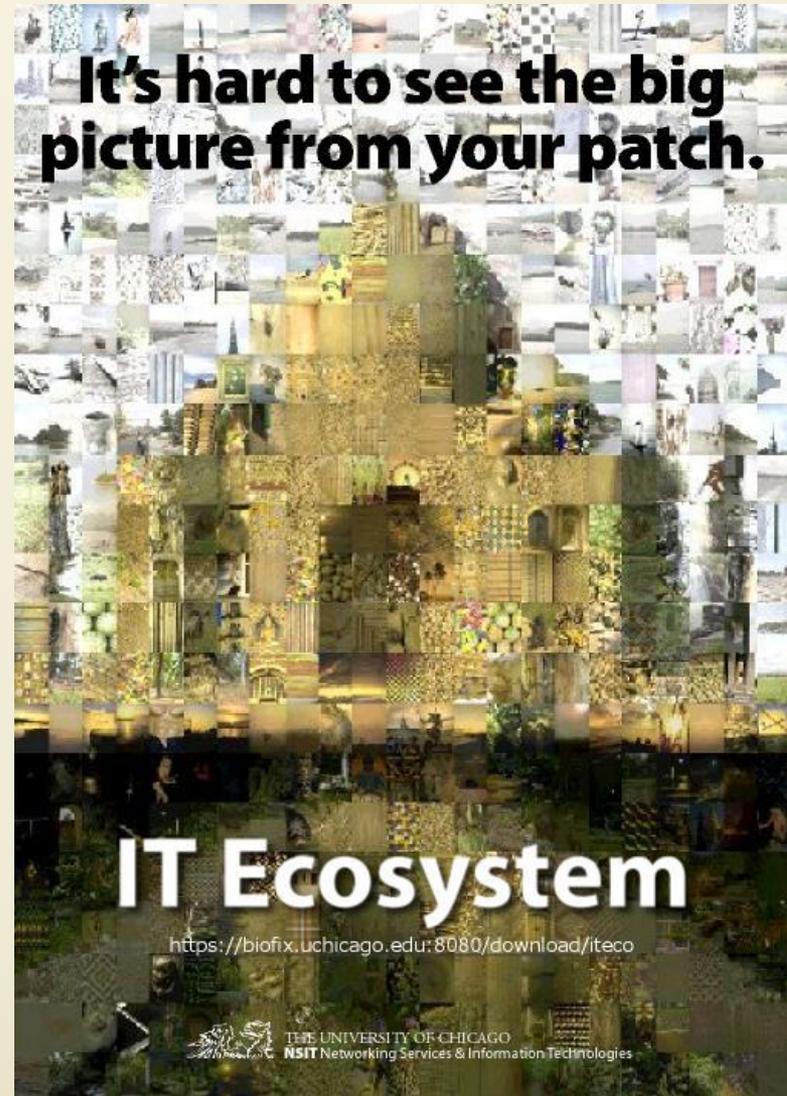


Federated Identity, Shibboleth, and InCommon

Tom Barton
University of Chicago

Who Am I?

- ◆ Sr Dir, Integration
- ◆ Shepherding
 - Data management
 - Security
 - Storage
 - Identity management
- ◆ Policy & informational stuff
- ◆ Internet2/MACE
 - Middleware architect
 - WG chair
 - InCommon TAC



What problem does (*Federated*) Identity Management address?

- ◆ Many usernames and passwords for users
- ◆ Many copies of personal data (*held by third parties*)
- ◆ Duplication of effort among service providers
- ◆ Difficulty sharing resources (*between institutions*)
- ◆ Anytime, anywhere access to resources
- ◆ Compliance with legislation (FERPA, GLB...) and institutional policy

- ◆ In short, the *yet another account* problem



The Challenging Way

Home

Circle University
joe@circle.edu
Dr. Joe Oval
Psych Prof.
SSN 456.78.910

Password #1

Service Providers

Grant Admin Service
ID #2 J.o.v
Dr. Joe Oval
Psych Prof.
SSN 456.78.910
Password #2



Grading Service
ID #3 Jo456
Dr. Joe Oval
Psych Prof.
Password #3



Archive Service
ID #4 j.o.123
Joe Oval
Psych Prof.
DOB: 4/4/1955
Password #4



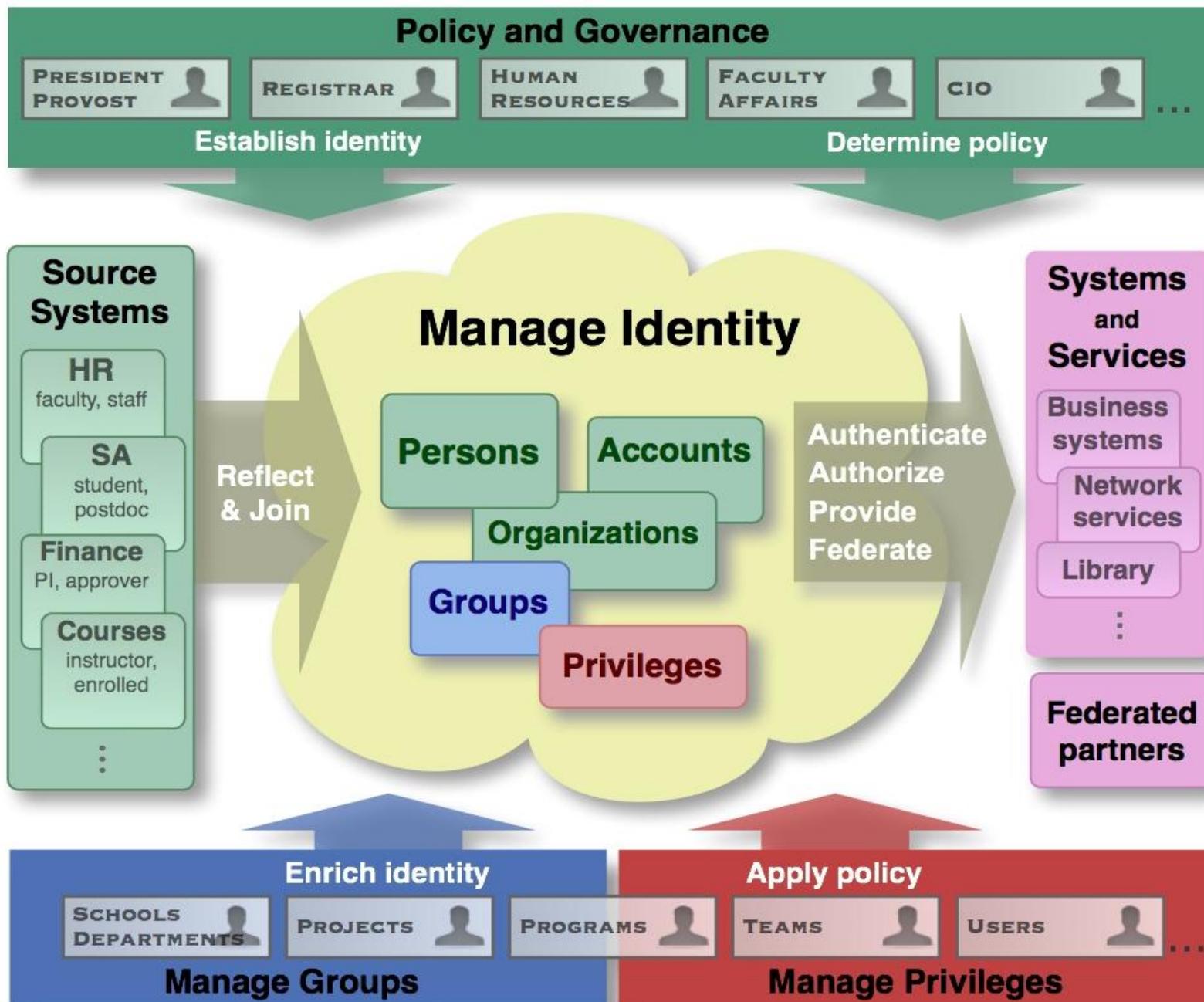
No coordination

Proprietary code

Batch uploads

????



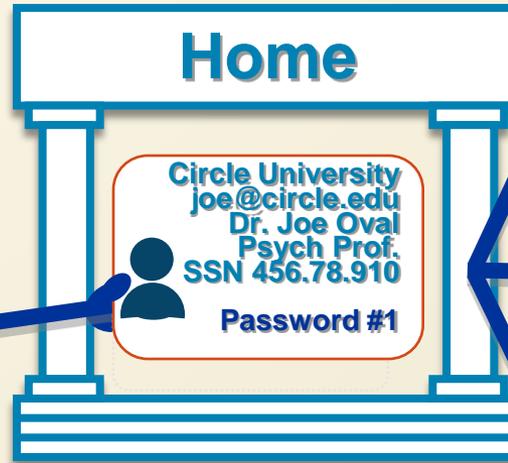


What (Federated) Identity Management offers

- ◆ Efficient scalability
- ◆ Highly leveraged centralized operations
 - Common identifiers
 - Authentication
 - Access information management
 - Accuracy & timeliness
 - Auditability
- ◆ Service providers still do access control
- ◆ Security and privacy

The Federated Way

yes!



1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home org and user control privacy



Internet2/MACE

Identity & Access Management



◆ Shibboleth



◆ InCommon Federation



◆ Grouper



◆ Comanage

- Identity services & application domestication

◆ Privilege & access management

- MACE-Paccman working group

◆ eduPerson & edu* schema, white papers, etc

- MACE-Directories working group



What is Shibboleth?

- ◆ Open source standards-based web single sign-on
 - Supports SAML v1.1 & SAML v2
 - SAML = Security Assertion Markup Language, OASIS standard
- ◆ Supports the Federated Identity model
 - Identity Provider (IdP) authenticates the browser user and provides Assertions about the user
 - Service Provider (SP) validates the Assertions, makes an Access Control decision, and provides Resources
 - Each player is identified by a unique entityID and authenticated by reference to independently established metadata
- ◆ Leverages enterprise identity management

system

THE UNIVERSITY OF
CHICAGO



Authenticate @Home

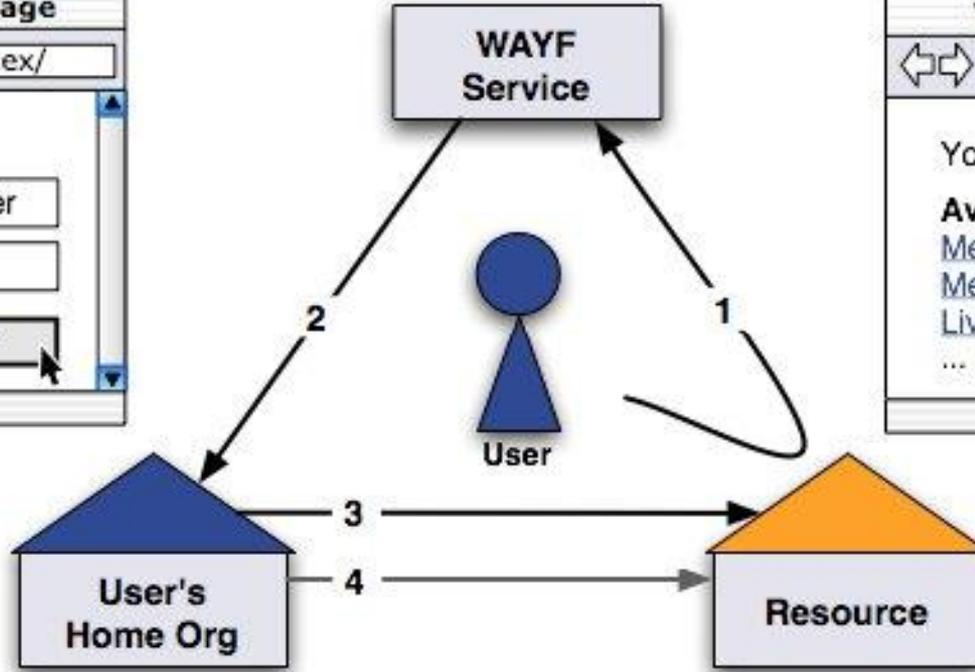


Authorize @Resource



"IdP"

"SP"



Federated Identity

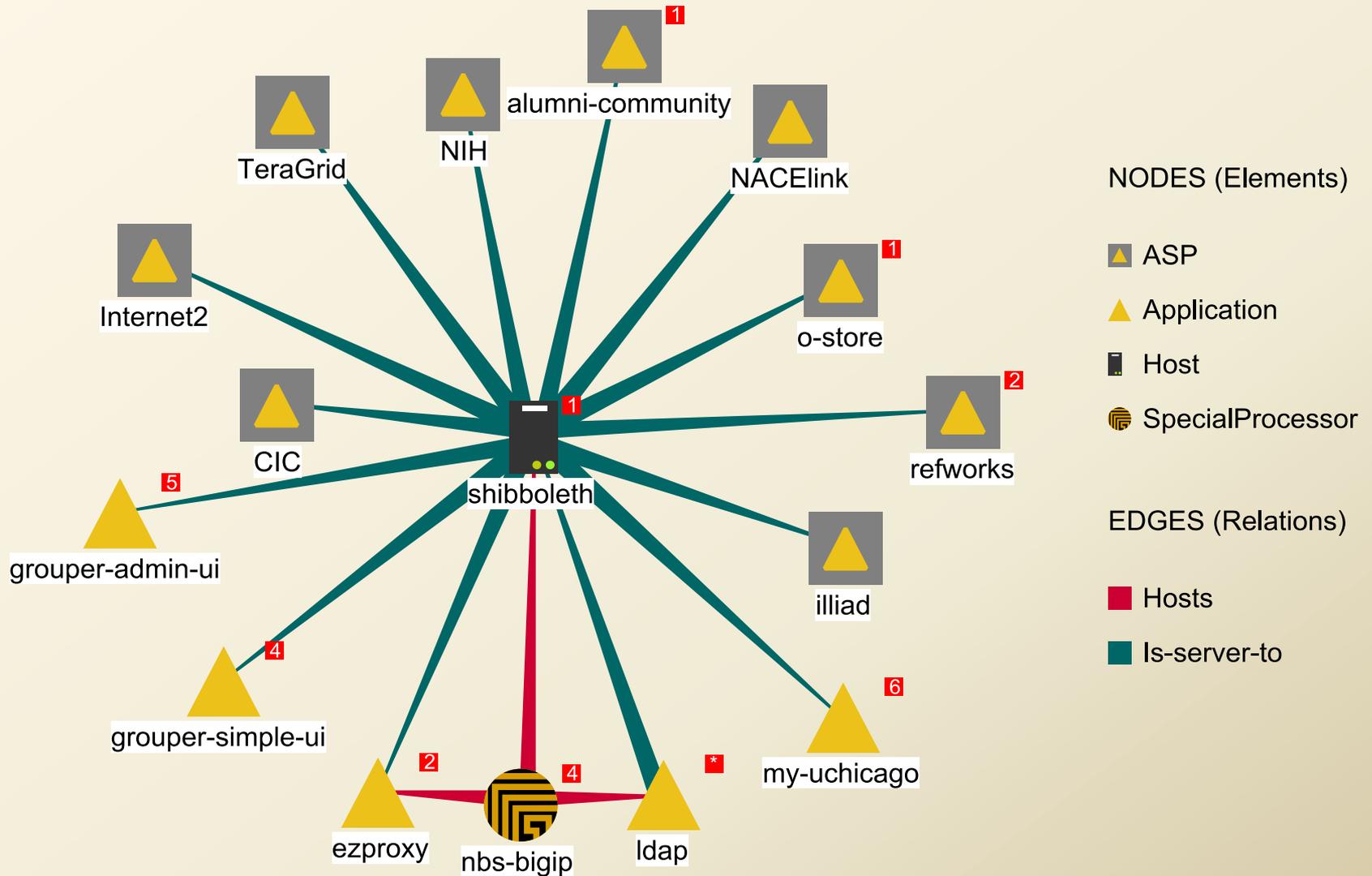
ala  Shibboleth

What Does Shibboleth Provide?

- ◆ SSO access to both campus and external web-based applications
- ◆ Protects user privacy
 - Selective attribute release
 - Pseudonymous identifiers available
- ◆ Integrates well with other SAML2 software
 - Many commercial Service Providers are SAML2 friendly
- ◆ Adoption by 20+ Higher Education/Research federations around the world
- ◆ Commercial professional services and technical support increasingly available



Shibboleth use @ U Chicago



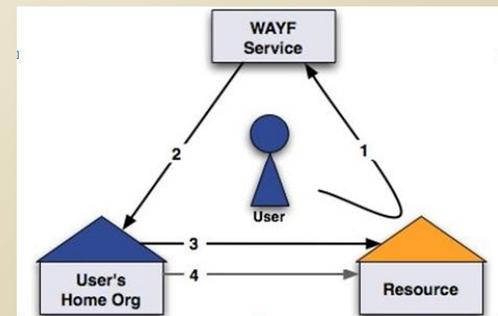
Demo U Chicago Shibboleth SSO

- ◆ U Chicago application ([portal](#))
- ◆ Library remote access ([Acta Mathematica](#))
- ◆ Internet2 wiki ([CAMP Program Cmte](#))
- ◆ CIC SharePoint ([more about this later](#))



What just happened?

- ◆ **my.uchicago.edu**
 - Start of SSO – U Chicago login. No WAYF needed.
 - My roles, groups, name, email, etc, sent from U Chicago IdP to campus portal.
- ◆ **E-journal**
 - U Chicago Library e-journal finder linked to U Chicago shibbolized web proxy. No WAYF needed.
 - Non-shib access to vendor site, to change soon.
- ◆ **Internet2 wiki**
 - InCommon Federation's WAYF invisible due to persistent cookie.
 - Only attribute released is my name.
- ◆ **CICme**
 - CIC members all belong to InCommon.
 - CIC-specific WAYF.
 - Name & email attributes released.



Committee on Institutional Cooperation: “CICme” Federated SharePoint

- ◆ CIC = Big Ten + U Chicago
 - Hundreds of committees and work groups
 - 1-5 members per institution each
 - ~1900 total CICme users
 - Provosts to operational staff
- ◆ Avoid the “yet another account” problem
- ◆ Demonstrate feasibility & value of federation in support of other CIC activities
- ◆ Minimize impact to member campus IT

ClCme

ASP.NET Forms Authentication

Direct
(username/pwd)

Shibboleth
lazy session

SQL Membership Provider

ASP.NET Authorization

SQL Role
Provider

SQL Membership DB
(users and roles)



What's a Federation?

- ◆ A group of member organizations who agree to a set of rules
 - End-user organizations act as identity providers (IdPs), authenticate end users, release information (attributes) about individuals to service providers per policy or contract
 - Service providers (SPs) accept assertions from IdPs and use to authorize access
- ◆ An independent body managing the trust relationships between members
- ◆ An efficient way to scale identity management across organizations
- ◆ A community or marketplace, when successful



What's a Federation Operator do?

- ◆ Register members
 - Validate organizational identifiers
 - Authenticate organizational contacts
 - Execute participation agreement
- ◆ Distribute federation metadata
- ◆ Establish standards or provide guidance
 - Federating technologies
 - Attribute syntax & semantics
 - Identity Assessment Framework - Level of Assurance
- ◆ Problem resolution
- ◆ Outreach
- ◆ Community support

The Role of the Federation

1. Agreed upon attribute vocabulary & definitions: member of, role, unique identifier, courses, ...



2. Criteria for identity management practices (user accounts, credentialing, etc.), privacy stewardship, interop standards, technologies
3. Trusted exchange of participant information
4. Trusted "notary" for all federation members



InCommon Federation: Essential Data

- ◆ US R&E Federation, a 501(c)3
- ◆ Members are universities, government agencies, national labs, and their partners
- ◆ 146 organizations and growing
- ◆ Surpassed 3 million faculty, staff, and students in February 2009
- ◆ Operations managed by Internet2
- ◆ www.incommonfederation.org



Joining InCommon

- ◆ Execute Participation Agreement
- ◆ Pay fees (NB. Non-normative info!)
 - Application - \$700
 - Annual membership - \$1000 per 20 entityIDs
- ◆ Provide Participant Operating Practices statement
 - Description of Identity Management practices (for Identity Provider membership)
 - Attribute requirements and associated practices (for Service Provider)
 - Not audited – self declared
- ◆ Admin & technical contacts
- ◆ Provide initial IdP or SP metadata



InCommon Identity Assurance Framework

- ◆ InCommon Identity Assurance Profiles
 - Bronze compatible with NIST 800-63 Level of Assurance 1
 - Silver compatible with NIST 800-63 Level of Assurance 2
- ◆ Specifies criteria used to assess identity providers
 - Written for and by HE community
 - Contrast with OMB's CAF: not all Assertions about all Principals need have the same LoA
- ◆ Participant's internal audit performs assessment
 - Auditor sends attestation letter to InCommon
- ◆ New program – no one's cleared the hurdle yet
 - Several are in process

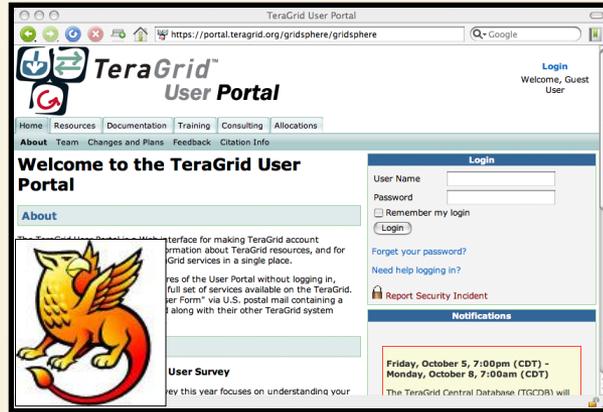


Why bother with LoA?

- ◆ We're told to. Security controls in the FIPS 199 sense
- ◆ We need to. The marketplace created by a federation needs a standard by which Service Providers and Identity Providers can talk about how loose or tight their practices are
- ◆ We want to. Federated access to scientific grids
 - Mapping between InCommon POP, Bronze, Silver and International Grid Trust Federation policies

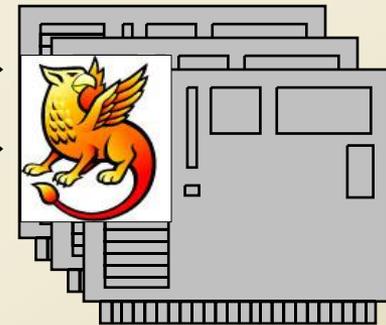


Campus



provision accounts

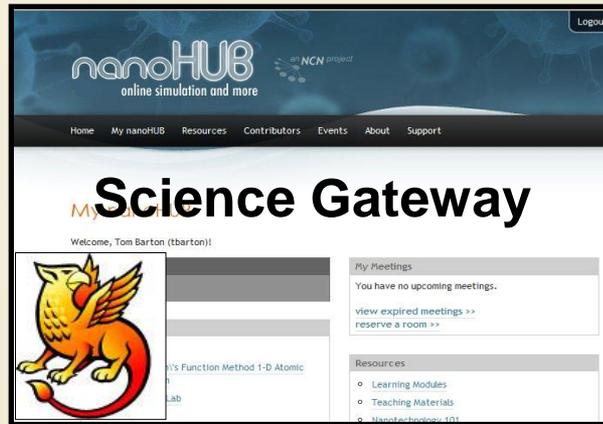
TeraGrid Resources



run monitor

attributes

InCommon Federation



run monitor

