Single Sign-On Multiple Benefits via Alaska K20 Identity Federation

20 May 2011

BTOP Partner Meeting

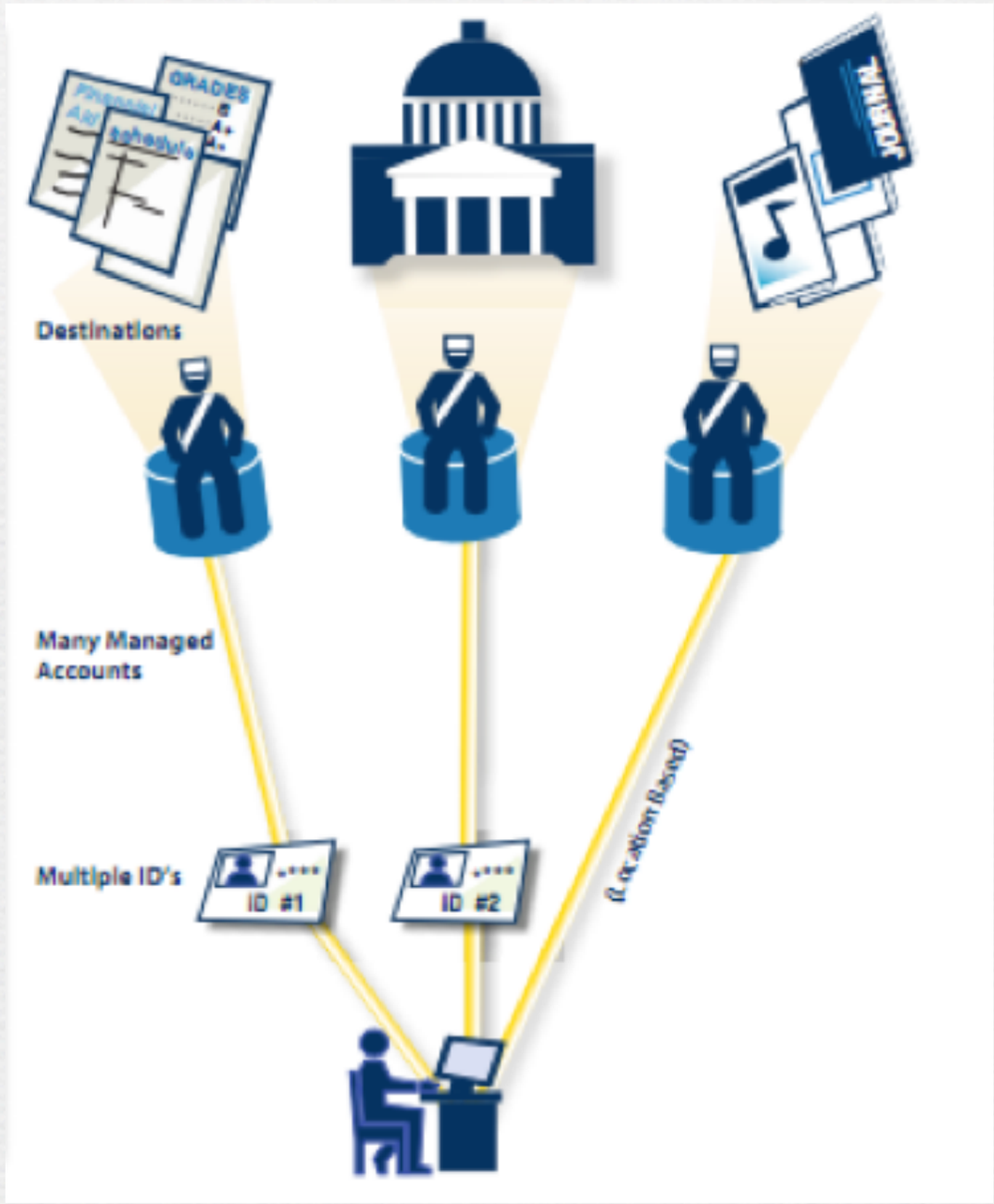
Anchorage, Alaska

Challenge

- Many valuable online information resources,
- But managing access is increasingly unwieldy:
- Too many accounts...too many passwords...
- Too many support requests

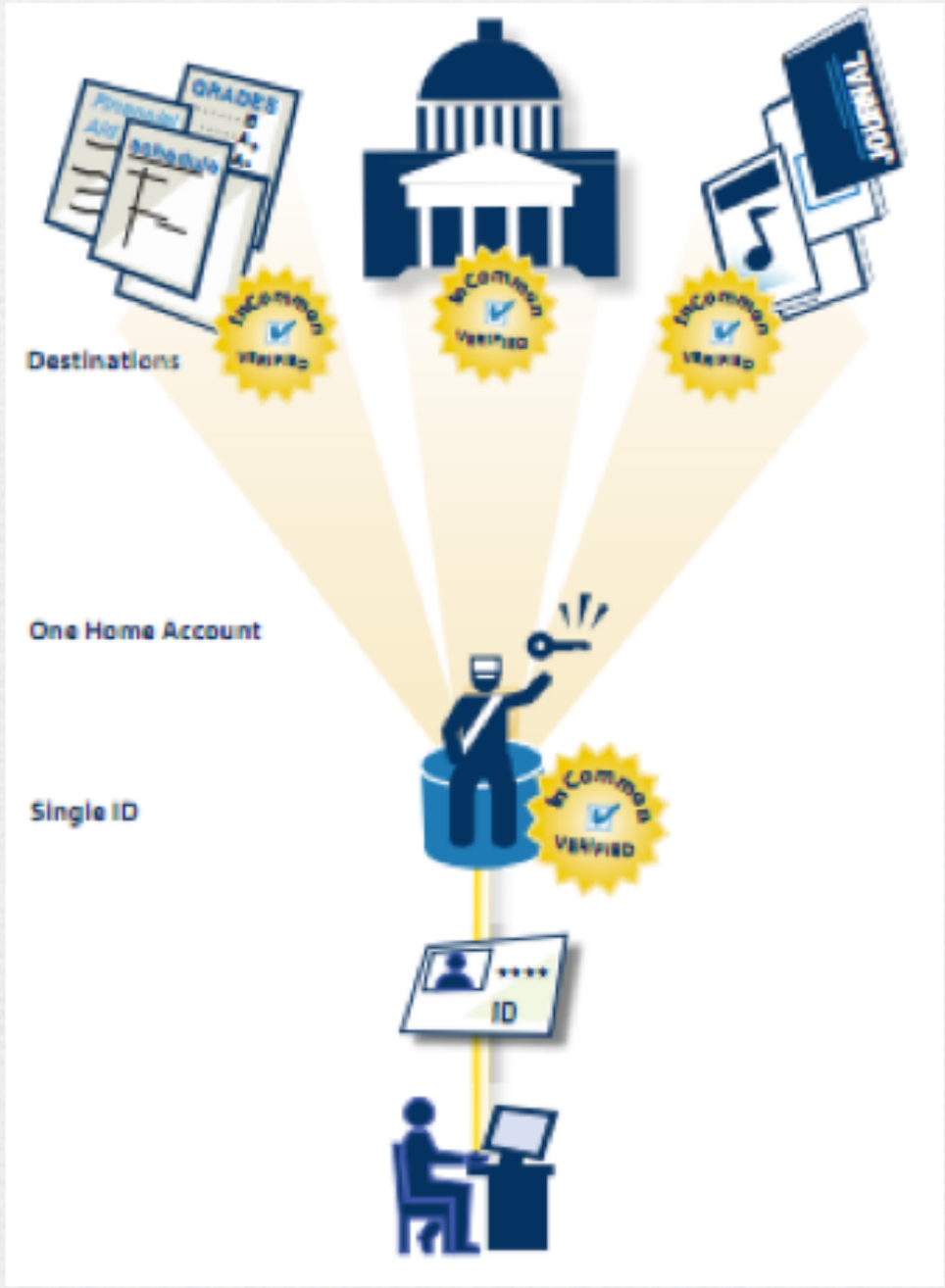
Access Without Federation

- Everyone has many accounts
- Access based on location
- Every information provider has to manage many accounts
- Adding new users or new information resources takes a lot of work (many places to update)



Access With Federation

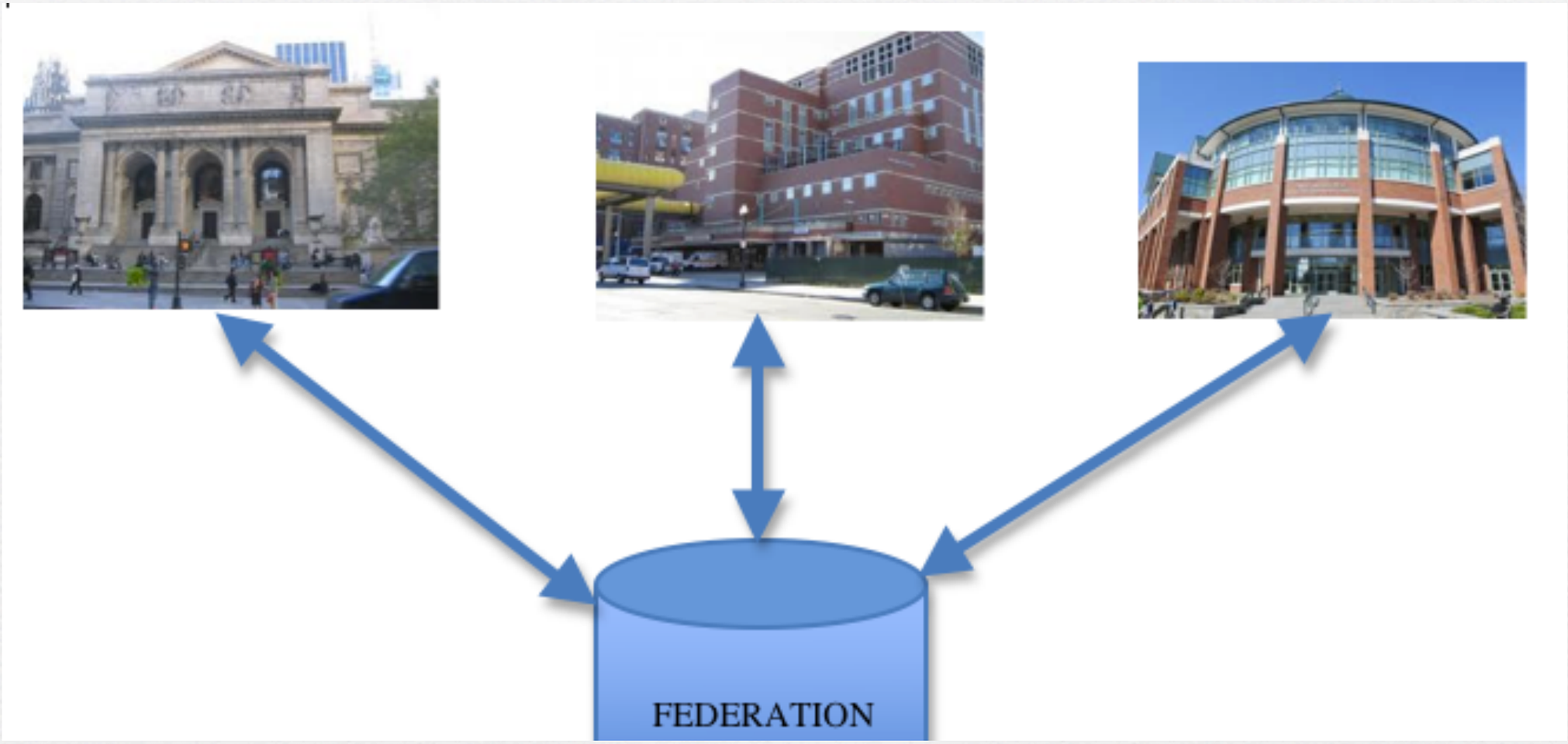
- User has a single login; home provides login and users' roles
- Resource providers need not manage/support user accounts
- Access based on users' roles instead of account or location
- New users and new resources integrated quickly (only one Place to update)



What's the Magic?

- Without federation, access is based on many:many trust relations (resources:users)
- Unsustainable to manage and support as number of users and number of resources increase
- In a federation, the resources and users' home institutions establish trust via their trust in the federation
- Each new resource, home, or user requires only a single additional trust relation: user-home for new user; home-federation for a new home; or resource-federation for new resource

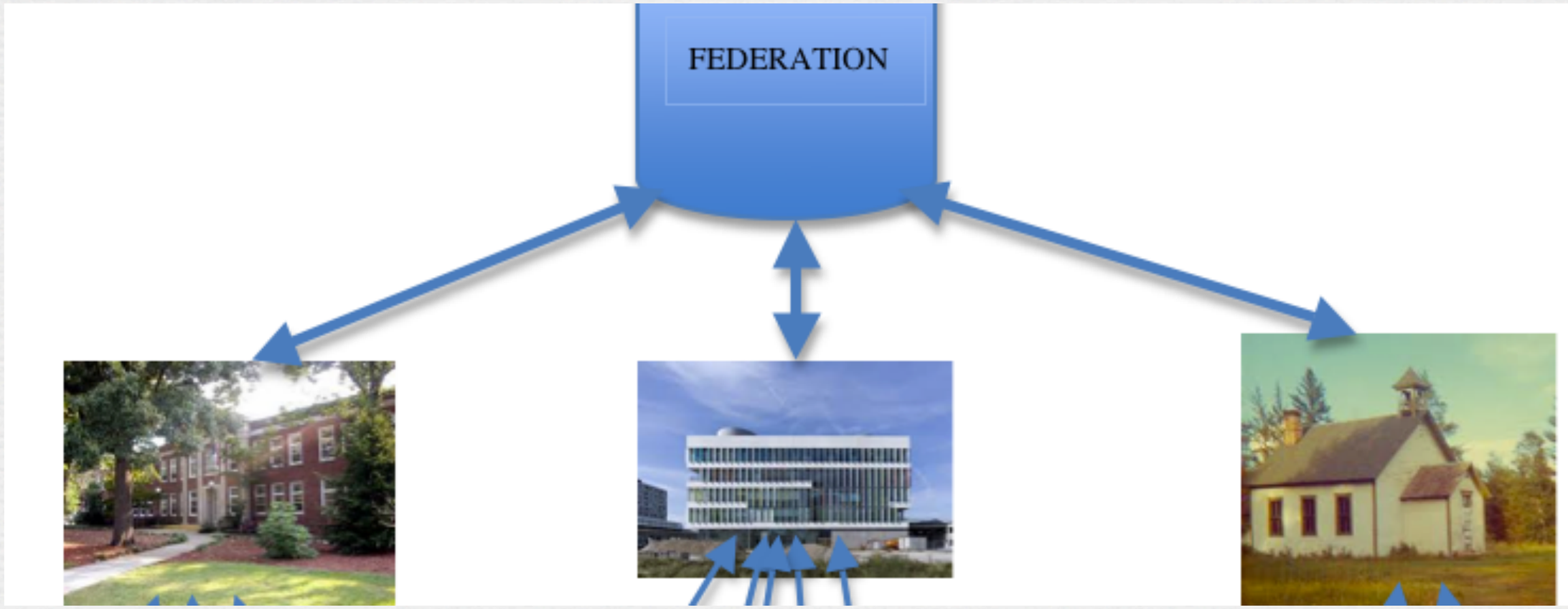
How Federation Works 1



- Each resource or information provider establishes trust with the federation
- A one-time event, with a single external entity

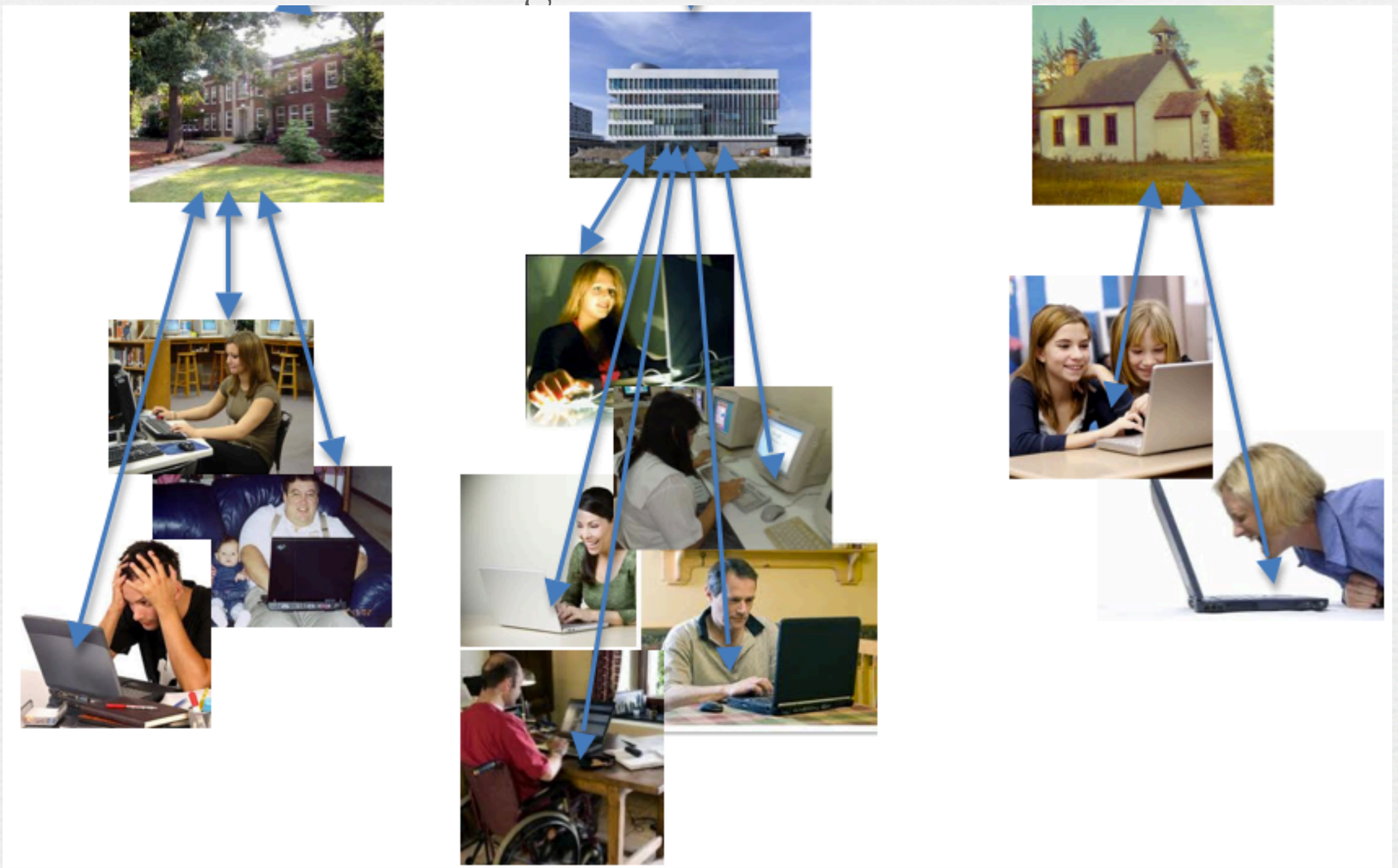
How Federation Works 2

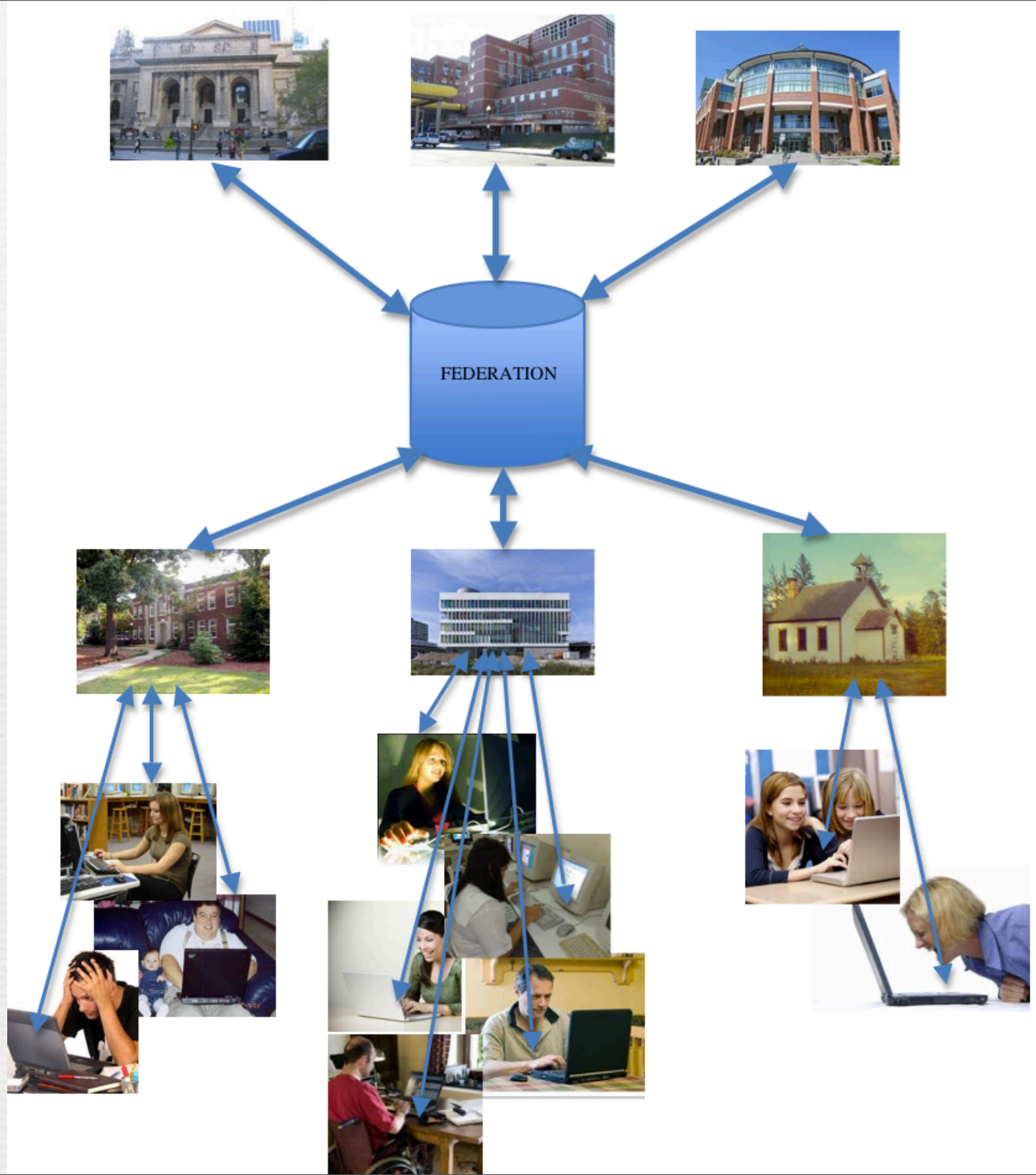
- Each school or other institution with users establishes trust with the federation
- A one-time event, with a single external entity



How Federation Works 3

- Each user has one home institution
- That's the one login that user needs




FEDERATION

Benefits for Resources

- Reduce or even eliminate the burden of managing user accounts and passwords
- Determine what users can access or do based on the users' home institution assertion of roles (e.g., HS Biology Instructor or Honors English Student)
- Quickly deploy new resources to federation members (no elaborate provisioning)

Benefits for Schools

- No need to provision accounts (or revoke them) at every resource
- Enable appropriate access to resources by changing role or other attribute to accurately reflect status
- Provide access to more resources via the federation than could provide by negotiating for each

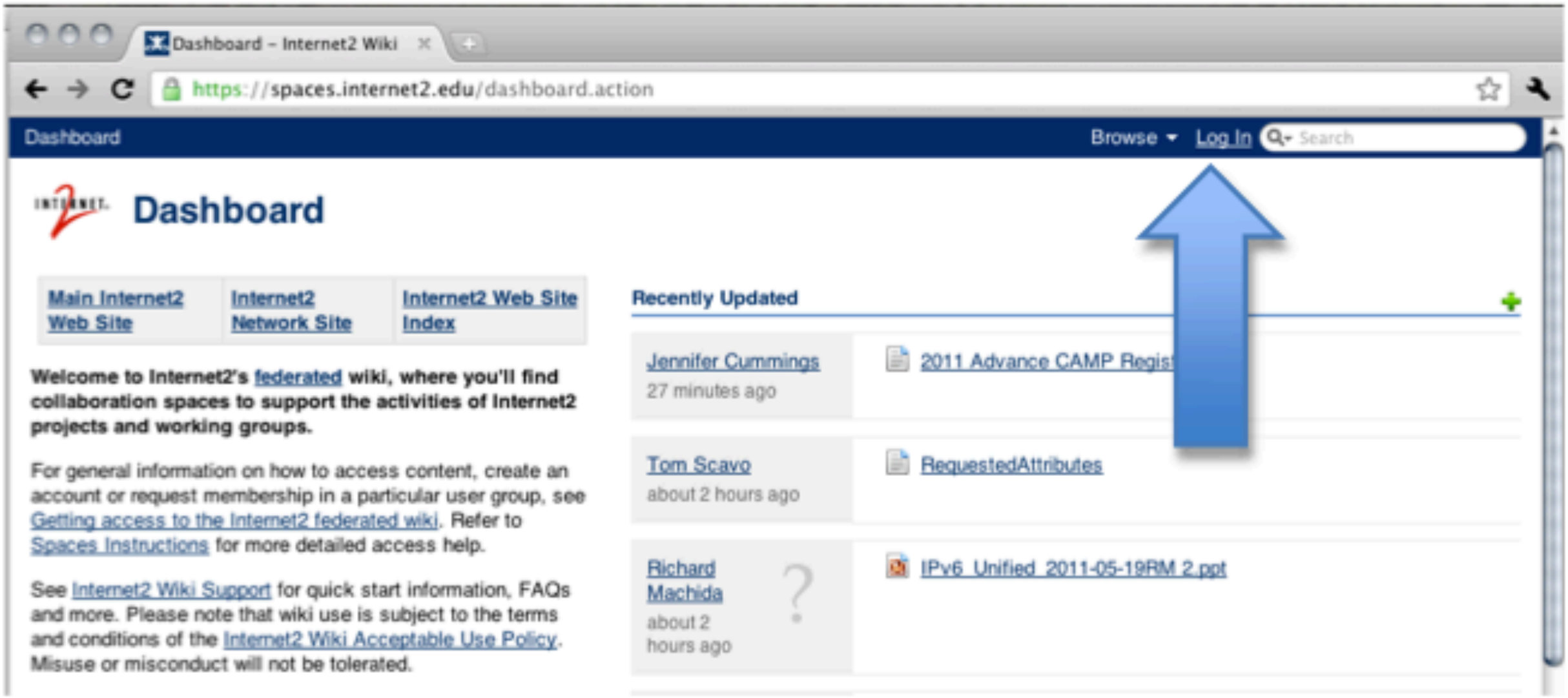
Benefits for students / users

- Keep track of just a single username and password for access to all federation resources
- Reduced threat of identity theft because passwords are not shared with information providers (login at home institution only)
- Increase privacy: resources receive only the data they need to provide appropriate access; may not even include name.
- Supports Single Sign-On: login once for access to multiple resources

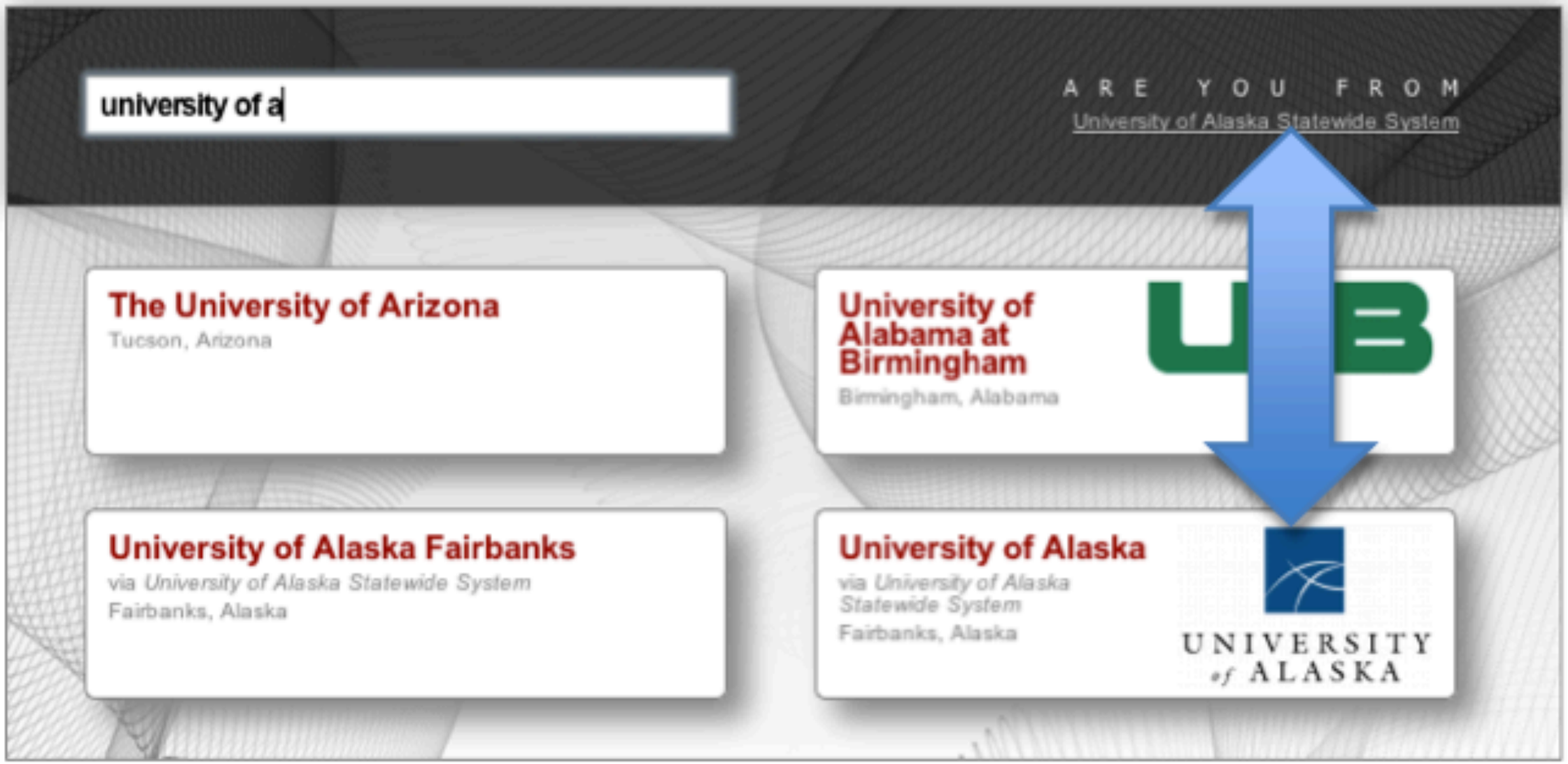
Demonstration: Single Sign-On in Federation

- Model is higher education federation InCommon
- Provides SSO access with UA credentials to multiple services
- Services hosted both at UA and elsewhere
- Simple uniform experience gaining access to multiple resources while protecting personal info

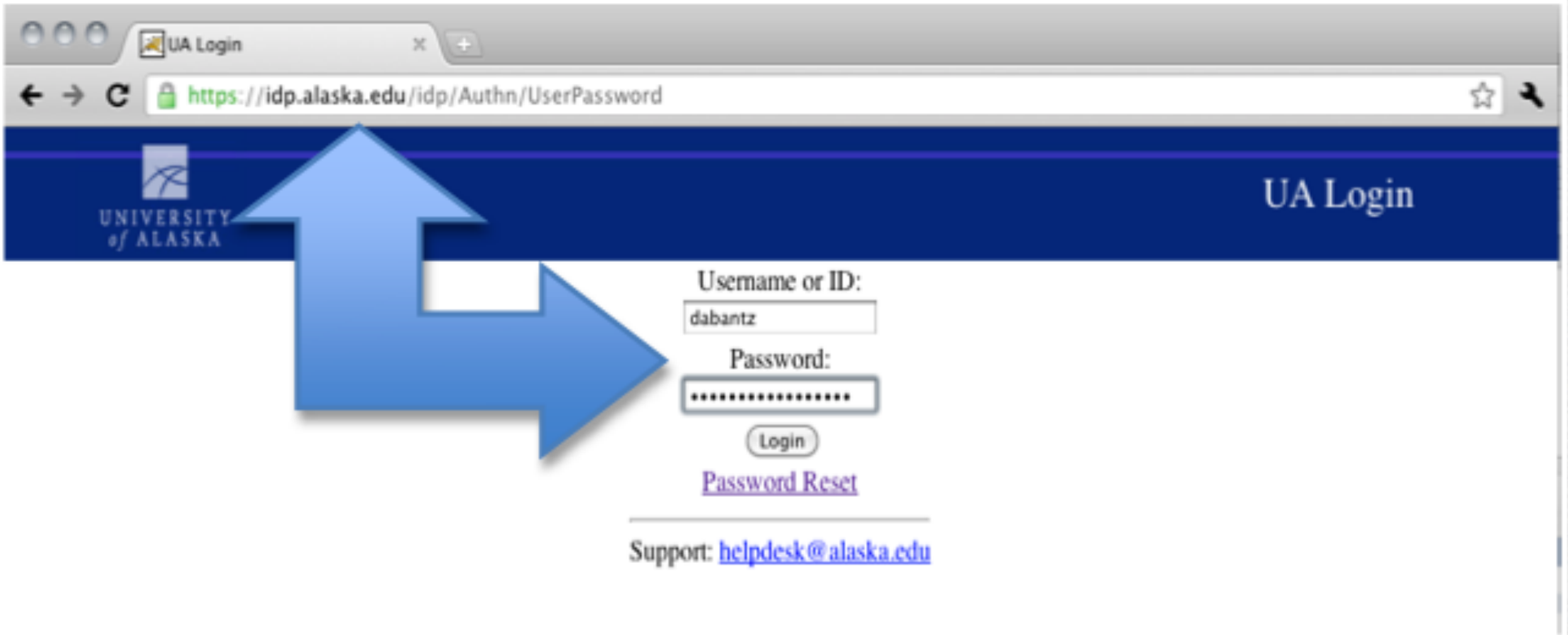
Initial login at an information service provider: click the “Log In” button to start:



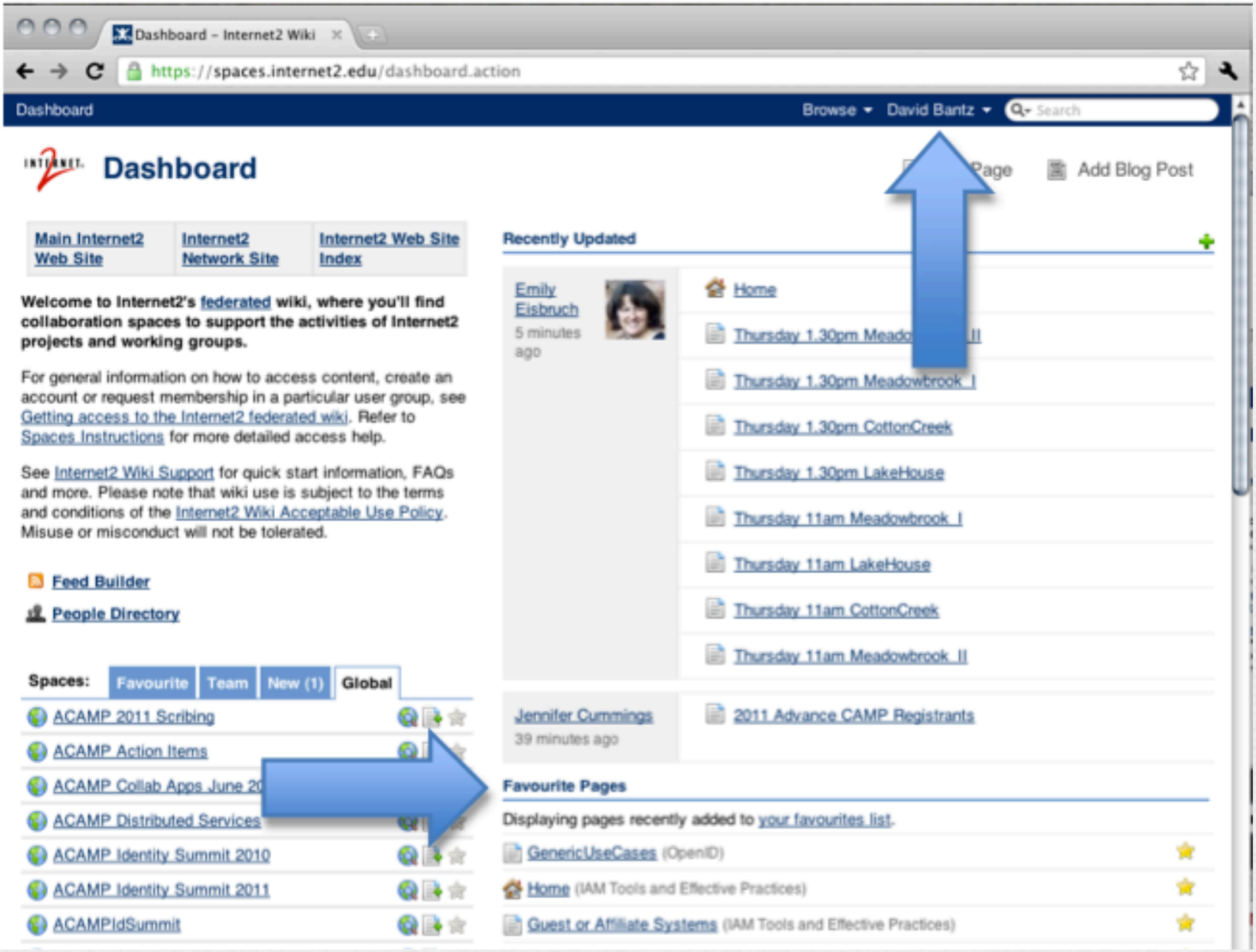
Designate my home institution: “Where are you from?”:



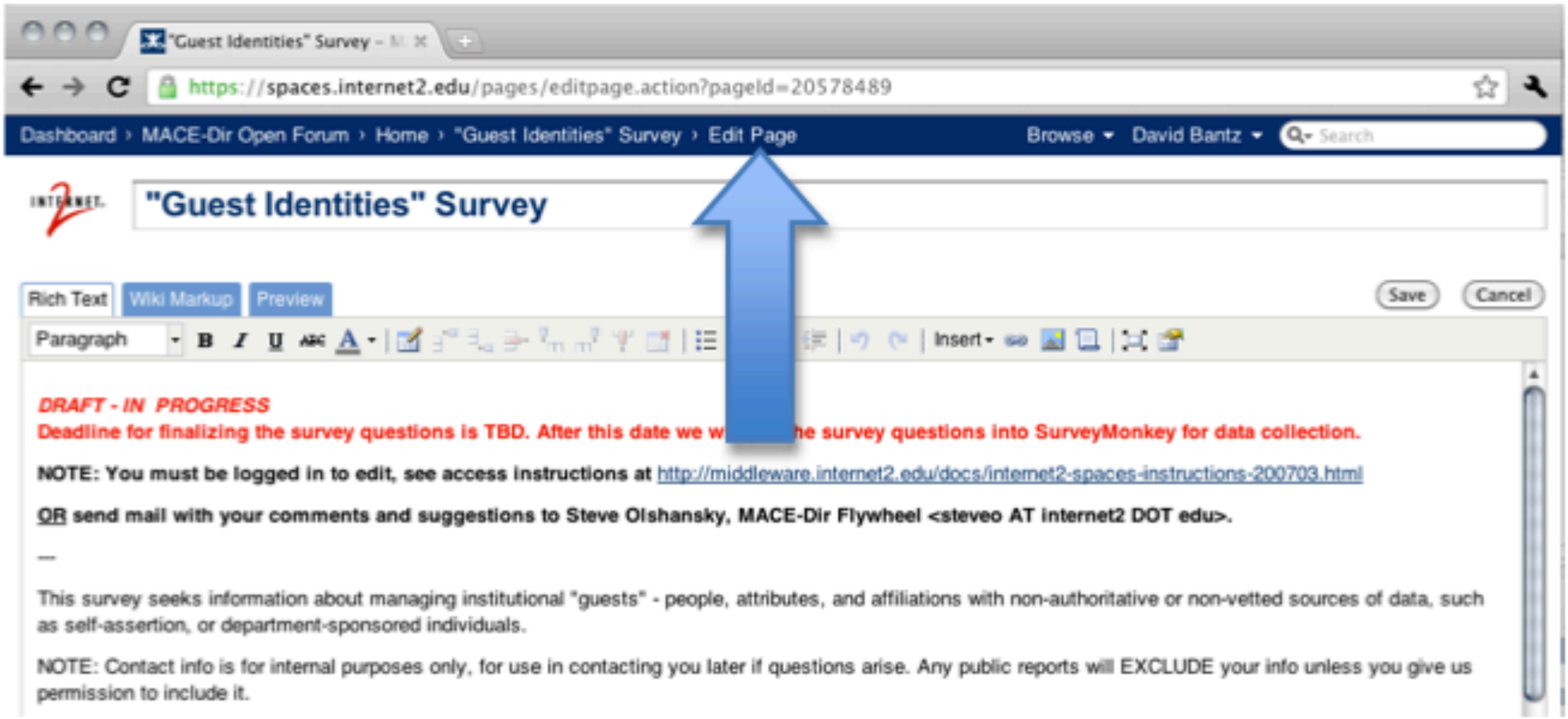
Type identifier and password to my home– not shared with the information service!



I'm logged in and look: service received my correct name and preferences:



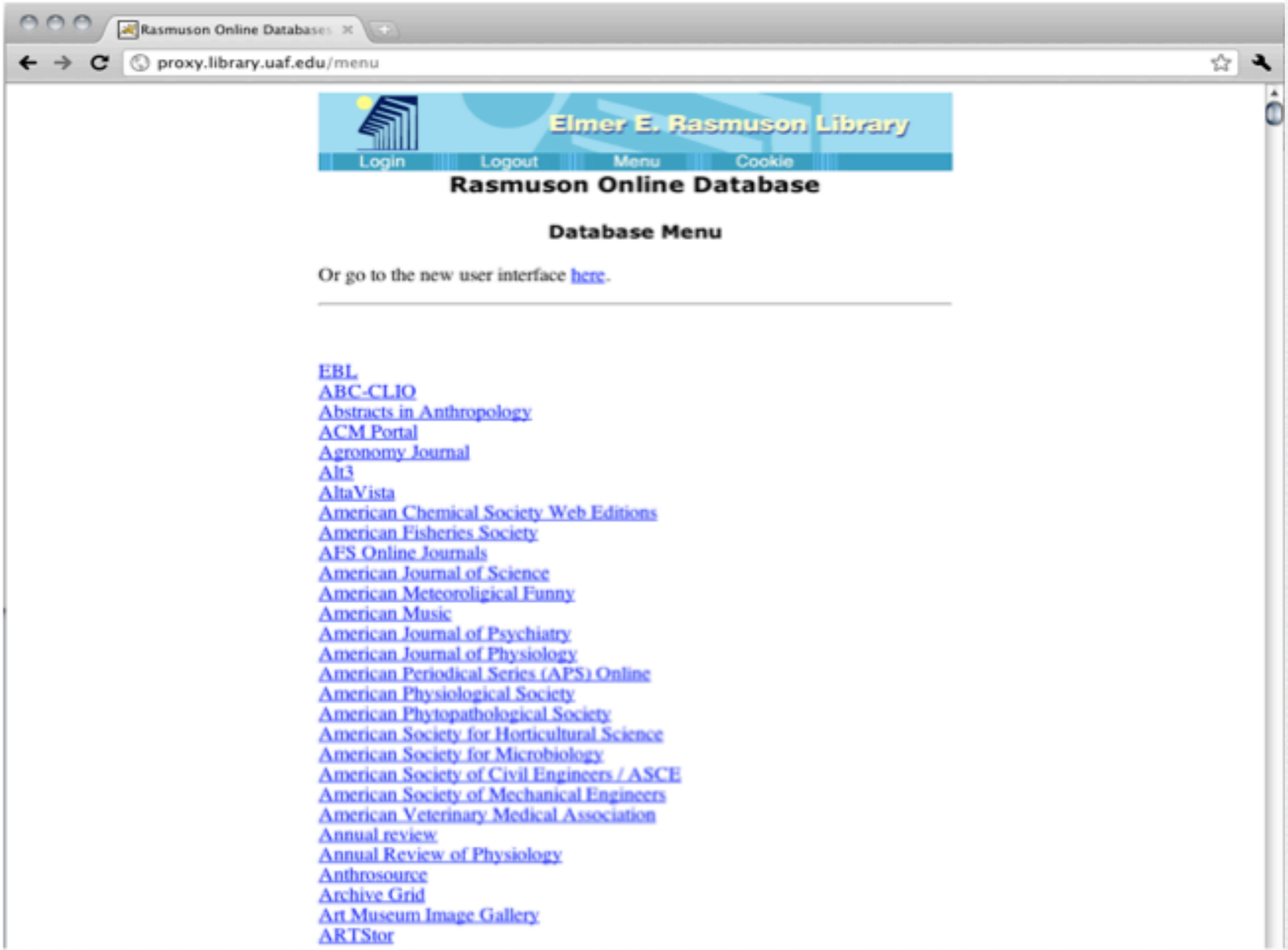
I am able to edit the pages I own:



Now I navigate to a different information service hosted elsewhere:

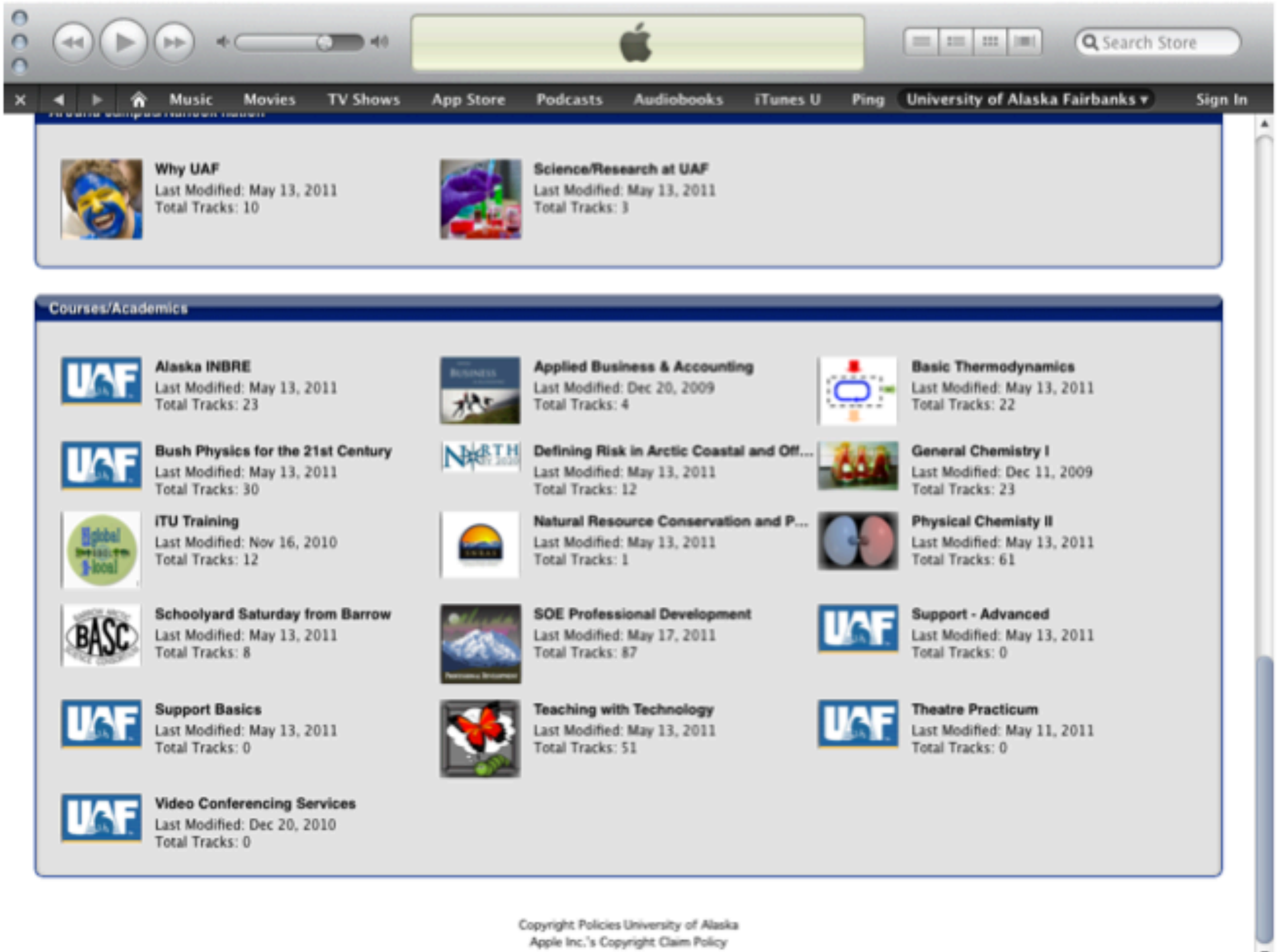
This time when I click "Login" to access licensed databases, this system sees I already have an authenticated session with my UA identity; I do NOT have to re-enter my username and password, but immediately see the databases I am allowed to use:

This time when I click "Login" to access licensed databases, this system sees I already have an authenticated session with my UA identity; I do NOT have to re-enter my username and password, but immediately see the databases I am allowed to use:



Now I want to listen to podcasts available to me as a UA person:

The service is able to use the same SSO session to enable my access to course content I can view based on my roles as student or instructor in various courses:



How To

- Establish agreements defining what federation members do to establish trust relations and operate federation
- Federation operation is essentially a repository of certificates (like the certificates used for secure web browsing) for every member
- Agree to utilize common open technologies for exchanging identity information (e.g., SAML protocol)
- Modest budget for federation operation and technical support to resources and schools to use it