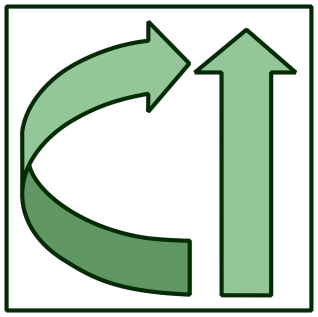


CILogon

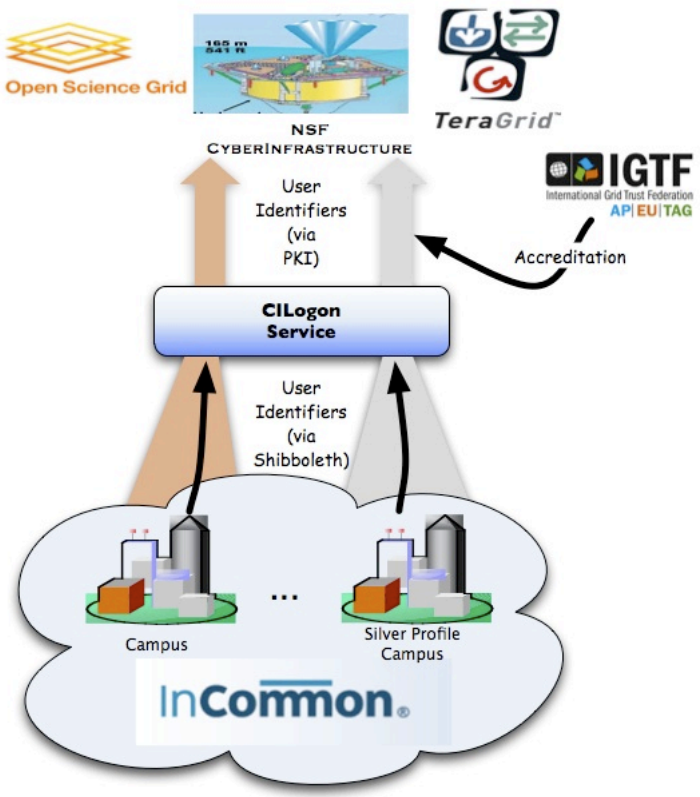
Bridges between Campus and National Cyberinfrastructure

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.

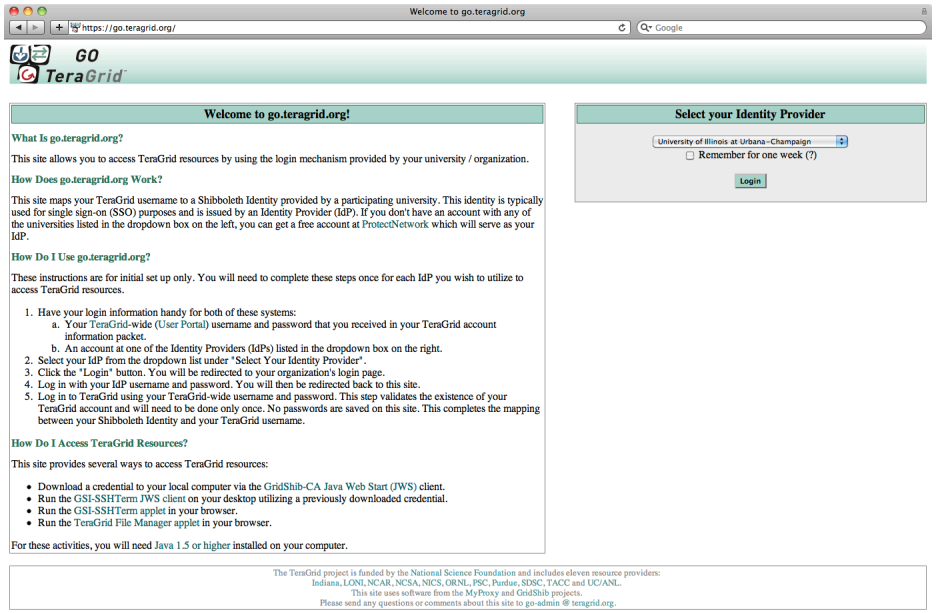
CILogon Goal

- Facilitate campus logon to CI
  - Leverage researchers' existing credentials at their home institution
  - Ease credential management for researchers and CI providers
- Bridge from:
  - Credentials issued by InCommon Federation members using SAML web browser single sign-on
- Bridge to:
  - X.509 certificates that satisfy the requirements of CI projects



Initial Success: go.teragrid.org

- Campus login to TeraGrid
- 31 campuses so far (including all CIC schools)
- In production since September 2009
- 1000+ certificates issued so far to 65+ users
- Integration with portal.teragrid.org underway
- IDtrust 2010 paper: "Federated Login to TeraGrid" (http://middleware.internet2.edu/idtrust/2010/)



New Service: cilogon.org

- No TeraGrid account required
- Delivers certificates to desktop or browser
- Available certificate lifetimes: from 1 hour to 13 months
- 3 Certification Authorities:
  - Silver: InCommon Silver IDs
  - Basic: any InCommon IDs
  - OpenID: any OpenIDs
- Available now!

Why certificates?

- Command-line interfaces, non-web apps
- Multi-stage, unattended batch workflows
- Significant worldwide CI investment in PKI
  - Software, operations, standards, etc.

International Grid Trust Federation

- Worldwide accreditation of grid CAs
  - Relying Parties: TeraGrid, Open Science Grid, European Grid Infrastructure, Worldwide LHC Computing Grid, and others
  - Standards: CA operations, key management, subscriber identity vetting, certificate profiles

www.igft.net

CILogon and IGTF

- CILogon CA operations, key management, and certificate profiles meet IGTF standards
- Issue: subscriber ID vetting & authentication
  - Goal: rely on campuses for this
  - Need minimum standards for campus practices
  - Approach: rely on InCommon Identity Assurance
- Status:
  - CILogon Silver CA accredited October 2010
  - Now waiting for InCommon Silver campuses…
  - CILogon Basic & OpenID CAs operating w/o IGTF accreditation

Challenges

- Identity Assurance:
  IGTF and InCommon Silver
- Identifiers
- Attribute Release

Identifiers

- We require globally-unique, persistent, non-reassigned identifiers
  - Ensure that each certificate subject is assigned to a unique individual
    - Also: issue multiple certificates with a consistent certificate subject to the same individual
  - Opaque identifiers are OK
  - Options:
    - eduPersonTargetedID (ePTID)
    - eduPersonPrincipalName (ePPN)
      - But ePPN may be reassigned

Attribute Release

- The “boarding process” challenge:
  - CI users are spread across many campuses
  - Often few CI users on each campus
- Each campus must approve release of attributes to cilogon.org / go.teragrid.org
  - CILogon needs ePTID/ePPN, mail, givenName and surname
  - Self-service sign-up: https://cilogon.org/secure/testidp/
- Excellent application for user consent based attribute release (uApprove)

Conclusions

- We're leveraging campus credentials for access to cyberinfrastructure
  - SAML to PKI bridges: go.teragrid.org & cilogon.org
- Improvements underway
  - InCommon Identity Assurance
  - Consent-based attribute release (uApprove)

Thanks

For more information:

www.cilogon.org

info@cilogon.org