PROCEEDINGS OF SCIENCE

CILogon: Enabling Federated Identity and Access Management for Scientific Collaborations

Jim Basney*
University of Illinois
E-mail: jbasney@illinois.edu

Heather Flanagan
Spherical Cow Group
E-mail: hlflanagan@sphericalcowgroup.com

Terry Fleury
University of Illinois
E-mail: tfleury@illinois.edu

Jeff Gaynor
University of Illinois
E-mail: gaynor@illinois.edu

Scott Koranda
Spherical Cow Group
E-mail: skoranda@sphericalcowgroup.com

Benn Oshrin
Spherical Cow Group
E-mail: benno@sphericalcowgroup.com

CILogon provides a software platform that enables scientists to work together to meet their identity and access management (IAM) needs more effectively so they can allocate more time and effort to their core mission of scientific research. CILogon builds on open source Shibboleth and COmanage software to provide an integrated IAM platform for science, federated worldwide via eduGAIN. CILogon serves the unique needs of research collaborations, namely to dynamically form collaboration groups across organizations and countries, sharing access to data, instruments, compute clusters, and other resources to enable scientific discovery. We operate CILogon via a software-as-a-service model to ease integration with a variety of science applications, while making all CILogon software components publicly available under open source licenses to enable re-use. Since CILogon operations began in 2010, our service has expanded from a federated X.509 certification authority (CA) to an OpenID Connect provider, SAML Attribute Authority, and multi-tenant collaboration platform. In this article, we describe the current CILogon system.

International Symposium on Grids & Clouds 2019, ISGC2019
31st March - 5th April, 2019
Academia Sinica, Taipei, Taiwan

*Speaker.

PoS(ISGC2019)031

1. Introduction

Scientific collaborations bring together researchers and infrastructure across academic institutions, cloud service providers, and international borders. Too often these collaborations are hindered by a hodgepodge of authentication and authorization mechanisms, requiring researchers to manage multiple credentials and disjoint permissions systems. The availability of federated identities, from providers including the OpenID Foundation (Google, Microsoft, etc.) and many Research and Education identity federations, such as the InCommon federation of US academic institutions, enables researchers to access cyberinfrastructure (CI) using their existing credentials. However, leveraging federated identity and managing the associated authorizations is challenging for all but the largest cyberinfrastructure projects. Many identity management technologies each provide one piece of the puzzle, but combining them into a coherent identity management platform is a daunting task. CILogon has evolved from a federated X.509 certification authority (CA) [1] to an integrated open source identity and access management platform for research collaborations, combining federated identity management with collaborative organization management. In this article, we describe the current CILogon system.

2. Leveraging Existing IAM Systems

CILogon leverages existing identity and access management (IAM) systems by 1) integrating with COmanage[1] for collaborative organization management, 2) using the open source Shibboleth[2] implementation of the Security Assertion Markup Language (SAML) [2] standard, and 3) interoperating with existing identity management federations, including InCommon, eduGAIN, and IGTF. We describe each of these existing IAM systems in the following subsections.

2.1 COmanage

COmanage enables a virtual organization (VO) to manage the entire lifecycle of collaboration. Beginning with onboarding, COmanage provides flexible and customizable enrollment flows to bring people and their federated identities onto the platform and create a collaborative organization (CO). Each CO may have multiple active enrollment flows tailored specifically for particular types of collaborators such as faculty, students, or staff, and each flow may onboard users by invitation, self signup, and even conscription. During enrollment, COmanage consumes the details about a user's federated or external identity as provided by their home organization or identity provider, and records it as an organizational identity. After enrollment the organizational identity is linked to the CO person identity representing the user as part of the CO. Because researchers today may hail from multiple organizations and often participate in multiple VOs simultaneously. COmanage supports linking multiple organizational identities to multiple CO person identities.

COmanage supports delegated management of the user and VO details necessary to support collaboration and access to applications. Users may be assigned multiple roles in the CO, and arbitrary sets of CO people can be pulled together into CO groups. COmanage supports the creation

[1] `https://www.internet2.edu/comanage/`
[2] `https://www.shibboleth.net/`

and management of multiple additional identifiers for a CO person record. These types of identifiers are often auto-generated at enrollment time and used to create specialized identifiers that can be consumed by applications. COmanage can provision the roles, groups, attributes, and identifiers for a CO person so that they can be consumed by applications and other infrastructure, and used to support authorization and tight integration. Out of the box, COmanage currently includes provisioning plugins for LDAP, Internet2 Grouper, GitHub, UNIX home directories, Mailman3, MediaWiki, Salesforce, and a JSON-based changelog. Custom plugins can be written for other services.

CO administrators can configure multiple flexible expiration policies on CO person records to support controlled offboarding. A user may transition from active to grace period status and then eventually to inactive or disabled status, with configurable transition times and notifications. When a CO person transitions to inactive status COmanage deprovisions the CO person roles, groups, and attributes so that revocation of access to applications happens automatically and in accordance with VO policies.

The current iteration of COmanage development began in 2010 with funding from an NSF grant awarded to Internet2 and has been deployed in production to support the gravitational wave astronomy community, the GÉANT-4 project in Europe, and the International Centers for Research program at the U.S. National Institute of Allergy and Infectious Diseases (NIAID), among other deployments.

2.2 Shibboleth

CILogon uses the open source Shibboleth software for SAML support. Shibboleth implements a SAML identity provider (IdP), which issues authentication and attribute assertions, and a SAML service provider (SP), which consumes authentication and attribute assertions. Shibboleth conforms to the Interoperable SAML Web Browser SSO Deployment Profile [3], including support for scalable trust management via SAML metadata exchange, as described in Section 2.4.

CILogon uses the Shibboleth SAML SP component to process SAML authentication and attribute assertions from SAML IdPs. The Shibboleth SP is an Apache HTTP server module that parses the SAML XML messages, verifies digital signatures and other SAML security properties, and (if verification is successful), sets Apache environment variables containing information from the assertion (i.e., the user's identity attributes). CILogon reads these environment variables to obtain the user information to include in subsequent X.509 certificates and OIDC claims.

2.3 Interoperable Global Trust Federation (IGTF)

Founded in October 2005, the IGTF (Interoperable Global Trust Federation, formerly the International Grid Trust Federation) establishes policies and guidelines for identity providers across its three member policy management authorities: APGridPMA covering Asia and the Pacific; EUGridPMA covering Europe, the Middle East, and Africa; and TAGPMA covering Latin America, the Caribbean, and North America. Since that time, the IGTF has been successful in achieving international acceptance of X.509 certificates for scientific computing, enabling large scientific collaborations such as the LHC Computing Grid. CILogon ensures that its X.509 certificates conform to IGTF guidelines for global interoperability.

2.4 InCommon

InCommon is a membership organization, with over 900 participants across higher education institutions, research organizations, and sponsored partners. Operated by Internet2, InCommon provides a SAML federation for secure single sign-on across identity providers and service providers operated by the participants. InCommon is recognized as a key component for "developing a coherent cyberinfrastructure from local campus to national facilities" [4]. InCommon's research and scholarship (R&S) program, launched in January 2012, provides a scalable approach to federated access from campuses to services that support research and scholarly activities. Prior to this program, services like CILogon that wanted to serve researchers from many InCommon member campuses needed to negotiate individually with each InCommon campus to enable attribute release, "unfortunately a time-consuming manual process" [5]. InCommon's R&S program provides a federation-scale alternative. Services apply to InCommon for inclusion in the R&S program, and InCommon "tags" accepted R&S services in SAML metadata. Then, participating InCommon campus identity providers release attributes to the "tagged" services. For services like CILogon, this eliminates the need for bilateral negotiation with each campus identity provider. InCommon helped develop an international version of R&S (called REFEDS R&S) to enable attribute release across federations, which has been key to enabling CILogon to scale globally.

2.5 eduGAIN

The eduGAIN service interconnects over 40 national identity federations from the United States (InCommon), Canada, Europe, Africa, Australia, Asia, and South America. InCommon joined the eduGAIN service in 2014 and enabled production interfederation in 2016. Without federation, SAML identity providers and service providers must establish bilateral trust, manually exchanging public keys and other service metadata, which scales poorly for scientific collaborations that may involve hundreds of institutions. Federations like InCommon solve this scalability challenge at the national level: identity providers and service providers join the national federation and register their public keys and other service metadata once with the federation, which distributes the information securely to the members. Prior to eduGAIN, identity providers and service providers needed to separately join each national federation to enable international interoperability. Now eduGAIN coordinates the exchange of metadata across federations, so registering with the service's "home" national federation scales globally.

InCommon's membership in eduGAIN enables the CILogon platform to support international identity providers. Through InCommon's eduGAIN connection, CILogon exports SAML metadata to international identity providers and imports SAML metadata from those providers. To enable international operation, we updated CILogon's IGTF accreditation in 2016 to cover international certificate issuance. As previously discussed, the international REFEDS research and scholarship (R&S) program is key to enabling release of user identity attributes from international identity providers to CILogon for authentication. Use of CILogon now spans the globe, supporting researchers from sites such as CERN in Switzerland, LRZ in Germany, GARR and INFN in Italy, KISTI in Korea, CESNET in the Czech Republic, and CNRS in France.

3. Technical Approach

Building on the existing identity and access management systems discussed in the previous section, CILogon creates an integrated identity and access management platform for science. The platform supports multiple authentication and authorization interfaces and multiple workflows for enrollment, provisioning, identity linking, and group management. This section presents the CILogon technical approach.

CILogon enables use of federated identities for access to research services, i.e., for cyberinfrastructure logon. Development of the CILogon service began in September 2009, and the CILogon service began production operation in September 2010. Since that time, over 50,000 researchers have used CILogon, with monthly usage growing to over 6,000 active users per month as seen in Figure 1.

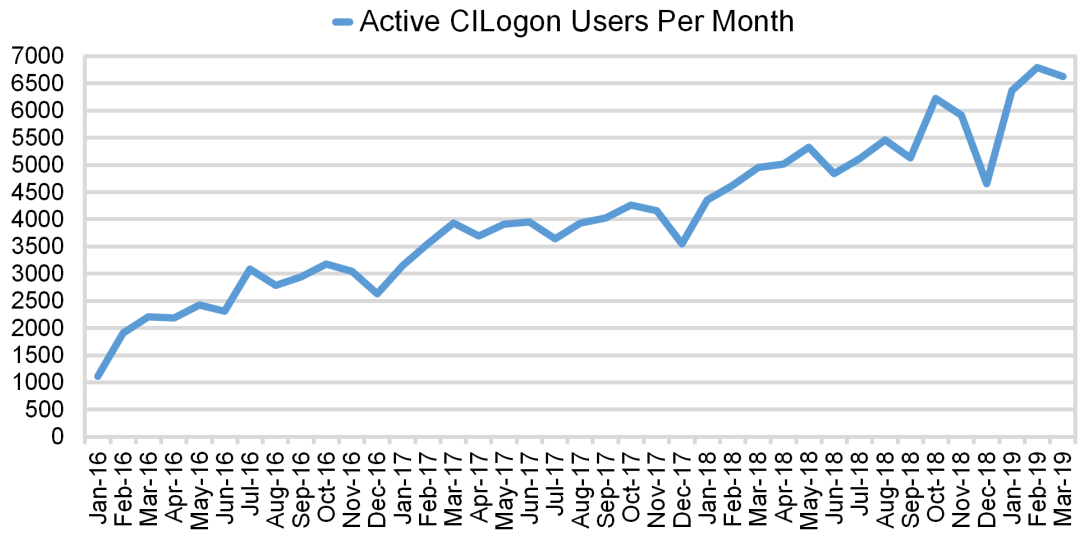

Figure 1: Number of Active CILogon Users Per Month

3.1 System Architecture

Figure 2 illustrates the components that make up the current CILogon system design. The User Registry provides storage for linked identities, multi-factor authentication (MFA) tokens, secure shell (SSH) keys, group memberships, and other user attributes. It is provided by COmanage.

CILogon supports authentication via multiple mechanisms. The SAML SP supports authentication from identity providers in the US InCommon federation as well as international identity providers through the eduGAIN service. The OIDC SP supports authentication using Google accounts. Support for additional OpenID Connect (OIDC) [6] providers may be added based on user demand. The OAuth SP supports authentication via GitHub, a web-based hosting service for version control of source code and other resources, and ORCID,[3] a service that provides persistent digital identifiers for researchers. The MFA module supports multi-factor authentication compatible with Google Authenticator, Duo, and other MFA apps.

[3] https://orcid.org/

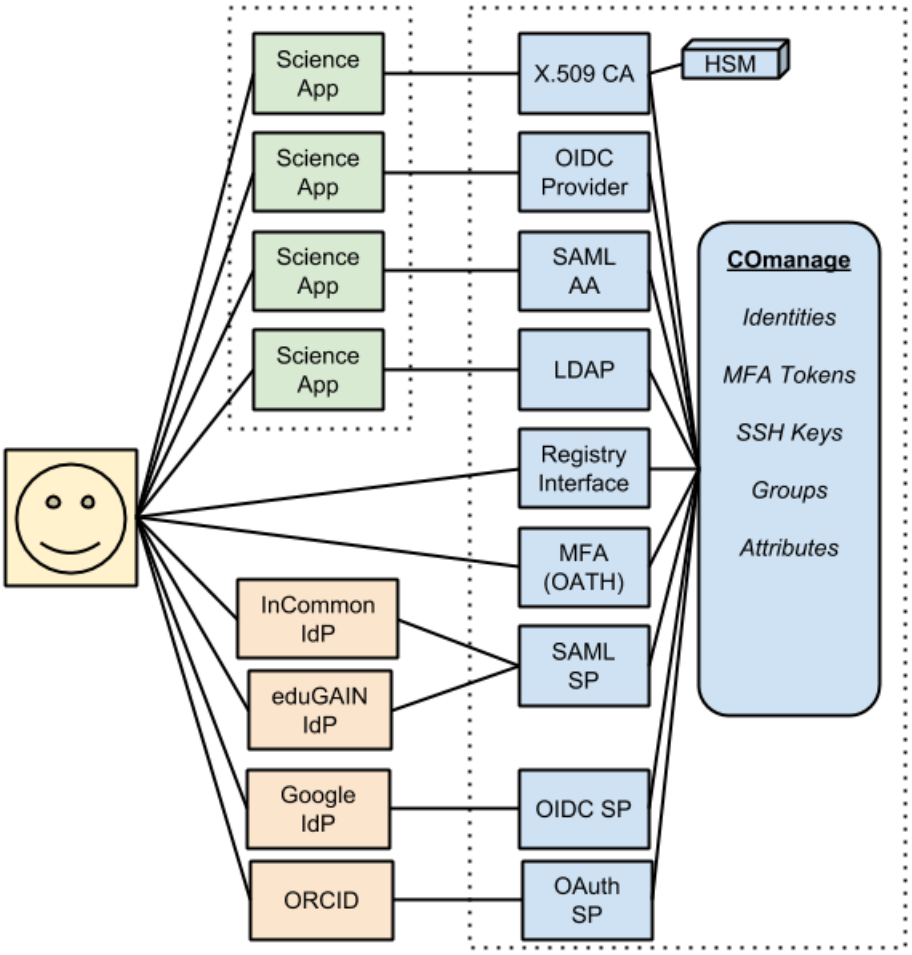

Figure 2: CILogon System Architecture

The User Registry Interface supports multiple application workflows, including user enrollment, identity linking, and group management. COmanage provides the user workflow functionality exposed by this interface.

CILogon provides multiple interfaces for science application integration. The LDAP interface supports user authentication and provides user attributes to applications via the standard LDAP protocol. The SAML AA interface provides a virtual organization (VO) attribute authority that issues assertions containing VO group membership information and other attributes that complement the attributes provided by InCommon/eduGAIN campus identity providers. The OIDC Provider enables application integration via the standard OpenID Connect protocol, providing user authentication and attributes without requiring direct application integration with hundreds of campus SAML identity providers. Lastly, the X.509 CA issues certificates containing user attributes for authentication to OSG, XSEDE, and other certificate-based cyberinfrastructure.

3.2 X.509 Certificates

CILogon issues certificates for authentication to distributed services used in collaborative science. CILogon relies on federated identity providers to identify certificate requesters, i.e., to provide the information about each requester to be included in each issued certificate. As an InCommon registered service provider, CILogon federates with identity providers operated by universities, so users can log on with their existing university password to obtain a certificate from CILogon. Users not affiliated with a university identity provider may authenticate using GitHub, Google, or ORCID identities. Users log on to CILogon from over 250 unique identity providers (IdPs) each month, out of over 4,500 identity providers available from eduGAIN.

CILogon provides a bridge from web browser based identity providers to X.509 certificates, which are supported by a wide variety of scientific cyberinfrastructure, including command-line, message-based, and multi-tier applications that are not well supported by web browser based security methods [5]. Users authenticate to CILogon using their web browser and then download a certificate to their desktop for use with certificate-based applications. The CILogon project works with science communities to provide custom interfaces to enable smooth integration of CILogon with specific science applications.

3.3 CILogon-COmanage Integration

CILogon integrates the COmanage software for collaboration management. COmanage support for configurable enrollment flows, roles, groups, identifiers, and expiration policies enables a VO to structure and manage the full collaboration lifecycle for its users.

CILogon integrates with COmanage via two standard interfaces: OIDC and LDAP. COmanage is an OIDC client to CILogon, so when users log on to COmanage (e.g., during an enrollment flow), the OIDC client component (mod_auth_openidc[4]) redirects their browser to CILogon for authentication, then CILogon redirects the browser back to COmanage with an OIDC id_token containing standard OIDC claims (e.g., name, email address, subject identifier, etc.) plus additional CILogon-specific claims (e.g., idp, affiliation) that COmanage can insert into the CO Person record. The COmanage LDAP Provisioner populates LDAP with user identity and VO membership information. Then, when users log on to science applications via OIDC, CILogon queries LDAP to obtain VO-specific information (e.g., group memberships) to include in OIDC claims. VO administrators have full control over the information contained in the CO Person records, the contents of LDAP, and the claims asserted to that VO's applications by the CILogon OIDC Provider. CILogon includes a new OIDC Client Management interface in COmanage that enables VO administrators to register their applications and define application-specific claim mappings.

3.4 LDAP

The Lightweight Directory Access Protocol (LDAP) is a workhorse of campus identity. LDAP provides a standard authentication protocol (typically password-based) supported by many applications. The LDAP directory also provides a standard interface for user profile and attribute information. CILogon enables users to set LDAP application passwords linked to their federated identities, to enable authentication to campus applications that support LDAP but not SAML or

[4] https://www.mod-auth-openidc.org/

OpenID Connect. CILogon's LDAP service also enables authorized applications to look up user profile and attribute information, including identity mappings between X.509 distinguished names, SAML eduPersonPrincipalNames, and ORCID identifiers to perform local authorization decisions based on the user's different identifiers.

As part of CILogon's LDAP support, we developed the voPerson LDAP schema [7] to address the attribute management needs of research collaborations. Existing LDAP schemas, such as eduPerson, organizationalPerson, and inetOrgPerson, assume the user's identity is managed by a single organization and do not support the identity linking scenarios that are key to the CILogon platform. The new voPersonExternalID attribute supports linked identifiers from external identity providers, and the new voPersonApplicationUID attribute supports application-specific identifiers, used when applications linked with the platform have unique requirements for user IDs.

3.5 SSH Key Management

Though custom Secure Shell (SSH) clients are available to support X.509 and SAML authentication, the public key authentication supported by standard SSH clients remains a popular method for single sign-on to campus compute clusters. Often, researchers that use compute clusters across multiple campuses and resource providers must register their SSH public keys separately with each provider. With CILogon, users can upload their SSH public keys once, then CILogon supports SSH public key lookup via LDAP for authorized access to compute clusters.

3.6 Web Single Sign-On Gateway

Supporting global-scale web single sign-on (SSO), to enable access from widely distributed research collaborators, is a significant challenge for cyberinfrastructure providers. Integrating multiple web SSO protocols (SAML, OAuth, OIDC) across hundreds of identity providers is a task out of reach for all but the largest cyberinfrastructure projects. The CILogon platform provides a web single sign-on gateway using the OpenID Connect (OIDC) standard that provides a one-time integration point to enable support for global-scale web SSO for scientific web applications.

A growing number of cyberinfrastructure services support the OIDC standard for federated identities. OIDC provides an identity layer on top of the OAuth 2.0 [8] protocol. Providing an OIDC interface to the CILogon platform enables access to the many InCommon/eduGAIN SAML identity providers via a single endpoint, saving cyberinfrastructure projects from the complexity of managing SAML federation at scale. CILogon's original SAML to OAuth 1.0 gateway was adopted by DataONE, Globus, OSG Connect, and the XSEDE User Portal for its ease of integration. The CILogon platform's SAML to OIDC (OAuth 2.0) gateway has been adopted by Ocean Observatories Initiative, OSC OnDemand, SeedME, and others.

3.7 SAML Attribute Authority

SAML-enabled cyberinfrastructure services may use InCommon authentication directly, but often InCommon identity providers do not provide the VO-specific attributes and group membership information needed for authorization. The CILogon platform provides a SAML attribute authority interface to user attributes and group information to support this use case. The Shibboleth Service Provider supports querying multiple SAML attribute authorities for attributes about an

authenticated user, allowing cyberinfrastructure services to combine user attributes from campus with attributes from the CILogon platform.

3.8 Linking ORCID Researcher Identities

The ORCID service, operated by a non-profit membership organization using open source software, provides persistent digital identifiers for researchers. The researcher's ORCID identifier can be linked to the researcher's institutional affiliations, but the identifier does not change when the researcher changes institutions. Thus, ORCID identifiers provide a persistent identity for researchers throughout their career that can be linked to their publications and other professional activities. The ORCID Public API provides an OAuth interface to authenticate a researcher's ORCID identifier, which CILogon uses to perform this linking. CILogon makes the identifier links available via LDAP, SAML, and OIDC interfaces. After performing the identity linking, users may authenticate to CILogon using their InCommon, eduGAIN, GitHub, Google, or ORCID credentials, and their ORCID identifier is included in the LDAP, SAML, OIDC, and/or X.509 assertions resulting from that authentication.

4. Related Work

Since the CILogon project began in 2009, multiple identity and access management solutions have emerged in support of research collaborations. We provide a brief review of related work in this section.

The AARC Blueprint Architecture (BPA)[5] documents the common elements seen in IAM deployments across many research projects. The BPA recognizes the important role of an IAM proxy service (like CILogon) that enables federation at scale, performs protocol translation, and manages community-based attributes and groups for centralized management to applications in the federation. Thus, we consider CILogon to be "BPA compliant."

eduTEAMS[6] is a European software-as-a-service offering launched in 2019 with many similarities to CILogon. eduTEAMS provides a SAML/OIDC proxy and a membership management service with support for community-specific customization similar to CILogon. In contrast to CILogon's tight coupling with COmanage, eduTEAMS allows communities to choose between COmanage, HEXAA, or Perun for membership management. eduTEAMS also supports deployment of services to an OpenStack environment managed by the collaboration, in contrast to CILogon's services which are operated on dedicated cloud resources. eduTEAMS does not include LDAP or X.509 support for application integration.

Unity[7] is an authentication service that supports federated identities (SAML, OpenID), along with management of user groups, attributes, and credentials. It supports integration via LDAP, OAuth, SAML, and PAM. It also integrates well with the UNICORE scientific computing middleware. Unity is open source software that can be installed and operated by the research collaboration, in contrast to CILogon's software-as-a-service model where the CILogon team operates the IAM services on the collaboration's behalf.

[5] `https://aarc-project.eu/architecture/`

[6] `https://www.geant.org/Innovation/eduteams`

[7] `https://www.unity-idm.eu/`

The InCommon Trusted Access Platform[8] delivers a packaged suite of components (Shibboleth Identity Provider, Grouper, and COmanage) with a set of APIs for identity and access management on campus. Since CILogon is constructed from a similar software stack (Shibboleth Service Provider, COmanage), CILogon has good interoperability with these deployments. For those campuses interested in the collaboration management services of COmanage, the CILogon platform provides a hosted option as an alternative to a local campus deployment.

Globus Auth [9] provides identity, profile, and group management as part of the Globus Service Platform. Globus Auth implements InCommon authentication via CILogon's OAuth interface. In this way, cyberinfrastructure such as OSG Connect and DOE KBase gain access to CILogon services by integrating with Globus Auth. Thus, Globus Auth subscribers benefit from CILogon enhancements, particularly support for international identity providers. While Globus Auth provides identity linking and group management capabilities, we believe the group management provided by COmanage in the CILogon platform introduces added benefits. COmanage provides significant flexibility in enrollment workflows, a robust plugin model, and standard interfaces to LDAP and SAML. Unlike Globus Auth, the CILogon platform, including COmanage, is open source.

Beyond Google and other social identity providers, a number of existing products and services offer collaboration and identity management, SAML-to-OIDC gateways, and integration with common workgroup applications. Some of the products are available as open source tools and can be readily downloaded and deployed by any group or project needing collaboration management. Each of these products and services, however, is focused on enterprise applications and only support the limited point-to-point model of federation. They do not readily scale, if at all, to support the number and diversity of federated identity providers necessary to enable international science projects and collaborations. In contrast, the CILogon platform is built on the large investment already made by the worldwide higher education and research community in regional and international identity federations.

5. Sustainability Model and Current Status

For science projects to rely on externally provided cyberinfrastructure, it must provide sustained reliability. The CILogon sustainability model has two components: a basic level of operational support for CILogon provided by XSEDE [10], and a pay-as-you-go "service for cost" support level for the integrated CILogon platform including COmanage functionality. Providing a "service for cost" sustainability model was a common request from multiple CILogon early-adopters. The "service for cost" model has two tiers of service: a basic tier that provides a multi-tenant service instance with a standard set of per-VO customizations, and a "full service" tier that provides dedicated service instances (for greater customization and scalability), VO control over code plugins, and other add-on services.

All CILogon software is publicly available from `https://github.com/cilogon` under Open Source licenses. Likewise, COmanage software is publicly available from `https://github.com/Internet2/comanage-registry` under an Open Source license. The CILogon platform is operational at `https://cilogon.org/`.

[8] `https://www.incommon.org/tap/`

6. Conclusion

The current CILogon platform builds on prior work by the CILogon and COmanage projects to provide federated identity and collaborative group management for research cyberinfrastructure. In our operational experience, support for scalable identity federation, customizable enrollment flows, and multiple standards-compliant integration interfaces is effective for enabling a variety of collaborative research applications. Our software-as-a-service model enables science projects to support hundreds of identity providers with common user and group management across multiple applications, hiding the complexities of international identity federation and protocol interoperability. CILogon unlocks the potential of large federations like InCommon and eduGAIN for research collaborations.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1547268.

References

[1] J. Basney, T. Fleury and J. Gaynor, *CILogon: A federated X.509 certification authority for cyberinfrastructure logon*, *Concurrency and Computation: Practice and Experience* **26** (2014) [https://doi.org/10.1002/cpe.3265].

[2] S. Cantor, J. Kemp, R. Philpott and E. Maler, *Assertions and protocols for the OASIS Security Assertion Markup Language (SAML) v2.0*, Tech. Rep. saml-core-2.0-os, OASIS, 2005.

[3] W. Hoehn, S. Cantor, R. Horbe, T. Scavo, E. Goodman, B. Bieber et al., *SAML v2.0 implementation profile for federation interoperability*, Tech. Rep. Version 1.0, Kantara Initiative, 2018.

[4] C. Stewart, J. Pepin, J. Odegard, T. Hauser, S. Fratkin, G. Almes et al., *Developing a coherent cyberinfrastructure from local campus to national facilities: Challenges and strategies*, Tech. Rep. Workshop Report and Recommendations, EDUCAUSE Campus Cyberinfrastructure Working Group and Coalition for Academic Scientific Computation, February, 2009.

[5] V. Welch, A. Walsh, W. Barnett and C. Stewart, *A roadmap for using NSF cyberinfrastructure with InCommon*, in *Proceedings of the 2011 TeraGrid Conference: Extreme Digital Discovery*, TeraGrid Conference, (New York, NY, USA), 2011, https://doi.org/10.1145/2016741.2016771.

[6] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros and C. Mortimore, *OpenID Connect Core 1.0*, tech. rep., OpenID Foundation, November, 2014.

[7] B. Oshrin, S. Koranda and J. Basney, *voPerson object class and recommendations*, Tech. Rep. Version 1.1, CILogon Project, Dec., 2018. 10.5281/zenodo.2649298.

[8] D. Hardt, *The OAuth 2.0 authorization framework*, RFC 6749, IETF, October, 2012.

[9] S. Tuecke, R. Ananthakrishnan, K. Chard, M. Lidman, B. McCollam, S. Rosen et al., *Globus Auth: A research identity and access management platform*, in *IEEE International Conference on e-Science (e-Science)*, pp. 203–212, Oct, 2016, https://doi.org/10.1109/eScience.2016.7870901.

[10] J. Towns, T. Cockerill, M. Dahan, I. Foster, K. Gaither, A. Grimshaw et al., *XSEDE: Accelerating scientific discovery*, *Computing in Science Engineering* **16** (2014) 62 [https://doi.org/10.1109/MCSE.2014.80].

Acronyms

APGridPMA Asia Pacific Grid Policy Management Authority

CERN European Organization for Nuclear Research

CESNET Czech Republic research and education network

CI Cyberinfrastructure

CNRS French National Center for Scientific Research

CO Collaborative Organization

DOE Department of Energy

GARR Italian national research and education network

IAM Identity and Access Management

IdP Identity Provider (issues authentication and attribute assertions)

IGTF Interoperable Global Trust Federation

INFN Italian National Institute for Nuclear Physics

KISTI Korea Institute of Science and Technology Information

LDAP Lightweight Directory Access Protocol

LHC Large Hadron Collider

LRZ Leibniz Supercomputing Centre

MFA Multi-Factor Authentication

OIDC OpenID Connect, a simple identity layer on top of the OAuth 2.0 protocol

ORCID Open Researcher and Contributor ID

OSC Ohio Supercomputing Center

OSG Open Science Grid

REFEDS The Research and Education FEDerations group

SAML Security Assertion Markup Language

SP Service Provider (consumes authentication and attribute assertions)

SSH Secure Shell

SSO Single Sign-On

TAGPMA The Americas Grid Policy Management Authority

VO Virtual Organization

XSEDE NSF's Extreme Science and Engineering Discovery Environment