



# SIF for US Science

Michael Helm  
Esnet  
09 June 2011



# What is driving us (crazy) in identity?



Multiple axes of semi-independent variables ....

- Public identity to enterprise to project specific identity
- Convenience, low overhead to rigorous, highly secure
- Web apps ... command line tools ... mixed use
- SAML ... OpenID Connect ... pure OpenID/OAuth ...  
Kerberos ... X.509 ... ssh ... your legacy id
- NIST LOA ... EU standards ... industry practice ... our  
(science) practice
- h/w tokens ... OTP gizmos ... passwords ... gatewayed  
credentials (delegation)

# How do we resolve this?



Focus on a few things that work ... be flexible though

For the US:

- Recognize the need for multiple, layered identity
- Focus on NSTIC as the model for dealing with public ID
- Pick SAML as the platform for doing ID business
  - This translates to SIF (a/k/a SciFed) and DOE-ICAM in DOE lab space
- Look closely at web vs command-line issues - this is a huge problem for collaborations and determines what we need to support
  - Can command-line tools be phased out -or- become web-dependent?

# What do YOU need to do?



## US projects:

You need to tell your project leadership, your site leadership, and anyone else who makes decisions, to make sure *both projects and sites* join SIF and InCommon.

You need to tell your *Program Office* and your *funders* that this federation needs to happen.

This is how you got DOEGrids CA 10 years ago, and this is how you will get federation. It's not anybody's job to do this yet.

## Non-US projects:

You need to make it clear to US projects that they need to do this. This is how you got DOEGrids CA 10 years ago....

# SIF - Science Identity Federation



The next part of the slide deck is the argument for SIF to US DOE national lab participants - CIOs, IT staff, projects.

# Science Identity Challenges



- Collaborations need scalable "security" infrastructure
  - Authentication ... Authorization ... Identity
- Environment is diverse
  - DOE sites ... Projects ... Academia ... Industry
- Different security and identity objectives
- Internet is changing
  - Social network
- Internet identity and security environment is changing
  - Software, protocols, APIs, principles and practices
- Efficiency and process
  - We have a lot of identity "process" locked up in sites
  - Why build new identity silos for each new service?



- **Interoperable Identity for DOE labs**
- *... based on the well-known*
- **Shibboleth authentication & authorization software from [Internet2](#)**
- *... so that labs can also*
- **Federate with InCommon**
  - US Higher Education Shibboleth Federation: see [InCommonfederation.org](http://InCommonfederation.org)
- .... and other federations as needed

# What Is InCommon?

A screenshot of a Mozilla Firefox browser window displaying the InCommon website. The page title is "Current InCommon Participants". The main content area features a table with three columns: "Higher Education Participants (202)", "Government and Nonprofit Laboratories, Research Centers, and Agencies (8)", and "Sponsored Partners (72)". Each column lists several member organizations with blue underlined links. A sidebar on the left contains a navigation menu with items like "Home", "New to InCommon?", "Participants and Affiliates", and "Assurance Profiles".

Higher Education Participants (202)	Government and Nonprofit Laboratories, Research Centers, and Agencies (8)	Sponsored Partners (72)
<a href="#">American University</a>	<a href="#">Argonne National Laboratory</a>	<a href="#">Absolute Software, Inc.</a>
<a href="#">Arizona State University</a>	<a href="#">Energy Sciences Network (ESNet)</a>	<a href="#">ALEKS Corporation</a>
<a href="#">Augsburg College</a>	<a href="#">Fermi National Accelerator Laboratory</a>	<a href="#">Alexander Street Press</a>
<a href="#">Baylor College of Medicine</a>	<a href="#">Lawrence Berkeley National Laboratory</a>	<a href="#">Apple - iTunes U</a>
<a href="#">Baylor University</a>		<a href="#">Atlas Systems, Inc.</a>
<a href="#">Boise State University</a>		<a href="#">BioOne, Inc.</a>
<a href="#">Brown University</a>		<a href="#">Blackboard, Inc.</a>
<a href="#">California Institute of Technology</a>		<a href="#">Blatant Media Corporation</a>
		<a href="#">Buxton Group</a>

<http://www.incommon.org/>





## Why do we need this?



- DOE's science projects are large-scale collaborations
- Projects rely on sites for infrastructure
- Project membership: academia in US and abroad

The best answer for this is InCommon federation



# Science Collaborations (Sample)



- HE Physics
  - LHC collaborations (ATLAS, CMS, ...)
  - Daya Bay (neutrino)
- Nuclear Physics
  - RHIC
- Fusion
  - ITER
- "Basic Energy Sciences" - Materials, Geo, Bio
  - User facilities (\*-beam scattering)
- Biology/Environmental
  - Genome
  - Biofuels



# DOE User facilities



- DOE provides over 60 scientific user facilities
- Unique, unparalleled "toolbox" for scientific research
- They come and go

*Can we make new and existing user facilities easier to use?*



# Entanglement



- Many partnerships between DOE and academia
  - Scientific personnel
  - User facilities
- Cross-agency support
  - NSF
  - NOAA
  - and others

*We need a broadly-supported identity infrastructure.*



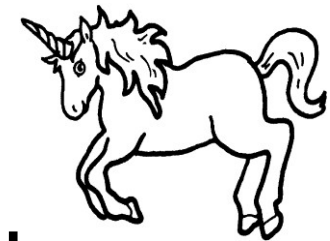
## What are we doing today?



- SIF is functioning as a sub-federation of InCommon
- 3-year *voluntary* membership program
- *Next:* Focus on getting IDPs up and in production in InCommon

# Challenges

- Just getting IDPs up!
- Standards - our community does not understand LOA / NIST 800-63 / ICAM
  - Academia/foreign *really* don't understand this
- No one cares about identity - they care about *applications*
- Magical thinking -
- Support - this is no one's job to build





# SIF contact information



- <http://groups.google.com/group/science-federation>
- *Or*
- Go to **groups.google.com** and
- Search for **science federation**
- *Or*
- Contact me:
- Michael Helm
- [helm@es.net](mailto:helm@es.net) **+1-510-621-7353**