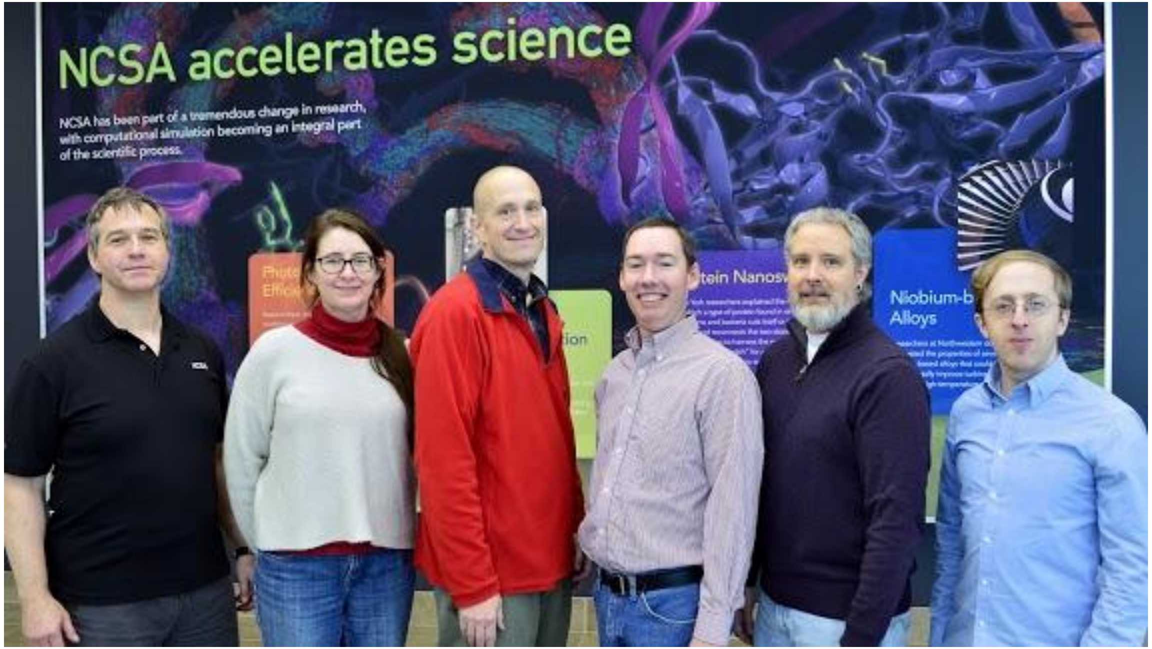
CILogon

Enabling Federated Identity and Access Management for Scientific Collaborations

Jim Basney
jbasney@ncsa.illinois.edu

FIM4R@FNAL
September 12 2019

who we are


NCSA accelerates science
NCSA has been part of a tremendous change in research, with computational simulation becoming an integral part of the scientific process.
Niobium-b
Alloys

ncsa.illinois.edu

sphericalcowgroup.com

our vision

enable logon to scientific cyberinfrastructure (CI)

seamless IAM for academic research collaborations

use your campus identity (InCommon/eduGAIN/Shibboleth)

manage onboarding/offboarding/attributes/groups/roles in one place (COmanage)

integrate with a variety of research apps
(OIDC, SAML, LDAP, X.509, SSH)

realizing our vision

- align with InCommon Trusted Access Platform
  - (https://www.incommon.org/software)
  - Shibboleth, COmanage, Grouper
- provide hosted services
  - common IAM platform across many collaborations
  - growing CILogon operations (since 2010)
  - reliability / sustainability

our baseline: REFEDS R&S

Attribute release continues to be a stumbling block.

We follow the REFEDS Research & Scholarship policy.

Does your campus support REFEDS R&S?

https://refeds.org/research-and-scholarship

https://cilogon.org/testidp/

SIRTFI

Security Incident Response
Trust Framework for Federated Identity

https://refeds.org/sirtfi

REFEDS

August 2019 CILogon stats

6800 active users

280 active identity providers

55 identity providers missing R&S attributes

5 identity providers missing SIRTFI

⇨ 1 added SIRTFI on Aug 30 ⇦

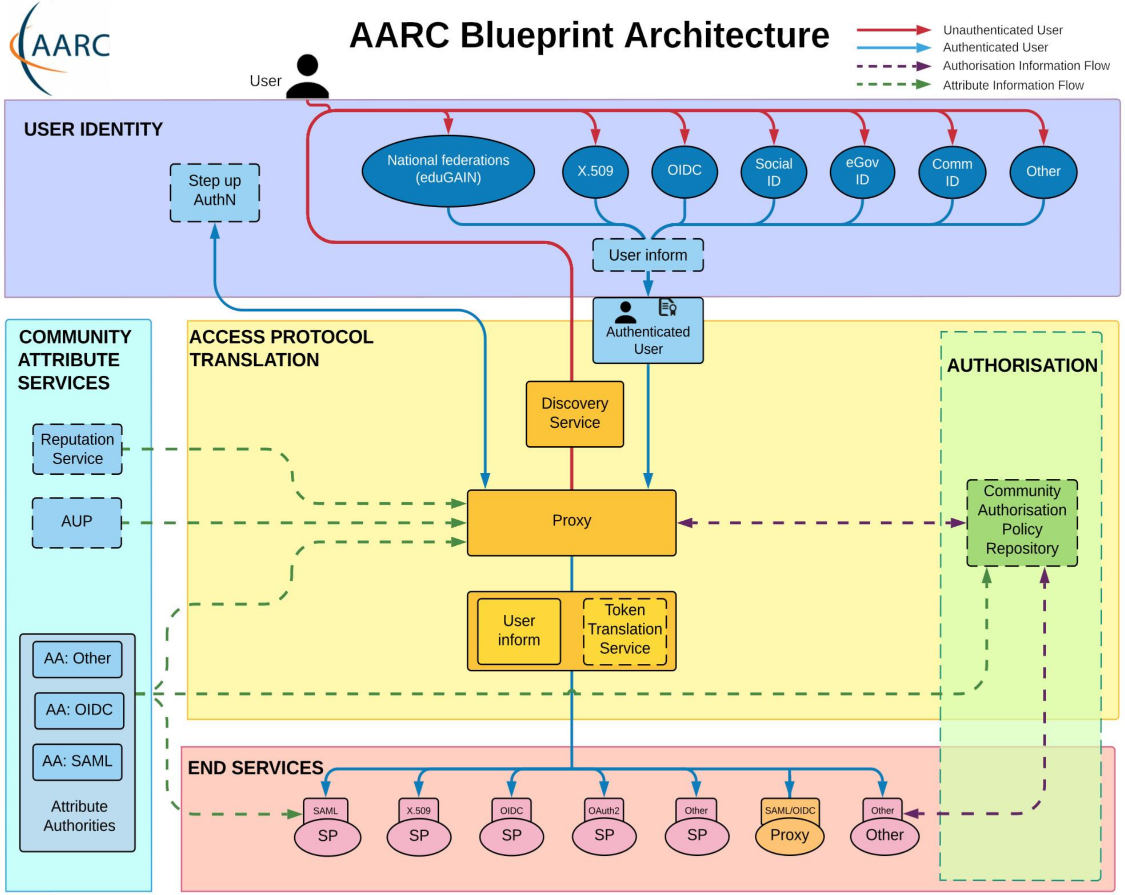
September 2019 eduGAIN stats

63 national federations

3076 identity providers

612 identity providers support REFEDS R&S

473 identity providers support SIRTFI



AARC Blueprint Architecture

https://aarc-project.eu/architecture/

COmanage-as-a-Service

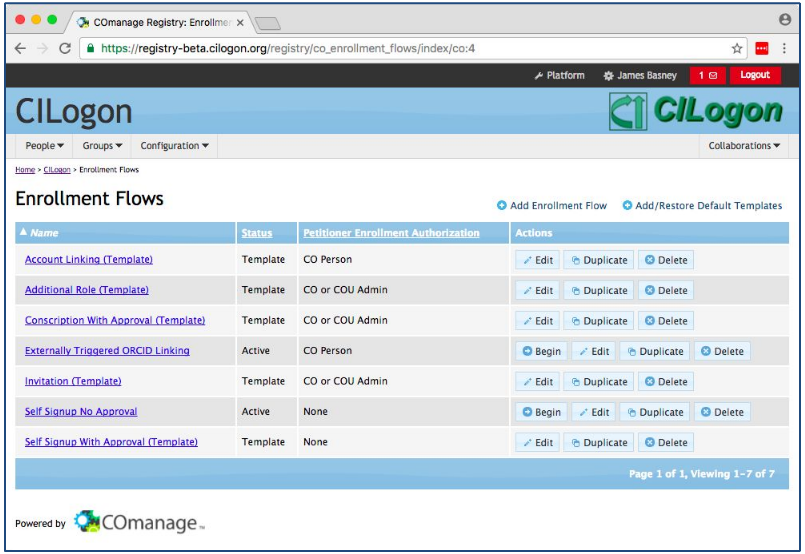
Collaboration managed:

enrollment flows

expiration policies

self service permissions

pipelines


COmanage Registry: Enrollme
https://registry-beta.cilogon.org/registry/co_enrollment_flows/index/co:4
Platform
James Basney
1
Logout
CILogon
CILogon
People
Groups
Configuration
Collaborations
Home > CILogon > Enrollment Flows
Add Enrollment Flow
Add/Restore Default Templates

Enrollment Flows

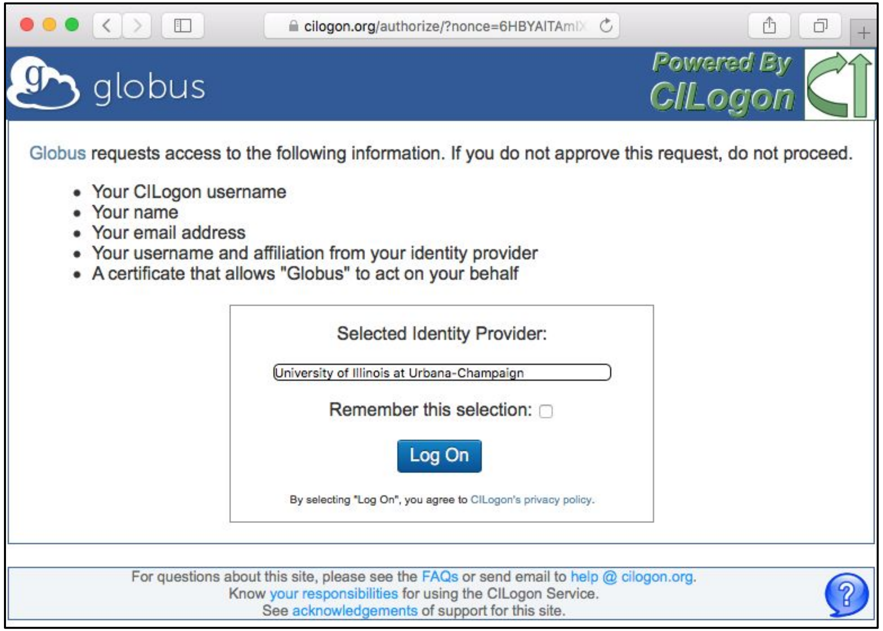
Name	Status	Petitioner Enrollment Authorization	Actions
Account Linking (Template)	Template	CO Person	Edit Duplicate Delete
Additional Role (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Conscription With Approval (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Externally Triggered ORCID Linking	Active	CO Person	Begin Edit Duplicate Delete
Invitation (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Self Signup No Approval	Active	None	Begin Edit Duplicate Delete
Self Signup With Approval (Template)	Template	None	Edit Duplicate Delete

Page 1 of 1, Viewing 1-7 of 7

Powered by COmanage

https://www.cilogon.org/comanage

OIDC for R&E



Globus requests access to the following information. If you do not approve this request, do not proceed.

- Your CILogon username
- Your name
- Your email address
- Your username and affiliation from your identity provider
- A certificate that allows "Globus" to act on your behalf

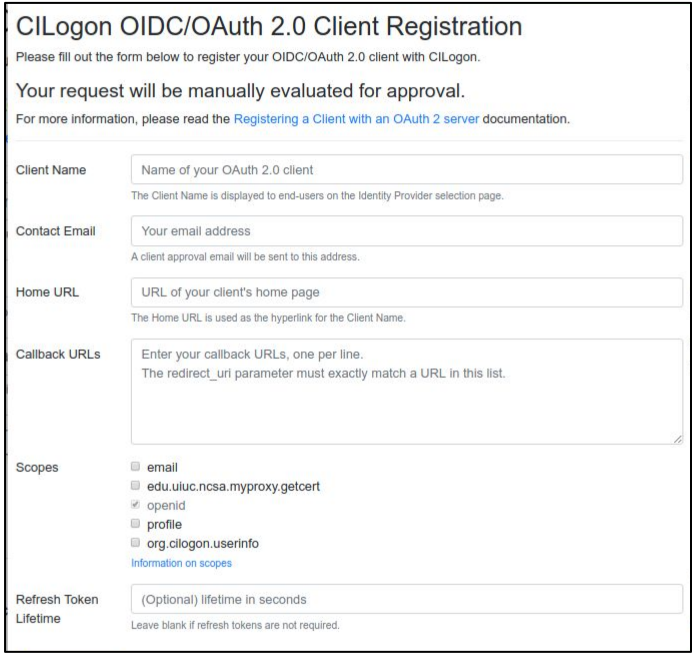
Selected Identity Provider:

University of Illinois at Urbana-Champaign

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 OIDC/OAuth 2.0 Client Registration

Please fill out the form below to register your OIDC/OAuth 2.0 client with CILogon.

Your request will be manually evaluated for approval.

For more information, please read the Registering a Client with an OAuth 2 server documentation.

Client Name: Name of your OAuth 2.0 client
The Client Name is displayed to end-users on the Identity Provider selection page.

Contact Email: Your email address
A client approval email will be sent to this address.

Home URL: URL of your client's home page
The Home URL is used as the hyperlink for the Client Name.

Callback URLs: Enter your callback URLs, one per line.
The redirect_uri parameter must exactly match a URL in this list.

Scopes:
☐ email
☐ edu.uiuc.ncsa.myproxy.getcert
☑ openid
☐ profile
☐ org.cilogon.userinfo
Information on scopes

Refresh Token Lifetime: (Optional) lifetime in seconds
Leave blank if refresh tokens are not required.

https://openid.net/wg/rande/

SAML-Proxy-as-a-Service

For applications with limited SAML support:

- only one IdP
- no SAML metadata

Providing collaboration-managed identities

- linked identities
- co attributes/groups

https://github.com/IdentityPython/SATOSA

voPerson

an LDAP attribute schema (object class) with usage recommendations for VOs

voPersonApplicationUID	voPersonExternalID
voPersonAuthorName	voPersonID
voPersonCertificateDN	voPersonSoRID
voPersonCertificateIssuerDN	voPersonStatus

https://voperson.org/

CILogon OSG CA retired

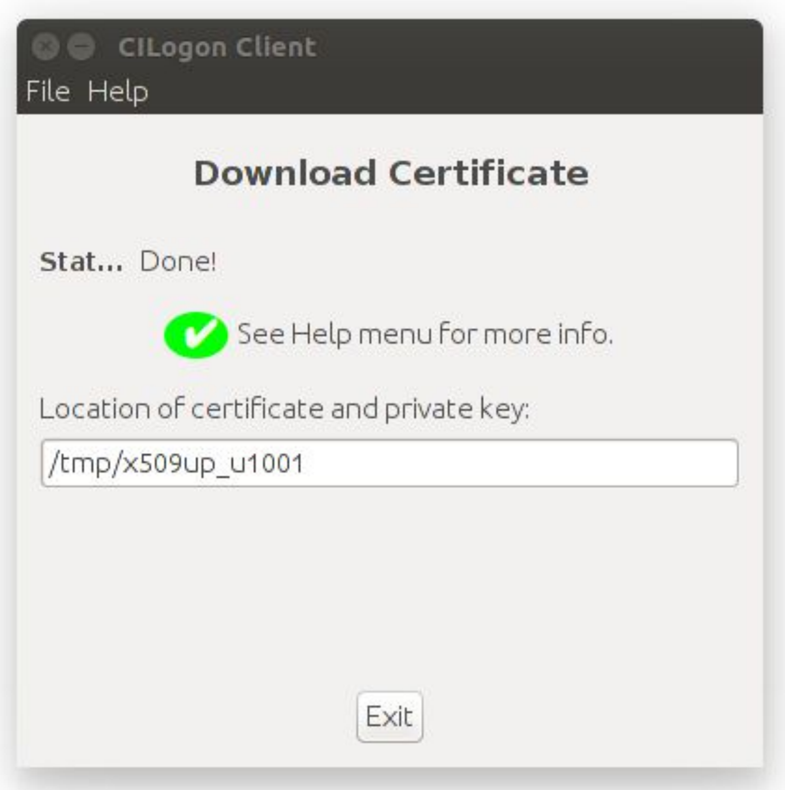
Use InCommon IGTF Server CA or Let’s Encrypt CA for host certificates

https://opensciencegrid.org/docs/security/host-certs/

Use federated identity with for user certificates from CILogon

https://opensciencegrid.org/docs/security/user-certs/

retiring CILogon Java Web Start



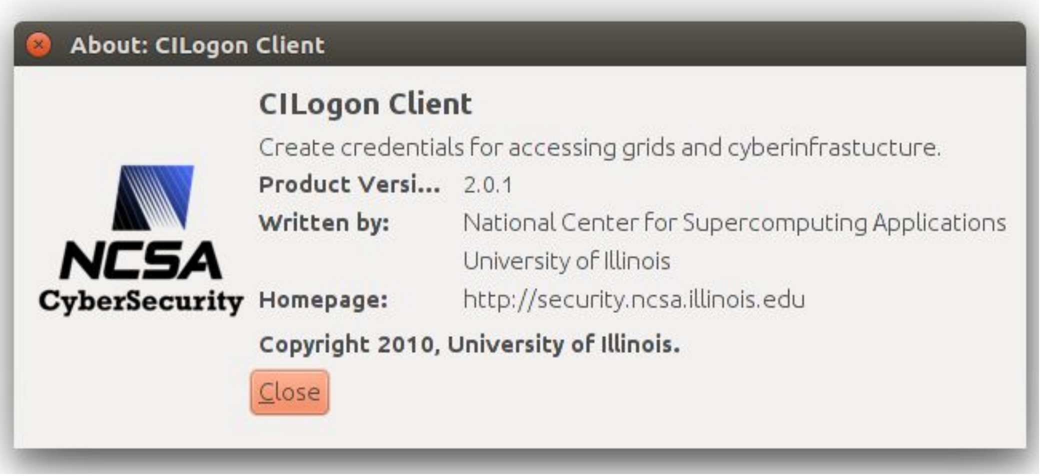
Download Certificate

Stat... Done!

✓ See Help menu for more info.

Location of certificate and private key:

/tmp/x509up_u1001



CILogon Client

Create credentials for accessing grids and cyberinfrastucture.

Product Versi...	2.0.1
Written by:	National Center for Supercomputing Applications University of Illinois
Homepage:	http://security.ncsa.illinois.edu

Copyright 2010, University of Illinois.

www.cilogon.org

CILogon OAuth1 [not yet] retired

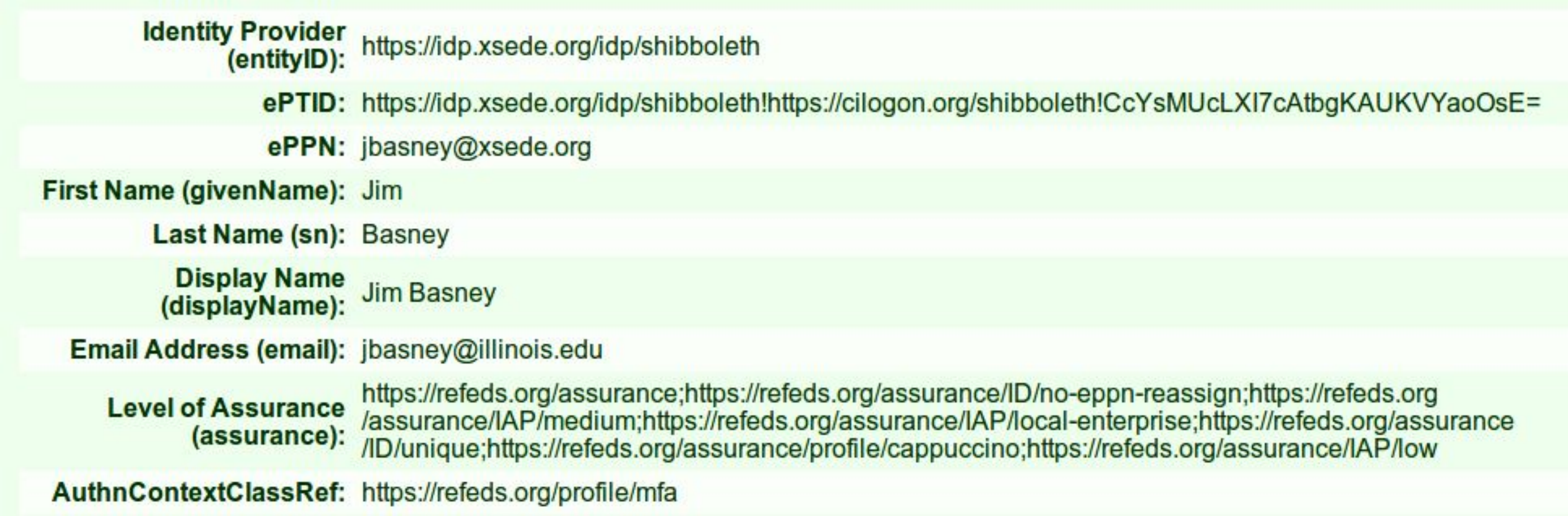
Not accepting new OAuth1 registrations

Migrating remaining OAuth1 clients to OIDC

Targeting mid-2020 for OAuth1 retirement

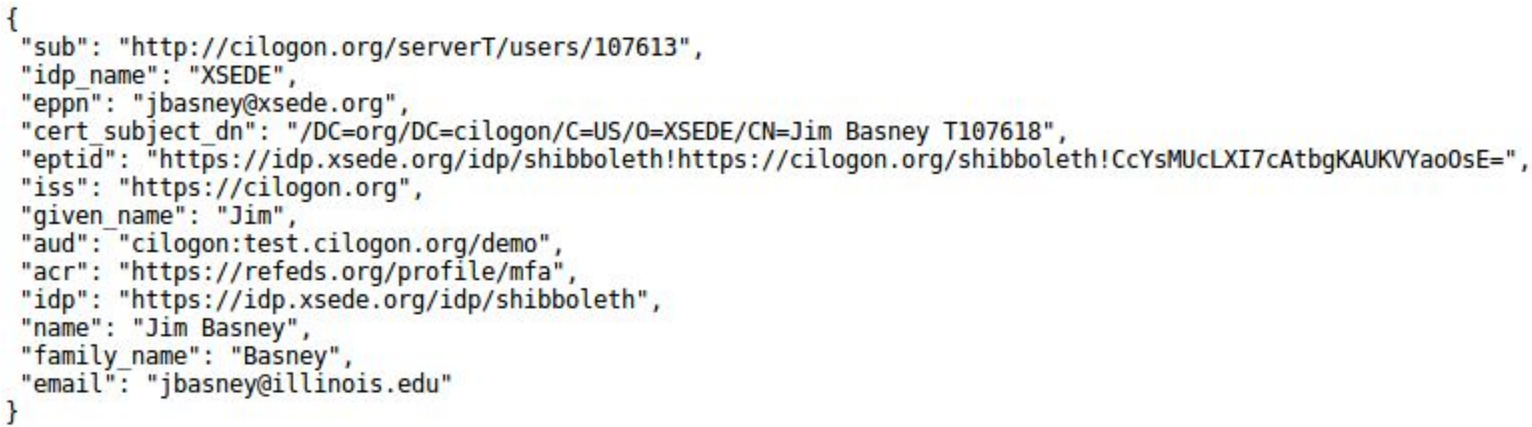
https://www.cilogon.org/oidc

REFEDS Assurance

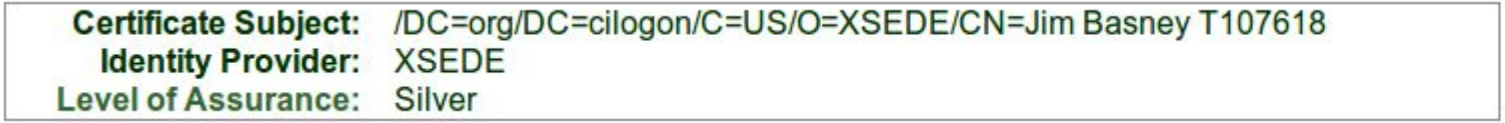


Identity Provider (entityID):	https://idp.xsede.org/idp/shibboleth
ePTID:	https://idp.xsede.org/idp/shibboleth!https://cilogon.org/shibboleth!CcYsMUcLXI7cAtbgKAUKVYaoOsE=
ePPN:	jbasney@xsede.org
First Name (givenName):	Jim
Last Name (sn):	Basney
Display Name (displayName):	Jim Basney
Email Address (email):	jbasney@illinois.edu
Level of Assurance (assurance):	https://refeds.org/assurance;https://refeds.org/assurance/ID/no-eppn-reassign;https://refeds.org/assurance/IAP/medium;https://refeds.org/assurance/IAP/local-enterprise;https://refeds.org/assurance/ID/unique;https://refeds.org/assurance/profile/cappuccino;https://refeds.org/assurance/IAP/low
AuthnContextClassRef:	https://refeds.org/profile/mfa

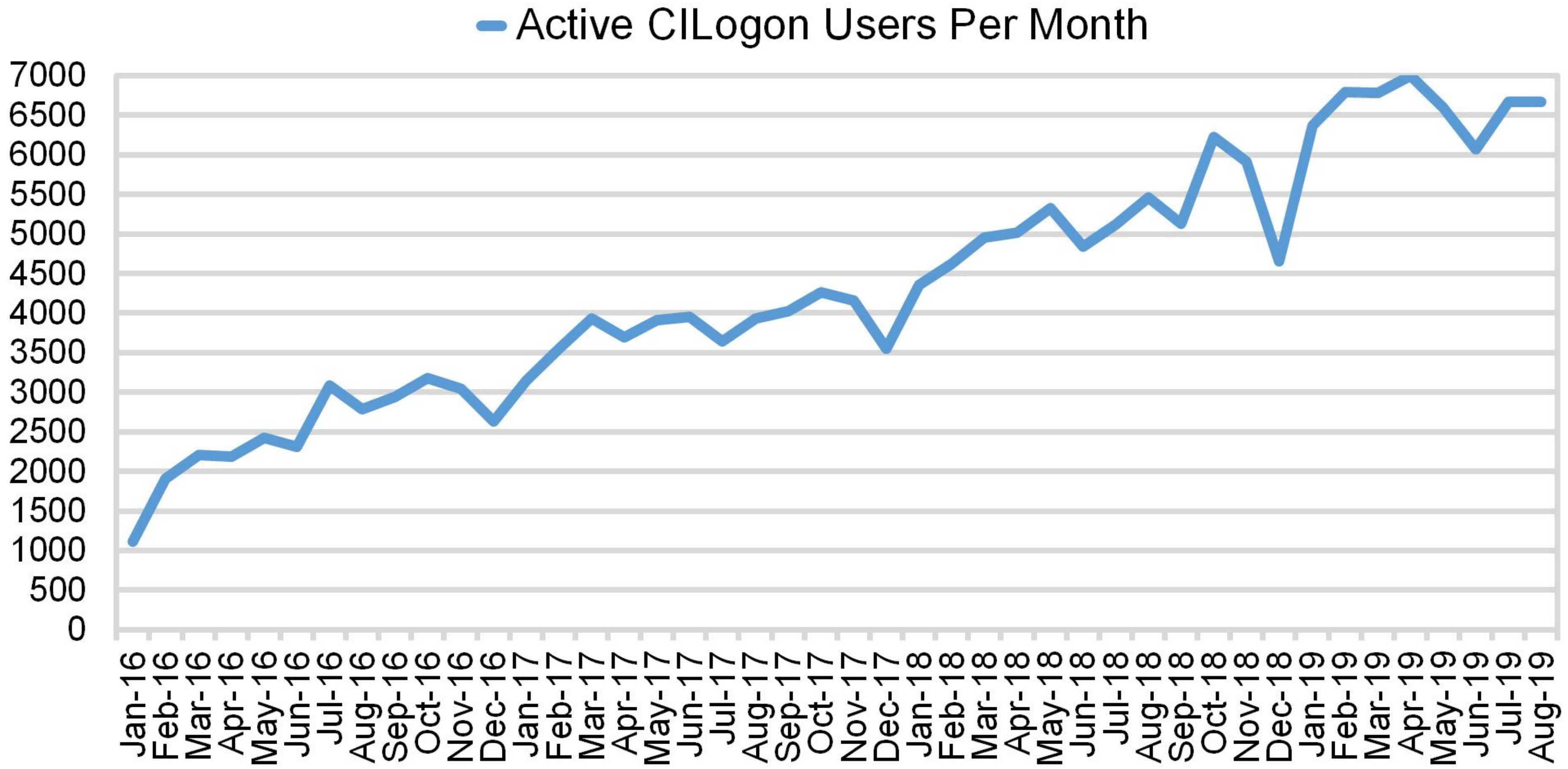
REFEDS Assurance



```
{
 "sub": "http://cilogon.org/serverT/users/107613",
 "idp_name": "XSEDE",
 "eppn": "jbasney@xsede.org",
 "cert_subject_dn": "/DC=org/DC=cilogon/C=US/O=XSEDE/CN=Jim Basney T107618",
 "eptid": "https://idp.xsede.org/idp/shibboleth!https://cilogon.org/shibboleth!CcYsMUcLXI7cAtbgKAUKVYaoOsE=",
 "iss": "https://cilogon.org",
 "given_name": "Jim",
 "aud": "cilogon:test.cilogon.org/demo",
 "acr": "https://refeds.org/profile/mfa",
 "idp": "https://idp.xsede.org/idp/shibboleth",
 "name": "Jim Basney",
 "family_name": "Basney",
 "email": "jbasney@illinois.edu"
}
```



Certificate Subject:	/DC=org/DC=cilogon/C=US/O=XSEDE/CN=Jim Basney T107618
Identity Provider:	XSEDE
Level of Assurance:	Silver


Active CILogon Users Per Month
7000
6500
6000
5500
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
Jan-16
Feb-16
Mar-16
Apr-16
May-16
Jun-16
Jul-16
Aug-16
Sep-16
Oct-16
Nov-16
Dec-16
Jan-17
Feb-17
Mar-17
Apr-17
May-17
Jun-17
Jul-17
Aug-17
Sep-17
Oct-17
Nov-17
Dec-17
Jan-18
Feb-18
Mar-18
Apr-18
May-18
Jun-18
Jul-18
Aug-18
Sep-18
Oct-18
Nov-18
Dec-18
Jan-19
Feb-19
Mar-19
Apr-19
May-19
Jun-19
Jul-19
Aug-19

Thanks!

contact:

help@cilogon.org

jbasney@ncsa.illinois.edu