Federation, InCommon, and LoA

Tom Barton

University of Chicago

Federated Access in 30 seconds

4. If attributes are acceptable to resource policy, access is granted!

3. Authorization: Privacy-preserving exchange of agreed upon attributes

2. Federation-based trust exchange to verify partners and locations

1. Authentication: single-sign-on at home institution

Online Resource

Attributes: Anonymous ID, Staff, Student, ...

Metadata, certificates, common attributes, federation registration authority, Shibboleth

Home Institution – user signs in

Current InCommon Participants

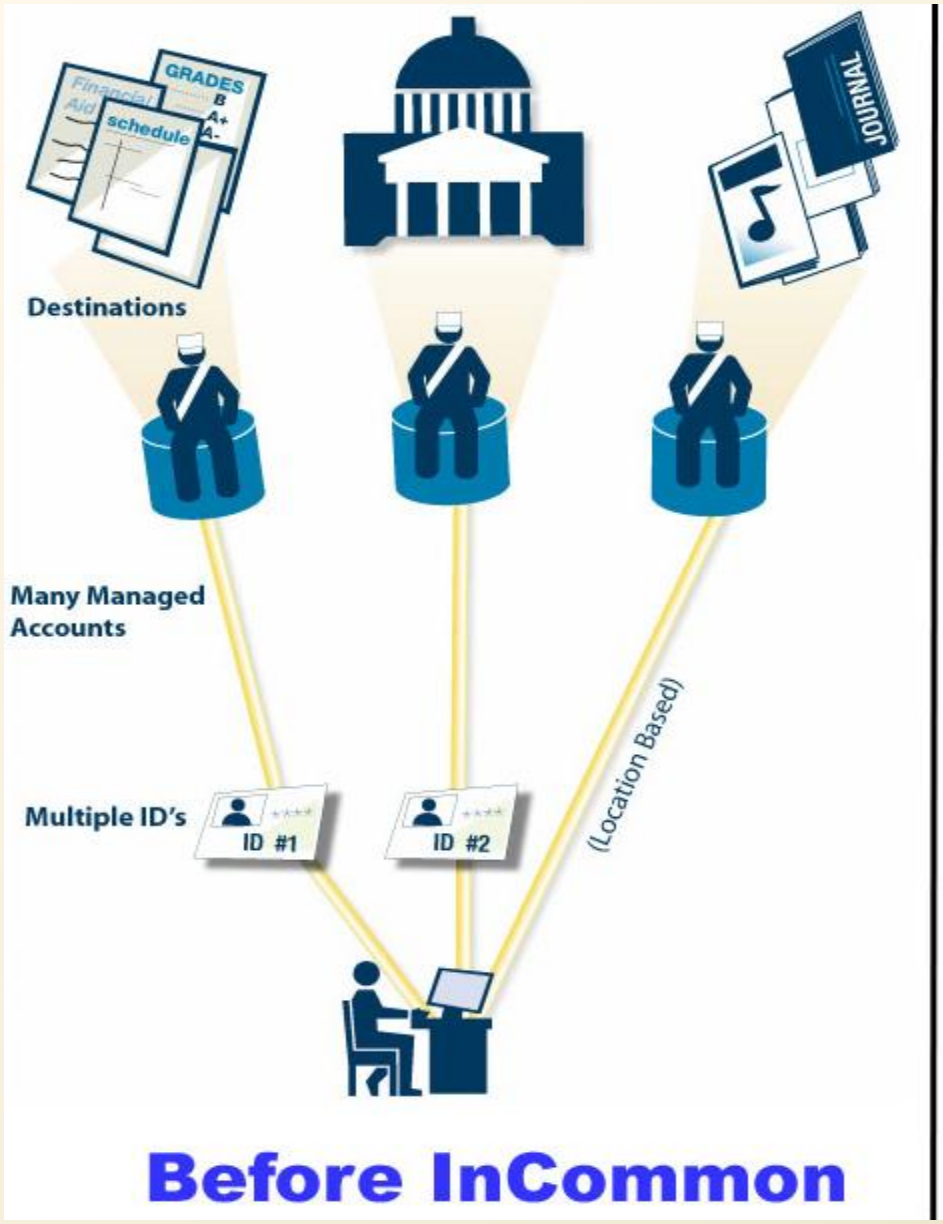
A community of more than **4 million end users**

(November 2009. Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System.)

153 Universities	6 Labs or Agencies	51 Sponsored Partners
Arizona State University	Energy Sciences Network (ESNet)	Absolute Software, Inc.
Augsburg College	Lawrence Berkeley National	Apple - iTunes U
Baylor University		Atlas Systems, Inc.
Brown University		Blatant Media Corporation
California Institute of Technology		Burton Group

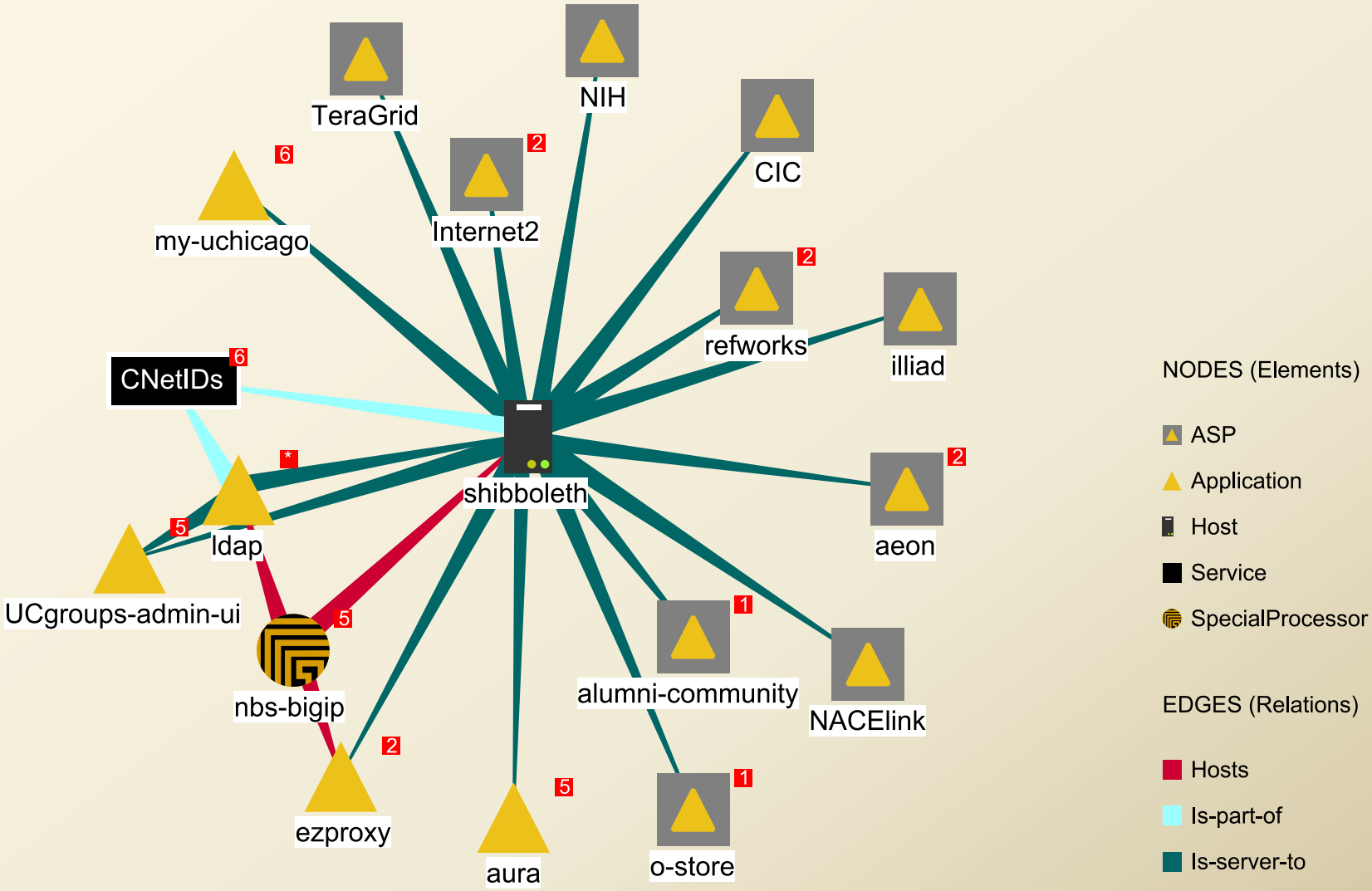
What's a Federation?

- 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 many organizations
- A community or marketplace, when successful


GRADES
B
A+
A-
Financial Aid
schedule
JOURNAL
Destinations
Many Managed Accounts
Multiple ID's
ID #1
ID #2
(Location Based)
Before InCommon


GRADES
B
A+
A-
Financial Aid
schedule
JOURNAL
InCommon
VERIFIED
Destinations
One Home Account
Single ID
ID
After InCommon

What U Chicago uses it for



InCommon Silver

- Comparable to NIST LoA2
- Based on OMB M-04-04 and NIST 800-63

- Covers all aspects of the IdM operation
- Two audits required
  - Every 2 years – confirm operation follows documented policy & procedure
  - One time – assess documented policy & procedure for Silver compliance

- InCommon keeps letter from Silver compliance auditor and publishes the fact of that IdP's compliance

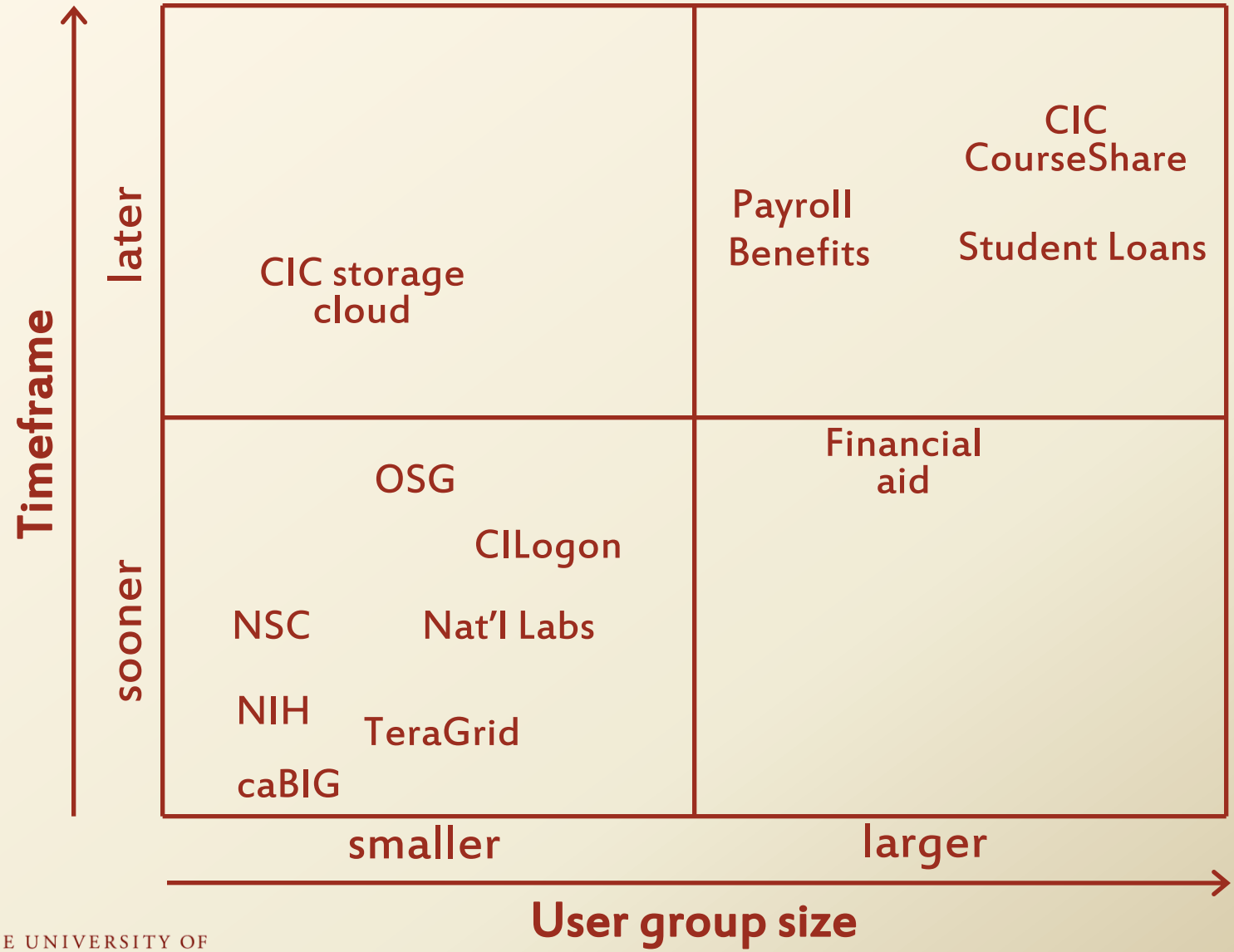
The CIC and InCommon Silver

- CIC CIOs decided in August 2009 that all CIC schools should be Silver certified by Fall 2011
- Why?
  - Expand inter-institutional collaboration among CIC schools
  - Influence emerging standards & practices in cloud and above campus services and elevate prominence of the CIC in connection with that
  - Sustain adoption of best IdM practices at CIC schools

From a recent letter from the CIC CIOs to Internet 2

"The CIC's commitment to identity management and federation of identities through InCommon is strong and our future dependency on InCommon is clear."

Which campus people need Silver assurance?



Pieces of Silver

- Piece A: Documentation of policies and procedures and standard operating practices
- Piece B: Strength of authentication and shared secrets
- Piece C: Registering identity subjects and issuing credentials to them

Documentation of policies and procedures and standard operating practices

Requirements	Issues or risks
Comprehensive IdM policies and procedures	No one really knows, unclear who gets to decide, weak documentation practice
Formal authority	Lack of clear governance
Criminal background checks for IdM staff	New mandate for Human Resources Department
Bi-annual audit	Scheduling & funding

Strength of authentication and shared secrets

Requirements	Issues or risks
Password complexity & lifetime	Resistance to change
Account lock-out	Resistance to change
Passwords stored appropriately	How campus portal handles passwords
Passwords only in secure channels	Remaining legacy systems (e.g. Macs & Active Directory

Registering identity subjects and issuing credentials to them

Requirements	Issues or risks
n/a	Which user groups are in scope for the campus Silver project?
Identity vetting & registration	Change existing process for on-boarding students or staff –OR– Implement a new IV&R process
Store breeder document numbers	Increase exposure of Personally Identifiable Information
Credential issuance process	Change online credential issuance process; new link with existing business processes

The view from Fall 2011

- Energize collaborative efforts across the CIC
- CIC campuses provide best possible support for scientific and scholarly collaboration
- CIC campuses poised to take full advantage of cloud/shared services
- For a large university, achieving Silver compliance can boost confidence on campus too