The Frontiers of Internet identity

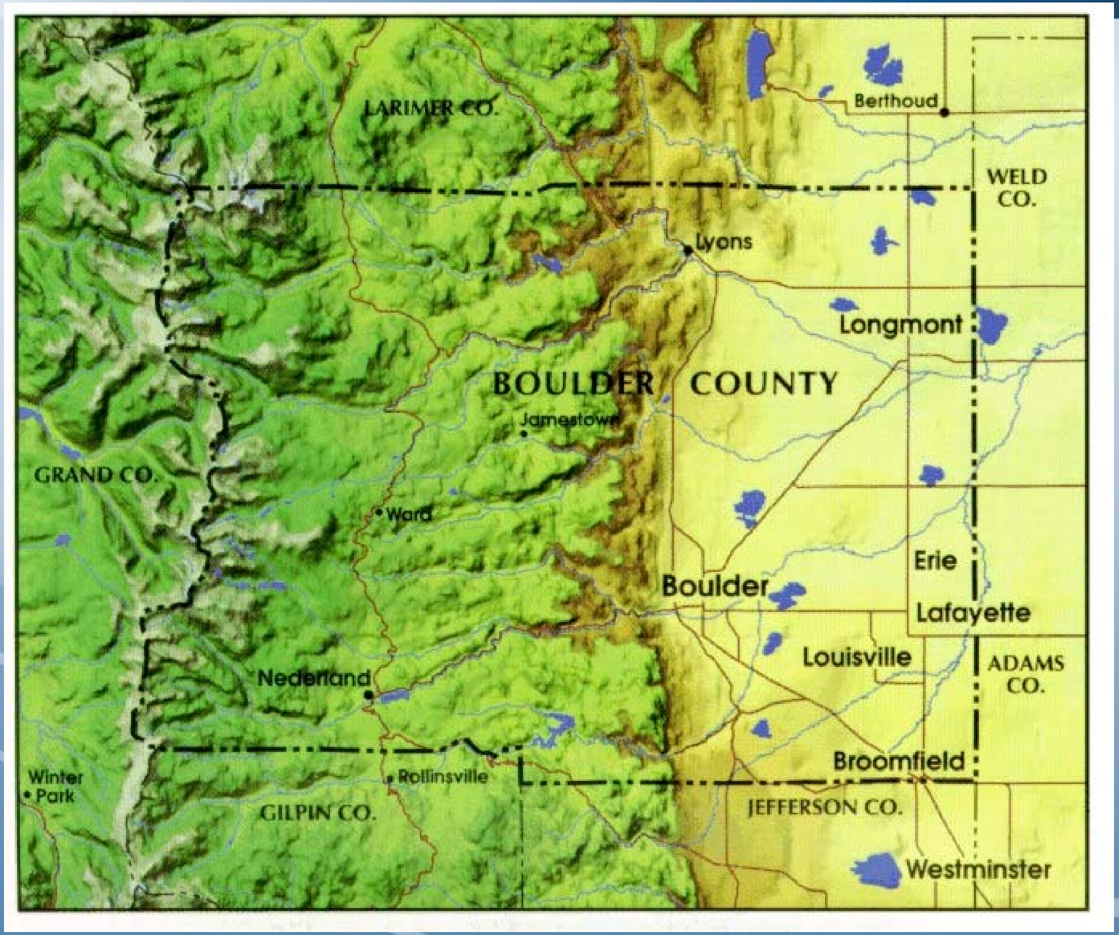
Topics

- Living on the Frontier
- The Frontiers of the Internet
- The First Frontiers of Internet identity
- The New Frontier
  - Discovery, Privacy Management
  - Interfederation and Non-web apps
  - The Attribute Ecosystem
- The Dangers of the Frontier

A Changing Frontier (and me)

kjk@internet2.edu

kjk@internet2.edu


LARIMER CO.
Berthoud
WELD CO.
Lyons
Longmont
BOULDER COUNTY
Jamestown
GRAND CO.
Ward
Erie
Boulder
Lafayette
Louisville
ADAMS CO.
Nederland
Broomfield
Winter Park
Rollinsville
GILPIN CO.
JEFFERSON CO.
Westminster

The original Internet frontiers

- Basic technology development (1970-1985)
  - TCP/IP, DNS, email, HTTP
- Basic marketplace development (1985-2000)
  - Widely usable clients
  - Business models and the web industry
  - Support
- Basic policy development

Texas Ranger 1

Lessons learned

- Modular and layered design
- A “narrow waist” of technology
- Open standards, open source
- Autonomous systems, loosely coupled
- Network multipliers a powerful force
- Most don’t understand at first, and then there is a tipping point and it is obvious to all.

The first Internet identity frontiers

- Two forms of Internet identity have experienced exponential growth in the last few years
- *Federated identity* leverages organizational identity, rich attributes and multiple levels of assurance
- *Consumer identity*, represented by Google, MSN, Yahoo, AOL, Facebook, etc provide convenient and lightweight identities for many popular sites
- Activities are moving beyond web applications, national borders, and beyond vertical sectors into ubiquity

A bit of Federated Identity history

- Federated Internet identity work began in 2000 in the R&E sector
- Spread quickly into corporate sector via OASIS standards processes
  - Corporate use cases limited to bi-lateral relationships
  - R&E sector carried on multi-lateral federation work
- Created SAML, Shibboleth, InCommon, etc
- Widespread deployments began 2004-5 in R&E, government, and vertical sectors
- Building federations and trust more work than developing protocols

The Killer Apps

- Single sign on across a wide variety of resources – libraries, supercomputers, databases, instruments, collaboration tools
- Use of federated collaboration tools – wikis, foodle, lists, chat rooms, videoconferencing, etc.
- Access to federal government resources, from grants management to clinical trials and public medical information
- Roaming wireless access, integration with open identities and other low LOA base services

Texas Rangers 2

Lessons learned

- Modular and layered design
- A “narrow waist” of technology
- Open standards, open source
- Autonomous systems, loosely coupled
- Network externalities a powerful force
- Most don’t understand at first, and then there is a tipping point and it is obvious to all.

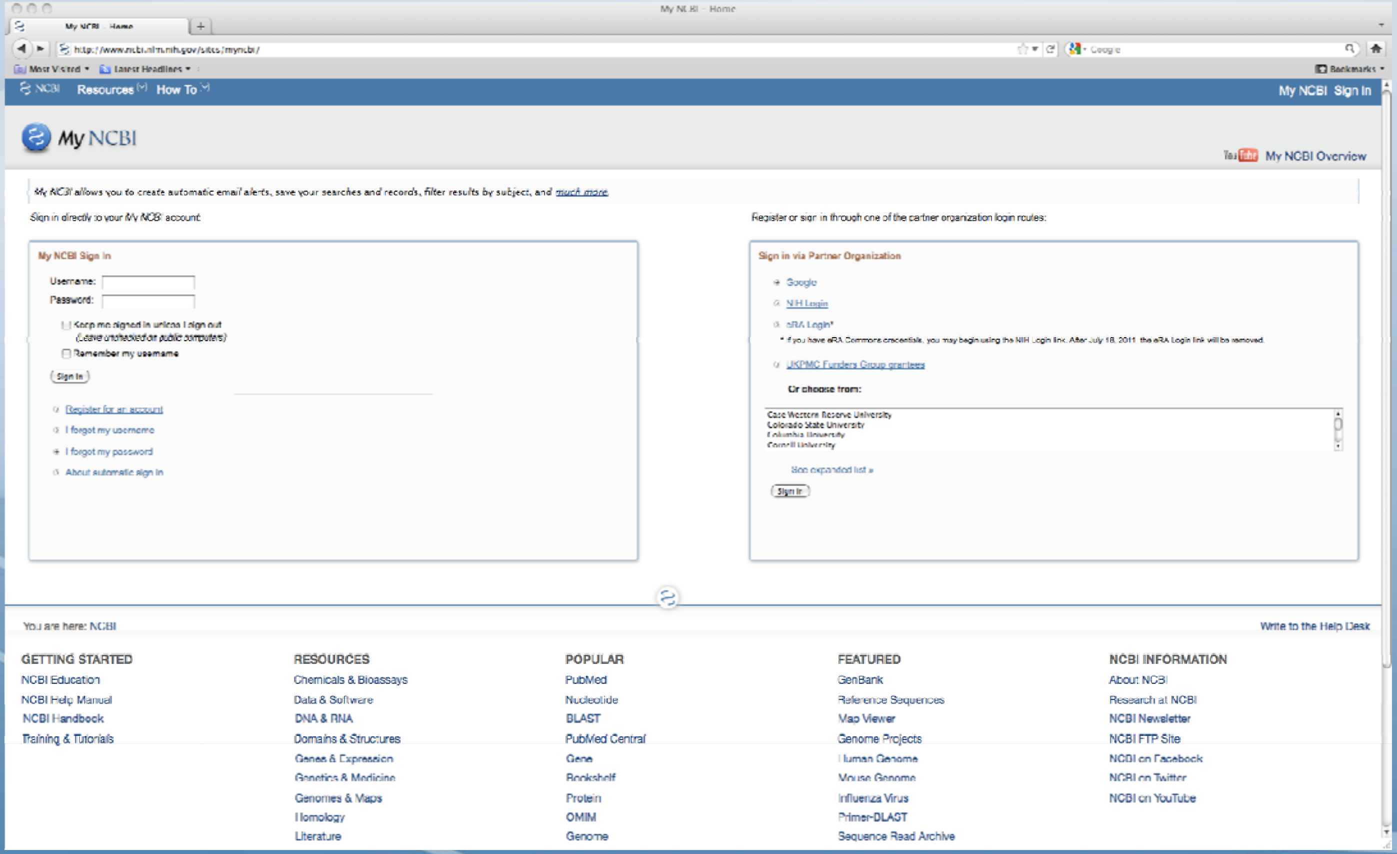
Texas Rangers Today

The Frontiers of Federation

- User Interactions
  - Discovery, Privacy managers, Silver and Gold
- Interfederation
  - Technical and Policy Needs
  - Integration with social Identities
- Integration into IETF protocols – going beyond the web
- Groups and Access Control
- Collaboration Management Platforms
- The Attribute Ecosystem

Discovery

- The process of directing an unauthenticated user back to an organization to be authenticated (happens at new browser launch, not at new window, etc.); already authenticated users are taken directly to the resource
- A non-scalable aspect, especially as the number of federations and IdP's grows exponentially
- An issue to be addressed by an SP
- Today often done by the federation WAYF; users can set cookies to default to IdP, good for up to a year.
- Lots of work in this space, from the new sticky discovery parts of Shibboleth to Google's Account Chooser



My NCBI allows you to create automatic email alerts, save your searches and records, filter results by subject, and much more.

Sign in directly to your *My NCBI* account

My NCBI Sign In

Username:

Password:

□ Keep me signed in unless I sign out
(Leave unchecked on public computers)

□ Remember my username

Sign In

- Register for an account
- I forgot my username
- I forgot my password
- About automatic sign in

Register or sign in through one of the partner organization login routes:

Sign in via Partner Organization

- Google
- NIH Login
- eRA Login*

* If you have eRA Commons credentials, you may begin using the NIH Login link. After July 18, 2011, the eRA Login link will be removed.

- UKPMC Funders Group grantees

Or choose from:

Case Western Reserve University
Colorado State University
Columbia University
Cornell University

See expanded list »

Sign In

You are here: NCBI

Write to the Help Desk

GETTING STARTED
NCBI Education
NCBI Help Manual
NCBI Handbook
Training & Tutorials

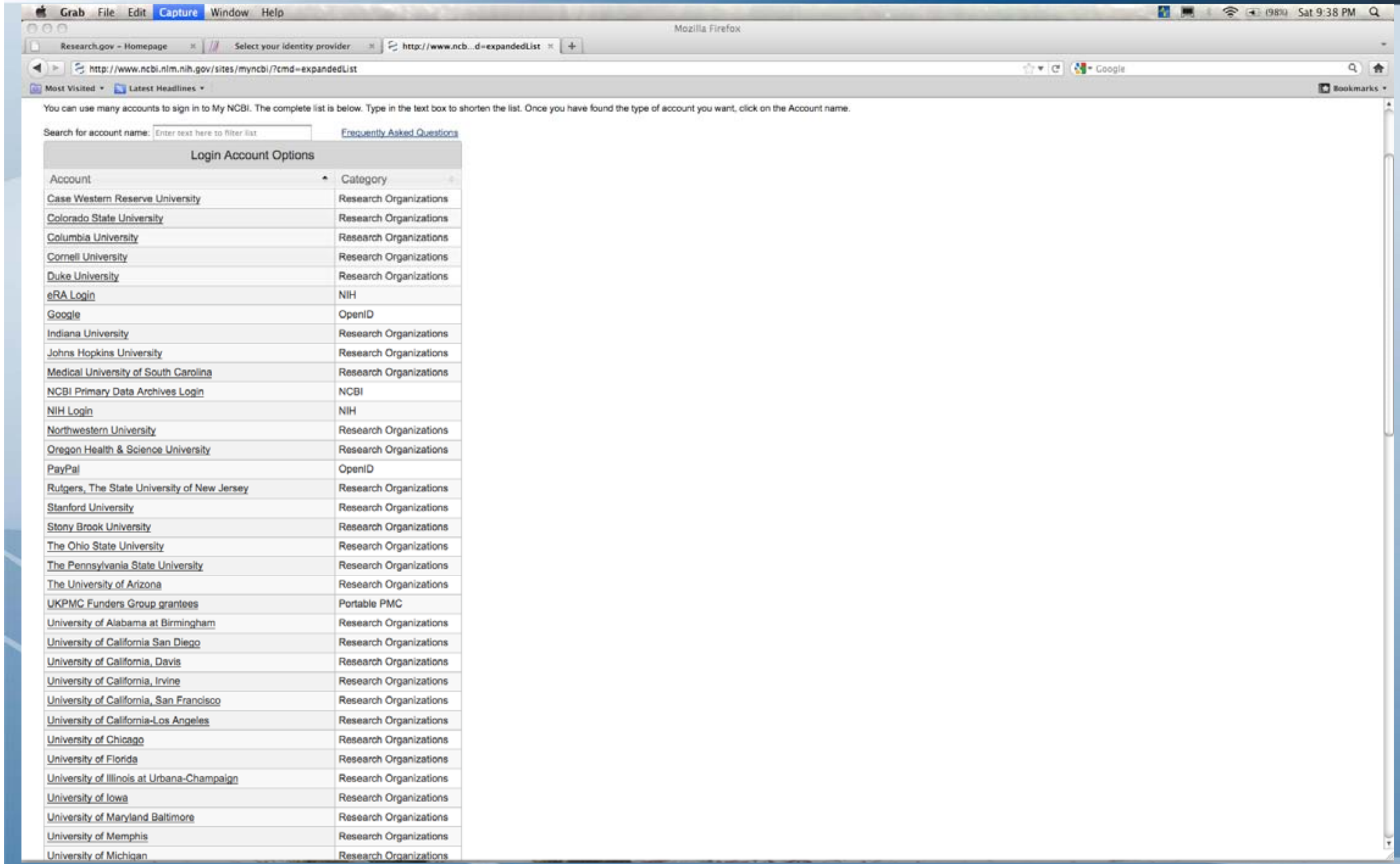
RESOURCES
Chemicals & Bioassays
Data & Software
DNA & RNA
Domains & Structures
Genes & Expression
Genetics & Medicine
Genomes & Maps
Homology
Literature

POPULAR
PubMed
Nucleotide
BLAST
PubMed Central
Gene
Bookshelf
Protein
OMIM
Genome

FEATURED
GenBank
Reference Sequences
Map Viewer
Genome Projects
Human Genome
Mouse Genome
Influenza Virus
Primer-BLAST
Sequence Read Archive

NCBI INFORMATION
About NCBI
Research at NCBI
NCBI Newsletter
NCBI FTP Site
NCBI on Facebook
NCBI on Twitter
NCBI on YouTube

kjk@internet2.edu



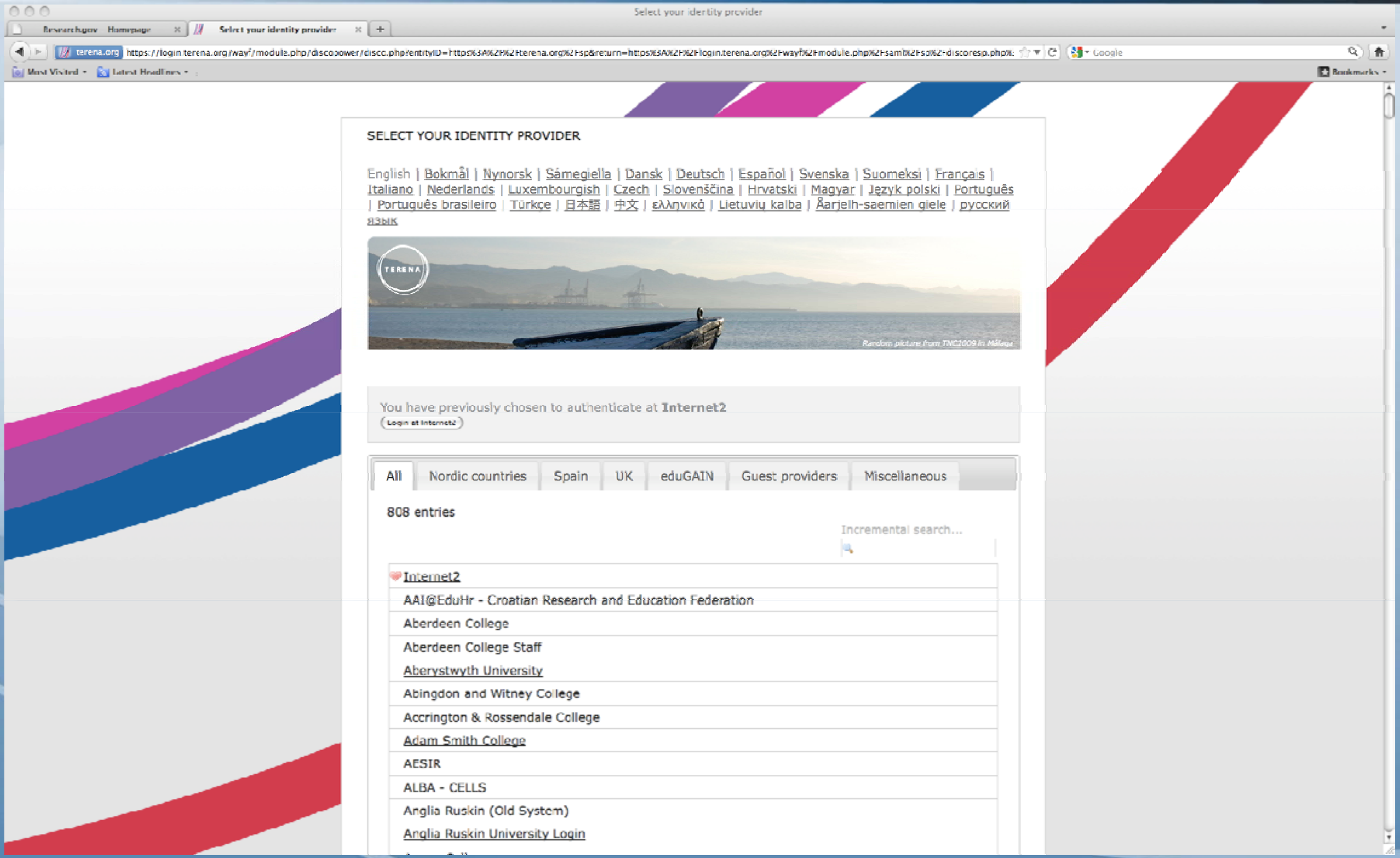
You can use many accounts to sign in to My NCBI. The complete list is below. Type in the text box to shorten the list. Once you have found the type of account you want, click on the Account name.

Search for account name: Enter text here to filter list

Frequently Asked Questions

Login Account Options

Account	Category
Case Western Reserve University	Research Organizations
Colorado State University	Research Organizations
Columbia University	Research Organizations
Cornell University	Research Organizations
Duke University	Research Organizations
eRA Login	NIH
Google	OpenID
Indiana University	Research Organizations
Johns Hopkins University	Research Organizations
Medical University of South Carolina	Research Organizations
NCBI Primary Data Archives Login	NCBI
NIH Login	NIH
Northwestern University	Research Organizations
Oregon Health & Science University	Research Organizations
PayPal	OpenID
Rutgers, The State University of New Jersey	Research Organizations
Stanford University	Research Organizations
Stony Brook University	Research Organizations
The Ohio State University	Research Organizations
The Pennsylvania State University	Research Organizations
The University of Arizona	Research Organizations
UKPMC Funders Group grantees	Portable PMC
University of Alabama at Birmingham	Research Organizations
University of California San Diego	Research Organizations
University of California, Davis	Research Organizations
University of California, Irvine	Research Organizations
University of California, San Francisco	Research Organizations
University of California-Los Angeles	Research Organizations
University of Chicago	Research Organizations
University of Florida	Research Organizations
University of Illinois at Urbana-Champaign	Research Organizations
University of Iowa	Research Organizations
University of Maryland Baltimore	Research Organizations
University of Memphis	Research Organizations
University of Michigan	Research Organizations



Select your identity provider
Research.gov Homepage
Select your identity provider
terena.org
https://login.terena.org/wayf/module.php/discopower/disco.php?entityID=https%3A%2F%2Fterena.org%2Fsp&return=https%3A%2F%2Flogin.terena.org%2Fwayf%2Fmodule.php%2Fsaml%2Fsp%2Fdiscoresp.php%
Google
Most Visited
Latest Headlines
Bookmarks

SELECT YOUR IDENTITY PROVIDER

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Español | Svenska | Suomeksi | Français | Italiano | Nederlands | Luxembourgish | Czech | Slovenščina | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 中文 | ελληνικά | Lietuvių kalba | Åarjelh-saemien giele | русский язык

TERENA
Random picture from TNC2009 in Málaga

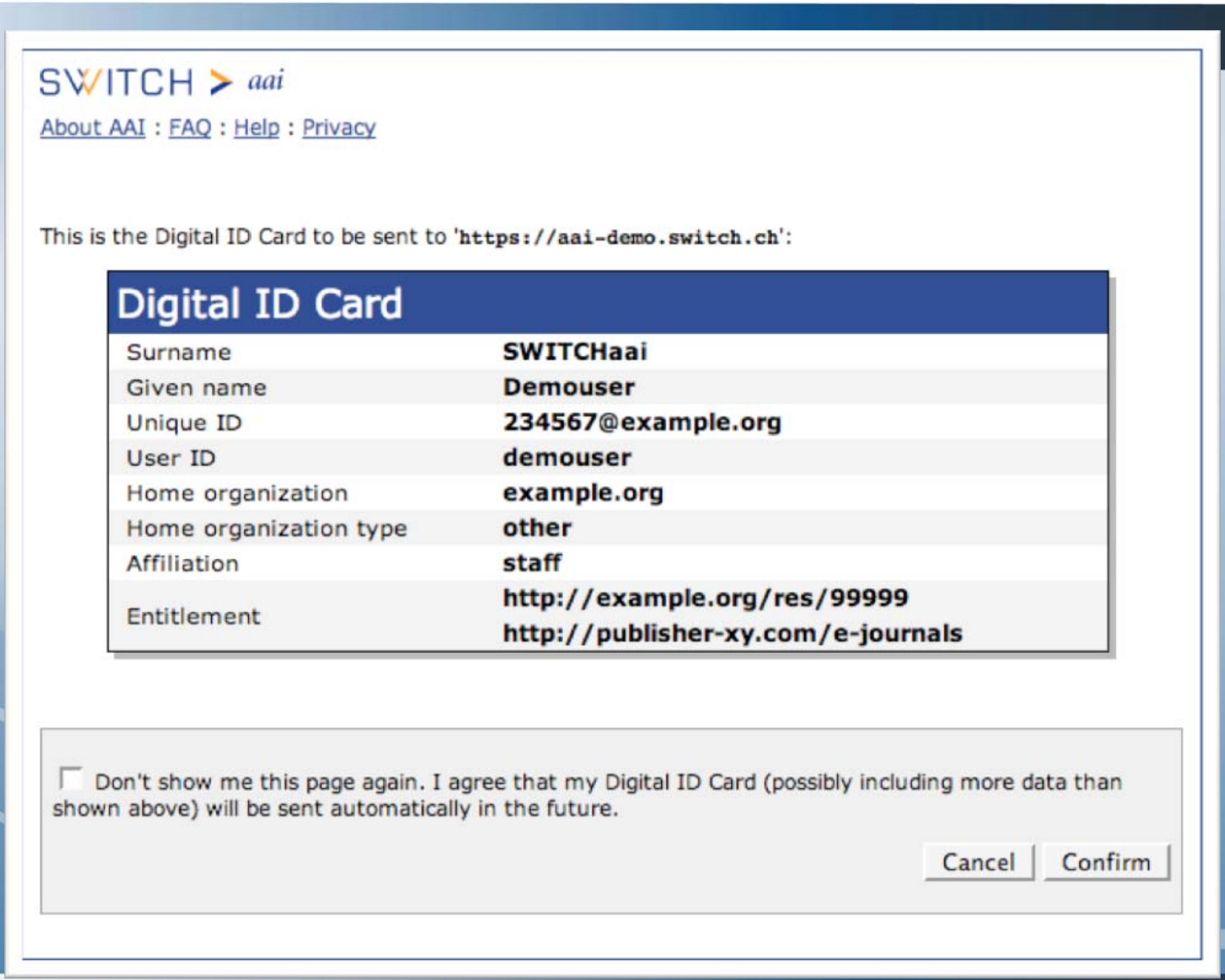
You have previously chosen to authenticate at **Internet2**

808 entries

- Internet2
- AAI@EduHr - Croatian Research and Education Federation
- Aberdeen College
- Aberdeen College Staff
- Aberystwyth University
- Abingdon and Witney College
- Accrington & Rossendale College
- Adam Smith College
- AESIR
- ALBA - CELLS
- Anglia Ruskin (Old System)
- Anglia Ruskin University Login

User managed privacy

- Provide users with control, and guidance, over the release of attributes
  - Includes consent, privacy management, etc.
  - Using opaque identifers (content providers, wikis), visible identifiers (wikis, TG, LMS, financial services), entitlements (content providers, VO's), etc.
- Basic controls (uApprove) now built into Shibboleth, but largely untapped in deployments.
- Human interface issues largely not yet understood – getting the defaults right, putting the informed into informed consent, etc.



This is the Digital ID Card to be sent to '`https://aai-demo.switch.ch`':

Digital ID Card

Surname	**SWITCHaai**
Given name	**Demouser**
Unique ID	**234567@example.org**
User ID	**demouser**
Home organization	**example.org**
Home organization type	**other**
Affiliation	**staff**
Entitlement	**http://example.org/res/99999** **http://publisher-xy.com/e-journals**

□ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Silver and Gold

- Applications are beginning to request higher levels of authentication for important transactions
  - Grant administration, access to sensitive data, grids, etc.
- Can be a painless personal process and a painful institutional process
  - Personal use of two factor authentication and better one-time identity proofing
  - Institutionally, the need to document processes, record events, audit, etc.

Interfederation

- Connecting autonomous federations
- Critical for global scaling, accommodating state and local federations, integration across vertical sectors
- Has technical, financial and policy dimensions
- Technical solutions include eduGAIN and MDX
- Policy activities in eduGAIN, Kalmar2 Union, Kantara, Refeds

MDX/PEER – metadata exchange protocol

- Institutions and organizations will pick a registrar to give their metadata to
- Institutions and organizations will pick an aggregator (or several) to get their partners metadata from
- Aggregators exchange metadata with each other and registrars
- If this sounds like DNS registration and routing, it is, one layer up

Social to SAML Gateways

- A way to bring social identities (e.g. Google, MSN, Facebook, etc.) into the federated world
- Answers many, many use cases
  - Parent access to university student bills
  - Outreach of science organizations to broader communities
  - Citizens to government services
- Software developed by Sweden et al and is being deployed at several levels

Groups and Access Control

- Federated identity creates the need for tools to manage the access control at the resources; lists of 1,000 permitted federated users are a drag to maintain.
- Groups set at the identity provider can be expressed as attributes for simple but powerful access control at resources.
- Groups need to handle federated users and themselves be federated; they need to work the same for social and organizational use cases
- Most organizations have more groups than users…
- One of the true frontiers and urgent given the scale of users

Thinking beyond the web

- All those mobile devices
- All those infrastructure elements – routers, firewalls
- Lots of apps want to leverage federated identity
- Several approaches at work
  - Using Oauth to pass a token from web to app
  - Project Moonshot to modify IETF protocols (GSSAPI, EAP, etc) to provide a broad set of app opportunities
    - Two possible transports – Radius and SAML

Collaborations and Virtual Organizations

- IdM is a critical dimension of collaboration, crossing many applications and user communities
- Virtual organizations represent critical communities of researchers sharing domain resources and applications as well as general collaboration tools. Providing a unified identity management platform for collaboration is essential in a multi-domain, multi-tool world.
- Lots of activities in domesticating applications to work in a federated world, moving from tool-based identity to collaboration-centric identity.

Collaboration Platforms

- Integrated set of collaboration apps (wikis, listprocs, CVS, file share, calendaring, etc)
- Integration of at least identity and access control via group memberships
- Extends identity and access controls to domain apps
- Repackages successful enterprise technologies for a collaborative/project/VO setting
  - Federated identity, group management, directories, and security token services (aka credential convertors)
  - Allows integration of VO and enterprise IdM

The Attribute Ecosystem

- Authentication is very important, but identity is just one of many attributes
- And attributes provide scalable access control, privacy, customization, linked identities, federated roles and more
- We now have our first transport mechanisms to move attributes around – SAML and federations
- There will be many sources of attributes, many consumers of attributes, query languages and other transport mechanisms
- Together, this attribute ecosystem is the “access control” layer of the Internet
- Discussions began with the Tao of Attribute workshop and are finally active at Kantara, ISOC, IIW, etc.

Back to the Frontier

- Much remains to be discovered
- The excitement of the exponential
  - Its not hard for 100, but we’re talking 3 Billion
- Lacking some basic utilities
- Has uncertain policy territory
- Is always worth the ride

Time for me to go home…

kjk@internet2.edu