A Federated X.509 Certification Authority for CyberInfrastructure Logon

Jim Basney, Terry Fleury, Jeff Gaynor
{jbasney,tfleury,gaynor}@illinois.edu

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.
CILogon – https://cilogon.org/

- Provides personal digital certificates for access to cyberinfrastructure
- Uses federated authentication for user identification
Federated Authentication

• Log on to CILogon using your campus (InCommon) or Google (OpenID) account

[Diagram of a login screen with fields for NetID and password, followed by a 2-step verification process.]
Bridging InCommon and IGTF

• Translating mechanism and policy across higher education and grid trust federations
Multiple Levels of Assurance

- CILogon Silver CA is accredited by IGTF
  - IGTF profile for CILogon Basic and CILogon OpenID CAs under development
- Using InCommon Silver (Level 2) identities
- Google Authenticator support for second authentication factor
Integrated with CyberInfrastructure
Integrated with Globus Online
Add Your Identity Provider

• If your campus identity provider isn’t yet working with CILogon, please let us know!

InCommon Research and Scholarship program helps services connect with identity providers.
Conclusions

• CILogon issues personal digital certificates using federated authentication
  – Bridging InCommon and IGTF
  – Supporting multiple levels of assurance
  – Integrated with cyberinfrastructure

• InCommon supports cyberinfrastructure providers through the R&S program

• Let’s collaborate on the use of federated identities with cyberinfrastructure!
Thanks!

info@cilogon.org
jbasney@illinois.edu

www.cilogon.org/faq

Please visit our poster!