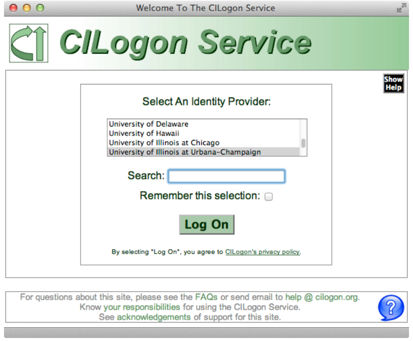
CILogon-HA:
Higher Assurance Federated Identities for DOE Science

PI: Jim Basney <jbasney@ncsa.illinois.edu>

Sep 2012 - Aug 2015

OBJECTIVES

- Support use of federated identities via web browsers and other interfaces.
- Support adoption of the InCommon assurance program.
- Enable interoperable use of federated identities via international standards.



Select An Identity Provider:

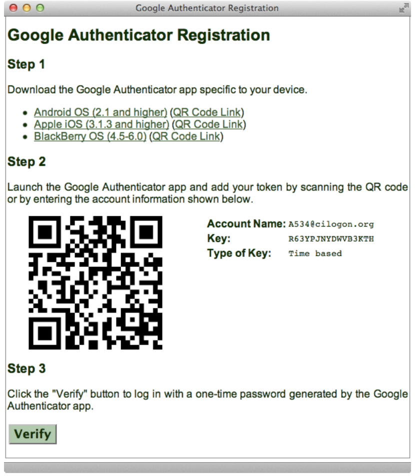
University of Delaware
University of Hawaii
University of Illinois at Chicago
University of Illinois at Urbana-Champaign

Search:

Remember this selection: □

By selecting "Log On", you agree to CILogon's privacy policy.

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.



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.

IMPACT

CILogon-HA enables convenient and secure access by university researchers to DOE facilities for **collaborative science using higher assurance identities** provided by the nation's universities through the InCommon assurance program.

PROGRESS & ACCOMPLISHMENTS

- Use of InCommon Silver (LOA 2) federated identities from Virginia Tech to Open Science Grid via CILogon-HA
- Google Authenticator (OATH) second factor authentication supported by CILogon-HA

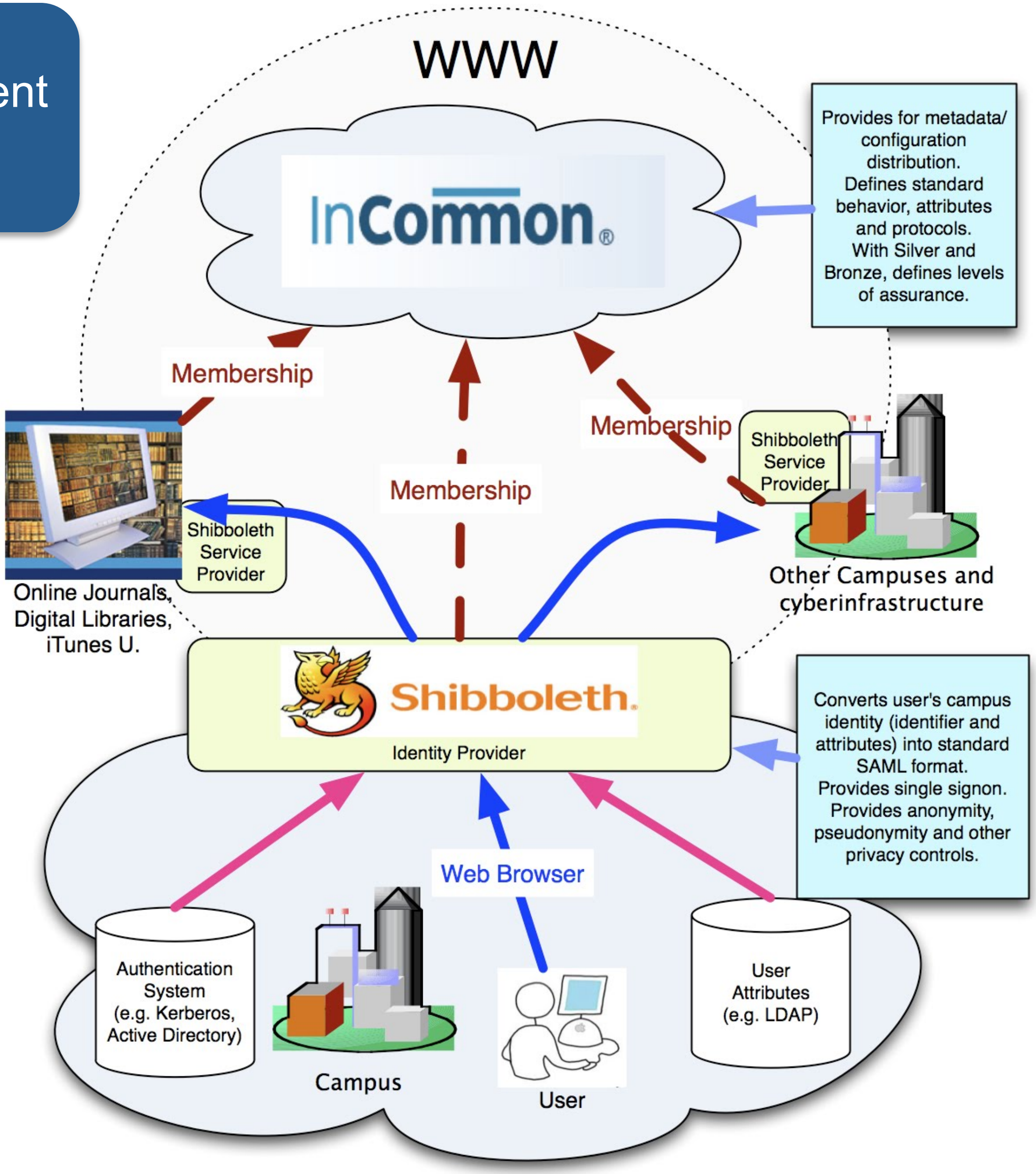
CILogon

www.cilogon.org

Talk Outline

- Identity Federation
- Levels of Assurance
- CILogon-HA Project
  - – CILogon CAs
  - – Two factor authentication
  - – Federated identity outside the browser
  - – Partner projects

Federation eases the credential management burden for users and service providers.

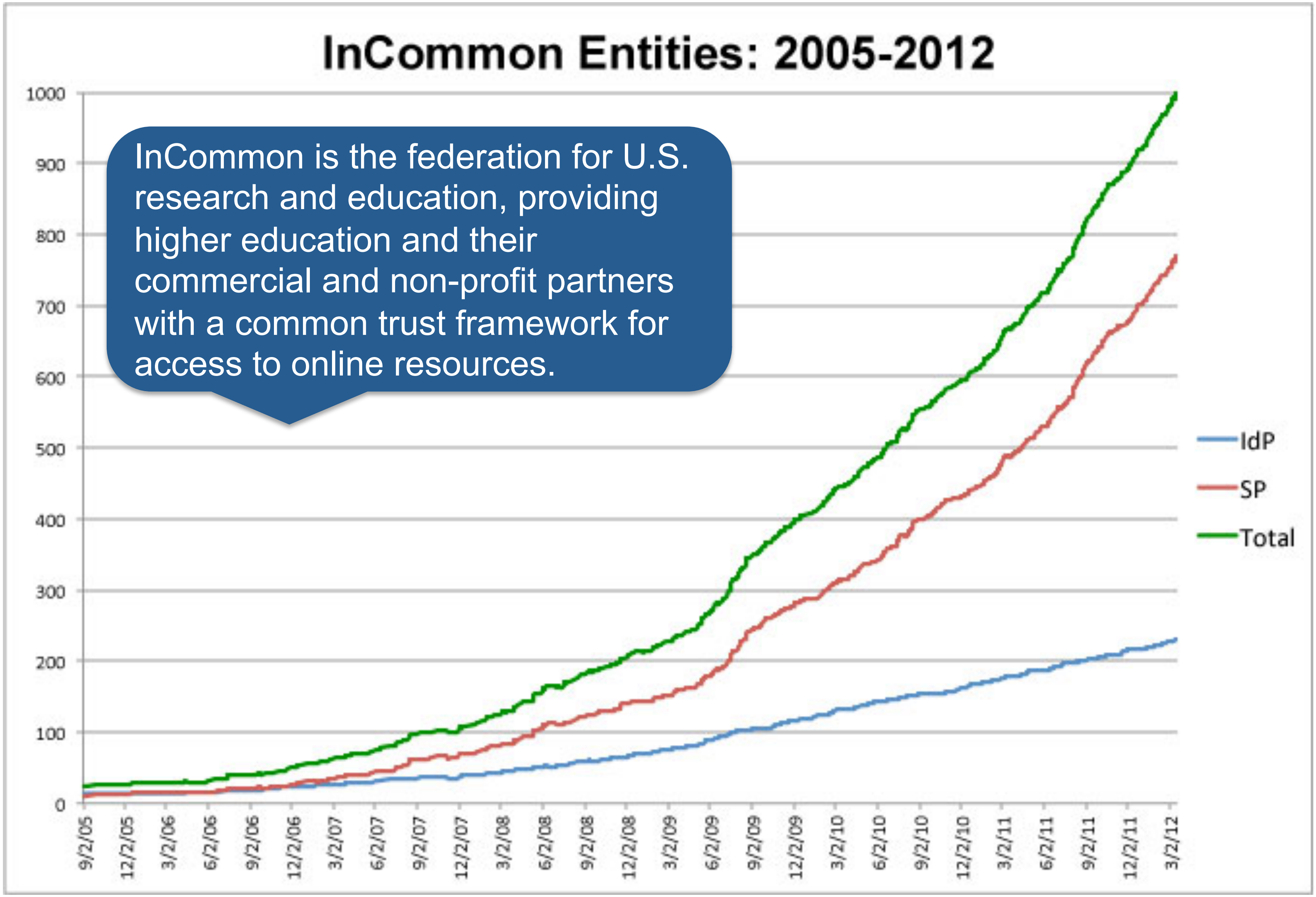

WWW
InCommon®
Membership
Membership
Membership
Shibboleth Service Provider
Online Journals, Digital Libraries, iTunes U.
Shibboleth Service Provider
Other Campuses and cyberinfrastructure
Shibboleth
Identity Provider
Web Browser
Authentication System (e.g. Kerberos, Active Directory)
Campus
User
User Attributes (e.g. LDAP)

Provides for metadata/ configuration distribution. Defines standard behavior, attributes and protocols. With Silver and Bronze, defines levels of assurance.

Converts user's campus identity (identifier and attributes) into standard SAML format. Provides single signon. Provides anonymity, pseudonymity and other privacy controls.

CILogon

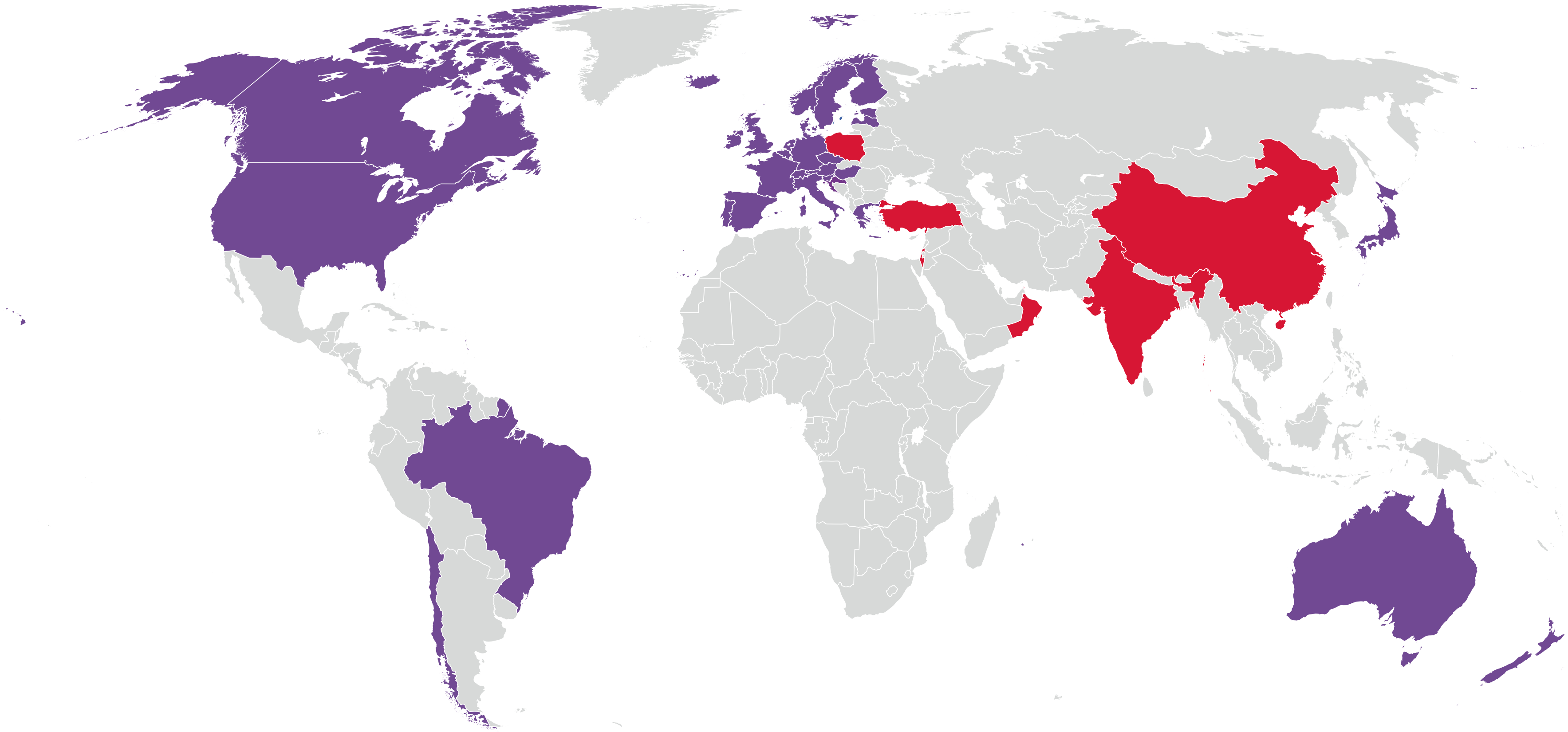
www.cilogon.org



InCommon is the federation for U.S. research and education, providing higher education and their commercial and non-profit partners with a common trust framework for access to online resources.

Research and Education Identity Federations

REFEDS



🟪 **Identity Federations in production**

AT	ACOnet Identity Federation
AU	Australian Access Federation AAF
BE	Belnet R&E Federation
BR	CAFe
CA	Canadian Access Federation CAF
CH	SWITCHaai
CL	COFRe
CZ	eduID.cz
DE	DFN-AAI
DK	WAYF
EE	TAAT
ES	SIR
FI	Haka
FR	Fédération Éducation-Recherche
GR	GRNET
HR	AAI@EduHr
HU	eduID.hu
IE	Edugate
IT	IDEM
JP	GakuNin
LV	LAIFE
NL	SURFfederatie
NO	FEIDE
NZ	Tuakiri New Zealand Access Federation
PT	RCTSaai
SE	SWAMID
SI	ArnesAAI Slovenska
UK	UK Access Management Federation for Education and Research
US	InCommon
int	IGTF

🟥 **Identity Federations in pilot**

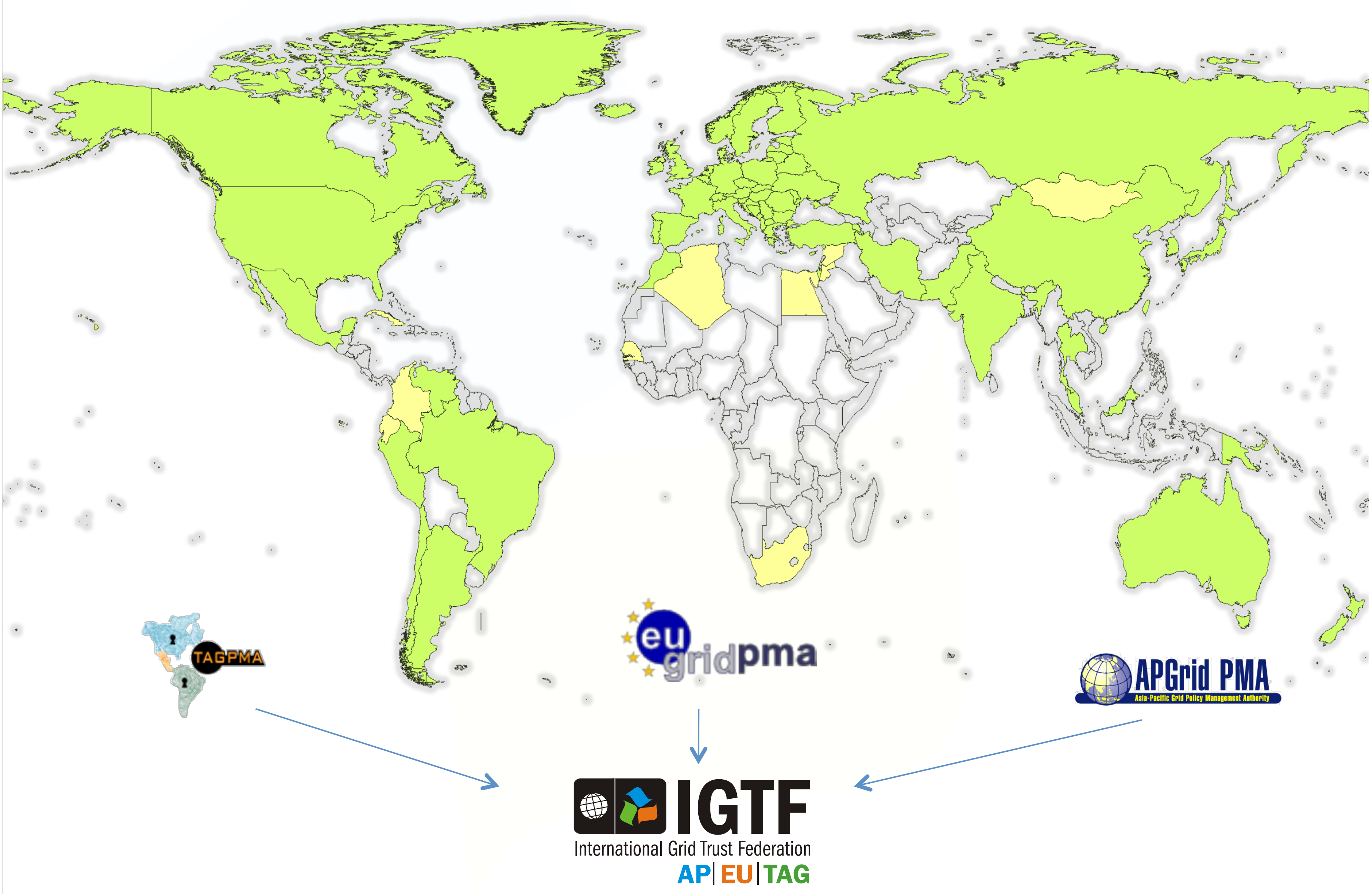
CN	CARSI
IN	INFED
OM	Oman Knowledge ID Federation
PL	Poland Identity Federation
TR	ULAKAAI
IL	IsraGrid Federation

This map is intended to provide a high-level overview of countries with identity federations.

Last update: 14 January 2013

CILogon

www.cilogon.org


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

Levels of Assurance

- LOA requirements differ across scientific collaborations
  - Open access with usage reporting
  - IGTF accreditation
  - 2-factor authentication
- NIST 800-63 & US ICAM Trust Framework
  - Level 1:No identity proofing. Basic strength of authentication.
  - Level 2: Basic identity proofing. Single factor remote network authentication.
  - Level 3: Strong identity proofing. Multi-factor remote network authentication.
  - Level 4: In-person identity proofing. Tamper evident hardware cryptographic authentication tokens.

InCommon Assurance Program

- Launched in February 2012
- InCommon is an approved
  US ICAM Trust Framework Provider
  (www.idmanagement.gov)
- LOA 1 – InCommon Bronze
- LOA 2 – InCommon Silver
- Virginia Tech was first InCommon Silver certified identity provider (Sep 2012)
- More info: www.incommon.org/assurance

International Assurance Standards

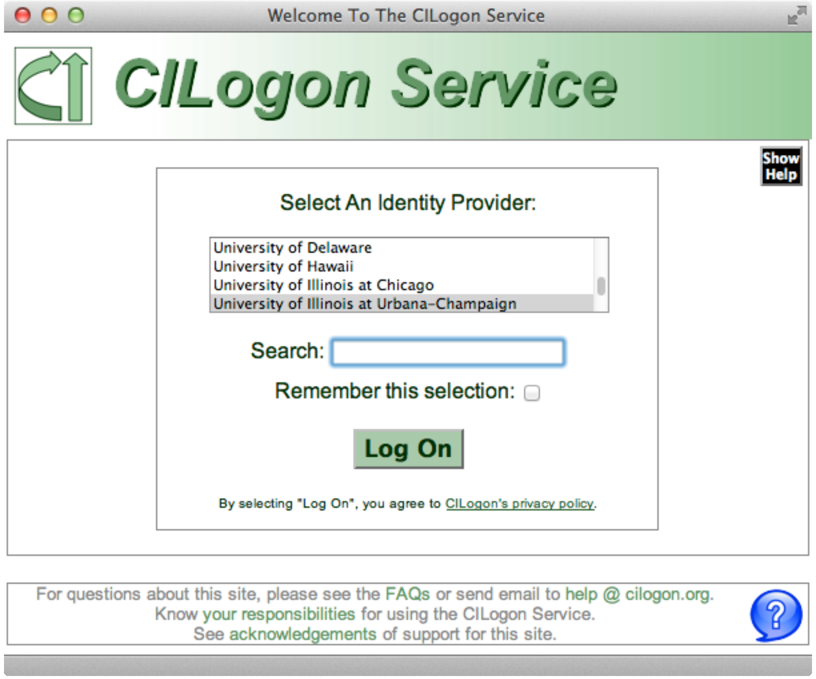
- REFEDS activities
  - LOA for R&E Federations
    - https://refeds.terena.org/index.php/LOA_for_RANDE_Federations
  - LEGO - Linked Education and Government Online
    - https://refeds.terena.org/index.php/LEGO
- IANA LOA registry
  - http://levelofassurance.org/
- Kantara Identity Assurance
  - http://kantarainitiative.org/idassurance/
- Open Identity Exchange (OIX)
  - http://openidentityexchange.org/certification-process

CILogon-HA Activities

- Issuing IGTF accredited certificates via InCommon Silver accredited identity providers.
- Engaging with DOE scientific collaborations (such as Open Science Grid) on use of federated identities.
- Expanding support for federated authentication outside the browser.
- Adopting multi-factor authentication for federated identities.
- Establishing international interoperability for DOE science collaborations using higher assurance federated identities.
- Exploring high assurance identities from commercial providers (Google, PayPal, Verizon, etc.).

CILogon Service (https://cilogon.org)

- Developed by NSF-funded CILogon project (Sep 2009 – Aug 2013)
- Supports InCommon and OpenID authentication
- Delivers X.509 certificates to desktop, browser, and portals
- Available certificate lifetimes: from 1 hour to 13 months
- Supports close integration with CI projects
- See also:
  - http://www.cilogon.org/faq
  - http://www.cilogon.org/news
  - http://ca.cilogon.org



Select An Identity Provider:

University of Delaware
University of Hawaii
University of Illinois at Chicago
University of Illinois at Urbana-Champaign

Search:

Remember this selection: □

By selecting "Log On", you agree to CILogon's privacy policy.

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.

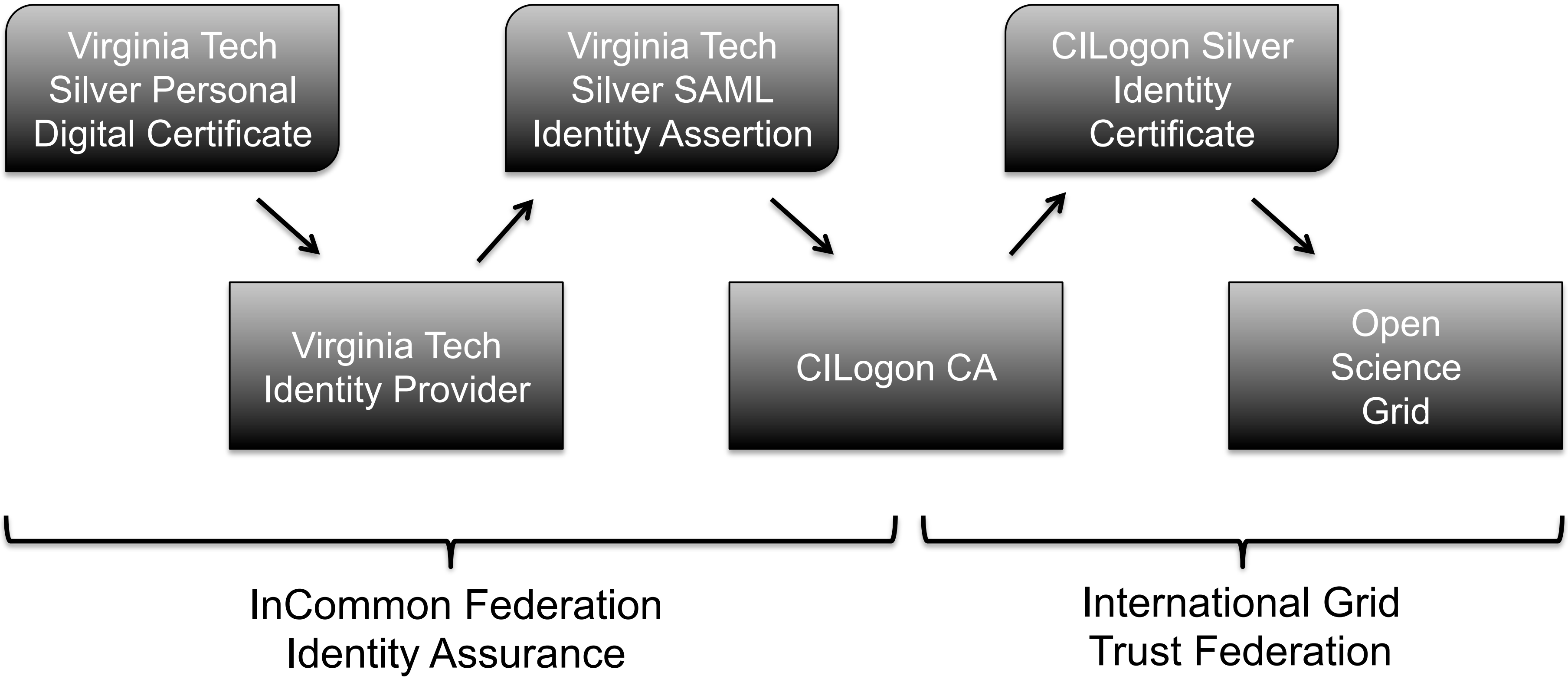
CILogon and IGTF

- 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

LOA of CILogon CAs

CA	Registration Authorities	User Identities	Accreditation
Silver	InCommon Silver IdPs (ICAM LOA 2)	LOA 2	IGTF
Basic	InCommon IdPs	Varies	None
OpenID	OpenID Providers (ICAM LOA 1)	Self asserted	None

Virginia Tech to OSG with Silver



Virginia Tech Silver Personal Digital Certificate

Virginia Tech Identity Provider

Virginia Tech Silver SAML Identity Assertion

CILogon CA

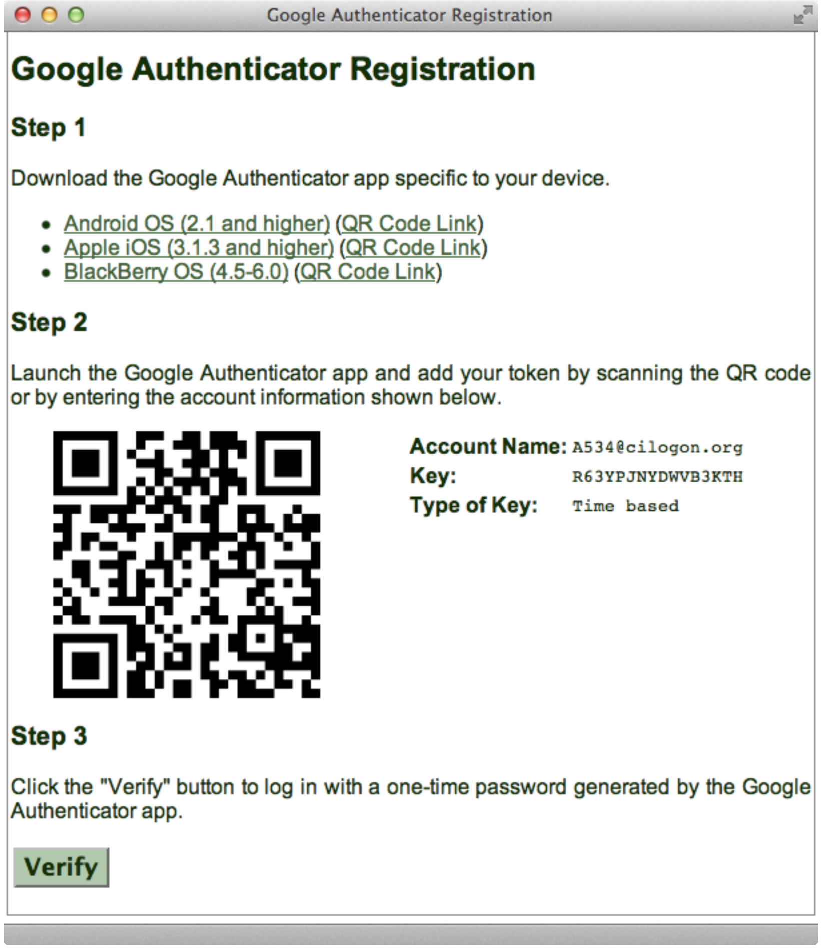
CILogon Silver Identity Certificate

Open Science Grid

InCommon Federation Identity Assurance

International Grid Trust Federation

Adding a 2nd Factor



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)

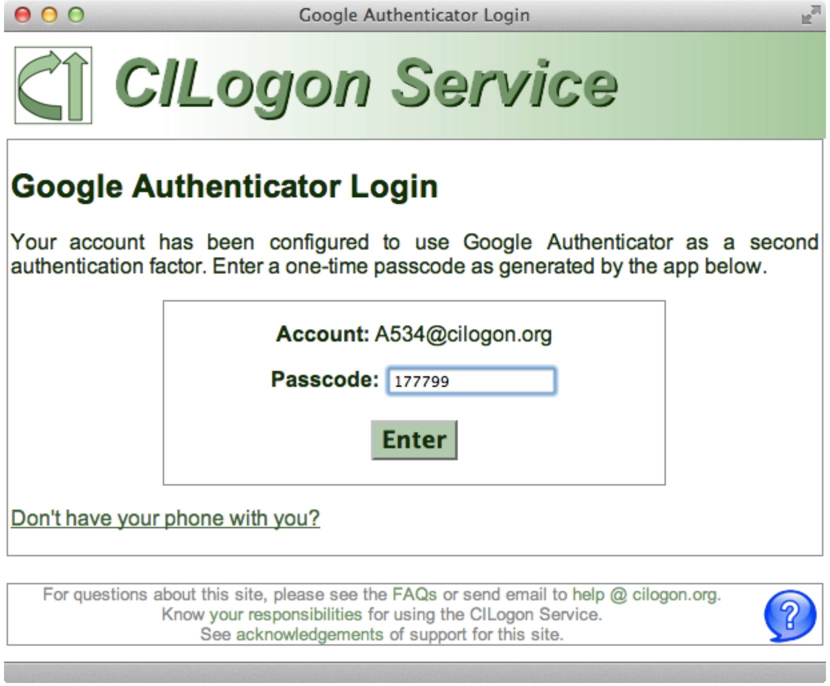
Step 2

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.



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

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.

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 Illinois, U Washington, U Chicago, U Wisconsin-Madison, LIGO, LTER, and ProtectNetwork
  - More info: www.cilogon.org/ecp
- Also following Project Moonshot (www.project-moonshot.org)

ECP Example

```
$ curl -O 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> LIGO Scientific Collaboration
  2> LTER Network
  3> ProtectNetwork
  4> University of Chicago
  5> University of Illinois at Urbana-Champaign
  6> University of Washington
  7> University of Wisconsin-Madison
  8> Specify the URL of another IdP

Choose [3]: 5
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=University of Illinois at Urbana-Champaign/
CN=James Basney A534
Creating proxy .................................. Done
Your proxy is valid until: Thu Mar 14 18:26:56 2013
$ gsissh citest.example.edu
[jbasney@citest ~]$
```

CILogon-HA Partner Projects

- We're working today with OSG, XSEDE, LIGO, DataONE, LTERN, OOI, Globus Online, CVRG, and others
- We're looking for additional partner projects
  - Adoption of higher assurance federated identities
  - Use of federated identities outside the browser
  - International interoperability

Thanks!

www.cilogon.org

info@cilogon.org
jbasney@illinois.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.