Enabling Federated Identity and Access Management for Scientific Collaborations

Jim Basney
jbasney@ncsa.illinois.edu
FIM4R@FNAL
September 12 2019
who we are

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
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
COmanage-as-a-Service

Collaboration managed:
- enrollment flows
- expiration policies
- self service permissions
- pipelines

https://www.cilogon.org/comanage
OIDC for R&E

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

<table>
<thead>
<tr>
<th>voPersonApplicationUID</th>
<th>voPersonExternalUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>voPersonAuthorName</td>
<td>voPersonID</td>
</tr>
<tr>
<td>voPersonCertificateDN</td>
<td>voPersonSoRID</td>
</tr>
<tr>
<td>voPersonCertificateIssuerDN</td>
<td>voPersonStatus</td>
</tr>
</tbody>
</table>

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

Exit

About: CILogon Client

CILogon Client
Create credentials for accessing grids and cyberinfrastructure.

Product Version... 2.0.1

Written by: National Center for Supercomputing Applications
University of Illinois

Homepage: http://security.ncsa.illinois.edu

Copyright 2010, University of Illinois.

Close
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

<table>
<thead>
<tr>
<th>Identity Provider (entityID):</th>
<th><a href="https://idp.xsede.org/idp/shibboleth">https://idp.xsede.org/idp/shibboleth</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>ePTID:</td>
<td><a href="https://idp.xsede.org/idp/shibboleth!https://cilogon.org/shibboleth!CcYsMUcLX17cAtbgKAUKVYaoOsE=">https://idp.xsede.org/idp/shibboleth!https://cilogon.org/shibboleth!CcYsMUcLX17cAtbgKAUKVYaoOsE=</a></td>
</tr>
<tr>
<td>ePPN:</td>
<td><a href="mailto:jbasney@xsede.org">jbasney@xsede.org</a></td>
</tr>
<tr>
<td>First Name (givenName):</td>
<td>Jim</td>
</tr>
<tr>
<td>Last Name (sn):</td>
<td>Basney</td>
</tr>
<tr>
<td>Display Name (displayName):</td>
<td>Jim Basney</td>
</tr>
<tr>
<td>Email Address (email):</td>
<td><a href="mailto:jbasney@illinois.edu">jbasney@illinois.edu</a></td>
</tr>
<tr>
<td>AuthnContextClassRef:</td>
<td><a href="https://refeds.org/profile/mfa">https://refeds.org/profile/mfa</a></td>
</tr>
</tbody>
</table>
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!CcYsMUCjLXI7cAtbgKAUKVYao0sE=",
    "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"
}
```
Thanks!

contact:
help@cilogon.org
jbasney@ncsa.illinois.edu