



CILogon Certificate Authority

Jim Basney

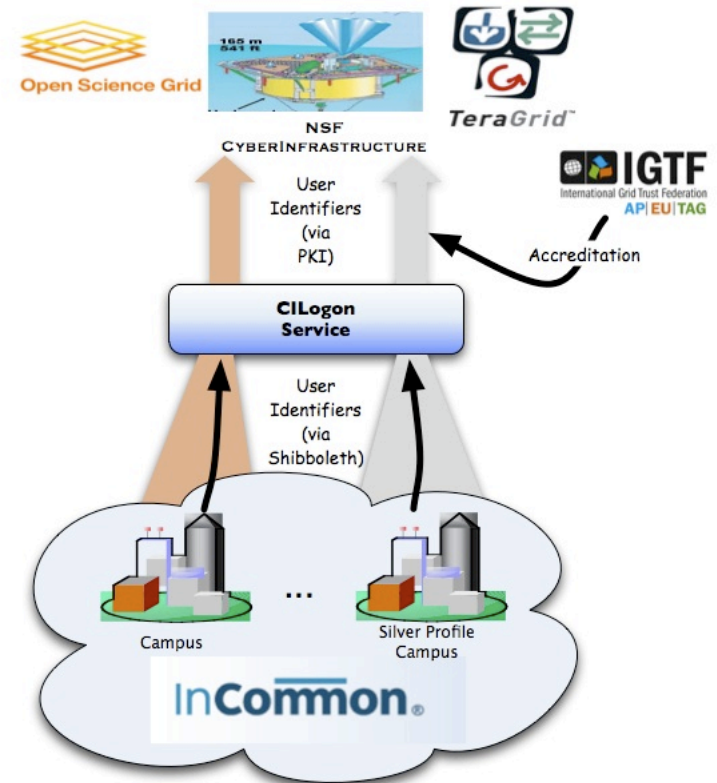
jbasney@ncsa.uiuc.edu



National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign

CILogon Certificate Authority

- 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



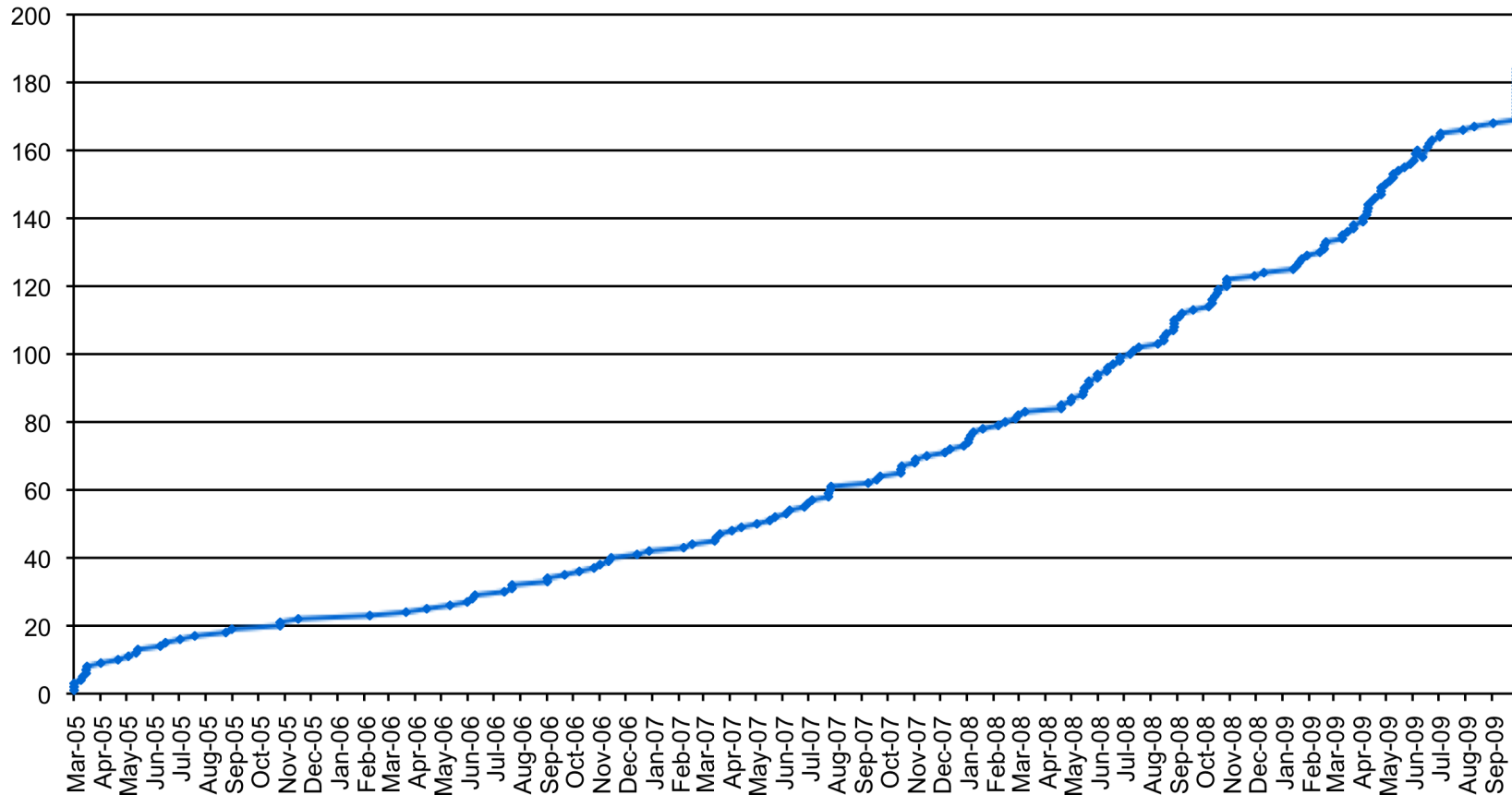
This material is based upon work supported by the National Science Foundation under grant numbers 0850557 and 0943633. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

InCommon 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 Federation Membership Growth



Number of institutions in InCommon, showing growth from 2005-2009. InCommon today federates over 160 universities and represents over 3.6 million users. (Image courtesy InCommon.)

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
 - Scheduled for production in Fall 2010
 - <http://www.incommonfederation.org/assurance>
 - Consistent with NIST SP 800-63 LOA 2

InCommon 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

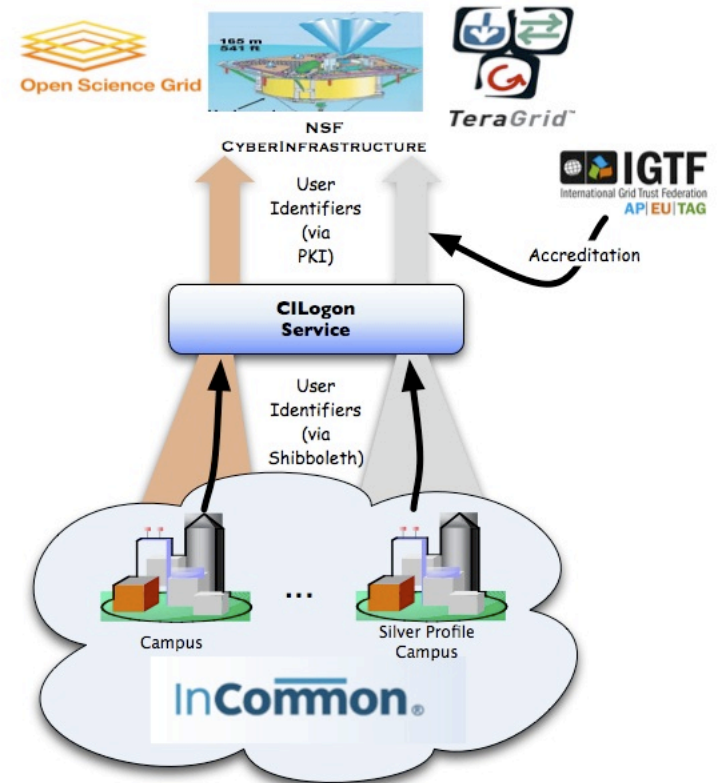


- International Grid Trust Federation (IGTF) consists of
 - The Americas Grid Policy Management Authority (TAGPMA)
 - European Policy Management Authority for Grid Authentication (EUGridPMA)
 - Asia Pacific Grid Policy Management Authority (APGridPMA)
- These groups set standards for and accredit CA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

NCSA GridShib CA (https://go.teragrid.org/)	CILogon CA (IGTF/Silver instance)
Identity Vetting: TeraGrid Allocations Process	Identity Vetting: InCommon Member Institutions
IdP Vetting: Individual agreements between NCSA and IdPs	IdP Vetting: InCommon Silver accreditation process, including audits
Certificate Subject Common Name: Full Name from NCSA User Database Plus serial number to uniquify	Certificate Subject Common Name: Full Name from SAML attributes Plus ePTID (?) to uniquify
User Community: O(10k) NCSA users from O(500) institutions	User Community: O(10k)+ NSF CI users from O(2k) institutions
Software: MyProxy, GridShib CA, Shibboleth	Software: MyProxy, GridShib CA, Shibboleth
Location: NCSA machine room	Location: NCSA machine room plus offsite instance for load balancing / fail-over
HSMs: SafeNet Luna PCI	HSMs: netHSM (vendor TBD)

Project Timeline

- September 2009: Project Start
- April 2010 (Planned):
 - Prototype Service Deployed
 - TAGPMA accreditation
- September 2010 (Planned):
Operational Service Deployed
- Next Steps
 - Submit CP/CPS to TAGPMA
 - Deploy prototype service



Working with SURAGrid

- What can we do to make the CILogon CA useful to SURAGrid?
 - Very interested in SURAGrid requirements and recommendations
- Can we work together to promote InCommon adoption?
 - Including adoption of InCommon Silver
- We'll be looking for beta testers next year
 - Can SURAGrid help us find users and success stories?
- What are the best forums for continued discussions?