CILogon-HA: Higher Assurance Federated Identities for DOE Science

Final Technical Report

DOE award: DE-SC0008597 (University of Illinois)

Project PI: James Basney <jbasney@illinois.edu>

Award Period: September 2012 through August 2015

Executive Summary

The CILogon-HA project extended the existing open source CILogon service (initially developed with funding from the National Science Foundation) to provide credentials at multiple levels of assurance to users of DOE facilities for collaborative science. CILogon translates mechanism and policy across higher education and grid trust federations, bridging from the InCommon identity federation (which federates university and DOE lab identities) to the Interoperable Global Trust Federation (which defines standards across the Worldwide LHC Computing Grid, the Open Science Grid, and other cyberinfrastructure). The CILogon-HA project expanded the CILogon service to support over 160 identity providers (including 6 DOE facilities) and 3 internationally accredited certification authorities. To provide continuity of operations upon the end of the CILogon-HA project period, project staff transitioned the CILogon service to operation by XSEDE.

Supporting Open Science Grid

In August 2013, Open Science Grid launched OSG Connect (https://osgconnect.net/), which "offers investigators simple and efficient access to distributed high throughput computing resources required by many of today's most challenging problems in science, engineering, and the humanities." OSG Connect supports easy sign up and sign in using federated campus identities through a combination of underlying technologies: Globus Nexus, CILogon, and InCommon. Globus Nexus, part of Globus Online, provides identity and group management for OSG Connect. Globus Nexus in turn relies on CILogon to enable access via campus identities through the InCommon federation. The result is that researchers can easily access OSG Connect using their existing campus logins.

In January 2015, Open Science Grid decided to partner with XSEDE and the CILogon project to provide a dedicated CILogon OSG Certification Authority (CA) to issue digital certificates to the OSG community. CILogon-HA project staff deployed this new OSG CA instance and worked with OSG staff to integrate it with the OSG Information Management system and obtain international accreditation by the Interoperable Global Trust Federation (IGTF) for this CA. Figure 1 illustrates the integration between the OSG User Registration web interface at Indiana University and the CILogon back-end CA services at NCSA and NICS, including dedicated hardware security modules (HSMs). CILogon-HA project staff coordinated with XSEDE operations staff for the ongoing production operation of the CILogon OSG CA service.

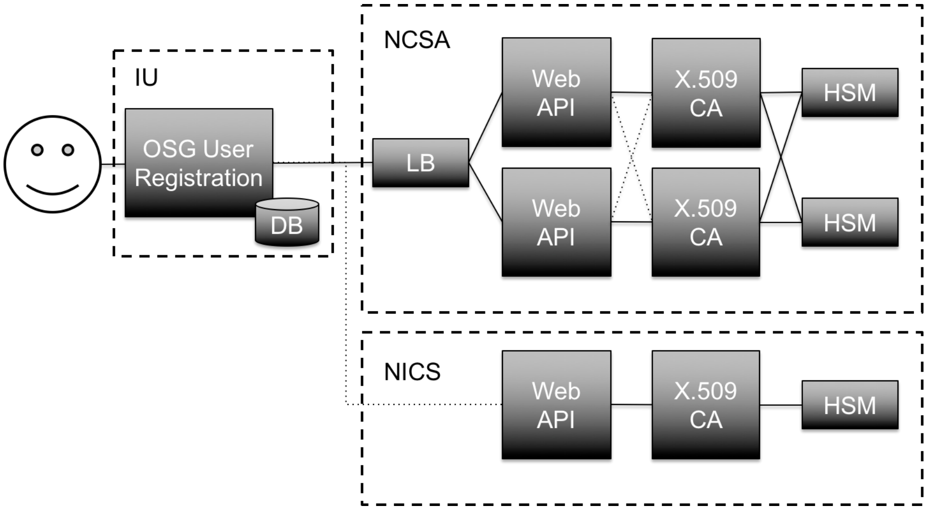

Figure 1. The CILogon OSG CA provides certificates based on OSG User Registration.

Interoperating with Universities and DOE Labs

When the CILogon-HA project started in September 2012, CILogon interoperated with 60 InCommon identity providers, including ANL and LBNL. In the 3 years of the project, this number grew to 162 identity providers, including BNL, ESnet, FNAL, and ORNL. In many cases, adding identity providers to CILogon involved outreach by CILogon-HA project staff to provide assistance to identity provider administrators. CILogon-HA project staff also helped develop and grow the InCommon Research and Scholarship (R&S) program that facilitates connections between InCommon identity providers and research service providers like CILogon. As illustrated in Figure 2 below, the InCommon R&S program enabled connections with over 50 identity providers over the CILogon-HA project period.

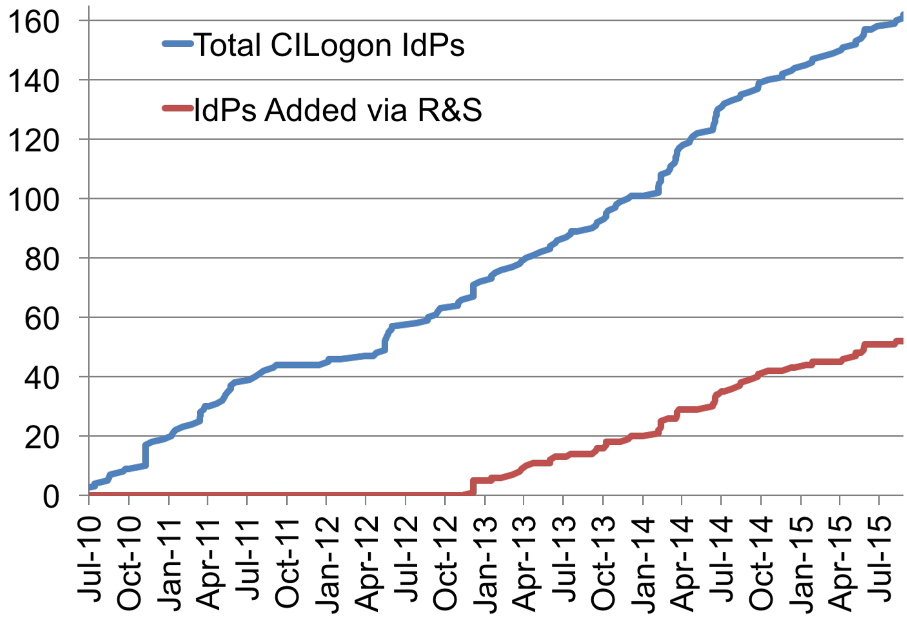

Figure 2. CILogon now supports over 160 identity providers.

In February 2014, the US ATLAS project launched ATLAS Connect (http://connect.usatlas.org/), which provides a version of OSG Connect tailored to the US ATLAS physics community. Like OSG Connect, ATLAS Connect supports sign in via CILogon for federated InCommon access. In support of ATLAS Connect, CILogon-HA staff worked with InCommon staff to increase the number of InCommon identity providers available to ATLAS Connect users. At the start of this process, out of 44 US ATLAS collaborating institutions, 40 operated InCommon identity providers of which 23 interoperated with CILogon. After the outreach, CILogon supported an additional 12 identity providers from US ATLAS collaborating institutions. In 2016 the CILogon project will perform a similar effort to support US CMS (http://connect.uscms.org) under new National Science Foundation funding.

Supporting a Growing User Community

Over the duration of the CILogon-HA project, the CILogon user community grew from 800 users to over 6,000. Integrations with Globus, LIGO, OSG Connect, ATLAS Connect, and the XSEDE Portal brought a steady stream of new users to CILogon for federated access to these services. Figure 3 illustrates this steady growth in use of the CILogon service as new integrations came online.

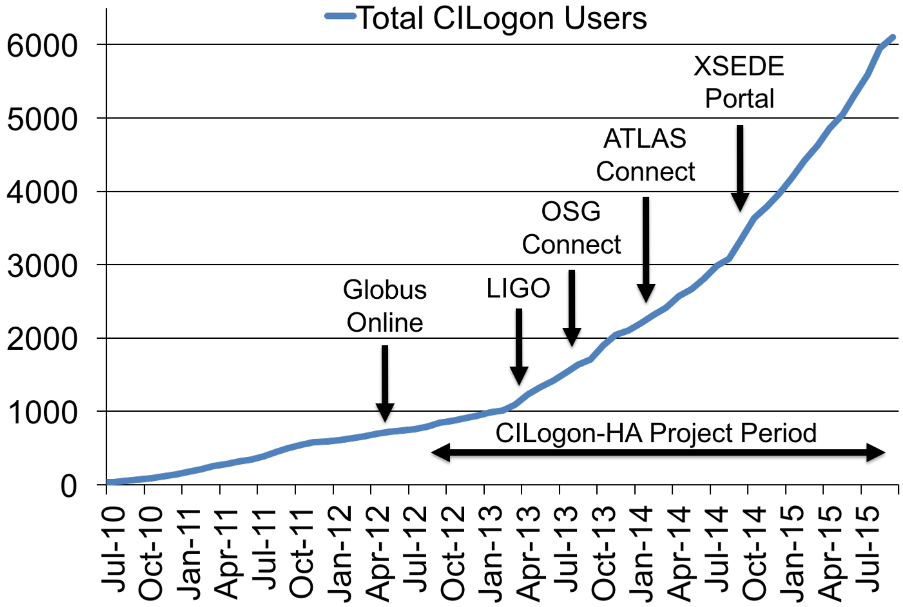

Figure 3. The CILogon user base grew from 800 users to over 6,000 during the project period.

Support for LIGO after DOEGrids CA Retirement

With the retirement of the DOEGrids CA in 2013, LIGO migrated to using the CILogon Basic CA in production for issuing user certificates for LIGO Data Grid access. LIGO users run the ligo-proxy-init command to authenticate with their @LIGO.ORG (albert.einstein) credentials to obtain a short-lived (3 day) certificate from the CILogon Basic CA. By obtaining short-lived certificates on demand using their existing LIGO identities, LIGO users can avoid the complexities of manually requesting, downloading, managing, and renewing long-lived certificates. In fact, LIGO users need not know anything about CILogon or X.509 certificates to use ligo-proxy-init and do their work on the LIGO Data Grid. Behind the scenes, ligo-proxy-init uses the SAML ECP protocol via InCommon to authenticate to CILogon, enabling CILogon to issue certificates via the command-line for LIGO identities.

Supporting Multiple Levels of Assurance

In September 2012, Virginia Tech became the first university in the country to achieve the InCommon Silver level of assurance, which CILogon can translate into a credential accredited by the Interoperable Global Trust Federation (IGTF) for acceptance by Open Science Grid and other cyberinfrastructure around the world. CILogon-HA staff collaborated with staff at Virginia Tech and Open Science Grid to demonstrate end-to-end access to Open Science Grid resources using these higher assurance credentials. Because of CILogon's IGTF accreditation, Virginia Tech researchers can also use their credentials for access to XSEDE (Extreme Science and Engineering Discovery Environment) and other computing infrastructure supporting research around the world.

To support international adoption of multiple levels of assurance, CILogon-HA project staff participated in the development of a new IGTF authentication profile called Identifier-Only Trust Assurance with Secured Infrastructure (IOTA). The IOTA profile recognizes that cyberinfrastructure providers and virtual organizations often vet user identities according to their own requirements, reducing their reliance on the identity vetting performed by CAs. IOTA requires CAs to ensure unique identification of users, but IOTA CAs are not required to verify the user's legal name or check government issued identity documents. The IOTA profile was finalized and adopted in April 2014.

The CILogon-HA project submitted the CILogon Basic CA for accreditation under the IOTA profile, after performing the necessary policy documentation and operational updates to comply with the requirements of the profile. IGTF policy review was completed in April 2014 and operational review was completed July 2014, thereby enabling CILogon to provide IGTF certificates to users from all InCommon identity providers, using IGTF accredited CAs at both the Silver and Basic levels of assurance. Expanding access to IGTF certificates beyond the Silver level of assurance is particularly valuable given the slow adoption of the InCommon assurance program. Virginia Tech remains the only InCommon identity provider approved at the Silver level of assurance.

CILogon-HA added support for multi-factor authentication via two approaches. First, access to CILogon from Virginia Tech at the Silver level uses a multi-factor smartcard issued by Virginia Tech to researchers. Second, CILogon-HA can add a second authentication factor as a "step-up" level of assurance for certificate issuance. CILogon-HA added support for the Google Authenticator mobile app, which implements one-time passwords according to the open standards developed by the Initiative for Open Authentication (OATH) (unrelated to OAuth). CILogon's second factor support is designed to accommodate multiple methods, and CILogon may support additional methods (such as Duo) in the future according to community requirements.

Operation by XSEDE

The CILogon-HA project transitioned operations of the CILogon service to XSEDE (https://xsede.org/) in order to sustain the CILogon service for its users beyond the current award period. This included following the XSEDE systems engineering process to align CILogon with XSEDE's operational policies and procedures, as well as establishing geographic redundancy for the CILogon service, with a new secondary CILogon instance at the National Institute for Computational Sciences (NICS) on the Oak Ridge National Lab (ORNL) campus. XSEDE and Open Science Grid established a Memorandum of Understanding regarding their shared use and support of the CILogon service. XSEDE Operations completed acceptance testing in January 2015 and accepted CILogon for production.

Conclusion

The CILogon-HA project enabled significant growth in the use of federated identities for DOE science, in partnership with Open Science Grid, Globus, and the DOE labs. The project achieved international accreditation of multiple certification authorities at different levels of assurance, and transitioned the CILogon service to production operation by XSEDE.

References

- Jim Basney, Terry Fleury, and Jeff Gaynor, "CILogon: A Federated X.509 Certification Authority for CyberInfrastructure Logon," XSEDE Conference, July 2013, San Diego, CA. http://dx.doi.org/10.1145/2484762.2484791
- Jim Basney, Terry Fleury, and Jeff Gaynor, "CILogon: A Federated X.509 Certification Authority for CyberInfrastructure Logon," Concurrency and Computation: Practice and Experience, 2014. http://dx.doi.org/10.1002/cpe.3265