CILogon Project Overview

www.cilogon.org

This material is based upon work supported by the National Science Foundation under grant numbers 0850557 and 0943633. 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 National Science Foundation.

CILogon Personnel

- Principal Investigators

Jim Basney

Randy Butler

Von Welch

- Research Programmers

Venkat Yekkirala

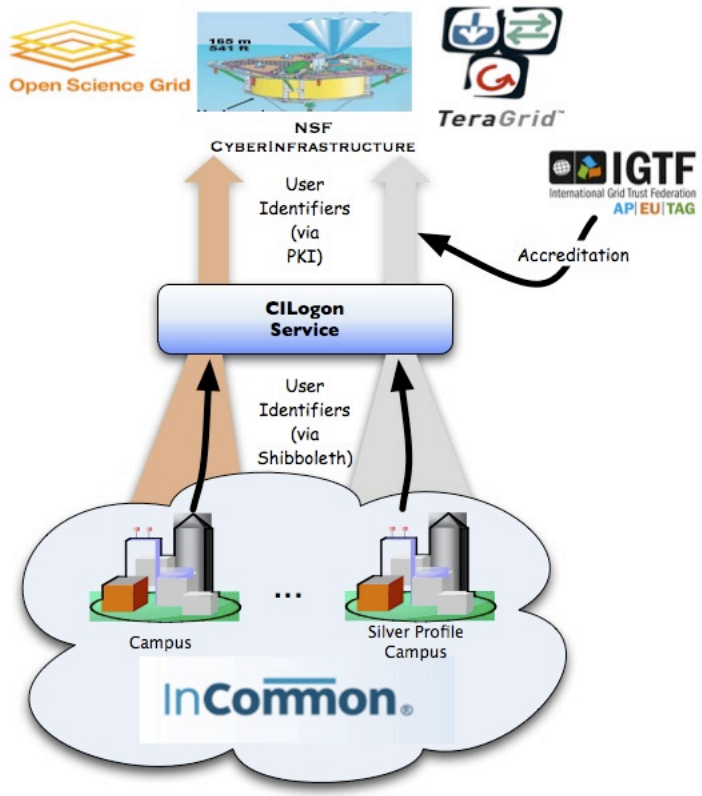
Additional staff to be hired

CILogon: Goals

- Foster secure, usable authentication for cyberinfrastructure (CI)
- Provide a new **service** that issues digital credentials to the NSF research community
- Provide community-driven **software** development and support:
  - MyProxy (http://myproxy.ncsa.uiuc.edu)
  - GridShib (http://gridshib.globus.org)
  - GSI-OpenSSH (http://grid.ncsa.uiuc.edu/ssh)

CILogon Service

- Facilitate campus login to NSF CI
  - Leverage researchers' existing identities at their home institution
  - Ease identity management for researchers and CI providers
- Bridge from:
  - Identity credentials issued by research institutions participating in the InCommon Federation using Shibboleth/SAML web browser single sign-on
- Bridge to:
  - X.509 PKI credentials that satisfy the requirements of NSF CI projects

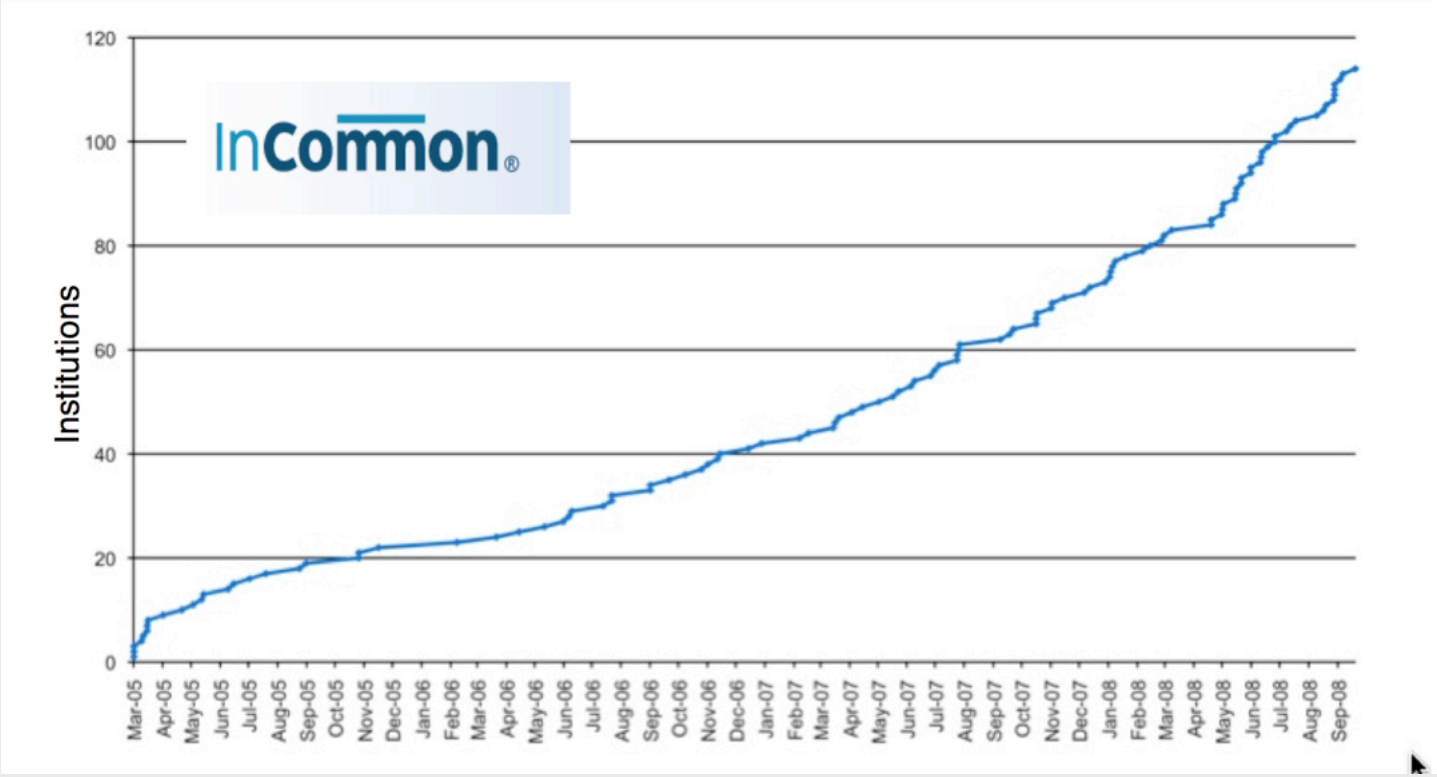


Federation

An organization of higher education and research institutions that defines standards and policies for exchange of user identity information

http://www.incommonfederation.org/

InCommon® Membership Growth



Number of institutions in InCommon, showing growth from 2005-2008. InCommon today federates over 160 universities and represents over 3.6 million users. (Image courtesy InCommon.)

Silver

- Identity management policies and procedures differ across InCommon members
- InCommon Silver Identity Assurance Profile defines common standards for identity vetting, system management and security, recordkeeping, revocation, audits, and name management
  - Pilot adoption underway by InCommon members
  - http://www.incommonfederation.org/assurance
  - Consistent with NIST SP 800-63 LOA 2

Silver

- InCommon Silver satisfies IGTF requirements
  - Critical for IGTF accreditation of CILogon Service
  - http://sl.cilogon.org/incommon-slcs-map.pdf
- We will operate two CAs:
  - Basic level and Silver/IGTF level

- International Grid Trust Federation (IGTF) consists of
  - The Americas Grid Policy Management Authority (TAGPMA)
  - European Policy Management Authority for Grid Authentication (EUGridPMA)
  - Asia Pacific Grid Policy Management Authority (APGridPMA)
- These groups set standards for and accredit CA operators according to relying party requirements
- CILogon service will be submitted for TAGPMA accreditation

Why PKI?

- CI applications:
  - Command-line clients
  - N-tier workflows
  - Unattended/batch jobs
  - Message-based protocols (SOAP, ESB)
- Non-HTTP protocols:
  - GRAM, GridFTP, SSH
- Significant community investment (GSI, IGTF)

CILogon Software: MyProxy

- Credential Management Service
  - Online CA issues certificates
  - Credential repository stores proxy certificates
- Supports many authentication methods: passphrase, certificate, Kerberos, Pubcookie, VOMS, PAM, LDAP, SASL, OTP
- Used by TeraGrid, EGEE, ESG, and others

http://myproxy.ncsa.uiuc.edu

CILogon Software: GridShib

- Provides interoperability between Shibboleth and grid security (GSI)
- **GridShib CA** issues certificates based on Shibboleth authentication
- **GridShib for Globus Toolkit** performs SAML-based authorization for GT web services
- **GridShib SAML Tools** bind SAML assertions to proxy certificates
- Used by TeraGrid and others

http://gridshib.globus.org

CILogon Software: GSI-OpenSSH

- Adds GSI to OpenSSH
- Single sign-on login and file transfer service
- C and Java clients
- Incorporates High Performance Networking (HPN) patches from PSC

  http://www.psc.edu/networking/projects/hpn-ssh/
- Used by TeraGrid, LIGO, UK NGS, and others

  http://grid.ncsa.uiuc.edu/ssh

Demo

https://go.teragrid.org

CILogon Software Tasks

- Integration of dev.globus metrics
- GridShib CA OpenID support
- GridShib C support
- GridShib SAML2 support
- Credential renewal service
- MyProxy browser interface
- Improved MyProxy HSM support
- MyProxy peer-to-peer replication

Subject to change based on your input today!

Integration of dev.globus Metrics

- Standard metrics gathering capability used across Globus Toolkit components
- Add to MyProxy, GridShib, and GSI-OpenSSH
- Goals
  - Allow CI projects to gather usage statistics
  - Allow us to report usage information to NSF
- Usage statistics for logon services help CI projects report the number of unique users

GridShib CA OpenID Support

- OpenID (http://openid.net) is a protocol for web-based authentication and access control
  - Adopted by many commercial service providers
  - Earth System Grid has also adopted OpenID
- Goal: Extend GridShib CA front-end to support OpenID in addition to Shibboleth
  - Plug-in interface for other authentication methods

GridShib C Support

- GridShib for GT is currently Java-only
  - Based on Globus Java WS Core
- Goal: Provide SAML-based authorization for C services
  - GSI-OpenSSH, GridFTP, and GRAM5
- Requested by LIGO

GridShib SAML2 Support

- GridShib CA already supports SAML2
- Need SAML2 support in GridShib SAML Tools and GridShib for Globus Toolkit
  - For producing and consuming SAML2 assertions in proxy certificates
- Pursue interoperability with VOMS SAML2 profile

Credential Renewal Service

- Short-lived credentials mitigate the risk of theft and misuse
- Need credentials for long-lived workflows
- Credential renewal solutions using MyProxy today:
  - EGEE gLite Renewal Service
  - Condor-G
- Goal: Develop a general-purpose renewal service for Globus Toolkit

MyProxy Browser Interface

- MyProxy clients and GridShib CA support retrieving credentials to the desktop and into web portal sessions
- Web applications such as VOMS-Admin require credentials in the browser
  - Difficult to import credentials into the browser
- Goal: Provide an interface for retrieving credentials from MyProxy and GridShib CA directly into the browser
- Requested by LIGO

Improved MyProxy HSM Support

- MyProxy CA supports private key storage in Hardware Security Modules
  - Required for IGTF accreditation
  - Tested with Alladin and SafeNet HSMs
  - http://myproxy.ncsa.uiuc.edu/ca/engine/
- Goal: Improve quality of HSM support
  - Automated regression tests for multiple devices
  - Improved documentation for different devices
  - Updates for netHSMs and other new devices

MyProxy P2P Replication

- MyProxy CA replication is straightforward
- MyProxy repository currently supports a primary-backup passive replication scheme
  - Provides limited service when primary is down
  - Difficult to load-balance multiple servers
- Goal: Peer-to-peer repository replication for load-balancing with automated fail-over

  http://myproxy.ncsa.uiuc.edu/failover.html

Summary

- We have big plans!
- We need your input!
  - What can we do that would be most helpful to you?
  - What are your top identity management challenges?
  - How should we prioritize our task list?
  - Are there other tasks we should add?
    - If so, which tasks can we drop?
- How can we collaborate most effectively?
  - Testbeds, pilot projects, future meetings, etc.