

Federated Identity
for
Scientific Collaborations:
Policy Issues

Jim Basney
jbasney@ncsa.uiuc.edu

2nd Workshop on Federated Identity Systems for
Scientific Collaborations
STFC at Rutherford Appleton Laboratory in the UK
2-3 November 2011

About Me

- Project staff for:
 - Open Science Grid (www.opensciencegrid.org)
 - XSEDE (www.xsede.org) (TeraGrid follow-on)
- Member:
 - InCommon Technical Advisory Committee (www.incommon.org/about)
 - TAGPMA (www.tagpma.org)
- Project lead for:
 - CILogon (www.cilogon.org)
 - MyProxy (myproxy.ncsa.uiuc.edu)
 - GSI-OpenSSH (grid.ncsa.uiuc.edu/ssh)
 - www.sciencegatewaysecurity.org



What is my definition of a community?

- Simply: A group of scientists working together, using common cyberinfrastructure
- Examples:
 - *Virtual Organization* in Open Science Grid
 - *Science Gateway* in XSEDE
 - *Project* in XSEDE
 - *Research and Scholarship* community in InCommon
 - CILogon user community:
 - *Ocean Observatories Initiative* users
 - *DataONE* users

What must a community do to be recognized?

- Register a new Virtual Organization with OSG
(http://www.opensciencegrid.org/About/Getting_Started_with_OSG/Form_New_VO)
- Apply for an XSEDE Project allocation
(<https://www.xsede.org/allocations>)
- Register an XSEDE Science Gateway
(<https://www.xsede.org/register-gateway>)
- Register as an InCommon R&S Service Provider
(<https://spaces.internet2.edu/x/-IKVAQ>)
- Request a custom CILogon instance
(help@cilogon.org)

Federated ID Use Cases

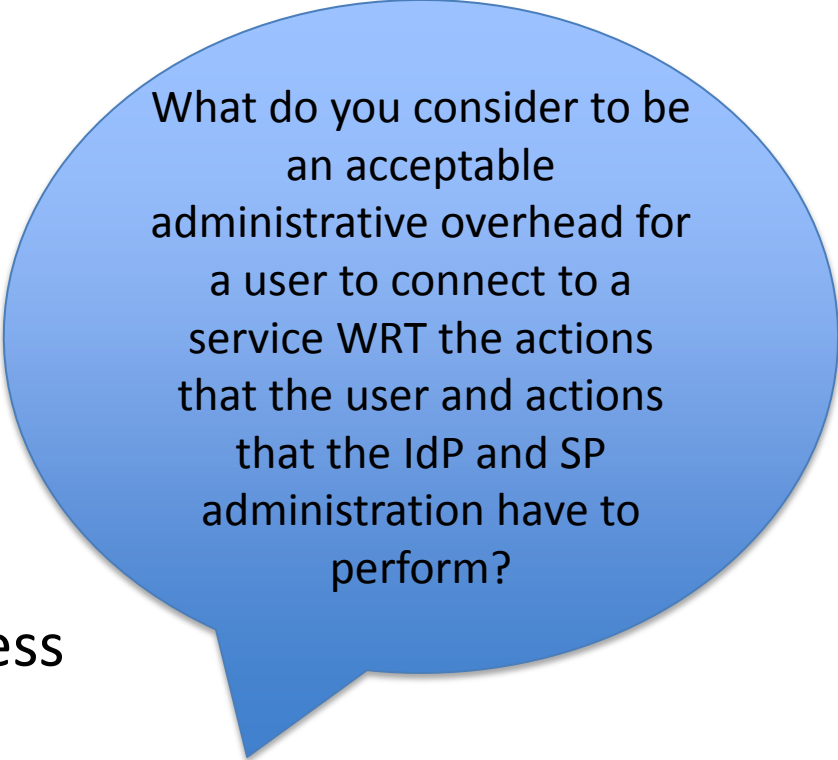
1. Federating project-managed identities (example: LIGO/Virgo)
2. Linking project-managed identities with external identities
 - SAML + OpenID + ...
 - International inter-federation
3. Integration across browser and non-browser (thick client, command-line, etc.) apps
4. Multi-tier apps: portals, glide-ins, pilot jobs

Lessons Learned

- InCommon today supports **browser SSO**
 - SAML->X.509 bridges are common for non-web apps (CILogon, TERENA Certificate Service, etc.)
 - SAML ECP adopted by ~5 InCommon IdPs so far (<http://www.cilogon.org/ecp>)
- Attribute release is a major challenge today for SPs that want to support many IdPs
- Google OpenID is a popular “catch-all” IdP
 - US ICAM LOA 1 certified (<http://openididentityexchange.org/certified-providers>)

Overhead of On-boarding

- User may need to approve attribute release
- User may need to provide additional information during a service-specific registration process
- IdP must scale to many SPs
 - Attribute release policy using federation managed SP “tags”
 - Federation metadata for UI elements, public keys, etc.
- SP must scale to many IdPs
 - Apply to federation(s), not individual IdPs
 - Leverage federation metadata as with idP
- User should not need to email IdP and SP administrators to make this work!



What do you consider to be an acceptable administrative overhead for a user to connect to a service WRT the actions that the user and actions that the IdP and SP administration have to perform?

Attribute Release Policies

- Per-Project / Per-SP doesn't scale
- Alternatives:
 - Release defined attribute bundles (targetedID, “directory attributes”), with user consent, to projects/SPs approved (“tagged”) by federation
 - Handle attribute release problems at SP
 - Automated request to IdP for attribute release
 - Don't leave user stranded – redirect to “catch-all” IdPs

Can IdPs serve many concurrent and distinct projects?

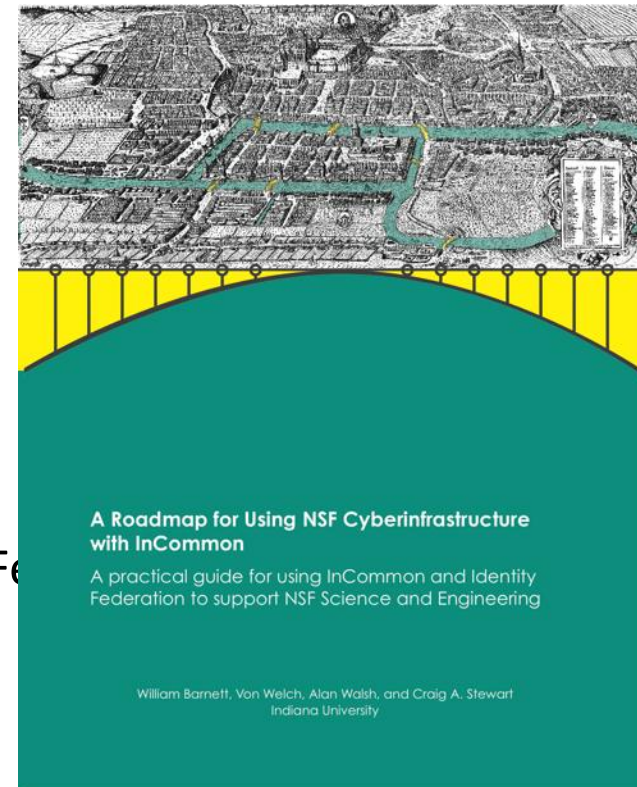
- Yes!
- Motivation
 - Expensive and inconvenient for every project to operate its own IdP(s)
 - Better to leverage cost of IdP operations across multiple projects
- How: General-purpose IdPs
 - Examples: University IdPs, IGTF CAs, Google OpenID, ProtectNetwork, Globus Online
 - Projects still need to manage their own attributes

Are there any efforts to bring harmonization of identity attributes across federations?

- Yes!
- MACE-Dir
(<http://middleware.internet2.edu/dir/>)
- REFEDS
(<http://www.terena.org/refeds>)

References

- A Roadmap for Using NSF CyberInfrastructure with InCommon
(<http://www.incommon.org/nsfroadmap>)
- An Analysis of the Benefits and Risks to LIGO When Participating in Identity Federations
(<http://www.google.com/search?q=LIGOIdentityFederationRiskAnalysis.pdf>)
- Federated Security Incident Response
(<https://spaces.internet2.edu/x/8o6KAQ>)



Thanks!

Questions/Comments?

Contact: jbasney@ncsa.uiuc.edu