Identity Management for Research Collaborations

Jim Basney
jbasney@ncsa.Illinois.edu

MAGIC@SC
Wed Nov 14 2018

This material is based upon work supported by the National Science Foundation under grant numbers 1547268, 1738962, and 1840003. 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.
federated identity management & collaborative organization management
Example: CILogon and JupyterHub

Use OAuthenticator to support OAuth with popular service providers

JupyterHub’s OAuthenticator currently supports the following popular services:

- Auth0
- Bitbucket
- CILogon
- GitHub
- GitLab
- Globus
- Google
- MediaWiki
- Okpy
- OpenShift

A generic implementation, which you can use for OAuth authentication with any provider, is also available.

voPerson: attributes for virtual organizations

- LDAP schema inspired by eduPerson
- Used by CILogon and COmanage
- Including:
  - voPersonAffiliation
  - voPersonApplicationUID
  - voPersonAuthorName
  - voPersonExternalID
  - voPersonPolicyAgreement
  - voPersonStatus
- To be adopted by REFEDS
CILogon Top 20 Identity Providers

- Fermi National Accelerator Laboratory
- LIGO Scientific Collaboration
- National Institutes of Health
- University of Michigan
- University of Illinois at Urbana-Champaign
- Purdue University Main Campus
- Johns Hopkins
- University of Chicago
- University of Minnesota
- Google

- Indiana University
- Stanford University
- Yale University
- CERN
- University of California-Los Angeles
- University of Florida
- Northwestern University
- Princeton University
- University of California, Berkeley
- Argonne National Laboratory

* As of October 2018

MAGIC@SC18 jbasney@ncsa.illinois.edu
X.509: Not Dead Yet

• CILogon issued 21,907 certificates in Oct 2018
• X.509 authentication for GridFTP and GSISSH still widely used
• CILogon Silver CA updated for REFEDS Assurance
Higher Assurance for XSEDE’s InCommon IdP

• Requires Duo MFA
  • https://refeds.org/profile/mfa

• Supports “vetted” and “unvetted” users
  • Self sign-up for XSEDE User Portal account
    • https://refeds.org/assurance/IAP/low
  • Users on peer-reviewed XSEDE allocations
    • https://refeds.org/assurance/IAP/medium
SciTokens: Capabilities for Distributed Scientific Computing

• Using standards
  • RFC 6749: OAuth 2.0 Authorization Framework
  • RFC 7519: JSON Web Token (JWT)
  • RFC 8414: OAuth 2.0 Authorization Server Metadata
  • OAuth 2.0 Token Exchange (IETF OAuth WG I-D)
• Working with CVMFS, HTCondor, and XRootD
  • https://github.com/scitokens

= token
Submit
Scheduler

Execute
Launcher

Data
Data Server

User
Token Manager

Job

Token Server

T
T
T

T

T

T

T
Custos: IAM for Science Gateways
Thanks!

jbasney@ncsa.Illinois.edu
@JimBasney
www.ncsa.Illinois.edu/~jbasney
https://orcid.org/0000-0002-0139-0640
"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov