Federating Identities for Researchers

Jim Basney
jbasney@ncsa.uiuc.edu

This material is based upon work supported by the National Science Foundation under grant number 0943633. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
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
A Roadmap for Using NSF Cyberinfrastructure with InCommon

A helpful guide for CI projects

Discusses the role of CILogon

www.incommon.org/nsfroadmap
Prior Work: go.teragrid.org

- Campus login to TeraGrid
- 35 campuses so far
- Uses TeraGrid ID vetting
- Available since Sep 2009
- TeraGrid to XSEDE transition in progress
- Integration with portal.xsede.org planned
- IDtrust 2010 paper: “Federated Login to TeraGrid” (http://middleware.internet2.edu/idtrust/2010/)
CILogon Service: cilogon.org

- No TeraGrid account required
- Supports InCommon and OpenID authentication
  - 43 InCommon IdPs so far
- Delivers certificates to desktop, browser, and portals
- Available certificate lifetimes: from 1 hour to 13 months
- Supports close integration with CI projects
- Available now!
- FAQ: www.cilogon.org/faq
Why certificates?

• Command-line apps, non-web apps
• Multi-stage, unattended batch workflows
• Significant worldwide CI investment in PKI
  – Software, operations, standards, etc.
Levels of Assurance

• LOA requirements differ across scientific collaborations
  – 2-factor authentication
  – IGTF accreditation
  – Open access with usage statistics

• CILogon LOA options:
  – InCommon Silver: US Gov’t ICAM Level 2
    • Produces IGTF accredited certificates
  – OpenID OIX: US Gov’t ICAM Level 1
  – InCommon “Basic”
CILogon Portal Delegation

- Science Gateways (portals) provide web interfaces to CI
  - Need credentials to access CI on researchers’ behalf
- CILogon Delegation Service allows researchers to approve certificate issuance to portals (via OAuth)

www.cilogon.org/portal-delegation
Integration Example: OOI
Integration Example: OOI
Integration Example: OOI
Integration Example: OOI
More Integration Examples
Support for Non-Browser Apps

• Option #1:
  – Use browser-based authentication (SAML, OpenID)
  – Get URL for certificate download (wget/curl)
    • Or use Java Web Start, etc.
  – Use certificate for non-browser authentication
  – *Unfortunately still requires a browser*

• Option #2
  – Use SAML Enhanced Client or Proxy (ECP) authentication *outside the browser* to download certificate
  – ECP adoption by InCommon campuses beginning
    • Successfully tested with U Washington, U Chicago, LTER, and ProtectNetwork
  – For more info: http://www.cilogon.org/ecp
ECP Example

$ curl -sSO https://cilogon.org/ecp.pl

$ perl ecp.pl --get cert -c create -k userkey.pem -o usercert.pem -t 12

Select an Identity Provider (IdP):
  1> LTER Network
  2> ProtectNetwork
  3> University of Chicago
  4> University of Washington
  5> Specify the URL of another IdP

Choose [2]: 2

Enter a username for the Identity Provider: jbasney

Enter a password for the Identity Provider: ************

$ grid-proxy-init -cert usercert.pem -key userkey.pem -hours 4

Your identity: /DC=org/DC=cilogon/C=US/O=ProtectNetwork/CN=Jim Basney A685

Creating proxy ....................... Done

$ gsissh citest.example.edu

[jbasney@citest ~]$
Thanks

For more information:

www.cilogon.org/faq

info@cilogon.org