CILogon and eduTEAMS: Collaboration and Virtual Organizations Made Easy

IAM Online
Wednesday, March 20, 2019

Jim Basney, National Center for Supercomputer Applications
Christos Kanellopoulos, GÉANT
Tom Barton, UChicago and Internet2
Academic collaboration and R&E federation

- Faculty, students, staff
- Data sets
- Intellectual property
- Specialized instruments
- Specialized computing
- At organizations everywhere
- Connected by global federation
We have global federation – aren’t we done yet?

68 countries

>5,400 eduGAIN entities

>16,700 total entities

(~25% InCommon)

>10,000,000 users
Get collaboration ready

- Enable basic collaboration
- Support high value resources
- Protect collaboration resources

- "Research & Scholarship" attribute release
  - Basic security - SIRTFI
  - Baseline Expectations
- REFEDS MFA Profile
- REFEDS Assurance

- Manage risk

Identity Providers implement

Academic Service Providers implement
Managing needs of a Service Provider

Commercial SP
- Box
- Google docs

Academic SP
- Ocean Observatories Initiative
- IU CI Gateway
Managing needs of a Service Provider

- Commercial SP
- Campus IdP
- Business ops
- contract
- Academic SP

InCommon
Managing needs of a Service Provider
Managing needs of a Service Provider

- Commercial SP
- Academic SP
- R&E federation
- Campus IdP
- Business ops
- VO service
- MOUs

- Authorization policy
- User identifiers and attributes
- Strong authentication
- Group/role management
- User support
- Credential translation
- Security

- Contract
Managing needs of a Service Provider

- **Commercial SP**: Contract
- **Campus IdP Business ops**: Security, Credential translation, User support, Group/role management, Strong authentication, User identifiers and attributes, Authorization policy
- **R&E federation**: MOUs, Academic SP
- **VO service**: Campus IdP, Business ops
Managing needs of a Service Provider

- Authorization policy
- User identifiers and attributes
- Strong authentication
- Group/role management
- User support
- Credential translation
- Security

Commercial SP
- Contract
- Campus IdP
  - Business ops

Academic SP
- MOUs
- R&E federation

VO service
- VO service
- VO service
- VO service

Campus IdP
- Campus IdP
- Campus IdP
- Campus IdP
- Campus IdP
- Business ops
Managing needs of a Service Provider

- Commercial SP
- Campus IdP
- Business ops
- VO service
- MOUs
- Academic SP
- R&E federation
- Campus IdP
- Campus IdP
- Campus IdP
- Campus IdP
- Campus IdP
- Campus IdP
- Business ops

- Authorization policy
- User identifiers and attributes
- Strong authentication
- Group/role management
- User support
- Credential translation
- Security

Inconsistent practices
Managing needs of a Service Provider

- Commercial SP
- Contract
- Campus IdP
- Business ops
- Authorization policy
- User identifiers and attributes
- Strong authentication
- Group/role management
- User support
- Credential translation
- Security
- Risk
- Inconsistent practices
- VO service
- MOUs
- Academic SP
- R&E federation
- Campus IdP
- Business ops
Life Sciences research communities user portal

User authentication services
- Credential translation
  - Proxy IdP is WWW
  - Some services are non-web e.g.
    - SSH access to a cloud VM
    - triggering file transfer between data archives
  - Conversion to X509

- Step-up Authentication
  1. User authenticates weakly using external authentication
  2. User authenticates with a second factor e.g. SMS-OTP or a mobile app

- Proxy Identity Provider
  - User has one ELIXIR identity
  - User can authenticate using external identities
  - Proxy Identity Provider consolidates the IDs

Relying services
- EGA
- eLearning
- Beacon
- Mailing lists
- Data archive
- Data transfer service

User authorisation services
- Dataset entitlements
  - User applies for access rights to a dataset
  - DAC approves
    - Endorsed user

- Group/role management
  - User can belong to one or more groups
  - Group memberships and roles are managed by group managers

- Bona fide role management
  - User applies for a bona fide status
  - User commits to a Code of Conduct
  - The community approves
    - Bona fide user

External authentication (e-infrastructures)
- eduGAIN Identity Providers
- Common Identity Providers

Log-in using Home Institution username & password
Log-in using Google, LinkedIn, ORCID etc.
Manage complexity of academic collaboration

Reduce the problem with …

- Common architecture (eg, AARC Blueprint Architecture)
- Common technical components (eg, COmanage)
- Community (AARC, Science Gateways Community Institute)
- Common services such as
  - CILogon (Jim)
  - eduTeams (Christos)

… and by Identity Providers getting collaboration ready
This material is based upon work supported by the National Science Foundation under grant numbers 0850557, 0943633, 1053575, 1440609, and 1547268 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.
who we are

ncsa.illinois.edu  sphericalcowgroup.com
our vision

seamless IAM for academic research collaborations
use your campus identity (InCommon/Shibboleth)
manage onboarding/offboarding/attributes/groups/roles in one place (COmanage)
integrate with a variety of research apps (OIDC, SAML, LDAP, X.509, SSH)
examples

grid computing
science gateways
jupyter notebooks
campus HPC clusters
realizing our vision

align with TIER (https://www.internet2.edu/tier)
  Shibboleth, COmanage, Grouper

provide hosted services
  common IAM platform across many collaborations

growing CILogon operations (since 2010)

reliability / sustainability
Open Source

CILogon (https://github.com/cilogon)
  OpenID Connect, OAuth, X.509
TIER (https://www.internet2.edu/tier)
  Shibboleth, COmanage, Grouper
IdentityPython (https://idpy.org/)
  pyFF, SATOSA
OpenLDAP
deployed to AWS

benefits of Net+ AWS
multiple availability zones
Docker containers in swarm mode
using R53 EC2 RDS ELB EFS
our baseline: REFEDS R&S

Attribute release continues to be the #1 stumbling block for new users.
We operate under the REFEDS R&S policy.
Does your campus support REFEDS R&S?
https://refeds.org/research-and-scholarship
https://test.cilogon.org/testidp/
InCommon REFEDS R&S IdPs

American University
Auburn University
Augusta University
Bates College
Binghamton University
Bucknell University
California State Polytechnic
California State University
Carleton College
Carnegie Mellon University
Cirrus Identity
Clemson University
Colgate University
Colorado School of Mines
Columbia University
Duke University
Duquesne University
Eastern Washington University
Emory University
Franklin & Marshall College
Harvard University
Haverford College
ICER - Mali
ICER - Uganda
Institute for Advanced Study
Internet2
Lafayette College
Lawrence Berkeley Natl Lab
LIGO Scientific Collaboration
MIT
Medical College of Wisconsin
NCSA
Naval Postgraduate School
New York University
North Carolina State University
North Dakota State University
Northeastern University
Northern Arizona University
Northern Illinois University
NYU Langone Health
Ohio State University
Oregon State University
Penn State
Portland State University
Purdue University
Rockefeller University
Southern Methodist University
Southern Oregon University
Space Telescope Science Institute
Stanford University
Stony Brook University
Syracuse University
Texas A & M University
The University of Memphis
Thomas Jefferson National Accelerator Facility
University of Alabama at Birmingham
University of Alaska
University of California
University of California
University of California
University of California
University of Chicago
University of Colorado at Boulder
University of Florida
University of Guam
University of Hawaii
University of Illinois at Urbana-Champaign
University of Iowa
University of Kentucky
University of Maryland Baltimore County
University of Michigan
University of Missouri System
University of Nebraska At Kearney
University of Nebraska Medical Center
University of Nebraska-Lincoln
University of Nevada
University of North Carolina at Chapel Hill
University of North Carolina At Charlotte
University of Oregon
University of Pittsburgh
University of Rochester
University of South Carolina
University of Texas at Arlington
University of Washington
University of West Florida
University of Wisconsin-Madison
University of Wyoming
Utah Valley University
Van Andel Research Institute
Virginia Polytechnic Institute & State University
Western Michigan University
XSEDE

CILogon

www.cilogon.org
informed consent
our 10 year history

2009 Federated login to TeraGrid. NSF ARRA award.
2010 CILogon operations begin. IGTF X.509 CAs operational.
2011 NSF SDCI award. OAuth support. InCommon Silver support.
2012 DOE ASCR award. Globus identity linking. InCommon R&S.
2013 XSEDE operations support. LIGO Data Grid use.
2016 NSF CICI award. eduGAIN support. OIDC support.
2017 COmanage support. AWS deployment.
2019 Transition to subscription funding model.
our path to sustainability

requests from CILogon clients
University of Illinois Office of Technology Management
not a typical transition to practice (TTP) story
no patents, no commercial use, open source software
aligned with REFEDS R&S
not a good fit for SBIR / STTR / I-Corps
TTP resources

Internet2 Eager TTP (Florence Hudson, Emily Nichols)
   https://spaces.at.internet2.edu/x/pAgZBg
South Alabama TTP (Alec Yasinsac)
   http://soc.southalabama.edu/TTP
SGCI Bootcamp (Michael Zentner, …)
   https://sciencegateways.org/engage/bootcamp
Trusted CI (Florence Hudson, Von Welch)
   https://trustedci.org/ttp
offered by the University

leveraging a variety of University support services
  Purchasing / Sponsored Programs / Contracts Services
  Grants and Contracts / NCSA Finance
program income fund → self supporting fund
SCG subcontract(s)
AWS billing
subscriber agreements & service activity rates
## our subscription model

<table>
<thead>
<tr>
<th>Service Tier</th>
<th>Service Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authentication Services</td>
<td>No charge</td>
</tr>
<tr>
<td>Basic Multi-tenant Collaboration Management Services</td>
<td>$1,200 per year</td>
</tr>
<tr>
<td>Full Service Production</td>
<td>$20,000 per year</td>
</tr>
<tr>
<td>Custom Support</td>
<td>Contact us</td>
</tr>
</tbody>
</table>

www.cilogon.org/subscribe
Enabling researcher and practitioner collaboration to accelerate cybersecurity research to practice via

- matchmaking
- business model coaching
- workshops

https://trustedci.org/ttp

2019 Cybersecurity Transition to Practice (TTP) Workshop

Wednesday, June 19th, 9am - 5pm. Chicago, IL

- Cybersecurity Topical Panels with Researchers and Practitioners
- Poster Session
- Thematic Co-creation breakouts for Research Transition to Practice

Request an invitation: https://trustedci.org/2019-ttp-workshop
Trusted CI One-on-One Engagements

Collaborations with NSF facilities and projects to address cybersecurity challenges (including IAM)

Currently accepting applications for second half of 2019:
https://trustedci.org/application/
Application Deadline: April 3
Thanks!

Contact:
help@cilogon.org
jbasney@ncsa.illinois.edu
eduTEAMS: “Virtual Organizations made easy”

Christos Kanellopoulos, GÉANT
January 2019:
59 Federations active
5 Federations with voting rights in process of joining
5292 entities
Advancing Technologies and Federating Communities

A Study on Authentication and Authorisation Platforms For Scientific Resources in Europe

FINAL REPORT
A study prepared for the European Commission
DG Communication Networks, Content & Technology
Federated Identity Management for Research Collaborations

Christopher John Atherton; Thomas Barton; Jim Basney; Daan Broeder; Alessandro Costa; Mirjam van Daalen; Stephanie Dyke; Willem Elbers; Carl-Fredrik Enelt; Enrico Maria Vincenzo Fasanelli; João Fernandes; Licia Florio; Peter Gietz; David L. Groep; Matthias Bernhard Junker; Christos Kanellopoulos; David Kelsey; Philip Kershaw; Cristina Knapp; Thorsten Kollegger; Scott Koranda; Mikael Linden; Filip Marinic; Ludek Matyska; Tommi Henrik Nyrönen; Stefan Paetow; Laura A D Paglione; Sandra Parlato; Christopher Phillips; Michal Prochazka; Nicholas Rees; Hannah Short; Uros Stevanovic; Michael Tarkovsky; Gerben Venekamp; Torn Vitez; Romain Wartel; Christopher Whalen; John White; Carlo Maria Zwolf

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

The authors also acknowledge the support and collaboration of many other colleagues in their respective institutes, research communities and IT Infrastructures, together with the funding received by these from many different sources. These include but are not limited to the following: (i) The Worldwide LHC Computing Grid (WLCG) project is a global collaboration of more than 170 computing centres in 43 countries, linking up national and international grid infrastructures. Funding is acknowledged from many national funding bodies and we acknowledge the support of several operational infrastructures including EGI, OSG and NDGF/NeIC. (ii) EGI acknowledges the funding and support received from the European Commission and the many National Grid Initiatives and other members. EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777536. (iii) The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2). (iv) Work on the development of ESGF's identity management system has been supported by The UK Natural Environment Research Council and funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration through projects IS-ENES (grant agreement no 228203) and IS-ENES2 (grant agreement no 312979). (v) Ludek Matyska and Michal Prochazka acknowledge funding from the RI ELIXIR CZ project funded by MEYS Czech Republic No. LM2015047. (vi) Scott Koranda acknowledges support provided by the United States National Science Foundation under Grant No. PHY-1700765. (vii) GÉANT on behalf of the GN4 Phase 2 project (GN4-2). The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 730941 (AARC2).
Components
- Proxy & Identity Hub
- Membership Management service
- Discovery Service
- Metadata Service
- Second Factor Authentication (Pilot!)

Characteristics
- Full implementation AARC Blueprint Architecture
- Single- and multi-tenant options
- Sustainability and strategic partnerships

A service to enable use of federated identity management in research & academic collaborations

Partner for any e-Infra or Research Infra including “long tail”, informal groups

https://www.eduteams.org
• Users sign in to services with their **community identity** via eduTEAMS

• Users **register once and access any service** (available to the their community)

• Reduces complexity for Service Providers by providing **one integration point for all services**

• Integration with GÉANT, EOSC and other communities and/or eduGAIN services
European Open Science Cloud
European Open Science Cloud
European Open Science Cloud
eduTEAMS Service
Provided by GÉANT to small and medium sized communities who want to get started with their virtual collaborations and take full advantage of the federated access without having to deal with the complexity of operating and supporting their own AAI. Supports multiple communities on the same platform. Provides everything required in order to securely collaborate and use services available to the GÉANT community and European Open Science Cloud.

eduTEAMS Dedicated
For communities requiring full control of their AAI, GÉANT can host and operate their own, dedicated AAI Service powered by the eduTEAMS technology. Communities can rely on the operational capabilities and expertise of GÉANT, while they are in full control of the policies, configuration and branding of their AAI.

eduTEAMS Bespoke
For those communities who require tailor-made functionality, such as integration with custom back-office and front-office systems, new features or enhancing their existing AAI with new functionality available in eduTEAMS, GÉANT can provide bespoke solutions based on the eduTEAMS technology, which can include a combination of consultancy,
eduTEAMS Service

- Shared platform that can be used by small-medium communities and the long tail of science
- Managed and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- eduTEAMS service policies
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services
eduTEAMS Service

- Shared platform that can be used by small - medium communities and the long tail of science
- Managed and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- eduTEAMS service policies
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

eduTEAMS Dedicated

- Dedicated, white-label service offering, specific to a community
- Managed by the community, operated by GEANT
- Community branding & community specific identifier
- Community managed policies
- Can be connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services
**eduTEAMS Service**
- Shared platform that can be used by small - medium communities and the long tail of science
- Managed and operated by GEANT
- eduTEAMS branding & eduTEAMS community identifier
- eduTEAMS service policies
- Connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

**eduTEAMS Dedicated**
- Dedicated, white-label service offering, specific to a community
- Managed by the community, operated by GEANT
- Community branding & community specific identifier
- Community managed policies
- Can be connected to EOSC (GEANT, EGI and EUDAT services)
- Onboarding of community specific services

**eduTEAMS Bespoke**
- Bespoke solution with tailor-made functionality
- Ownership model depended on the solution, operated by GEANT
- Consultancy, development and hosting of the service.
<table>
<thead>
<tr>
<th>Users</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>eduTEAMS Service</td>
<td>Production</td>
</tr>
<tr>
<td>Life Science AAI</td>
<td>Near Production</td>
</tr>
<tr>
<td>[ HPC Centers ]</td>
<td>Deployment</td>
</tr>
<tr>
<td>RedIRIS</td>
<td>Deployment</td>
</tr>
<tr>
<td>Photon and Neutron Community</td>
<td>Design</td>
</tr>
<tr>
<td>SURFnet</td>
<td>Design</td>
</tr>
<tr>
<td>GN4-3</td>
<td>Design</td>
</tr>
<tr>
<td>JISC</td>
<td>Discussion</td>
</tr>
</tbody>
</table>
We are working on it

- Feature: Component:Proxy
  Active Role Selection
- Feature: Component:Step-up
  Support for the Pilot Step-up Authentication Service
- Feature: Component:Proxy
  Component:Webapp
  IdP Attribute Release Check
- Feature: Component:Webapp
  Improved registration flow for Service Providers
- Component:Webapp
  New eduTEAMS website
- Feature: Component:TTS
  Support access to services that require certificate based authentication

+ Add another card

Coming soon

- Feature: Component:Proxy
  Component:Webapp
  Improvements in the generation of the eduTEAMS user identifier
- Compliance
  Support for Sirtfi on the eduTEAMS Service
- Compliance
  Update of the Acceptable Usage Policy for the eduTEAMS Service
- Feature: Component:MMS
  Component:Proxy
  Improved AUP acceptance process
- Feature: Component:Proxy
  Support of stepping up authentication flows in the eduTEAMS proxy
- Component:MMS
  Upgrade to COmanage 3.2

+ Add another card

Just shipped

- Feature: Component:Proxy
  Component:Webapp
  Support Sirtfi declarations in SAML metadata generation
- Feature: Component:MMS
  UI improvement on COmanage
- Component:MMS
  UI improvements on HE5AA
- Component:MMS
  UI improvements on Perun
- Compliance
  New version of the eduTEAMS Privacy Policy
- Feature: Component:MMS
  Component:Proxy
  Improved backend integration with COmanage and HE5AA
- Component:MMS
  Improved support for account linking
- Compliance
  Feature: Component:Proxy
  Improved support for informing the users about the attributes released to connected services

+ Add another card
Internet2 Global Summit (March 5 - 8)

Article in Connect (March)

IAM Online (March 20)

TNC 2019 (June 17 – 20)
eduTEAMS Service

Provided by GEANT to small and medium sized communities who want to get started with their virtual collaborations and take full advantage of the federated access without having to deal with the complexity of operating and supporting their own AAI. Supports multiple communities on the same platform. Provides everything required in order to securely collaborate and use services available to the GEANT community and European Open Science Cloud.

eduTEAMS Dedicated Service

For communities requiring full control of their AAI, GEANT can host and operate their own, dedicated AAI Service powered by the eduTEAMS technology. Communities can rely on the operational capabilities and expertise of GEANT, while they are in full control of the policies, configuration and branding of their AAI.

eduTEAMS Bespoke Service

For those communities who require tailor-made functionality, such as integration with custom back-office and front-office systems, new features or enhancing their existing AAIs with new functionality available in eduTEAMS, GEANT can provide bespoke solutions based on the eduTEAMS technology, which can include a combination of consultancy.

eduTEAMS Service Offerings

eduTEAMS provides a "Turn-key" solution for creating and managing Community AAIs following the AARC Blueprint Architecture.

There are three eduTEAMS SERVICE OFFERINGS. If you are interested in any of these offerings please contact us at support@eduteams.org.

If you are not sure which offering best fits your needs and want to see what eduTEAMS looks like, please try our Demo Service!
Thank you

https://www.eduteams.org

support@eduteams.org
Please evaluate today’s session

Upcoming Events

BaseCAMP: Hands-on with Federation and the InCommon Trusted Access Platform

August 13-15, 2019
Hyatt Regency, Milwaukee, Wisconsin
Incommon.org/basecamp
April 2019 IAM Online

Shibboleth Update
News from the Shibboleth Consortium and Scott Cantor, lead Shibboleth developer

April 10, 2019
2 pm ET | 1 pm CT | Noon MT | 11 am PT