CILogon: A Federated X.509 Certification Authority for CyberInfrastructure Logon

Jim Basney
jbasney@illinois.edu

Terry Fleury
tfleury@illinois.edu

Jeff Gaynor
gaynor@illinois.edu

National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
1205 West Clark Street
Urbana, Illinois 61801

ABSTRACT

CILogon provides a federated X.509 certification authority for secure access to cyberinfrastructure such as the Extreme Science and Engineering Discovery Environment (XSEDE). CILogon relies on federated authentication (SAML and OpenID) for determining user identities when issuing certificates. Federated authentication enables users to obtain certificates using existing identities (university, Google, etc.). Federated authentication also enables CILogon to serve a national-scale user community without requiring a large network of registration authorities performing manual user identification. CILogon supports multiple levels of assurance and custom interfaces for specific user communities. In this article we introduce the CILogon service and describe experiences and lessons learned from the first three years of operation.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Authentication*

General Terms

Security

Keywords

PKI, X.509, SAML, OpenID, OAuth, identity federation, grid computing, XSEDE, Shibboleth, InCommon

1. INTRODUCTION

Federated identity management enables service providers to accept identities from one or more external identity providers, reducing the need for service providers to issue identities directly to users and reducing the need for users to manage different identities and credentials for different services [1]. The CILogon project enables use of federated identities for access to research services, i.e., for cyberinfrastructure logon.

CILogon relies on the InCommon Federation, the United States education and research identity federation, whose members (higher education institutions, government and nonprofit laboratories, research centers and agencies, and their sponsored partners) implement the OASIS SAML standards for distributed identity management. Through the InCommon Federation, CILogon enables users to obtain X.509 certificates for their existing federated identities, i.e., using their login at their home university or institution. The certificates enable users to securely access certificate-based research services via standards such as TLS and WS-Security.

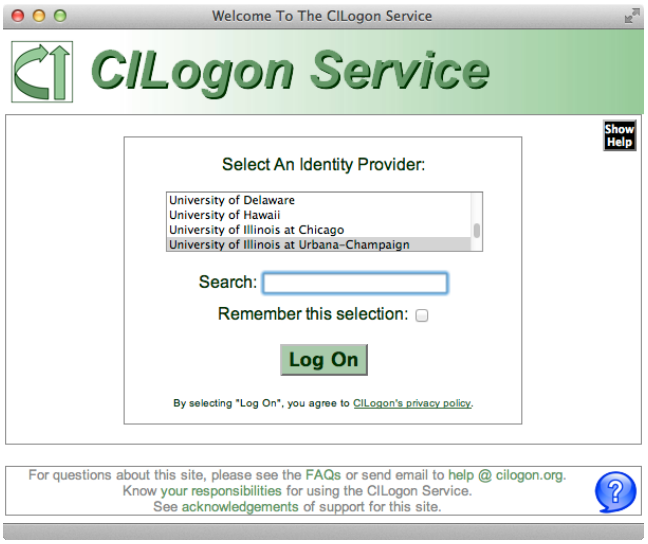

Figure 1. CILogon users choose from 88 identity providers.

Figure 1 shows the front page for the CILogon service, which has been operational since 2010. In this article we introduce the technical design of the service and describe experiences and lessons learned from the first three years of operation.

2. RELATED WORK

CILogon builds on prior work to enable federated login to TeraGrid (the precursor to XSEDE) [5]. This prior work provided a federated certification authority (CA) for TeraGrid users via an account linking process that bound a user's federated identity with the user's existing TeraGrid account, thereby leveraging the existing TeraGrid account allocations process for user identification. The federated CA obtained accreditation from the International Grid Trust Federation (IGTF) as a Short Lived Credential Service (SLCS) provider, enabling the issuance of internationally recognized X.509 certificates with validity periods up to twelve days. The CA offered a Java Web Start interface for installing certificates on the user's desktop using software developed by the GridShib project [8]. CILogon advances this prior work in many ways including: 1) eliminating all TeraGrid (XSEDE) dependencies to serve a wider user community (beyond TeraGrid/XSEDE), 2) offering additional user interfaces beyond

XSEDE '13, July 22 - 25 2013, San Diego, CA, USA

ACM 978-1-4503-2170-9/13/07…$15.00.

Java Web Start, and 3) supporting multiple levels of assurance with certificate lifetimes up to 13 months.

The TERENA Certificate Service (TCS) is an IGTF accredited federated X.509 CA serving Europe. The TCS web portal, built using the open source Confusa software, enables National Research and Education Networks (NRENs) in Europe to connect their SAML federations to the CA service. While both CILogon and TCS operate IGTF accredited federated CAs, they differ in their service areas (CILogon in the United States, TCS in Europe), their software stacks (CILogon using MyProxy and GridShib, TCS using Confusa), and in their support models (TCS as a subscription service for TERENA members, CILogon as grant-funded cyberinfrastructure).

3. USE CASES

The CILogon project has been working in collaboration with multiple cyberinfrastructure providers to enable functionality customized to the needs of specific user communities. In this section we describe these use cases and requirements.

3.1 XSEDE

To ensure a smooth transition, the Extreme Science and Engineering Discovery Environment (XSEDE) has maintained core security policies and mechanisms from the precursor TeraGrid project. The requirement for International Grid Trust Federation (IGTF) accreditation for all certification authorities (CAs) is of primary importance to CILogon. As CILogon is designed to avoid dependencies on the XSEDE allocations process for user identification, it is necessary for CILogon to find a strong user identification process that meets IGTF requirements while scaling to a national user community. As described in more detail below, CILogon has obtained IGTF accreditation of the CILogon Silver CA, which relies on the InCommon assurance program for SAML assertions that provide user identification consistent with IGTF requirements. XSEDE is now accepting certificates from the CILogon Silver CA, but use is limited because only the Virginia Tech identity provider has been accredited under the InCommon assurance program so far.

3.2 Open Science Grid

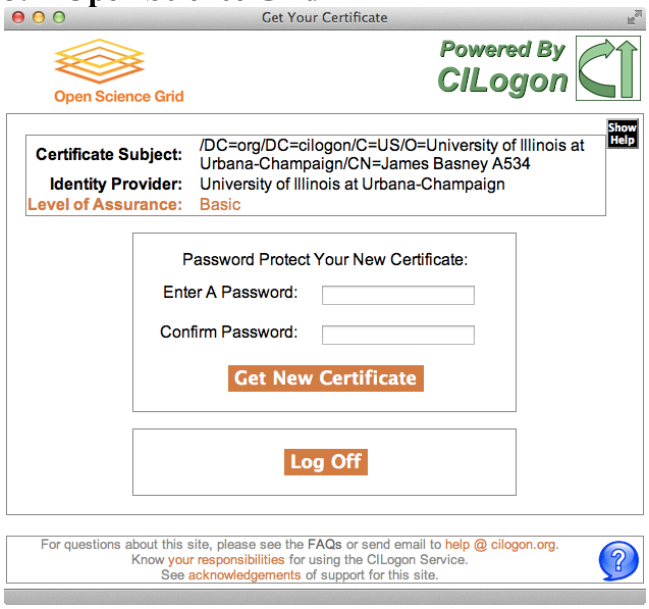

Figure 2. CILogon provides a custom interface for OSG users.

As with XSEDE, IGTF accreditation is very important for Open Science Grid (OSG), particularly for OSG's participation in the Worldwide Large Hadron Collider Computing Grid. OSG participants at Virginia Tech have successfully obtained certificates from the CILogon Silver CA and used them for access to OSG resources. Use of the CILogon Silver CA by OSG users from other organizations depends on their identity providers obtaining the requisite InCommon assurance certification.

OSG has also determined that lower level of assurance (i.e., non-IGTF) certificates are acceptable in some circumstances, such as when logging in to wikis. This allows OSG users from campuses that are not yet certified under the InCommon assurance program to obtain CILogon certificates for access to these OSG applications.

As seen in Figure 2, CILogon provides a custom interface for OSG users. This interface offers an approved-by-OSG set of identity providers and issues certificates using the SHA-1 hash algorithm (rather than the default of SHA-256) for compatibility with OSG's current software stack.

3.3 LIGO

The Laser Interferometer Gravitational Wave Observatory (LIGO) has added support for obtaining certificates from CILogon on the command line using LIGO's SAML identity provider (IdP). LIGO's IdP supports the SAML Enhanced Client or Proxy (ECP) profile for authentication to CILogon on the command line. LIGO is one of only seven InCommon IdPs that currently support SAML ECP. Other InCommon IdPs currently support only the SAML Web Browser Single Sign-On Profile.

LIGO can provision access to LIGO services for LIGO users in advance of those users obtaining a CILogon certificate, because LIGO and CILogon agreed on a deterministic algorithm for translating LIGO SAML identities to CILogon certificate distinguished names. This agreement ensures that LIGO users see no delay in obtaining and using their CILogon certificates for LIGO computing.

The LIGO identity management infrastructure supports over 800 geographically distributed project members accessing online resources including data repositories, instruments, data analysis services, and general-purpose computing resources. LIGO use cases for identity federation include collaboration with the European Virgo project and use of Globus Online file transfer services [6].

3.4 DataONE

For users of the Data Observation Network for Earth (DataONE), CILogon populates a custom certificate extension with DataONE-specific user attributes that DataONE nodes use for authorization. When users arrive at CILogon's custom interface for DataONE, CILogon servers query DataONE LDAP servers for user attributes to include in the user's certificate. DataONE uses both OAuth (web browser) and SAML ECP (command-line) interfaces to CILogon.

3.5 LTERN

The identity provider (IdP) operated by the Long Term Ecological Research Network (LTERN) was the first example of an IdP operated by a research project, rather than a university or corporation, to connect with CILogon. (LIGO was the second such IdP to connect with CILogon.) For researchers from campuses that are not yet InCommon participants, it is convenient to use an existing research project login for federated access. For example, many existing LTERN users are expected to use

DataONE, so the LTERN identity provider allows those users to easily access DataONE resources with their existing credentials. The DataONE IdP also supports SAML ECP for command line (i.e., non-browser) access.

3.6 OOI

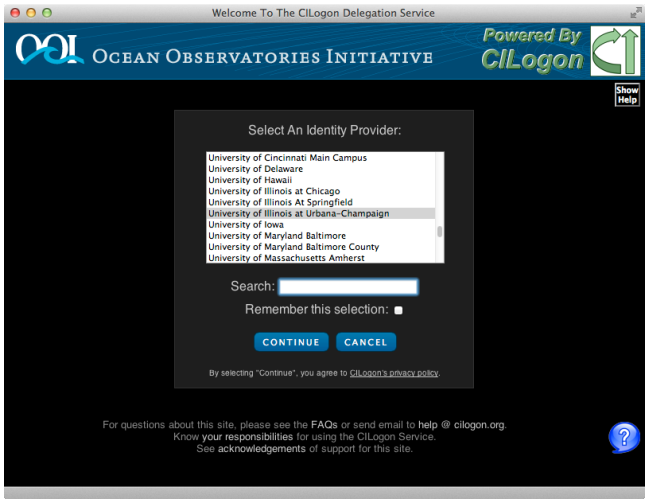

Figure 3. CILogon's OAuth interface enables OOI access.

The Ocean Observatories Initiative (OOI) motivated the development of CILogon's OAuth interface, which enables a user to delegate a certificate to the OOI web portal so it can act on the user's behalf. OOI uses a message-based infrastructure, and X.509 certificates enable message-based security via the XML Encryption and XML Signature standards. OOI was also an early adopter of CILogon's custom interface skinning, providing web page design consistency across the OOI and CILogon sites during user authentication, as seen in Figure 3.

3.7 Globus Online

Globus Online enables high performance, reliable file transfer via GridFTP and integrates with CILogon via OAuth for federated access. To facilitate automated account mapping using campus credentials, Globus Online provides a GridFTP authorization callout that consults a certificate extension containing the eduPersonPrincipalName (ePPN) attribute. CILogon inserts the ePPN value it receives from campus identity providers into the certificates it issues to support this Globus Online use case. This capability is currently used by researchers for access to University of Chicago data services.

3.8 CVRG

The CardioVascular Research Grid (CVRG) integrates with CILogon via OAuth for federated authentication to the CVRG portal and for use of Globus Online data transfer services by CVRG users. To enable this integration, CVRG developed a CILogon module for the Liferay portal framework.

4. TECHNICAL DESIGN

The CILogon technical design has evolved over time to satisfy the use cases described in the previous section.

4.1 System Architecture

The CILogon system consists of a web front-end, a user database, and a certification authority (CA) back-end. The web front-end implements SAML and OpenID user authentication, user interfaces for certificate issuance, and the OAuth interface for integrating with external web applications. The web front-end uses the user database to manage user sessions and user identities. The CA back-end issues X.509 certificates and certificate revocation lists, using CA keys stored in cryptographic hardware security modules.

4.2 Certificate Retrieval Interfaces

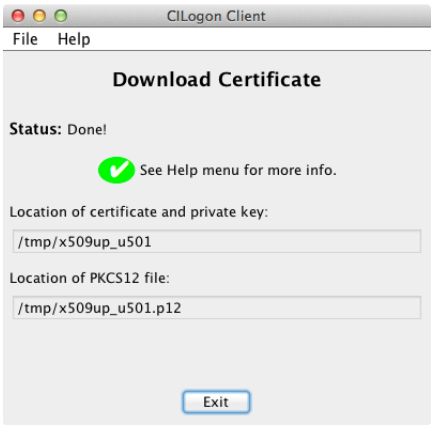

Figure 4. CILogon supports the GridShib Java client.

As we began to work with multiple cyberinfrastructure providers on use of CILogon, it became clear to us that the GridShib Java Web Start interface (shown in Figure 4) would not meet all the use cases that CILogon needed to support, e.g., closer integration with desktop and web applications. We also found that using Java on the desktop caused user support issues, including difficulty maintaining Java installations, ongoing Java virtual machine (JVM) compatibility challenges, slow JVM startup, and slow cryptographic performance. This led to the development of PKCS12, ECP, and OAuth interfaces in addition to the existing Java interface.

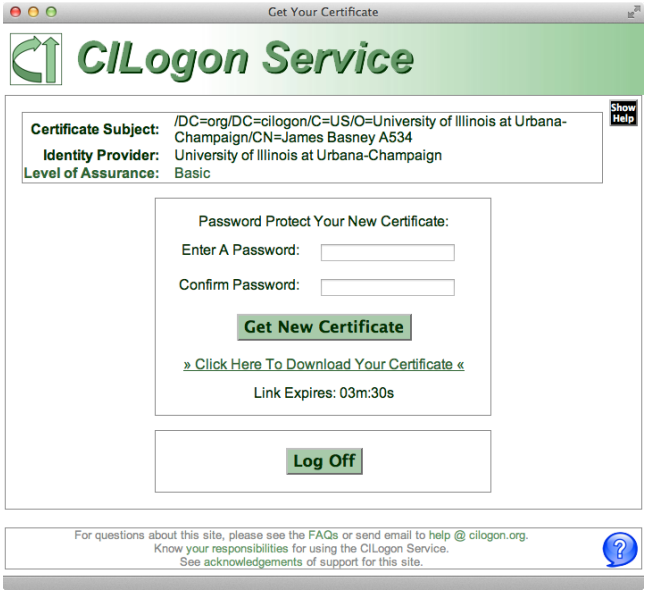

Figure 5. CILogon offers a direct PKCS12 download link.

The CILogon PKCS12 interface (shown in Figure 5) enables users to download (over HTTPS) a standard PKCS12 file containing their credentials, after logging in via SAML or OpenID using their web browser. The PKCS12 file format is understood natively by most X.509 implementations, including web browsers, OpenSSL, Java, and Globus. This interface generates the user's credentials on the server and then makes the credential file available for

download via a short-lived randomized HTTPS link. Traditionally IGTF has required client-side generation of user keys, which requires the use of client-side cryptographic software in the web browser or another application the user must install. Through discussion with IGTF we were able to obtain approval of server-side key generation for this PKCS12 interface. The use of a randomized HTTPS download link for the PKCS12 file allows users to download the file to their desktop or to a remote terminal session (by copying and pasting the URL) using standard HTTPS clients, without the need for custom client-side software installations.

The CILogon ECP interface enables users to authenticate to CILogon and download a certificate completely outside the web browser, using the SAML Enhanced Client or Proxy (ECP) profile. Currently seven InCommon identity providers support SAML ECP, including LIGO, LTERN, and ProtectNetwork. CILogon publishes a machine-readable list of ECP-enabled identity providers (IdPs), so CILogon ECP clients can download the current list and offer an up-to-date choice of IdPs for users.

The CILogon OAuth [2] interface enables users to delegate a certificate to web applications (such as science gateways) to act on their behalf. CILogon implements the same OAuth interface as the TeraGrid OAuth service [4] and OAuth for MyProxy [7]. Currently Globus Online, CVRG, DataONE, and OOI are using the CILogon OAuth interface.

4.3 Distinguished Names

Relying on federated authentication to identify certificate requesters means that CILogon must map SAML and OpenID user attributes to X.509 certificate contents. The distinguished names (DNs) in CILogon certificates must be persistent and globally unique to reliably identify the same person over time, so the DNs can be used in access control policies. CILogon DNs take the following form:

/DC=org/DC=cilogon/C=US/O=*IdP*/CN=*EndEntityName UID*

The "/DC=org/DC=cilogon/C=US" prefix ensures global uniqueness, due to CILogon's ownership of the cilogon.org domain name. CILogon has also registered this prefix with IGTF. The "/C=US" component indicates that CILogon primarily serves the United States, consistent with the IGTF "CA per country" model, but it is not intended to indicate the citizenship or nationality of a particular CILogon user. Unfortunately, the use of "/C=US" has been a source of confusion for CILogon users, but it is difficult to remove it from the established CILogon namespace prefix now.

Including the IdP name in the DN indicates the source of the identity, which can be helpful in cases where relying parties trust some IdPs more than others. For example, OSG is using the "/O=*IdP*" component of the DN to accept identities from a limited set of IdPs for some applications.

The common name (CN) component uniquely identifies the individual and is the most troublesome part of the DN. IGTF requires that the CN contains "an appropriate presentation of the actual name of the end-entity", i.e., the person's legal name. This gives the unfortunate property that if the person chooses to change their name, their certificate's CN must change, and any authorizations based on the previous DN must be updated.

Since legal names are not unique (example: "John Smith"), CILogon must add an additional disambiguator (UID) to the CN. SAML and OpenID unique identifiers are not good choices for inclusion in the CN because they can contain long hash values that are unwieldy to work with directly (and prompted users of CILogon to complain).[1] CILogon now constructs the UID in the CN in one of two ways. On request from SAML IdP operators that provide unique eduPersonPrincipalName values which take the form username@domainname, CILogon will use these values for the UID. This option has the benefit that the IdP (in particular, the LIGO IdP) can easily map back from the CILogon DN to the user's IdP identity. For other IdPs, CILogon generates a short unique serial number for each user and records it in the CILogon user database. To support multiple CILogon server instances, the serial number is prefixed with a server instance label, so "D534" is serial number 534 generated by server instance "D". Once generated, the UID is synchronized across all CILogon server instances via the CILogon user database so users receive consistent DNs, such as:

/DC=org/DC=cilogon/C=US/O=University of Illinois at Urbana-Champaign/CN=James Basney A534

4.4 Levels of Assurance

CILogon currently operates three Certification Authorities (CAs) to support multiple levels of assurance (LOA), as summarized in Table 1. The CAs differ in their procedures for subscriber authentication, identity validation, and naming but otherwise have consistent operational and technical security controls. Separating different identity vetting procedures across multiple CAs enables relying parties to accept certificates from a subset of the CILogon CAs according to their LOA requirements.

Table 1. CILogon CAs offer multiple levels of assurance.

CA	Registration Authorities	User Identities	Accreditation
Silver	InCommon Silver IdPs (ICAM LOA 2)	LOA 2 vetting	IGTF MICS CA
Basic	InCommon IdPs	Varies	None
OpenID	OpenID Providers (ICAM LOA 1)	Self-asserted	None

The top priority for the CILogon project is enabling secure access to cyberinfrastructure using campus credentials via the InCommon Federation. The nation's colleges and universities are natural identity providers for academic researchers, because of the strong relationships that researchers have with their campuses in their roles as faculty, staff, and students. Through the InCommon Identity Assurance program, many researchers will be able to obtain a standards-compliant credential from their university that is recognized at LOA "Level 2" according to the US Government ICAM Trust Framework [3]. With this LOA 2 credential, researchers will be able to obtain a CILogon Silver certificate approved by the International Grid Trust Federation (IGTF) for use worldwide. Currently, Virginia Tech is the only InCommon IdP to achieve InCommon Assurance accreditation, but users at other campuses may obtain a lower LOA CILogon Basic certificate using their campus credentials.

[1] The following SAML eduPersonTargetedID from University of Illinois and OpenID from Google illustrate the complexity of using these ID strings directly in certificate DNs:
urn:mace:incommon:uiuc.edu!https://cilogon.org/shibboleth!cyXC3O5fi0t1NBsW1NsOxZDyDd4=
https://www.google.com/accounts/o8/id?id=AItOawkMwlXe9BuV6E5grv-8DX8r7OftrrkjaXk

In some cases researchers will not be able to use their campus credentials with CILogon. For example, their campus may not yet be an InCommon member, or the researcher may not have an affiliation with a US university. In this case researchers may be able to access CILogon using an InCommon IdP operated by their research collaboration (such as LIGO or LTERN) or they could sign up for a free account from the commercial ProtectNetwork IdP. Researchers in other countries may be able to obtain certificates via their national federation using services similar to CILogon, such as the TERENA Certificate Service in Europe.

Another option is to use OpenID with CILogon. Using accounts with Google, PayPal, or VeriSign, researchers can authenticate to CILogon via OpenID to obtain a CILogon OpenID certificate. While this type of certificate has a lower level of assurance, it is not without value. The Open Identity Exchange (OIX) is an approved LOA 1 provider under the ICAM Trust Framework, and OIX has in turn certified these OpenID providers (Google, PayPal, and VeriSign) at LOA 1. While LOA 1 provides no identity verification (unlike LOA 2 and above), it provides a basic strength of authentication for knowing that the person authenticating today is the same person who authenticated with the same identity yesterday. In many cases, this LOA is sufficient for access to research services (as determined by the service provider). To maintain a consistent LOA for CILogon OpenID certificates, the CILogon project accepts OpenID authentication only from those providers that are certified at LOA 1 or above.

4.5 Multi-factor Authentication

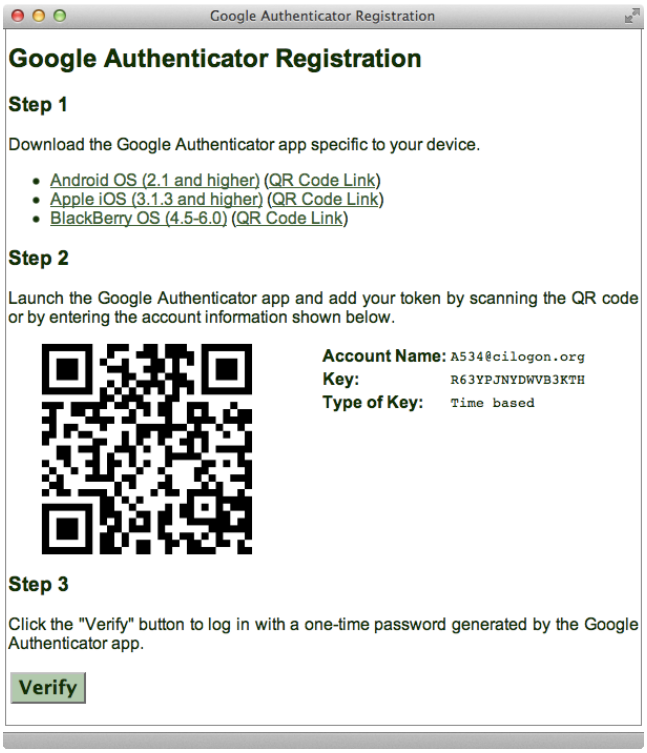

Figure 6. Users can register a second authentication factor.

CILogon supports adding a second authentication factor for greater assurance when issuing certificates. The current second factor method supported by CILogon is 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). However, CILogon's second factor support is designed to accommodate multiple methods, and CILogon can support additional methods (such as Duo Security) in the future to meet community requirements.

After users enable a second authentication factor via the registration interface shown in Figure 6, CILogon prompts for the second factor after users authenticate with their chosen identity provider, on all subsequent visits to CILogon, as shown in Figure 7. Users can disable their second factor at any time after logging in. In the future, CILogon will indicate in the issued certificate whether two-factor authentication was performed, so services accepting the certificate for authentication can better determine the level of assurance used to obtain the certificate.

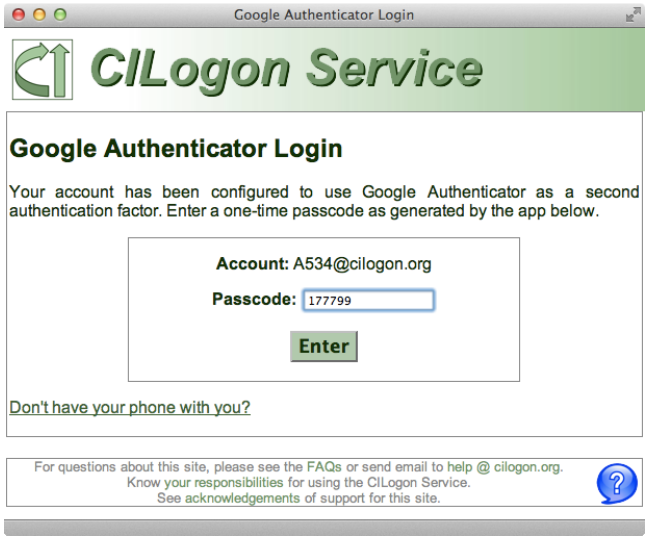

Figure 7. CILogon prompts for a second authentication factor.

Some identity providers already support two-factor authentication to CILogon, including Virginia Tech's Silver-level Personal Digital Certificate (PDC) and Google's 2-step verification. For identity providers that don't support two-factor authentication, CILogon's ability to add a second authentication factor can provide a useful step-up level of assurance for certificate issuance.

4.6 Requiring Re-Authentication

As discussed previously, CILogon relies on external identity providers for authentication of users. These identity providers (IdPs) implement web single sign-on (SSO), either via SAML (for InCommon IdPs) or OpenID (for Google, PayPal, and Verisign). If a user has recently logged on to a web site via an identity provider, SSO means that using the same identity provider to log on to CILogon won't require the user to authenticate again (i.e., won't require the user to type username and password again). The identity provider implements SSO by setting a cookie in the user's web browser to remember the user's identity. SSO avoids the inconvenience of typing passwords many times throughout the day and potentially reduces the risk of typing a password by mistake on an attacker's phishing web site. However, SSO requires users to maintain control over their web browsers, so someone else doesn't use their cookies to access web sites using their identity. Different identity providers set different lifetimes on SSO cookies. Some may set cookies to be removed when users close their browser; others may require users to explicitly log out to delete their cookie. Logging out reliably across many web sites (called single sign-out or single log out) is a significant challenge.

Some applications want to bypass SSO and require a user to authenticate again, for greater confidence that the user's identity is

correct and not being used by someone sharing the user's web browser. In SAML 2.0, the *ForceAuthn* attribute of the *AuthnRequest* can ask the IdP to require re-authentication. In OpenID, including *openid.pape.max_auth_age=0* in the authentication request has the same effect. CILogon partners can require re-authentication for their applications via CILogon interface customization.

4.7 Identity Provider Selection Interface

In our prior work for TeraGrid [5] we identified the scalability of the identity provider (IdP) selection interface as an open challenge. It was common at the time to offer a drop-down list of IdPs for the user to choose from, which became unwieldy for large numbers of IdPs. We have since found that adding a text box supporting incremental search, together with remembering the user's prior selection in a cookie, works well for selecting among the 88 IdPs currently supported by CILogon. We initially provided separate lists of SAML and OpenID providers, but this only caused confusion. Merging both types of IdPs into a single list resulted in a simpler interface.

4.8 Attribute Release

Until recently, services like CILogon, that want to serve researchers from many InCommon member campuses, needed to negotiate individually with each InCommon campus to enable federated access to the service (i.e., to enable release of user identity attributes). This is "unfortunately a time-consuming manual process" [9]. To automate this process as much as possible, CILogon provides a web interface for InCommon identity provider (IdP) administrators to test that their IdP works with CILogon and to add their IdP to CILogon's list in a self-service manner, as shown in Figure 8.

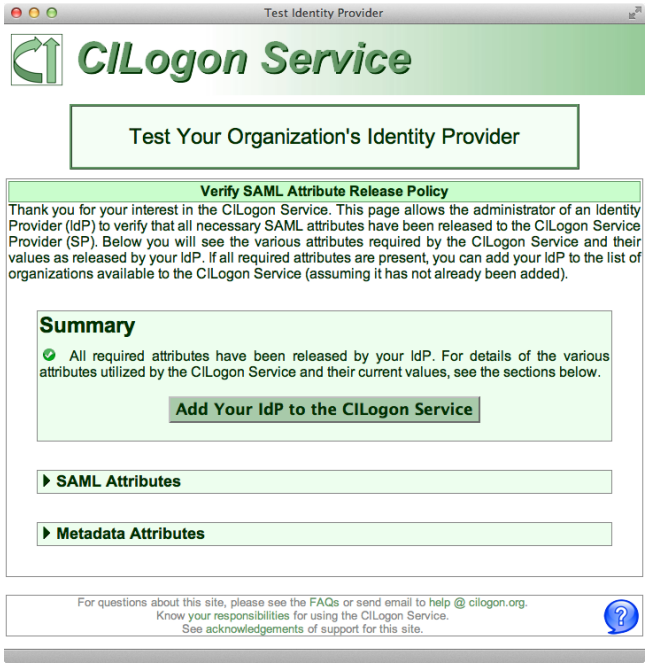

Figure 8. Administrators can add their IdP to CILogon.

Since December 2012, InCommon has provided a more scalable approach through the Research and Scholarship (R&S) program. CILogon staff helped to develop this program, and CILogon was the first service to apply for the program and was in the first group of approved R&S services. When services apply to InCommon for inclusion in the R&S program, InCommon reviews the application for technical and policy compliance, and then tags approved R&S services in SAML metadata. Participating InCommon campus identity providers allow access (i.e., release attributes) to the tagged services. For services like CILogon, this eliminates the need for bilateral negotiation with each campus identity provider.

Since CILogon launched in 2010, 69 InCommon IdP administrators added their IdPs via the CILogon web interface. Since the InCommon R&S program began tagging IdPs in December 2012, an additional 14 IdPs have been added automatically to CILogon through the R&S program. 34 IdPs that were already working with CILogon joined the R&S program for the benefit of service providers other than CILogon. Additionally, CILogon administrators added 2 InCommon IdPs manually prior to official service launch.

Continuing to grow the number of supported IdPs remains an important activity for CILogon, so that more users can access CILogon via their campus credentials. To gauge our progress, we periodically compare CILogon's list of supported IdPs against the campus affiliations of users of our partner projects. For example, the DataONE project identified 300 campuses that were home to anticipated DataONE users. Of those, 140 are currently InCommon members. Initially, only 17 of those campuses were federated with (i.e., releasing attributes to) CILogon. Over the past two years, that number has increased to 57. Overall, CILogon currently works with 85 out of 294 InCommon identity providers, plus 3 OpenID providers.

5. CONCLUSIONS

In its first three years of operation, the CILogon service has seen varied and growing use by cyberinfrastructure providers. To support this use, we have implemented a range of customizations to the CILogon service that were not originally envisioned at the start of the project. As additional identity providers support the InCommon Silver level of assurance, CILogon will achieve its potential as a national-scale certification authority with worldwide acceptance via the International Grid Trust Federation.

6. ACKNOWLEDGMENTS

The authors gratefully acknowledge contributions to the design and operation of the CILogon service from Randy Butler, Wendy Edwards, Neil Gorsuch, Von Welch, and Venkatesh Yekkirala.

This material is based upon work supported by the National Science Foundation under grant number 0943633 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.

7. REFERENCES

[1] Daan Broeder, Bob Jones, David Kelsey, Philip Kershaw, Stefan Lüders, Andrew Lyall, Tommi Nyrönen, Romain Wartel, and Heinz Weyer, "Federated Identity Management for Research Collaborations", April 2012. https://cdsweb.cern.ch/record/1442597

[2] E. Hammer-Lahav (ed.), "The OAuth 1.0 Protocol", IETF RFC 5849 (Informational), April 2010.

[3] Federal Identity, Credentialing, and Access Management: Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3, September 2009. http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

[4] Jim Basney and Jeff Gaynor, “An OAuth Service for Issuing Certificates to Science Gateways for TeraGrid Users,” TeraGrid Conference, July 18-21, 2011, Salt Lake City, UT. http://dx.doi.org/10.1145/2016741.2016776

[5] Jim Basney, Terry Fleury, and Von Welch, “Federated Login to TeraGrid,” 9th Symposium on Identity and Trust on the Internet (IDtrust 2010), Gaithersburg, MD, April 2010. http://dx.doi.org/10.1145/1750389.1750391

[6] Jim Basney, Scott Koranda, and Von Welch, “An Analysis of the Benefits and Risks to LIGO When Participating in Identity Federations,” LIGO document number LIGO-G1100964-v2, September 2011. https://dcc.ligo.org/public/0070/G1100964/002/LIGOIdentityFederationRiskAnalysis.pdf

[7] Jim Basney, Rion Dooley, Jeff Gaynor, Suresh Marru, and Marlon Pierce, “Distributed Web Security for Science Gateways,” Gateway Computing Environments Workshop (GCE11), November 17, 2011, Seattle, WA. http://dx.doi.org/10.1145/2110486.2110489

[8] Tom Barton, Jim Basney, Tim Freeman, Tom Scavo, Frank Siebenlist, Von Welch, Rachana Ananthakrishnan, Bill Baker, Monte Goode, and Kate Keahey, “Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, Gridshib, and MyProxy,” 5th Annual PKI R&D Workshop, April 2006. http://middleware.internet2.edu/pki06/proceedings

[9] William Barnett, Von Welch, Alan Walsh, and Craig Stewart, “A Roadmap for Using NSF Cyberinfrastructure with InCommon,” March 2011. http://hdl.handle.net/2022/13024