CILogon

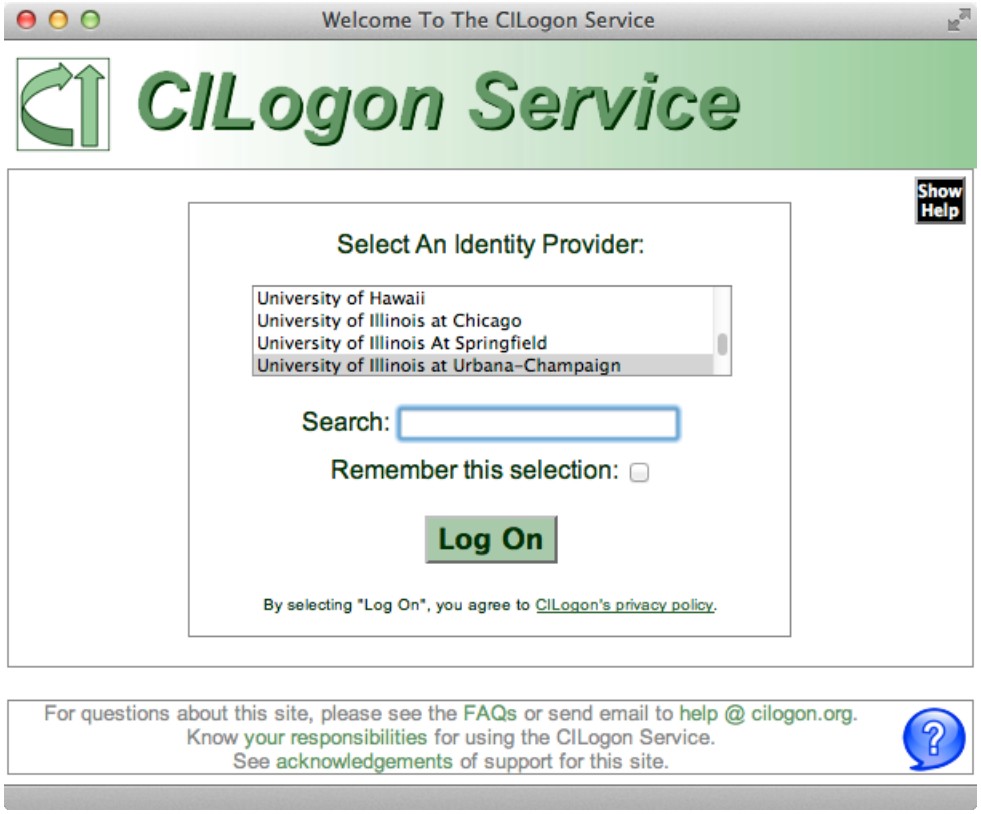
Middleware And Grid Interagency Coordination (MAGIC) at SC13

Jim Basney
jbasney@ncsa.illinois.edu

This material is based upon work supported by the National Science Foundation under grant numbers 0943633 and 1053575 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.

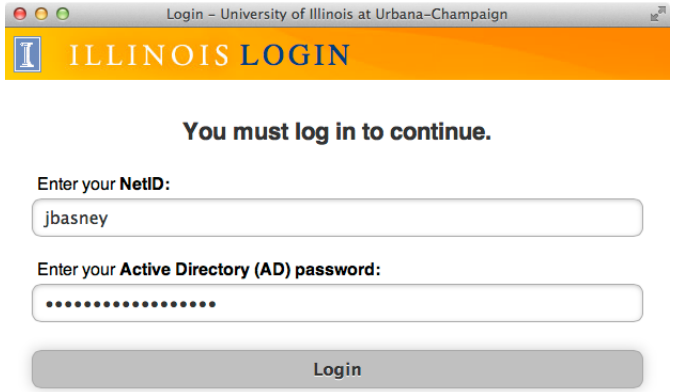
CILogon – https://cilogon.org/

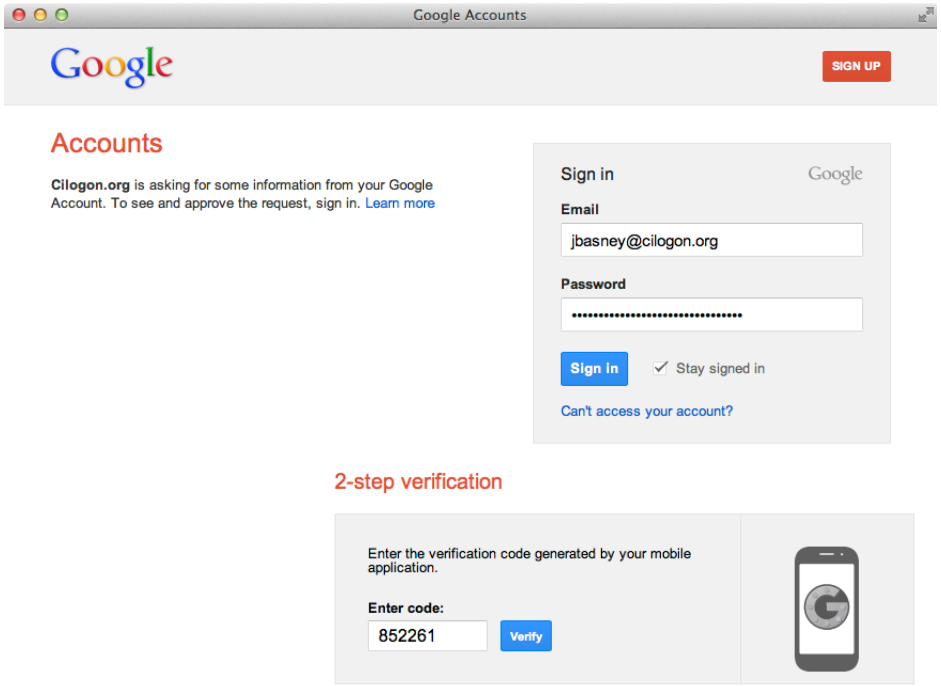
- Provides personal digital certificates for access to cyberinfrastructure
- Uses federated authentication for user identification



Federated Authentication

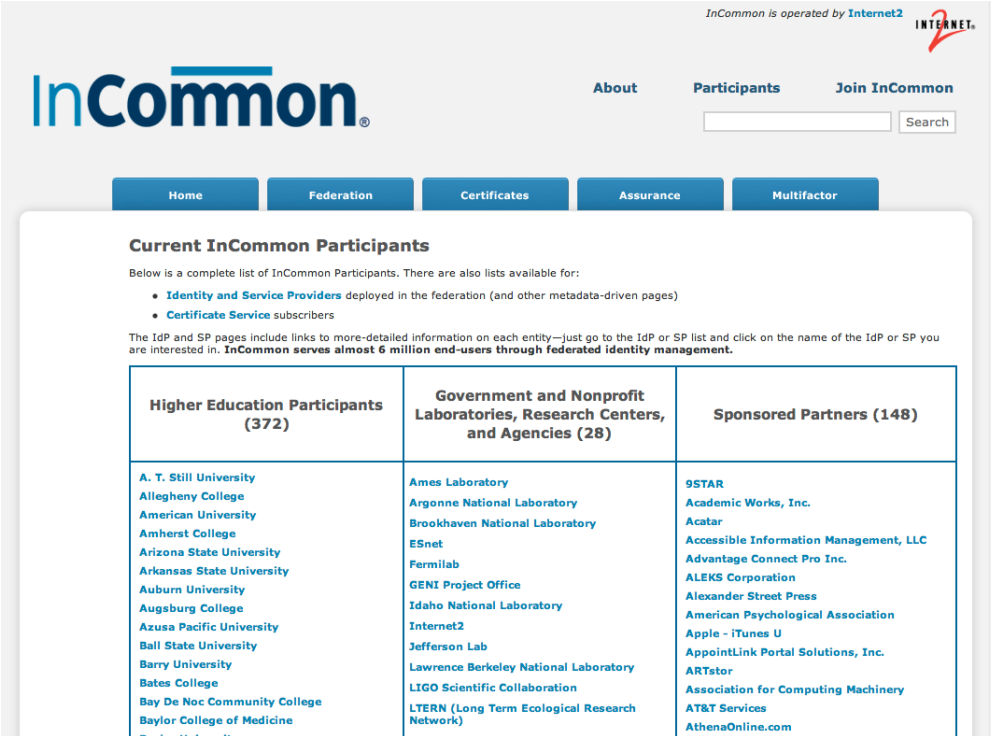
- Log on to CILogon using your campus (InCommon) or Google (OpenID) account

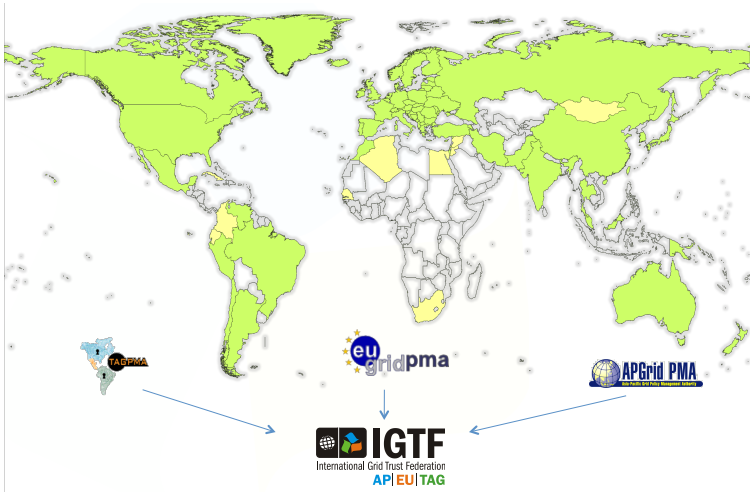




Bridging InCommon and IGTF

- Translating mechanism and policy across higher education and grid trust federations





Multiple Levels of Assurance

- CILogon Silver CA is accredited by IGTF
  - Using InCommon Silver (Level 2) identities
- IGTF IOTA profile for CILogon Basic under development
- Google Authenticator support for second authentication factor

http://wiki.eugridpma.org/Main/IOTASecuredInfraAP

Identifier-Only Trust Assurance with Secured Infrastructure Authentication Profile

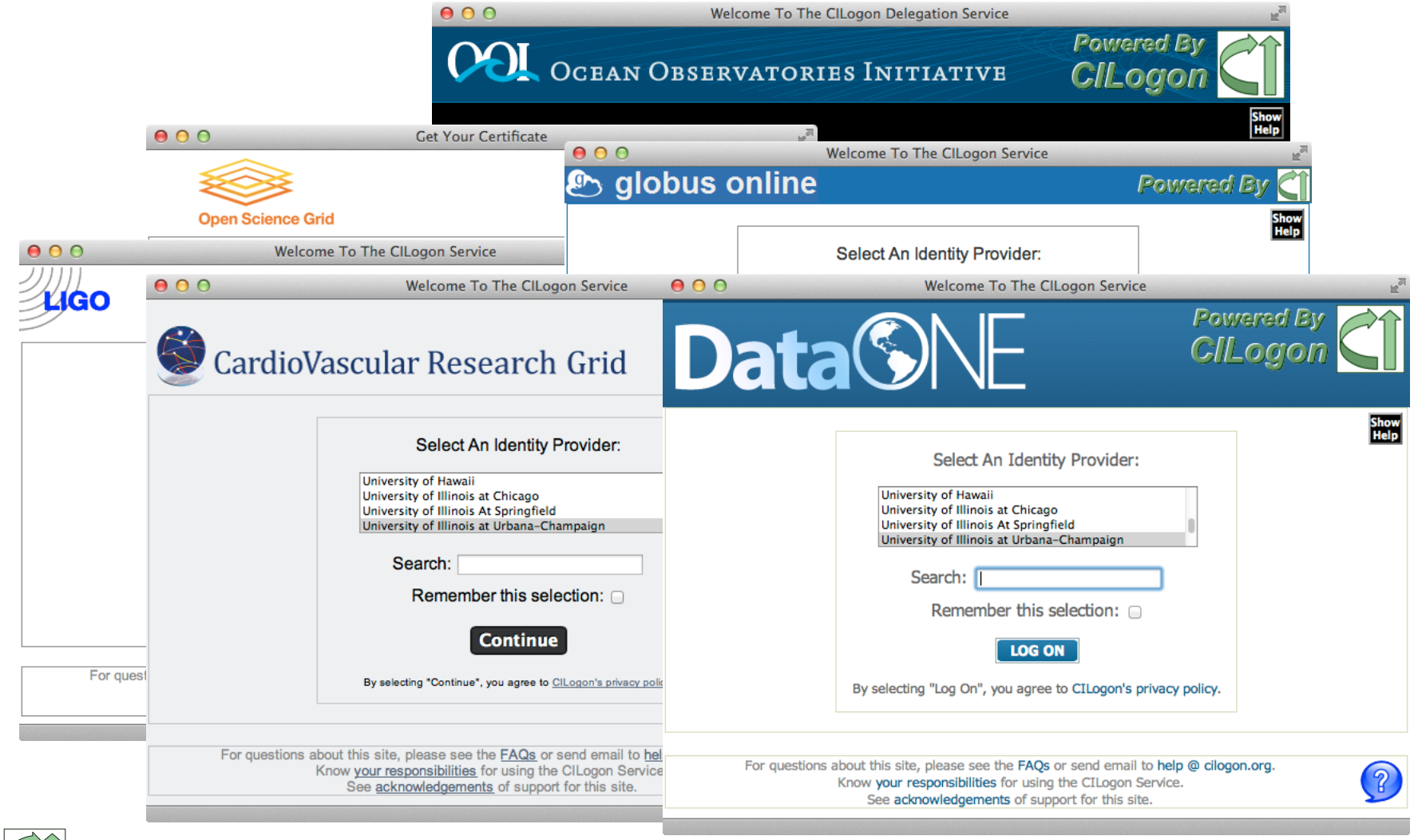
- Identifier-Only Trust Assurance with Secured Infrastructure Authentication Profile
- Abstract
- General Architecture
- Identification
  - Persistency of name binding
  - Naming
  - Renewal and re-keying
  - Retention of records
  - Traceability Requirements
- Operational Requirements
  - Policy and practice statement
  - Certificate and CRL profile
  - Revocation
- Security Requirements
  - Third parties involved in identity management
- Publication and Repository responsibilities
- Audits
- Privacy and confidentiality
- Compromise and disaster recovery
  - Due diligence for subscribers

Abstract

This is an Authentication Profile of the IGTF describing the minimum requirements on X.509 PKI authorities where the identity vetting is adequate to ensure unique, non-re-assigned identities, and generated by authorities using secured and trusted infrastructure. Such authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements, and credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers, and should be used in conjunction with complementary identification and vetting processes.

This Authentication Profile is managed by the EUGridPMA.

Integrated with CyberInfrastructure



Integrated with Globus Nexus

SignIn | Globus Online

globus online

Manage Data | Groups | News & Events | About | Support | Log In | Sign Up

Sign In

Sign Up with Globus Online

Use Your GlobusOnline login

alternate login

Username

Password

Sign In

Forgot Password?

Support

Select a different login

GlobusOnline
Argonne LCF
Argonne MCS & LCRC
BIRN
CLI Transition
EGI
ESG ANL
Exeter
Google
InCommon / CILogon
LRZ
NCSA
NCSA Blue Waters
NERSC
UChicago CI
UChicago iBi
UK NGS
WestGrid
XSEDE

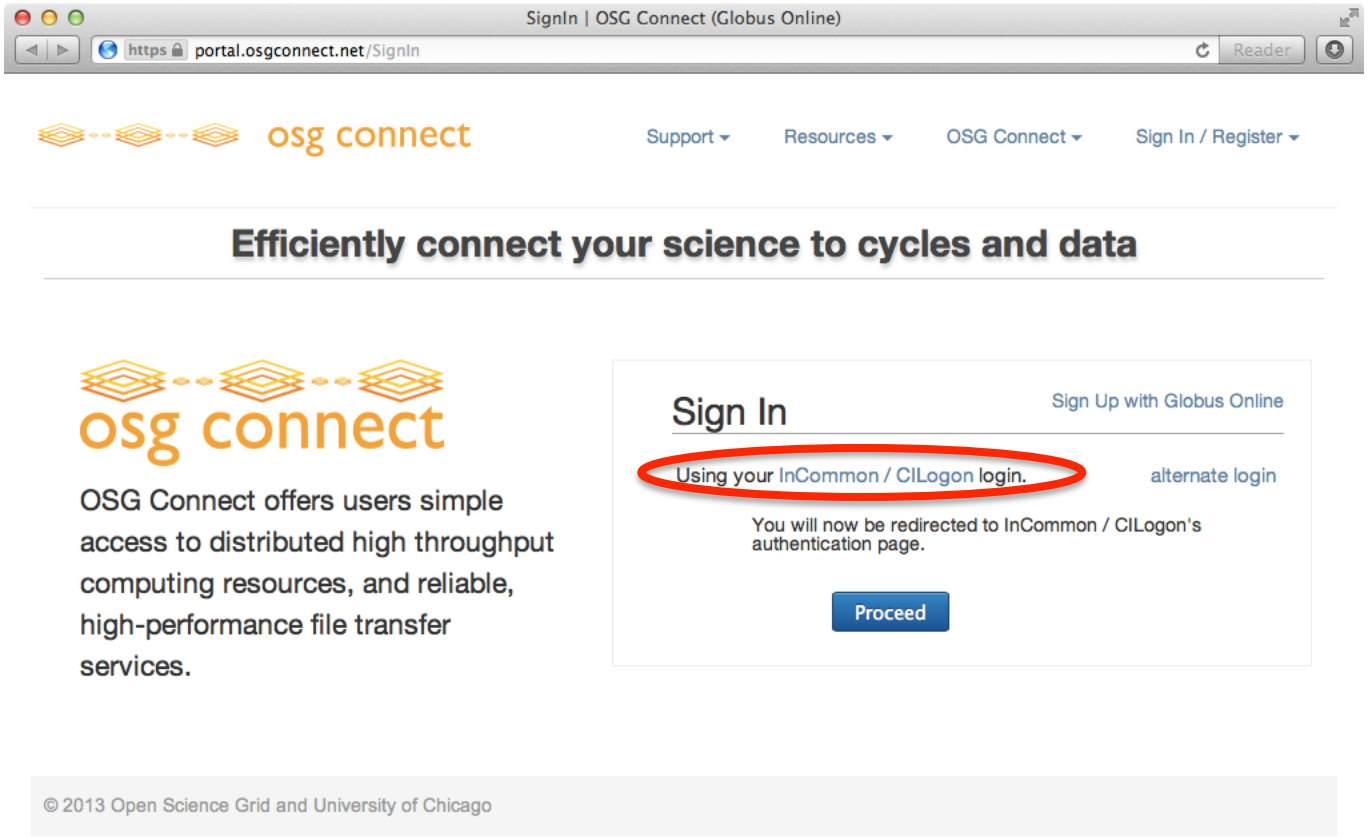
MANAGE DATA
start transfer
view transfer activity
manage endpoints

case studies

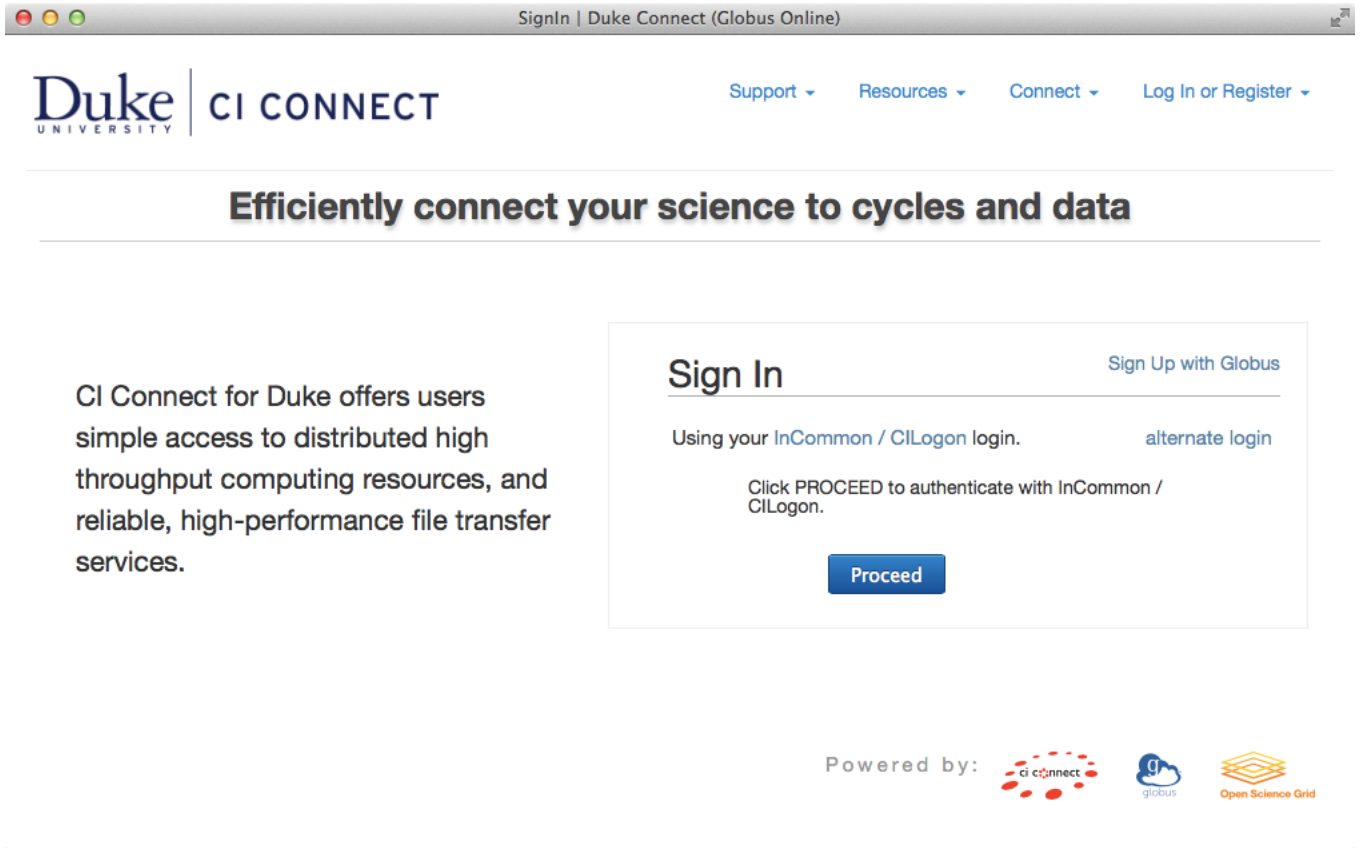
pro tips

Subscribe to Globus News & Updates

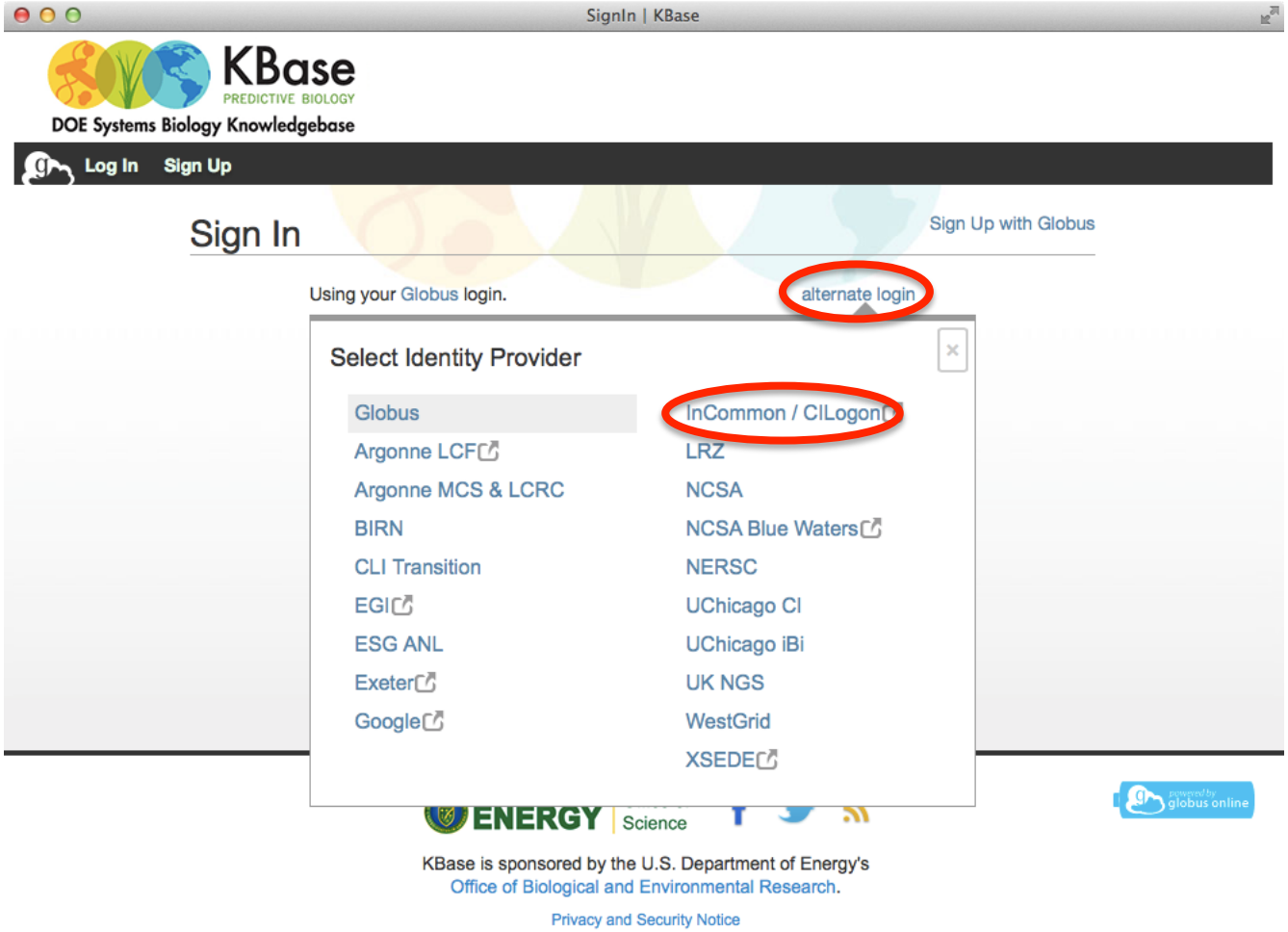
Used by OSG Connect



Used by CI Connect for Duke



Integrated with DOE KBase



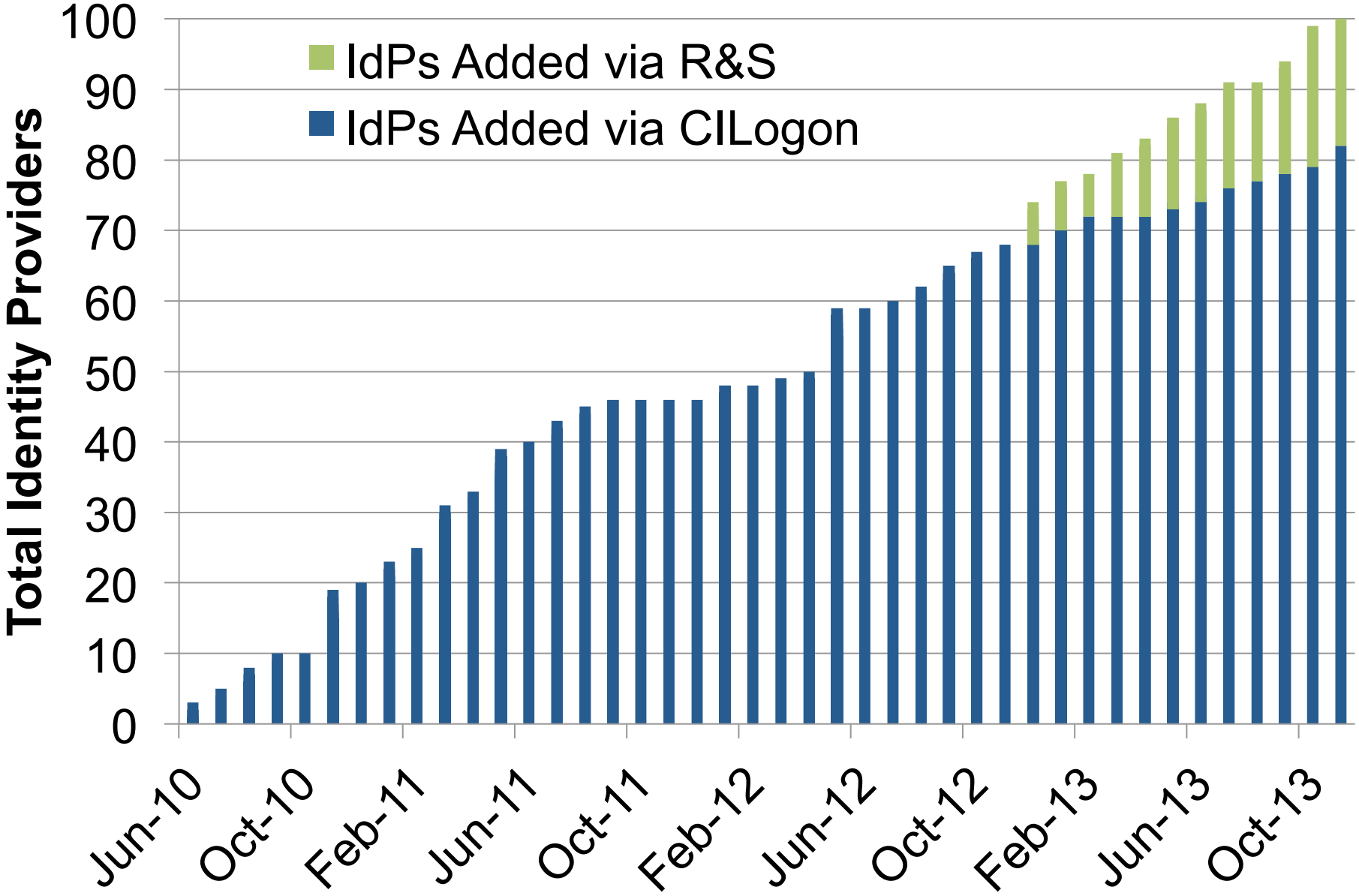
ligo-proxy-init using CILogon ECP

```
$ ligo-proxy-init scott.koranda
Your identity: scott.koranda@LIGO.ORG
Enter pass phrase for this identity:
Creating proxy ..................................... Done
Your proxy is valid until: Mar 5 13:45:16 2013 GMT
$ grid-proxy-info -all
subject  : /DC=org/DC=cilogon/C=US/O=LIGO/CN=Scott Koranda scott.koranda@ligo.org
issuer   : /DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Basic CA 1
identity : /DC=org/DC=cilogon/C=US/O=LIGO/CN=Scott Koranda scott.koranda@ligo.org
type     : end entity credential
strength : 2048 bits
path     : /tmp/x509up_u1000
timeleft : 71:59:52  (3.0 days)
```

CILogon and XSEDE

Extreme Science and Engineering Discovery Environment

- CILogon is
  - a component in the XSEDE architecture
  - entering the XSEDE engineering process: architecture, design, and security reviews and operational acceptance tests
- XSEDE can provide sustained operational support to CILogon users (DataONE, OOI, OSG, LIGO, etc.)


IdPs Added via R&S
IdPs Added via CILogon
Total Identity Providers
100
90
80
70
60
50
40
30
20
10
0
Jun-10
Oct-10
Feb-11
Jun-11
Oct-11
Feb-12
Jun-12
Oct-12
Feb-13
Jun-13
Oct-13

Adding an IdP to CILogon

- Use self-service web application or contact us for assistance

https://cilogon.org/requestidp/

Contact Information

Your Name:

Email Address:

Home Organization

Select an Organization: -- Choose one –or– Type one in below --

Don't See It? Enter Here:

Additional Information (Optional)

Please tell us more about yourself and your interest in the CILogon Service:

Submit

https://cilogon.org/testidp/

Verify SAML Attribute Release Policy

Thank you for your interest in the CILogon Service. This page allows the administrator of an Identity Provider (IdP) to verify that all necessary SAML attributes have been released to the CILogon Service Provider (SP). Below you will see the various attributes required by the CILogon Service and their values as released by your IdP. If all required attributes are present, you can add your IdP to the list of organizations available to the CILogon Service (assuming it has not already been added).

Summary

All required attributes have been released by your IdP. For details of the various attributes utilized by the CILogon Service and their current values, see the sections below.

Add Your IdP to the CILogon Service

SAML Attributes

Metadata Attributes

InCommon Federation Info: Service Categories

https incommon.org/federation/info/all-sp-categories.html#SPs

InCommon FEDERATION

Federation Info: About Organizations Entities

Federation entities provide services to InCommon participants at their discreti
and collaboration opportunities among InCommon participants. Our value as a c

InCommon Service Categories

InCommon Research and Scholarship program helps services connect with identity providers.

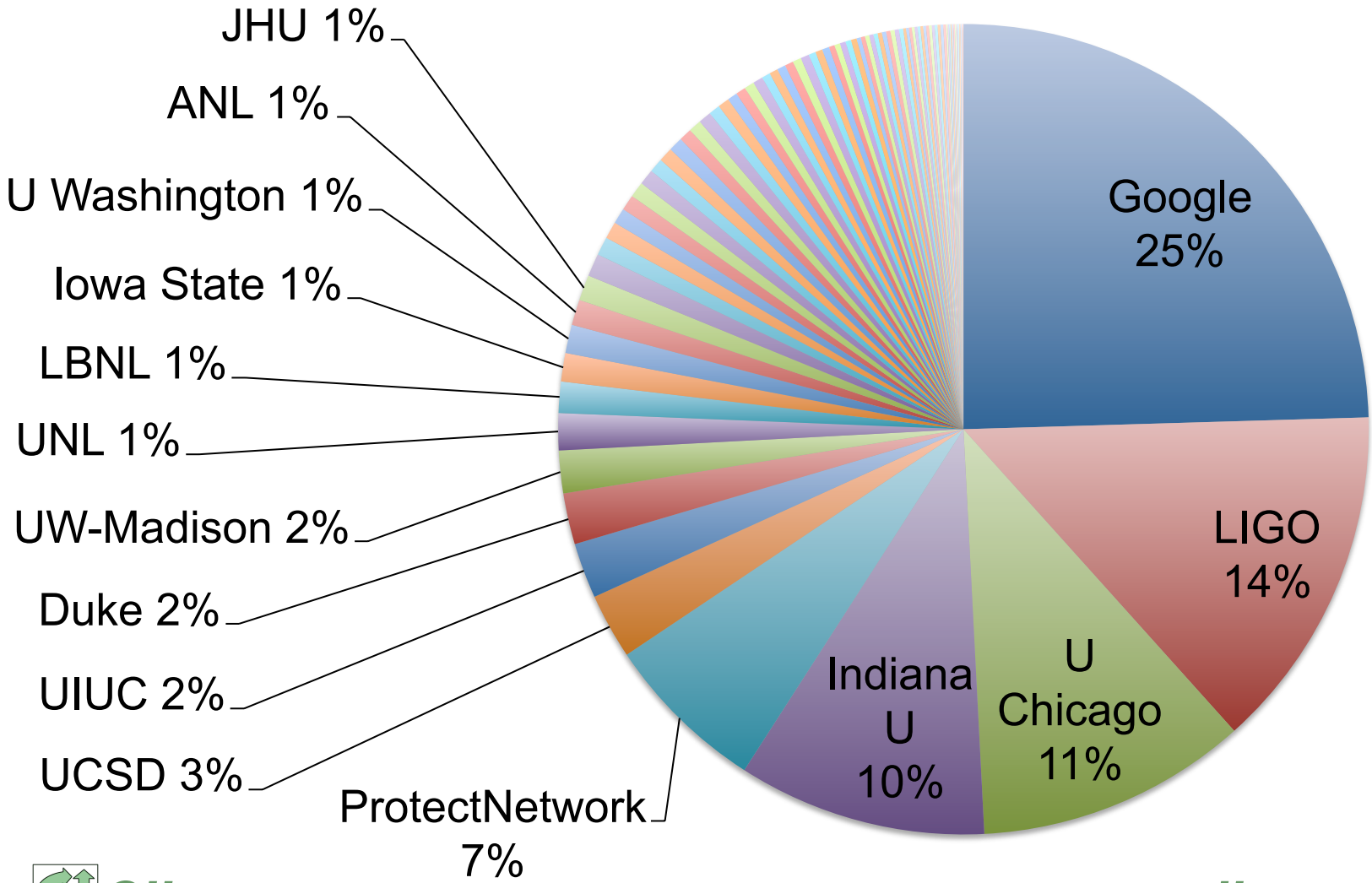
IdPs SPs

The following service providers belong to the indicated service category:

Service Provider Name	Service Category
CarmenWiki	research-and-scholarship
CILogon	research-and-scholarship
Collaboration Wiki Spaces at Internet2	research-and-scholarship
FileSender	research-and-scholarship
GENI Experimenter Portal	research-and-scholarship
GPN/UM Dropoff Services	research-and-scholarship
Indiana CTSI HUB	research-and-scholarship
LIGO CBC Wiki	research-and-scholarship
LIGO Wiki	research-and-scholarship
Multi-Factor Authentication (MFA) Cohortium Registry	research-and-scholarship
Multi-Factor Authentication (MFA) Cohortium Wiki	research-and-scholarship
Narada Metrics	research-and-scholarship
Open Science Data Cloud Console	research-and-scholarship

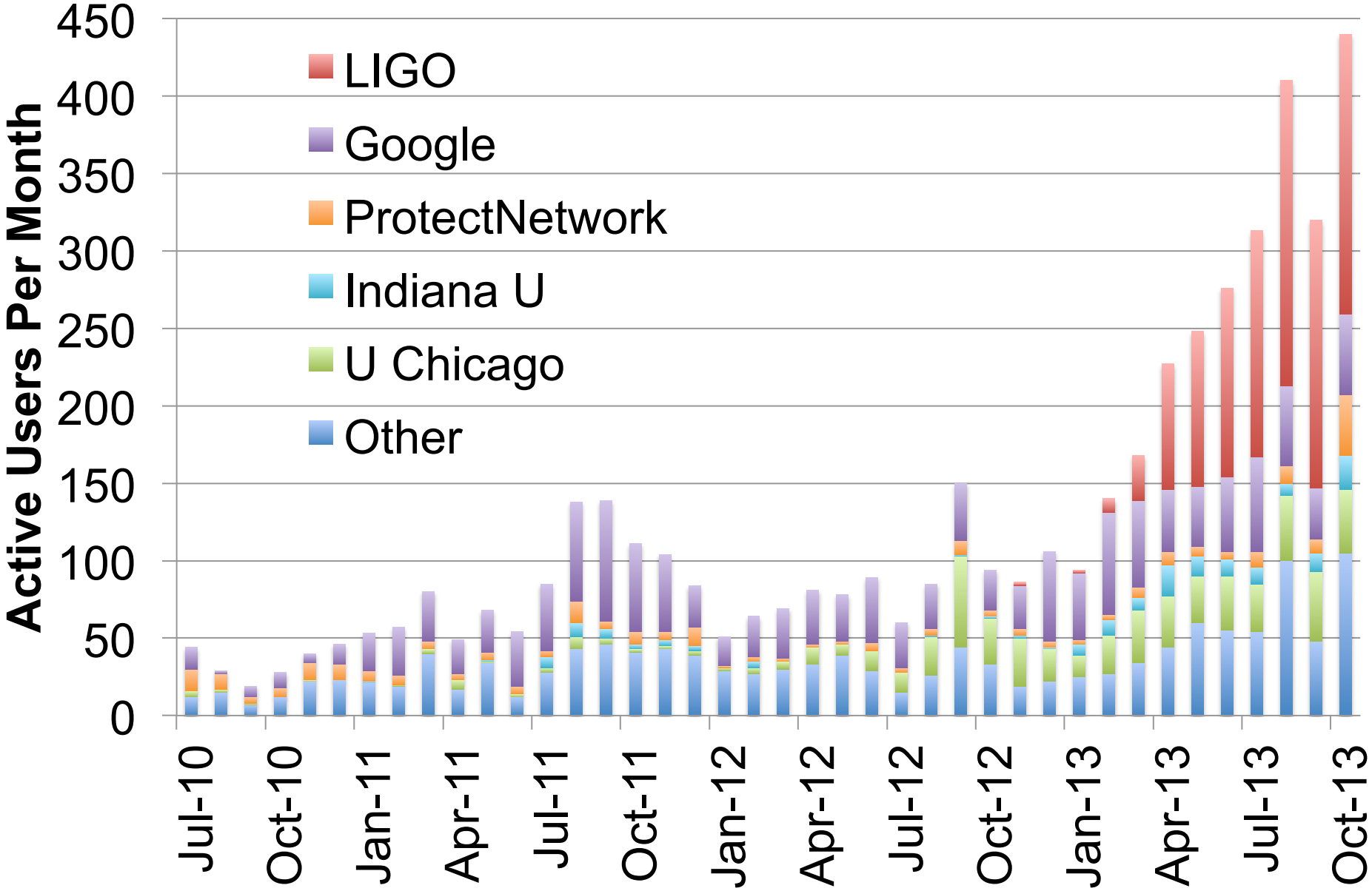
Service Category	# of SPs	# of IdPs
research-and-scholarship	15	60

Registered Users Per IdP



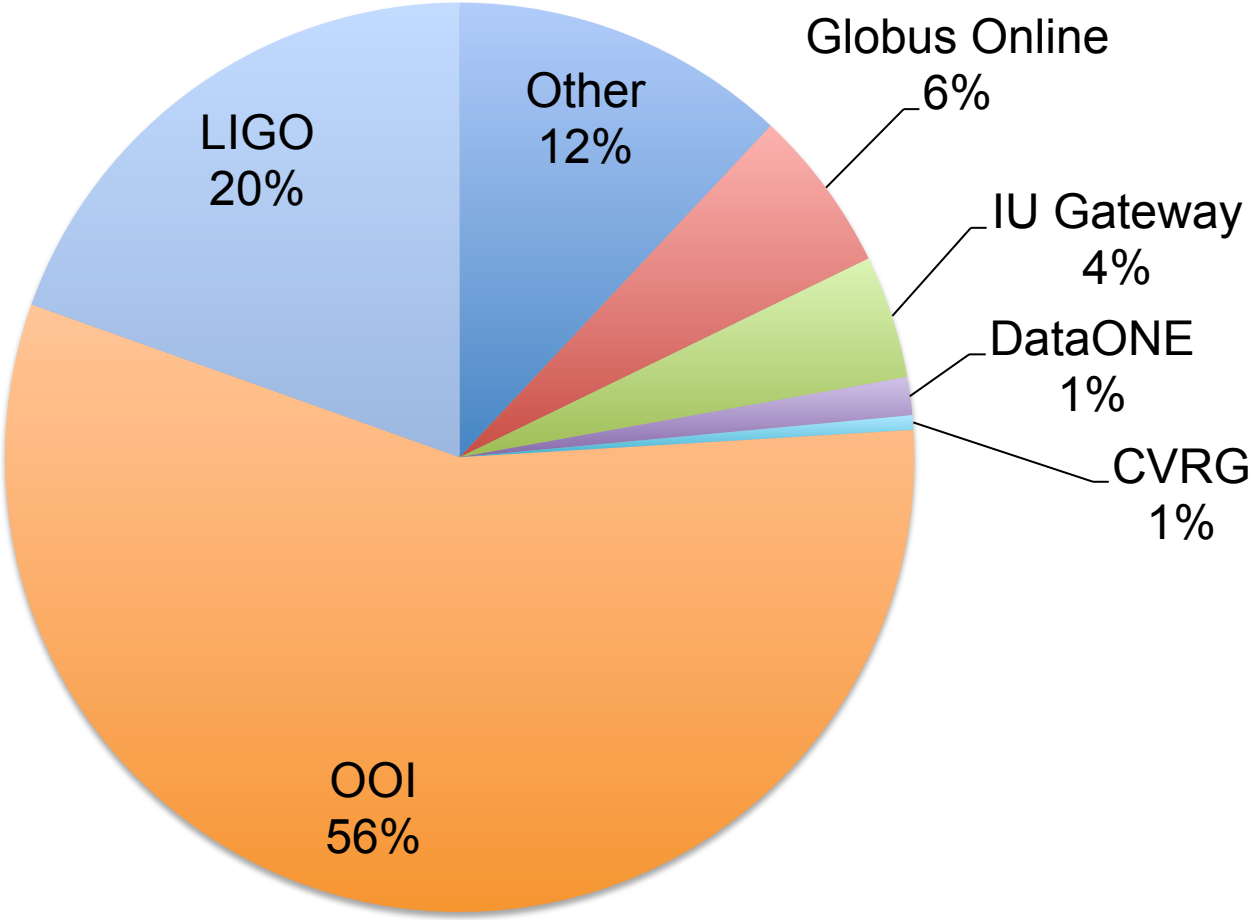
CILogon

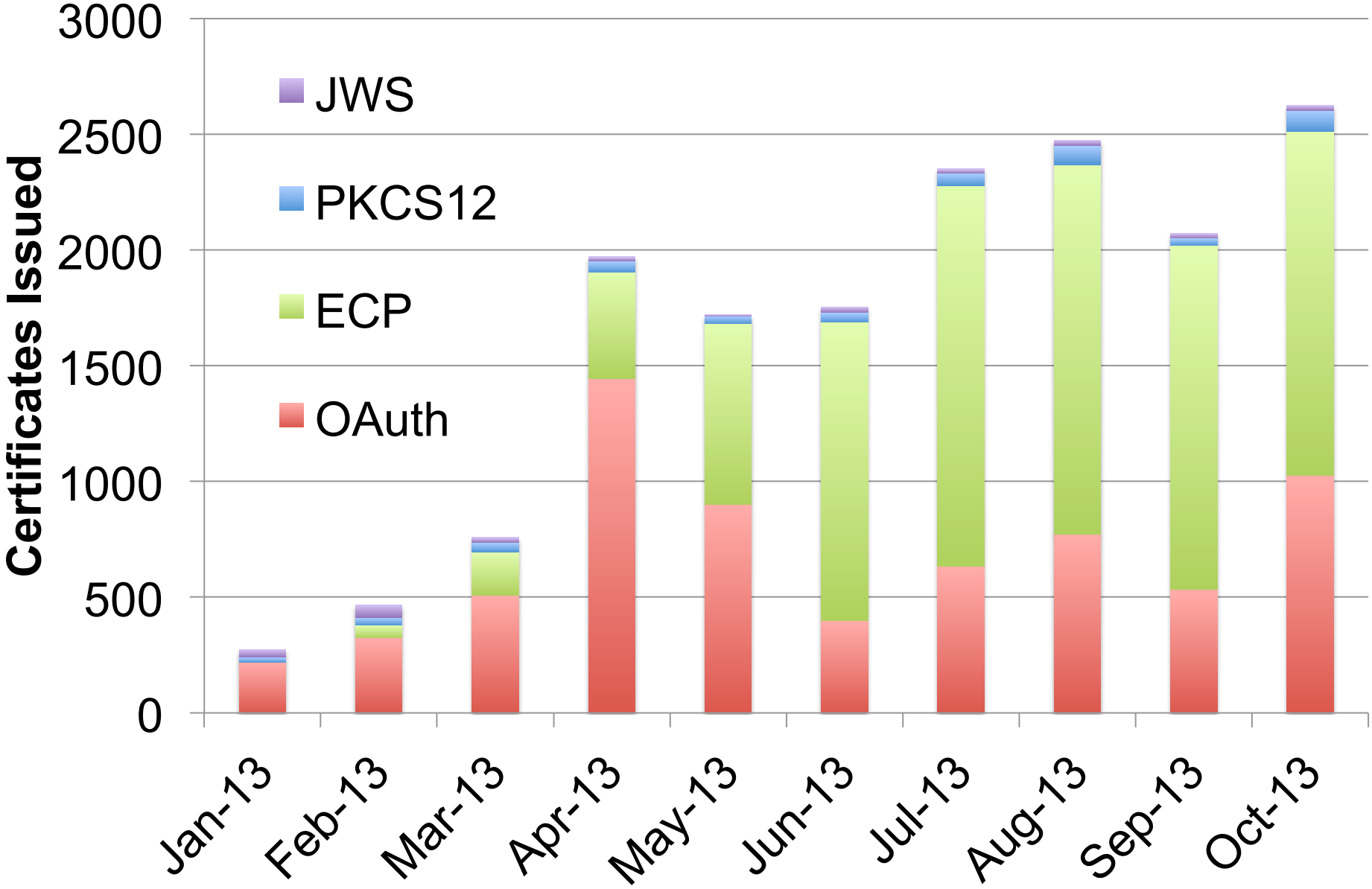
www.cilogon.org



CILogon www.cilogon.org

% of Total Certificates Issued



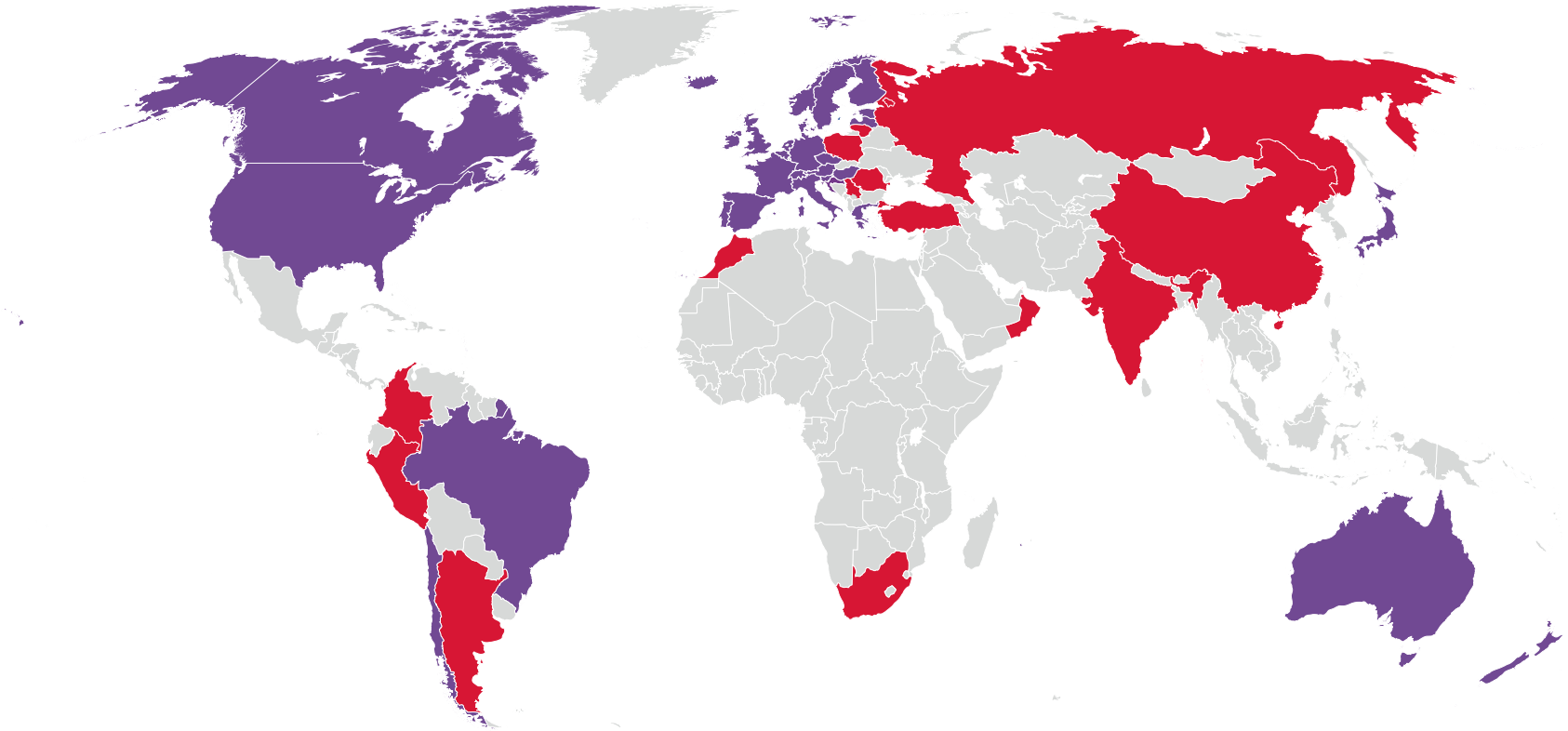

Certificates Issued
3000
2500
2000
1500
1000
500
0
JWS
PKCS12
ECP
OAuth
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13

What's Next

- SAML interfederation
  - InCommon joining eduGAIN this year
  - International attribute release
- Growth of federated online CAs
  - http://redmine.ogf.org/projects/idel-wg
- Level of Assurance (continued)
  - IGTF IOTA profile
  - Int'l adoption of Kantara standards
  - Security incident handling
  - Multi-factor authentication

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	SURFconext
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

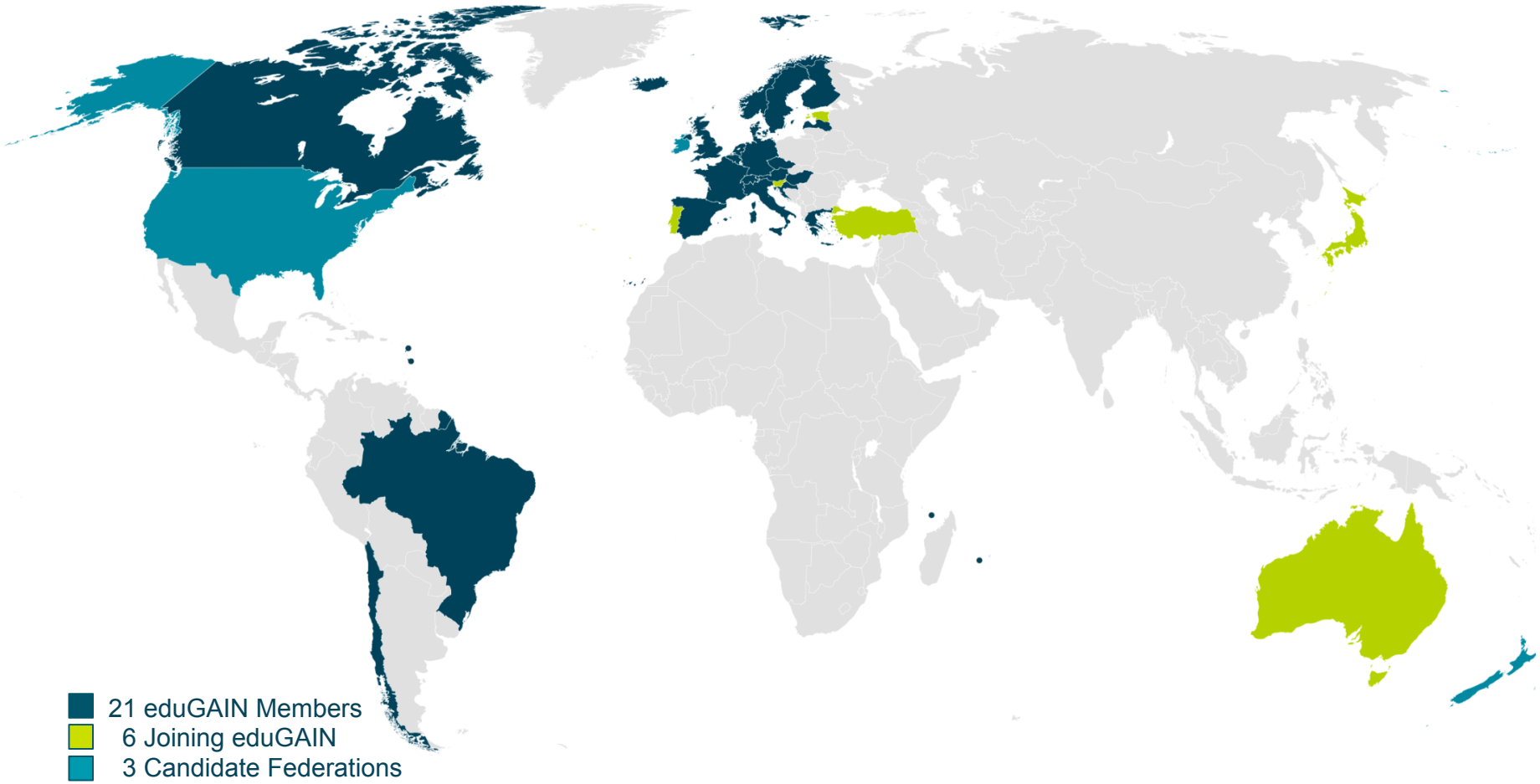
AR	MATE
CN	CARSI
COL	COLFIRE
IN	INFED
LT	LEFT
PE	INCA
MA	eduIDM
OM	Oman Knowledge ID Federation
PL	PIONIERId
RO	RoEduNet Federation
RS	iAMRES
RU	ФEDUrus AAI
TR	YETKİM
ZA	SAIF

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

Last update: 14 October 2013

refeds.org

eduGAIN Interfederation Participants



edugain.org

Thanks!

info@cilogon.org
jbasney@ncsa.illinois.edu

www.cilogon.org/faq

dx.doi.org/10.1145/2484762.2484791