obligation to interoperate with SPs or release any attributes*
- ▶ Experience is that most will interoperate but minority will release attributes

Research & Scholarship Entity Category

- ▶ SPs petition InCommon to be tagged as R&S
 - ▶ Both InCommon and REFEDs R&S now...
- ▶ IdPs may agree to release simple set of attributes to R&S SPs
 - ▶ Currently only InCommon R&S...
- ▶ gw-astronomy.org tagged both InCommon and REFEDS R&S
- ▶ Petition is straightforward and quick for LIGO (too quick?)

~~28 of the 72 US institutions operate InCommon R&S IdPs~~

51 of the 72 US institutions operate InCommon R&S IdPs

What to do?

InCommon Research & Scholarship Entity Category

- ▶ R&S participation has been passive activity for InCommon
- ▶ Send Tom Scavo list he will help solicit
- ▶ LIGO has done that and it helped
- ▶ Still some conspicuous missing IdPs
 - ▶ Harvard
 - ▶ Penn State
 - ▶ Berkeley
 - ▶ U of Texas
- ▶ More recently plans by InCommon Steering to advocate

“Research” Representation on InCommon Steering



- ▶ Von Welch appointed to one year term on InCommon Steering
- ▶ Director of Center for Applied Cybersecurity Research at IU
- ▶ Center for Trustworthy Scientific Cyberinfrastructure (CTSC)
- ▶ Long history in research computing infrastructure

The first thing I'd like to work on is getting all universities of interest to NSF projects to streamline scientific collaboration by sending those projects a user's name and email address when the user authenticates to the project using InCommon federated authentication.

Until “all” IdPs support R&S...

- ▶ Deployed “LIGO Guest” IdP of last resort
 - ▶ Completely separate IdP and IdMS
 - ▶ Once-off code, FTE expensive
 - ▶ InCommon IdPoLR WG (but does not exist today)
- ▶ Deployed Social-to-SAML gateway service (Cirrus)
 - ▶ Allow Google authentication
 - ▶ Hosted service
 - ▶ Gateway asserts ePPN and other attributes
 - ▶ COmanage identity linking
 - ▶ InCommon Social-to-SAML gateway service?

So far users appear to prefer the LIGO Guest IdP over Google...
UnitedID and other IdPoLR to be considered

Must not be any cost to users

Federated Identity Outside US

- ▶ Goal is to leverage eduGAIN
- ▶ SPs appearing in eduGAIN metadata only first step
- ▶ Only handful of eduGAIN IdPs support R&S
 - ▶ Many Swedish IdPs
 - ▶ A few Swiss
 - ▶ Unfortunately little overlap with LIGO use case
 - ▶ One IdP (and one user) in UK (thanks Rhys!)
- ▶ Overheard from EU federation operator:
We won't support REFEDs R&S. It's a black box to us.
- ▶ Brainstorming idea: large VO entity categories?
Sure, we'll release to tagged LIGO SPs.
- ▶ LIGO reviewing non-EU CoC draft (thanks Mikael)

Leverage help from REFEDs

- ▶ Nicole Harris (TERENA) has agreed to assist LIGO
- ▶ Work with IdPs through federation operators
- ▶ Pursue both interoperability and attribute release
- ▶ What legal issues await?
- ▶ Not all organizations and countries represented
- ▶ Rely on LIGO Guest and Social-to-SAML gateway for rest

Other Federation Issues besides Attribute Release

Federated Security Incident Response

- ▶ Hear about Sirtfi tomorrow...
- ▶ LIGO participating to some extent
- ▶ IdPs and SPs still have no obligation or agreement, moral or legal, to notify other of a security incident

Level of Assurance (LOA)

- ▶ LIGO participates on InCommon Assurance Advisory Committee
- ▶ Mostly ignore LOA now so as to not complicate attribute release issues



Slides courtesy of Jim Basney

CILogon – <https://cilogon.org/>

- Provides personal digital certificates for access to cyberinfrastructure
- Uses federated authentication for user identification



Federated Authentication

- Log on to CILogon using your campus (InCommon) or Google (OpenID) account

Login - University of Illinois at Urbana-Champaign

ILLINOIS LOGIN

You must log in to continue.

Enter your NetID:
jbasney

Enter your Active Directory (AD) password:

Login

Google Accounts

Google SIGN UP

Accounts

CILogon.org is asking for some information from your Google Account. To see and approve the request, sign in. [Learn more](#)

Sign in Google

Email
jbasney@cilogon.org

Password

Sign in Stay signed in

[Can't access your account?](#)

2-step verification

Enter the verification code generated by your mobile application.

Enter code:
852261 Verify

ligo-proxy-init using SAML ECP

```
$ ligo-proxy-init scott.koranda
Your identity: scott.koranda@LIGO.ORG
Enter pass phrase for this identity:
Creating proxy ..... Done
Your proxy is valid until: Mar 5 13:45:16 2013 GMT
$ grid-proxy-info -all
subject  : /DC=org/DC=cilogon/C=US/O=LIGO/CN=Scott Koranda scott.koranda@ligo.org
issuer   : /DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Basic CA 1
identity : /DC=org/DC=cilogon/C=US/O=LIGO/CN=Scott Koranda scott.koranda@ligo.org
type     : end entity credential
strength : 2048 bits
path     : /tmp/x509up_u1000
timeleft : 71:59:52 (3.0 days)
```

Integrated with CyberInfrastructure

Welcome To The CILogon Delegation Service
Ocean Observatories Initiative
Powered By CILogon

Get Your Certificate
Open Science Grid

Welcome To The CILogon Service
globus online
Powered By CILogon

Welcome To The CILogon Service
LIGO

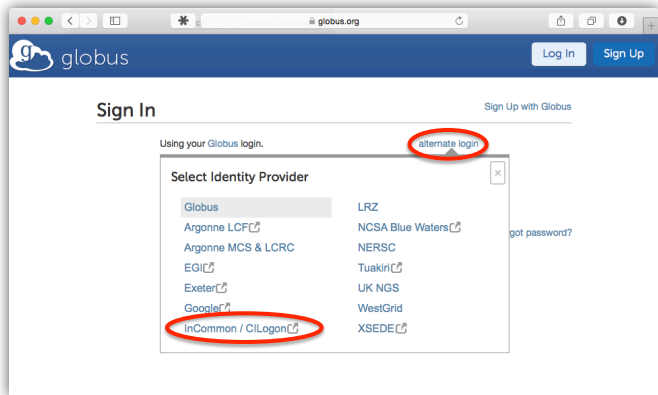
Welcome To The CILogon Service
CardioVascular Research Grid
Select An Identity Provider:
University of Hawaii
University of Illinois at Chicago
University of Illinois At Springfield
University of Illinois at Urbana-Champaign
Search:
Remember this selection:
Continue
By selecting "Continue", you agree to CILogon's privacy policy.

Welcome To The CILogon Service
DataONE
Powered By CILogon
Select An Identity Provider:
University of Hawaii
University of Illinois at Chicago
University of Illinois At Springfield
University of Illinois at Urbana-Champaign
Search:
Remember this selection:
LOG ON
By selecting "Log On", you agree to CILogon's privacy policy.

For questions about this site, please see the [FAQs](#) or send email to [help](#).
Know **your responsibilities** for using the CILogon Service.
See [acknowledgements](#) of support for this site.

For questions about this site, please see the [FAQs](#) or send email to [help @ cilogon.org](#).
Know **your responsibilities** for using the CILogon Service.
See [acknowledgements](#) of support for this site.

Integrated with Globus



Used by DOE KBase

The screenshot shows the KBase Predictive Biology DOE Systems Biology Knowledgebase Sign In page. The page title is "Sign In | KBase". The main heading is "Sign In" with a "Sign Up with Globus" link. Below the heading, it says "Using your Globus login." and there is a red circle around the "alternate login" link. A "Select Identity Provider" dialog box is open, listing various providers. "InCommon / CILogon" is highlighted with a red circle. The footer includes the U.S. Department of Energy logo, social media icons, and text stating "KBase is sponsored by the U.S. Department of Energy's Office of Biological and Environmental Research." and "Privacy and Security Notice".

Sign In | KBase

KBase
PREDICTIVE BIOLOGY
DOE Systems Biology Knowledgebase

Log In Sign Up

Sign In Sign Up with Globus

Using your Globus login. **alternate login**

Select Identity Provider

- Globus
- Argonne LCF
- Argonne MCS & LCRC
- BIRN
- CLI Transition
- EGI
- ESG ANL
- Exeter
- Google
- InCommon / CILogon
- LRZ
- NCSA
- NCSA Blue Waters
- NERSC
- UChicago CI
- UChicago IBI
- UK NGS
- WestGrid
- XSEDE

ENERGY Science

KBase is sponsored by the U.S. Department of Energy's
Office of Biological and Environmental Research.

Privacy and Security Notice

Used by OSG Connect

Sign In | OSG Connect (Globus Online)

https://portal.osgconnect.net/SignIn

osg connect Support Resources OSG Connect Sign In / Register

Efficiently connect your science to cycles and data

osg connect

OSG Connect offers users simple access to distributed high throughput computing resources, and reliable, high-performance file transfer services.

Sign In Sign Up with Globus Online

Using your InCommon / CILogon login. alternate login

You will now be redirected to InCommon / CILogon's authentication page.

Proceed

© 2013 Open Science Grid and University of Chicago

Used by ATLAS Connect

The screenshot shows a web browser window titled "OAuth Sign In | Atlas Connect". The address bar contains the URL: `https://portal.usatlas.org/OAuth#response_type=code&redirect_uri=https%3A%2F%2Fconnect.usatlas.org%2Foauth&client=Reader`. The page header includes the ATLAS logo and the word "CONNECT", along with navigation links for "Support", "Resources", "Connect", and "Log In or Register".

The main content area is titled "Sign In" and includes a "Sign Up with Globus" link. A grey box contains the following text:

This client is requesting access to your account:
Site: `https://connect.usatlas.org/oauth`
If you approve, please sign in.

Below this box, the text "Using your InCommon / CILogon login." is circled in red. To its right is a link labeled "alternate login".

Below the red circle, the text reads: "Click PROCEED to authenticate with InCommon / CILogon." A blue "Proceed" button is located below this text.

At the bottom of the page, it says "Powered by:" followed by logos for "US ATLAS Computing Facility", "globus", and "ci connect".

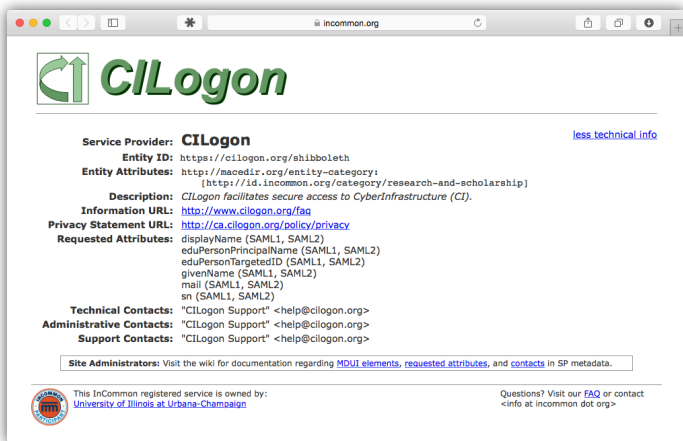
Integrated with Campus

The image displays three overlapping browser screenshots illustrating the integration of CILogon with various university portals:

- Top Screenshot:** A browser window at `cybergateway.iu.ts.edu` showing the "Cyberinfrastructure Gateway" for Indiana University. The "Login" link in the navigation menu is circled in red.
- Middle Screenshot:** A browser window at `transfer.rcac.purdue.edu` showing the Purdue University Research Computing (RCAC) portal. The "Log In" link is circled in red. A central box prompts users to "Access the Globus data transfer service by signing in with your Purdue Career Account".
- Bottom Screenshot:** A browser window at `portal.duke-ci-connect.net` showing the "CI CONNECT" portal for Duke University. The "Sign In" link is circled in red. A modal dialog box is open, displaying the text "Using your InCommon / CILogon login." circled in red, and a "Proceed" button.

Each screenshot also shows a "Proceed" button at the bottom of the login flow, indicating the final step in the authentication process.

InCommon R&S SP



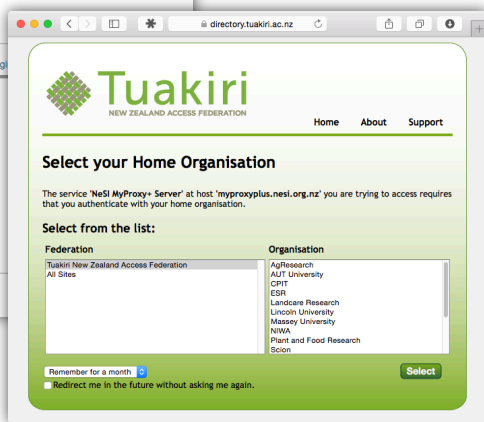
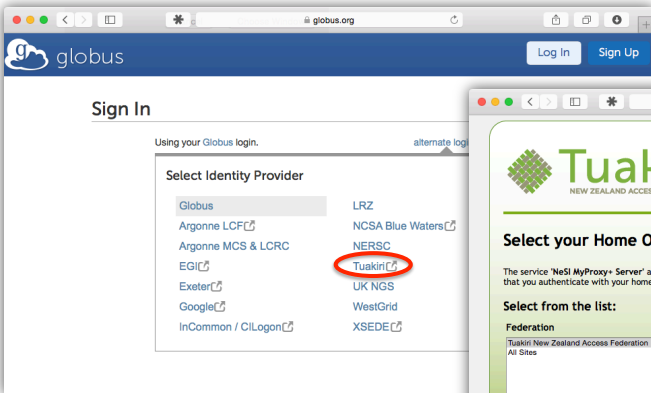
The screenshot shows a web browser window with the URL `incommon.org`. The page features the CILogon logo at the top left. Below the logo, the following metadata is displayed:

- Service Provider:** **CILogon** [less technical info](#)
- Entity ID:** `https://cilogon.org/shibboleth`
- Entity Attributes:** `http://macedir.org/entity-category: [http://id.incommon.org/category/research-and-scholarship]`
- Description:** *CILogon facilitates secure access to CyberInfrastructure (CI).*
- Information URL:** <http://www.cilogon.org/faq>
- Privacy Statement URL:** <http://ca.cilogon.org/policy/privacy>
- Requested Attributes:** `displayName (SAML1, SAML2)`
`eduPersonPrincipalName (SAML1, SAML2)`
`eduPersonTargetedID (SAML1, SAML2)`
`givenName (SAML1, SAML2)`
`mail (SAML1, SAML2)`
`sn (SAML1, SAML2)`
- Technical Contacts:** "CILogon Support" <help@cilogon.org>
- Administrative Contacts:** "CILogon Support" <help@cilogon.org>
- Support Contacts:** "CILogon Support" <help@cilogon.org>

A box at the bottom of the metadata section contains the text: **Site Administrators:** Visit the wiki for documentation regarding [MDUI elements](#), [requested attributes](#), and [contacts](#) in SP metadata.

At the bottom of the page, there is a logo for the University of Illinois at Urbana-Champaign and the text: "This InCommon registered service is owned by: [University of Illinois at Urbana-Champaign](#)". To the right, it says: "Questions? Visit our [FAQ](#) or contact <info at incommon dot org>".

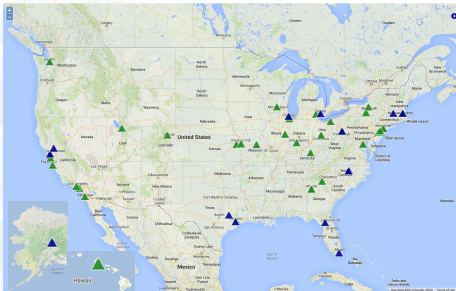
Replicating CILogon Internationally





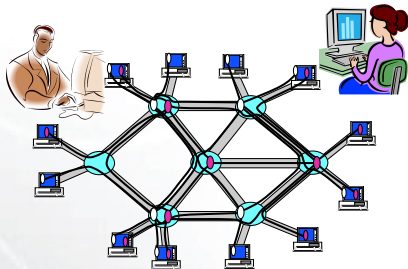
Slides courtesy of Tom Mitchell

- **G**lobal **E**nvironment for **N**etwork **I**nnovation
- A testbed for network research funded by the NSF



GENI Infrastructure Sites, 2014

GENI provides a deeply programmable network



<http://www.geni.net>

- GENI is a natural fit for InCommon
 - GENI's target audiences are researchers and educators
 - InCommon's target audience is the Research and Education Community
- GENI would prefer not to manage the account lifecycle
 - Usernames
 - Passwords
 - Institutional affiliations

As a service provider, joining InCommon can enable reduced barrier to entry for many potential users

InCommon: The Myth

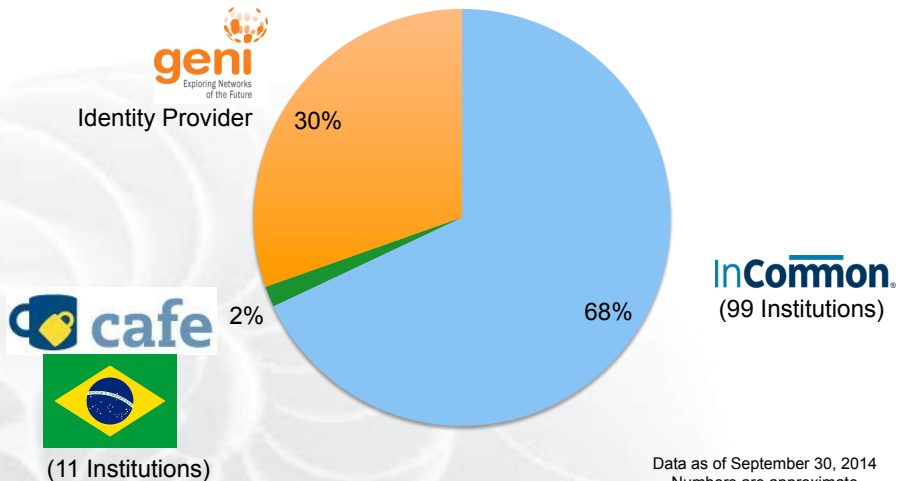
- If you join it, they will come
- Everyone in InCommon will have access to your service
- You can get detailed information like class enrollment

InCommon: The Reality

- You still have to market your service
- Nobody shares attributes with you by default
- You negotiate 1 by 1 with identity providers
- If they do share, you get limited attributes

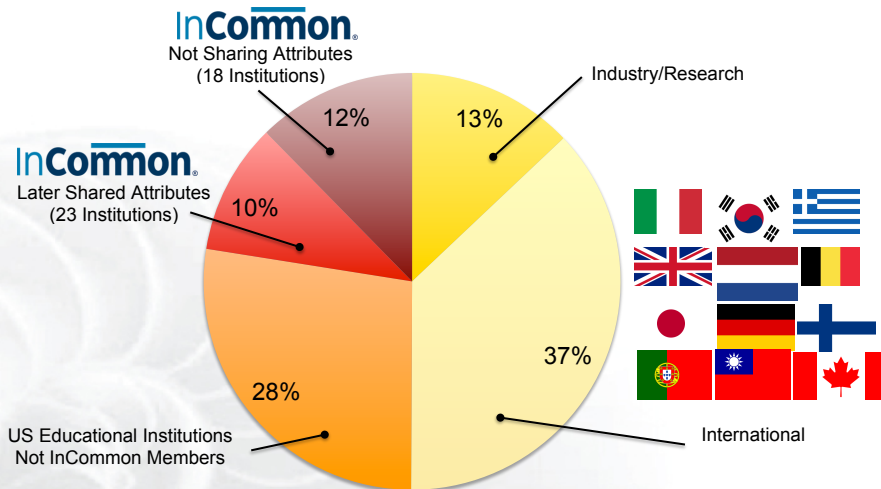
- R & S has made things much better
 - No more knocking on doors one by one
- Many schools are on board
- There are multiple service providers (SPs) pushing together
- R&S is easier for IdPs to configure than single SP release
- R&S provides campus members greater benefit
- InCommon has been *tremendously* helpful getting IdPs to share attributes with GENI

GENI Users by Federation



Data as of September 30, 2014
Numbers are approximate

GENI Identity Provider Accounts



Data as of September 30, 2014,
Numbers are approximate

When a user is denied access to GENI due to insufficient attributes we work with InCommon to request that the institution support R&S or release attributes to GENI.

We get a range of responses:

- Yes, we will
- We cannot release attributes due to:
 - FERPA
 - School/System rules
- We can release for staff & faculty, but not students
- Who is it that wants access?
 - GENI often doesn't know; we don't get attributes
- No response

InCommon R&S Service Providers

- ▶ Total of 18 SPs today
- ▶ LIGO is 7 of those
- ▶ CILogon and GENI 2 more
- ▶ Other half once-off SPs (not VOs)

Build it and they will come?