CILogon

Identity Management Challenges Middleware And Grid Interagency Coordination

Jim Basney
jbasney@ncsa.uiuc.edu

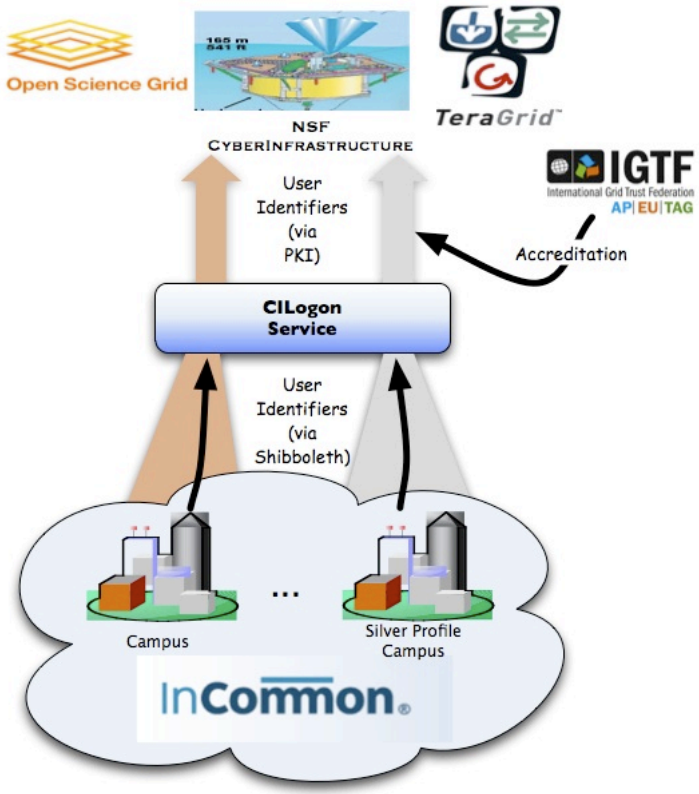
This material is based upon work supported by the National Science Foundation under grant number 0943633 and by the Department of Energy under award number DE-SC0008597. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government or any agency thereof.

Presentation Topics

- What problem space does CILogon address?
- What identity management issues are not addressed by CILogon?

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



CILogon Service
(https://cilogon.org)

- Supports InCommon and OpenID authentication
- Delivers certificates to desktop, browser, and portals
- Available certificate lifetimes: from 1 hour to 13 months
- Supports close integration with CI projects
- Available now!
- See also:

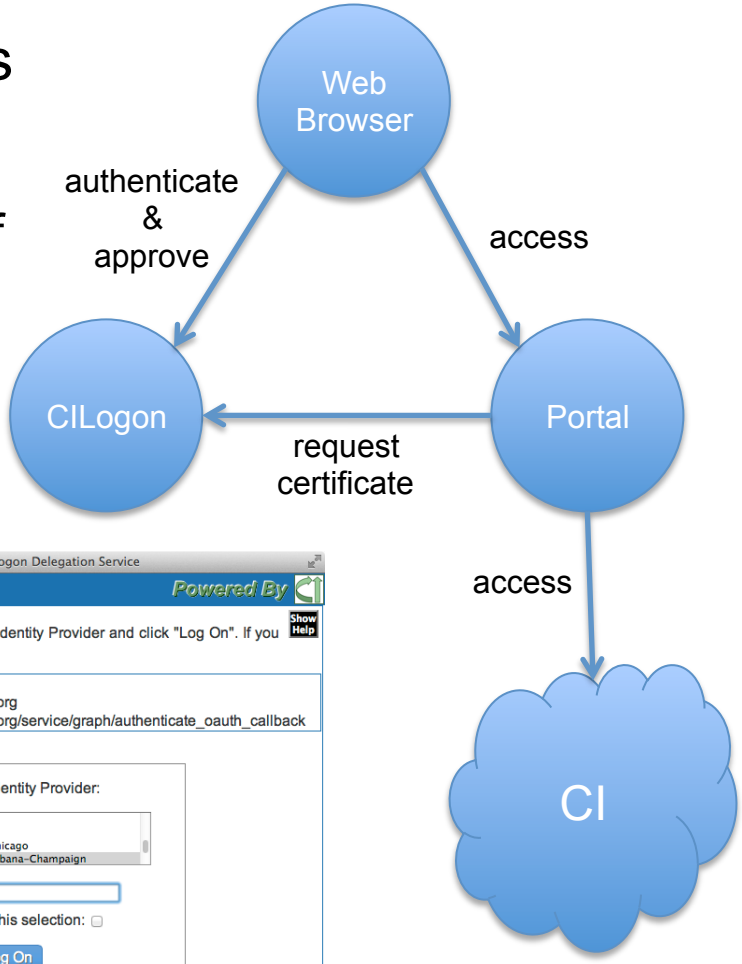
  http://www.cilogon.org/faq

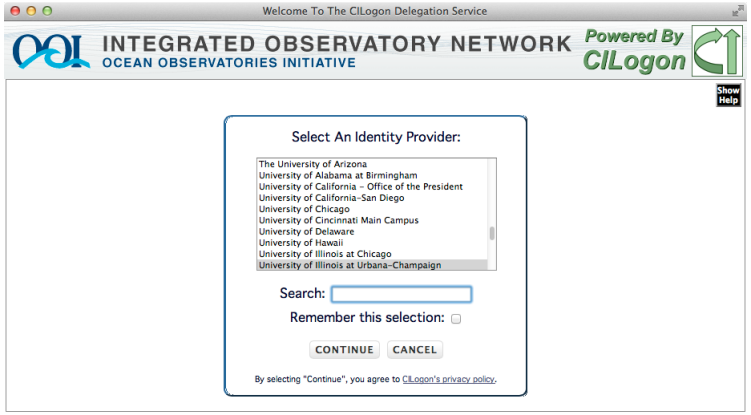
  http://www.cilogon.org/news

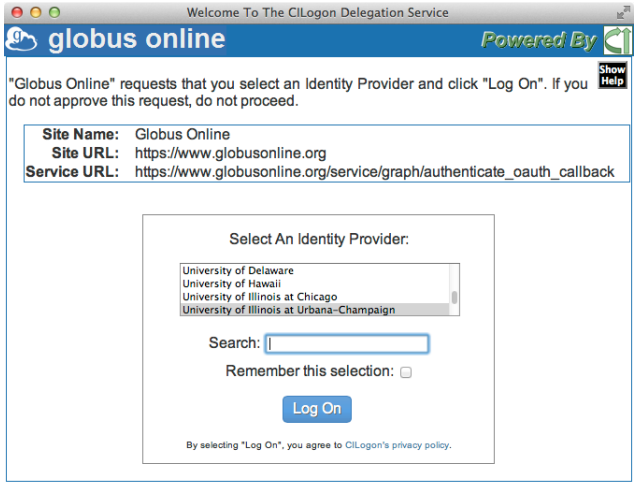
  http://ca.cilogon.org

CILogon Portal Delegation

- Grid Portals and Science Gateways provide web interfaces to CI
  - Portals/Gateways need certificates to access CI on researchers' behalf
- CILogon Delegation Service allows researchers to approve certificate issuance to portals (via **OAuth**)
- www.cilogon.org/portal-delegation







Levels of Assurance

- LOA requirements differ across scientific collaborations
  - 2-factor authentication
  - IGTF accreditation
  - Open access with usage reporting
- CILogon LOA options:
  - InCommon Silver: US Gov't ICAM Level 2
  - OpenID OIX: US Gov't ICAM Level 1
  - InCommon "Basic"
  - 2nd factor authentication (coming soon)

Adding a 2nd Factor

Google Authenticator Registration

Google Authenticator Registration

Step 1

Download the Google Authenticator app specific to your device.

- Android OS (2.1 and higher) (QR Code Link)
- Apple iOS (3.1.3 and higher) (QR Code Link)
- BlackBerry OS (4.5-6.0) (QR Code Link)

Step 2

Launch the Google Authenticator app and add your token by scanning the QR code or by entering the account information shown below.

Account Name: A534@cilogon.org
Key: R63YPJNYDWVB3KTH
Type of Key: Time based

Step 3

Click the "Verify" button to log in with a one-time password generated by the Google Authenticator app.

Verify

Google Authenticator Login

CILogon Service

Google Authenticator Login

Your account has been configured to use Google Authenticator as a second authentication factor. Enter a one-time passcode as generated by the app below.

Account: A534@cilogon.org

Passcode: 177799

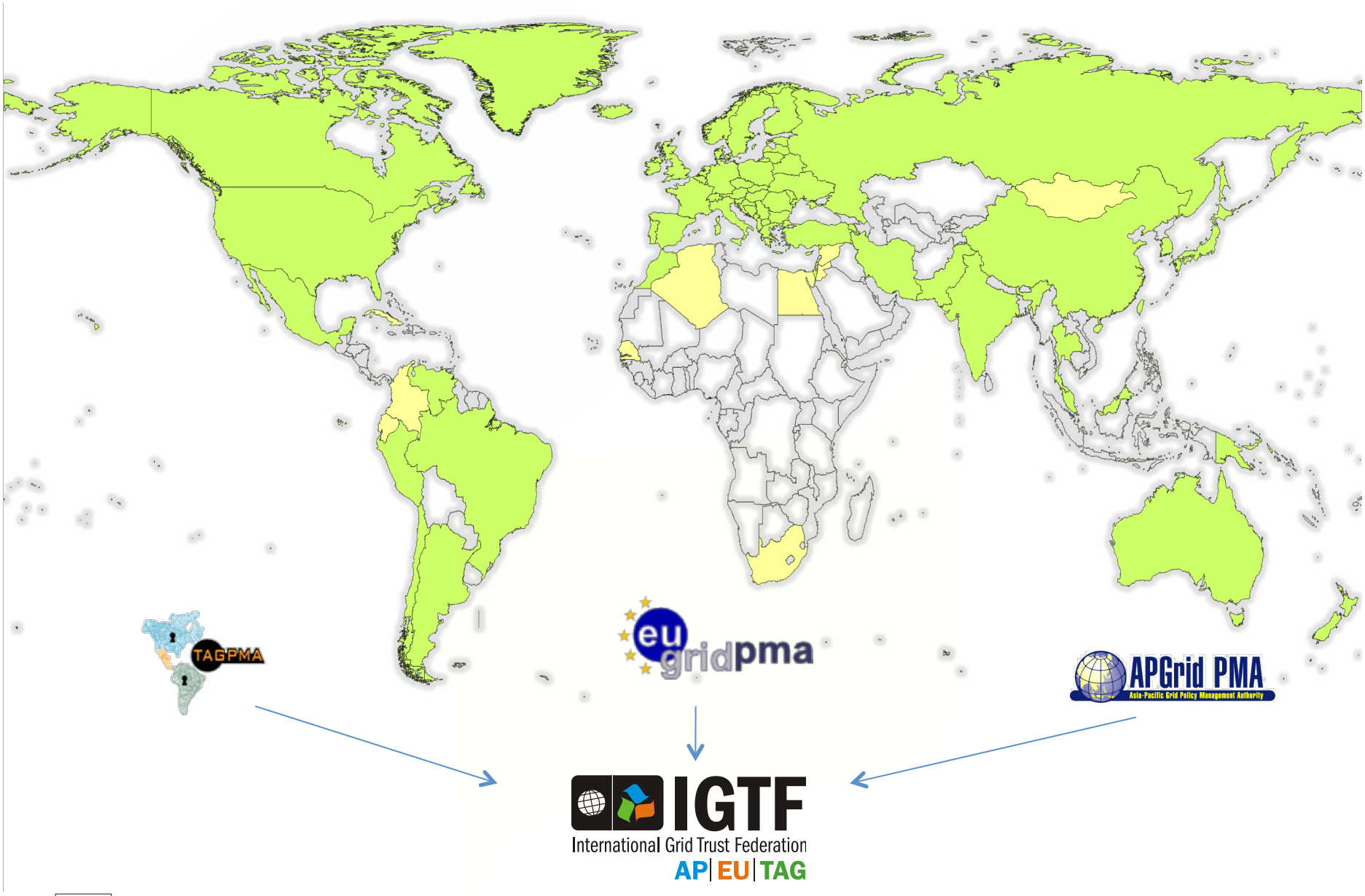
Enter

Don't have your phone with you?

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.

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)
  - Virginia Tech certified InCommon Silver (October 2012)
  - Virginia Tech members use CILogon Silver certificates to access Open Science Grid services (October 2012)
  - CILogon Basic & OpenID CAs being actively used w/o IGTF accreditation


TAGPMA
eugridpma
APGrid PMA
Asia-Pacific Grid Policy Management Authority
IGTF
International Grid Trust Federation
AP | EU | TAG

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
  - *Still requires a browser for initial authentication*
- 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, U Wisconsin-Madison, LIGO, 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 ~]$
```

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 challenge today for SPs that want to support many IdPs
  - New InCommon effort is addressing this challenge: https://spaces.internet2.edu/display/InCCollaborate/Research+and+Scholarship+Category
- Google OpenID is a popular “catch-all” IdP
  - US ICAM LOA 1 certified (http://openidentityexchange.org/certified-providers)

Out of Scope for CILogon

(CILogon depends on others
to address these issues)

- Initial identity vetting
- Linking multiple identities
- Name, email address, and IdP changes
- Authorization
- Group memberships
- Roles
- Credentialing users outside USA

Thanks!

For more information:

www.cilogon.org

info@cilogon.org