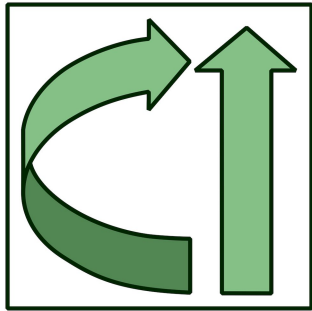


# CILogon 2.0



Jim Basney  
jbasney@ncsa.illinois.edu




This material is based upon work supported by the National Science Foundation under grant numbers 0850557, 0943633, 1053575, 1440609, and 1547268 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/>

- Enables use of federated identities for access to cyberinfrastructure
- Translates across federations and protocols

Welcome To The CILogon Service

 **CILogon Service**

Select An Identity Provider:

University of Hawaii  
University of Illinois at Chicago  
University of Illinois At Springfield  
University of Illinois at Urbana-Champaign

Search:


Remember this selection:

**Log On**

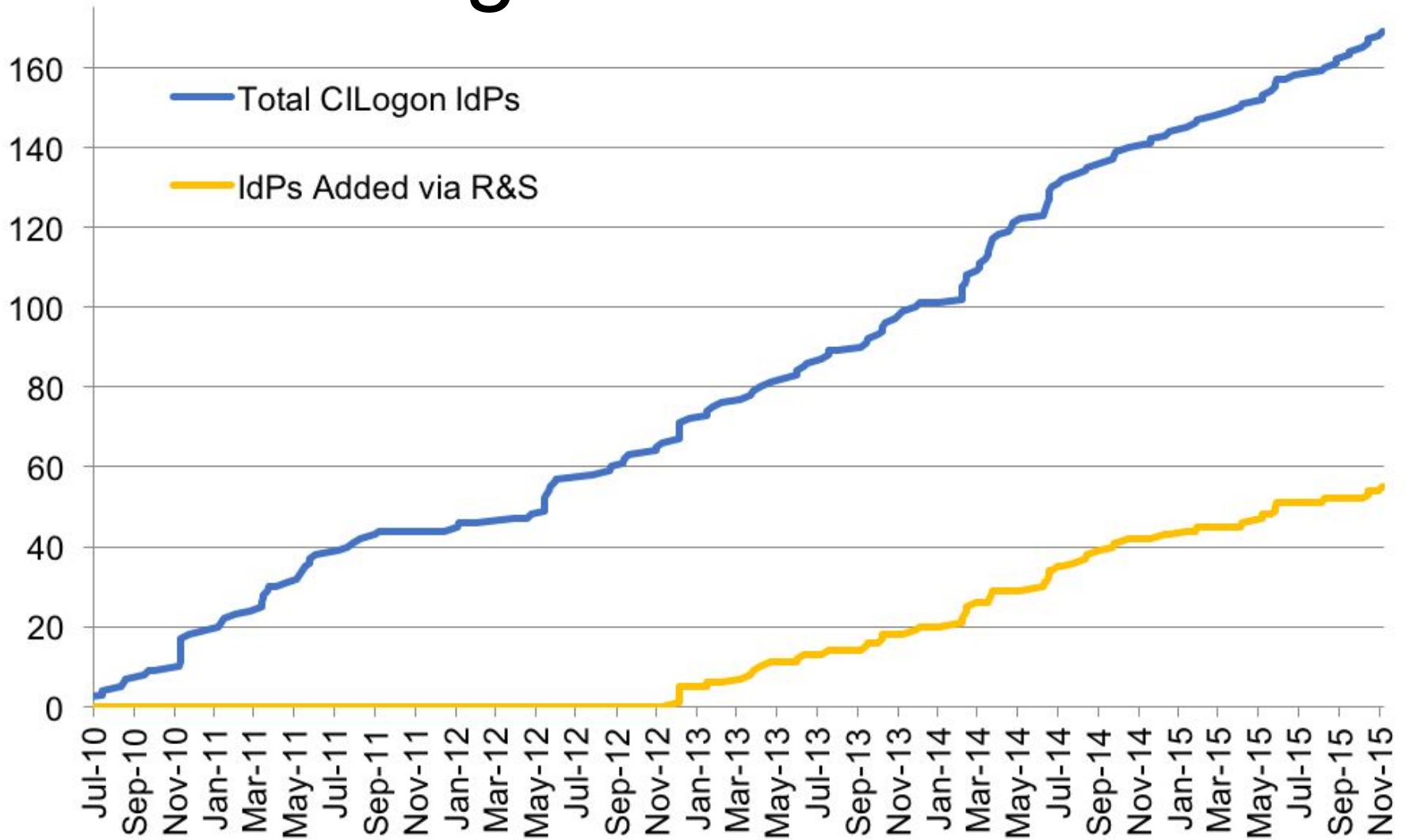
By selecting "Log On", you agree to [CILogon's privacy policy](#).

For questions about this site, please see the [FAQs](#) or send email to [help@cilogon.org](mailto:help@cilogon.org).  
Know your responsibilities for using the CILogon Service.  
See [acknowledgements](#) of support for this site.

Show Help

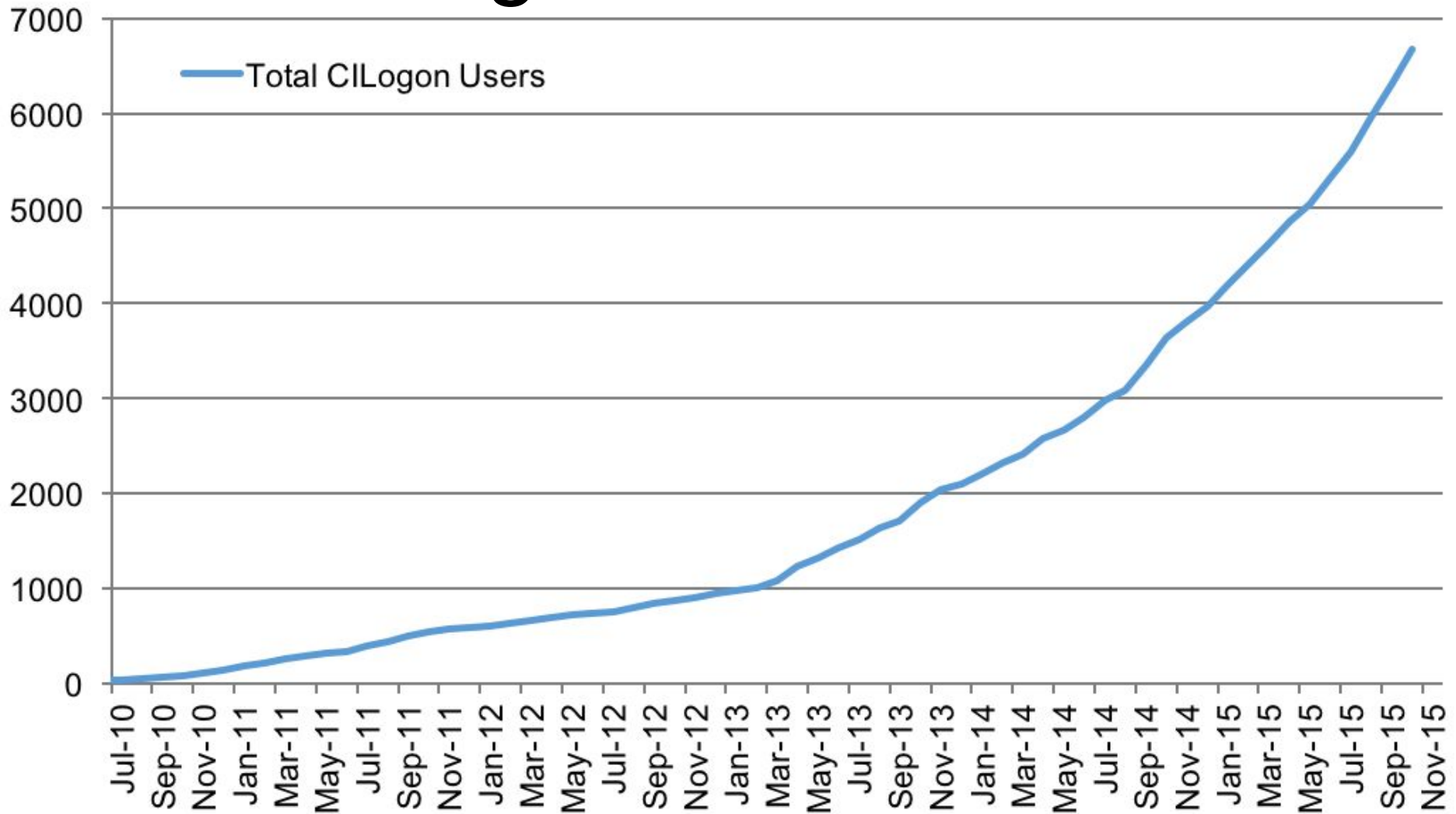


# CILogon IdP Growth



<https://groups.google.com/a/cilogon.org/forum/#!forum/idp-updates>

# CILogon User Growth



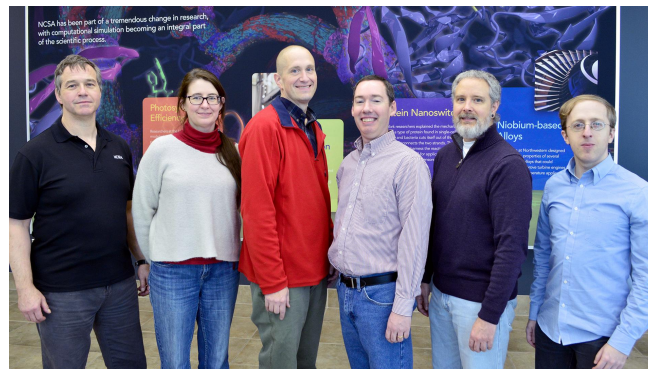
# CILogon 2.0 Project

- ❑ 3 year NSF CICI award
  - ❑ January 2016 - December 2018
- ❑ Provide an integrated open source Identity and Access Management (IdAM) platform for cyberinfrastructure
  - ❑ CILogon: federated identity management
  - ❑ COmanage: collaborative organization management
- ❑ Support *international* collaborations

# CILogon 2.0 Team Members



- ❑ Jim Basney
- ❑ Terry Fleury
- ❑ Jeff Gaynor
- ❑ Venkat Yekkirala
- ❑ Heather Flanagan
- ❑ Scott Koranda
- ❑ Benn Oshrin
- ❑ Arlen Johnson



# Science Partners

- ❑ NANOGrav Physics Frontiers Center
- ❑ Laser Interferometer Gravitational-Wave Observatory (LIGO)
- ❑ Data Observation Network for Earth (DataONE)



# Cyberinfrastructure Partners

XSEDE

Extreme Science and Engineering  
Discovery Environment



- ❑ Operational support
- ❑ Integration platform
- ❑ International use cases
- ❑ Support for European identities
- ❑ Using eduGAIN



# Project Deliverables

- ❑ CILogon-COmanage Integration
- ❑ VO collaboration management
- ❑ International Interfederation (eduGAIN)
- ❑ Linking ORCID identities
- ❑ Supporting Campus Cyberinfrastructure (LDAP and SSH Key Management)
- ❑ Multi-factor Authentication and Levels of Assurance
- ❑ Web Single Sign-On Gateway (IdPoLR, SAML AA, SAML-OIDC)

# CILogon-COmanage Integration

- ❑ Combine identity bridging (CILogon) with collaboration management (COmanage)
- ❑ Support configurable enrollment flows, roles, groups, identifiers, and expiration
- ❑ Issuing assertions and certificates containing VO-specific attributes

# International Interfederation

- ❑ Exploring two options:
  - ❑ International IdPs with US CILogon instance
  - ❑ EU CILogon instance linked with GÉANT's Trusted Certificate Service (TCS)
- ❑ Relying on eduGAIN and REFEDS R&S
- ❑ Pilot project with AARC underway

# Supporting Campus CI

- ❑ LDAP interface for campus applications that support LDAP but not SAML or OIDC
  - ❑ Linked X.509, SAML, OIDC, and ORCID IDs
  - ❑ Application-specific passwords
  - ❑ VO-specific user profile and attribute info
- ❑ SSH key management
  - ❑ SSH public keys linked with federated IDs
  - ❑ LDAP lookup for campus compute clusters

# MFA and LOA

- ❑ Use Multi-Factor Authentication (MFA) and signal its use in our assertions
  - ❑ OIDC Authentication Context Class Reference
  - ❑ X.509 certificate extension (policy OID)
- ❑ Pass along other Level of Assurance (LOA) information provided externally

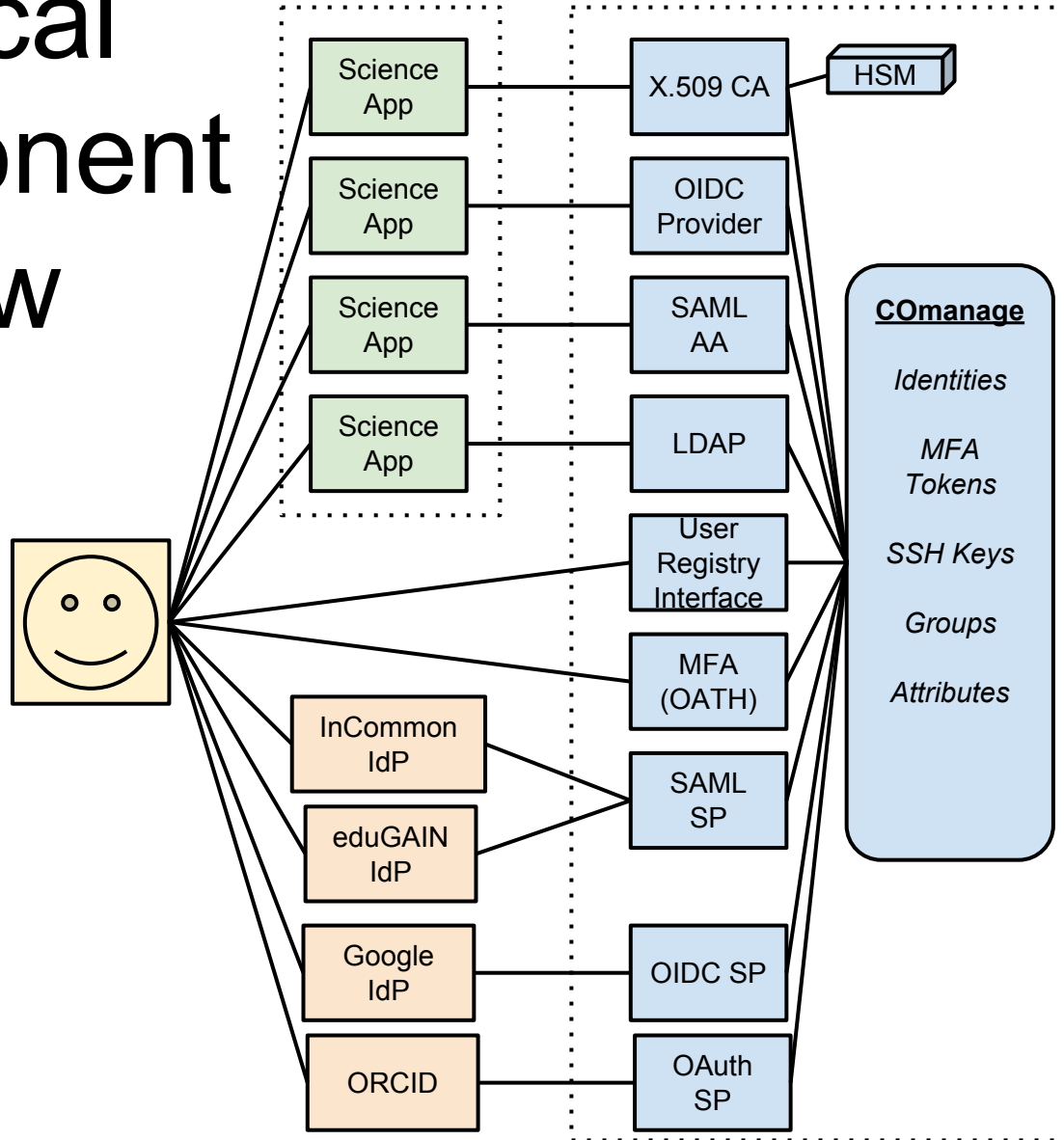
# Web Single Sign-On Gateway

- ❑ IdP of Last Resort (IdPoLR)
  - ❑ Adopting InCommon-recommended IdPoLR provider(s)
  - ❑ Providing additional IdPoLR if needed
- ❑ SAML Attribute Authority (AA)
  - ❑ Providing VO-specific attributes and group membership info for authorization
  - ❑ Using Shibboleth SP capability to query multiple SAML AAs (campus and VO attrs)

# Web Single Sign-On Gateway

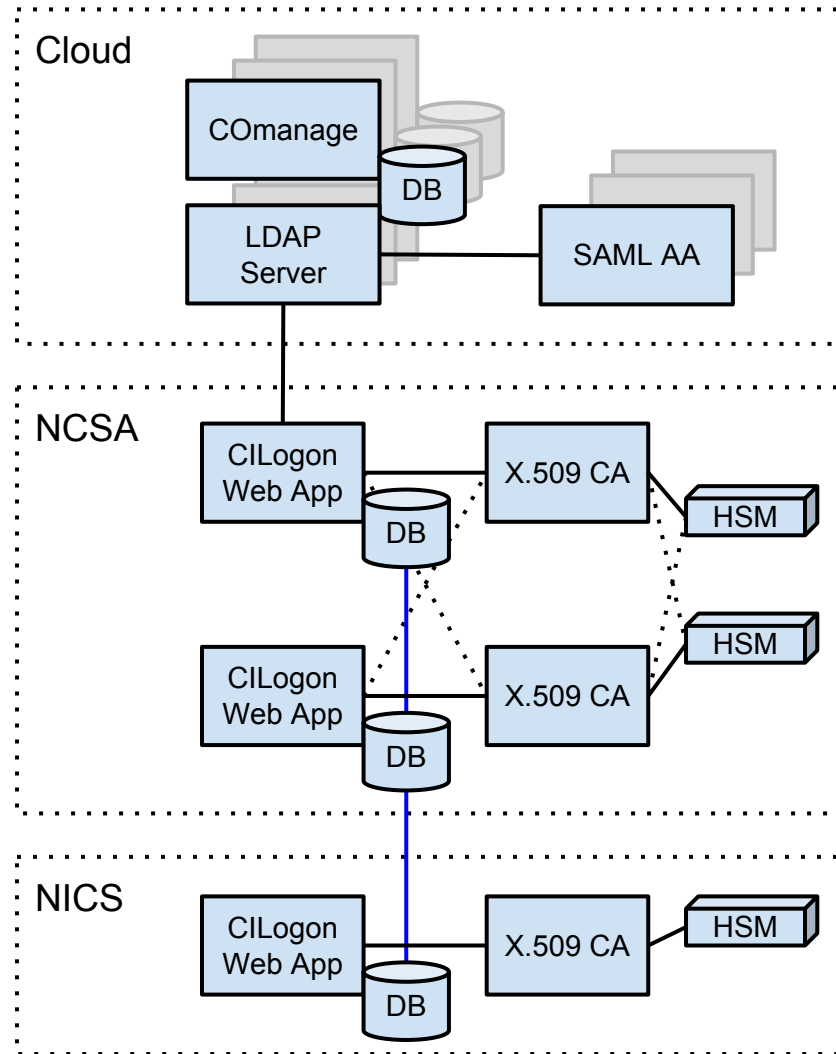
- ❑ SAML to OIDC Gateway
  - ❑ Making InCommon authentication available to apps that support OIDC but not SAML
  - ❑ Following on success of CILogon's SAML to OAuth 1.0 gateway
- ❑ Linking ORCID Researcher IDs
  - ❑ Using ORCID OAuth interface to link ORCID IDs with federated IDs
  - ❑ Including ORCID IDs in X.509, LDAP, SAML, and OIDC

# Logical Component View





# Deployment View



# Next Steps

- ❑ Working with the science projects
  - ❑ More partners welcome!
- ❑ Standardizing our OIDC claims
- ❑ Interfederation
  - ❑ InCommon will be eduGAIN-ready in February!
- ❑ ORCID ID linking
  - ❑ 1st CILogon-COmanage integration driver

# Thanks!

contact: [jbasney@ncsa.illinois.edu](mailto:jbasney@ncsa.illinois.edu)