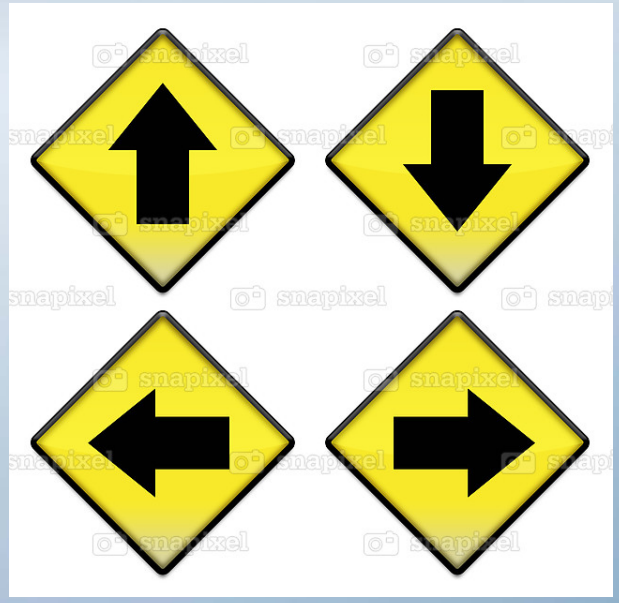
Internet identity: Forward in All Directions



Dr Ken Klingenstein,
Director, Middleware, Internet2

INTERNET2®

What's Happening

- Exponential growth in Federated Identity
- Exponential growth in Social Identity
- Integration of Internet identity
  - Interfederation
- The rise of attributes
  - For privacy, scalable access control

kjk@internet2.edu

Key players

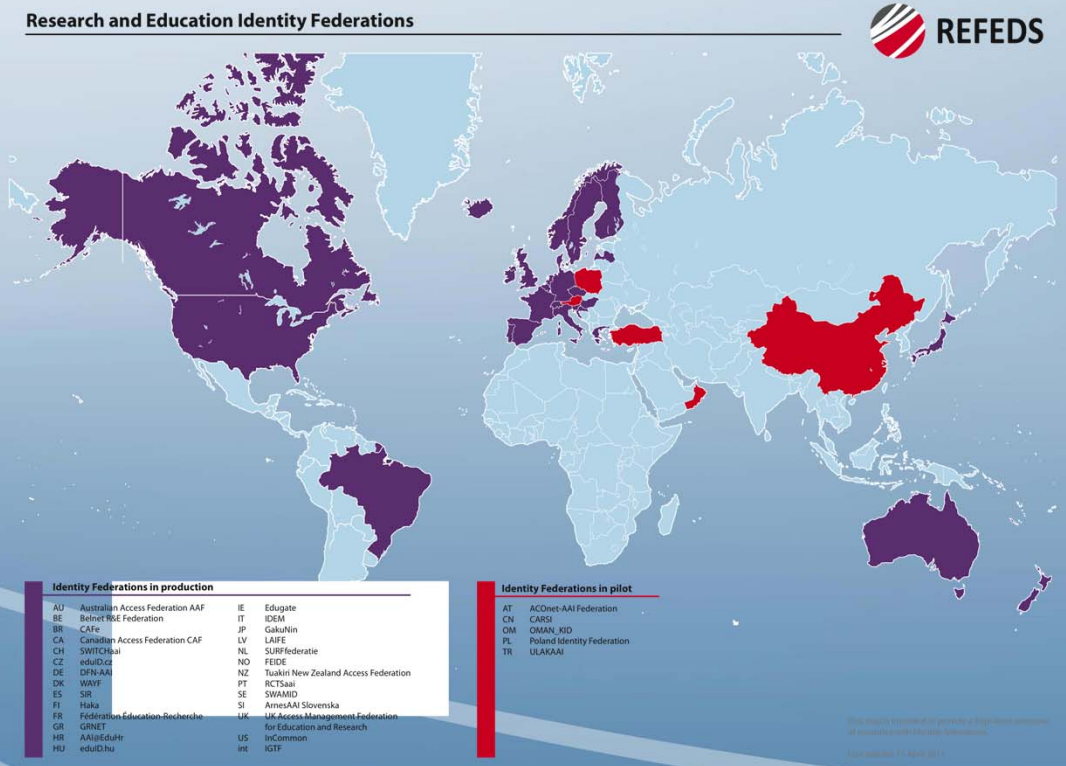
- NSF and the R&E community
- Google, MS, Paypal, etc.
- Mobile operators
- Government efforts
  - NSTIC, White House and NIST in US
  - STORK, etc in Europe
  - T-scheme in UK
- Standards groups – ISOC and IETF, OASIS, etc.

Federated Identity

- The now classic SAML 2.0 based meta-data driven trust federation, typically with a specified schema (eduperson+)
  - Shibboleth, OpenSAML, SimpleSAML, MS ADFS
- Thousands of applications now, from content-distribution to outsourced services, from access to supercomputers to access to national research grants, from student aid to student travel, from wikis to cloud services
- Started with NSF funding in R&E, but now has crossed over to health and medical, real estate, government, international electronic banking, and more.
- The infrastructure to provide leverage for other forms of identity

kjk@internet2.edu

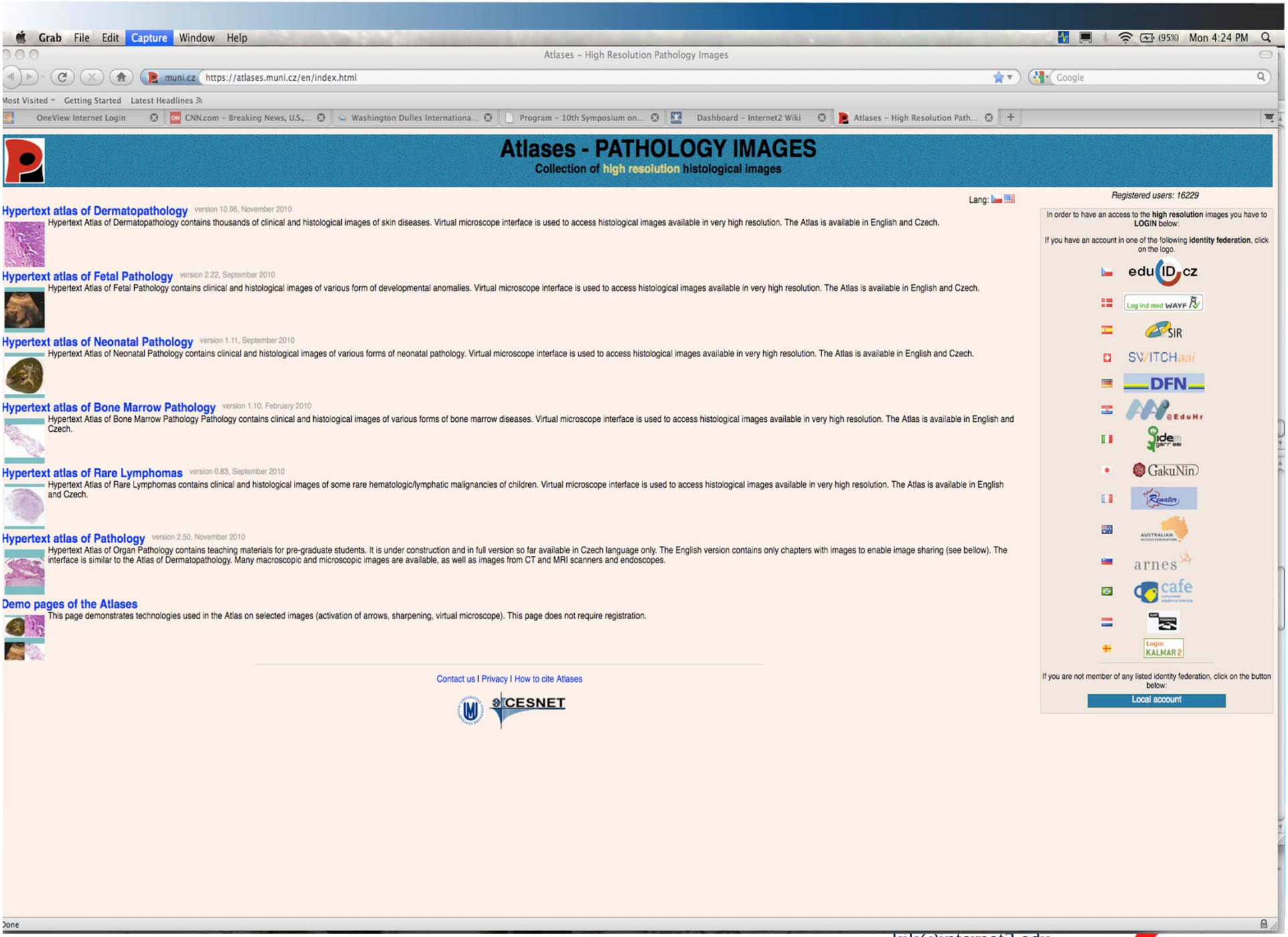
R&E Federations



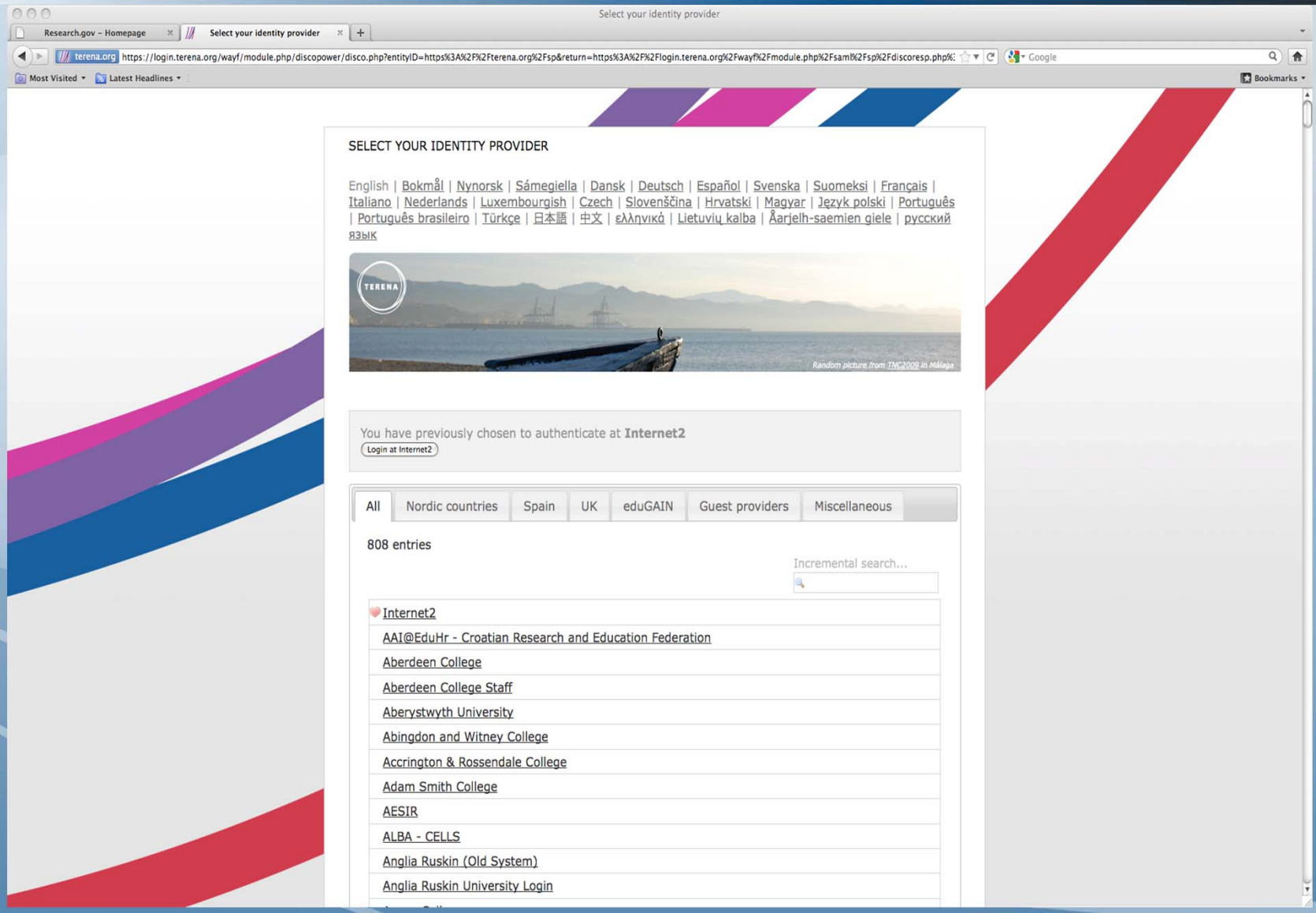
kjk@internet2.edu

International R&E federations

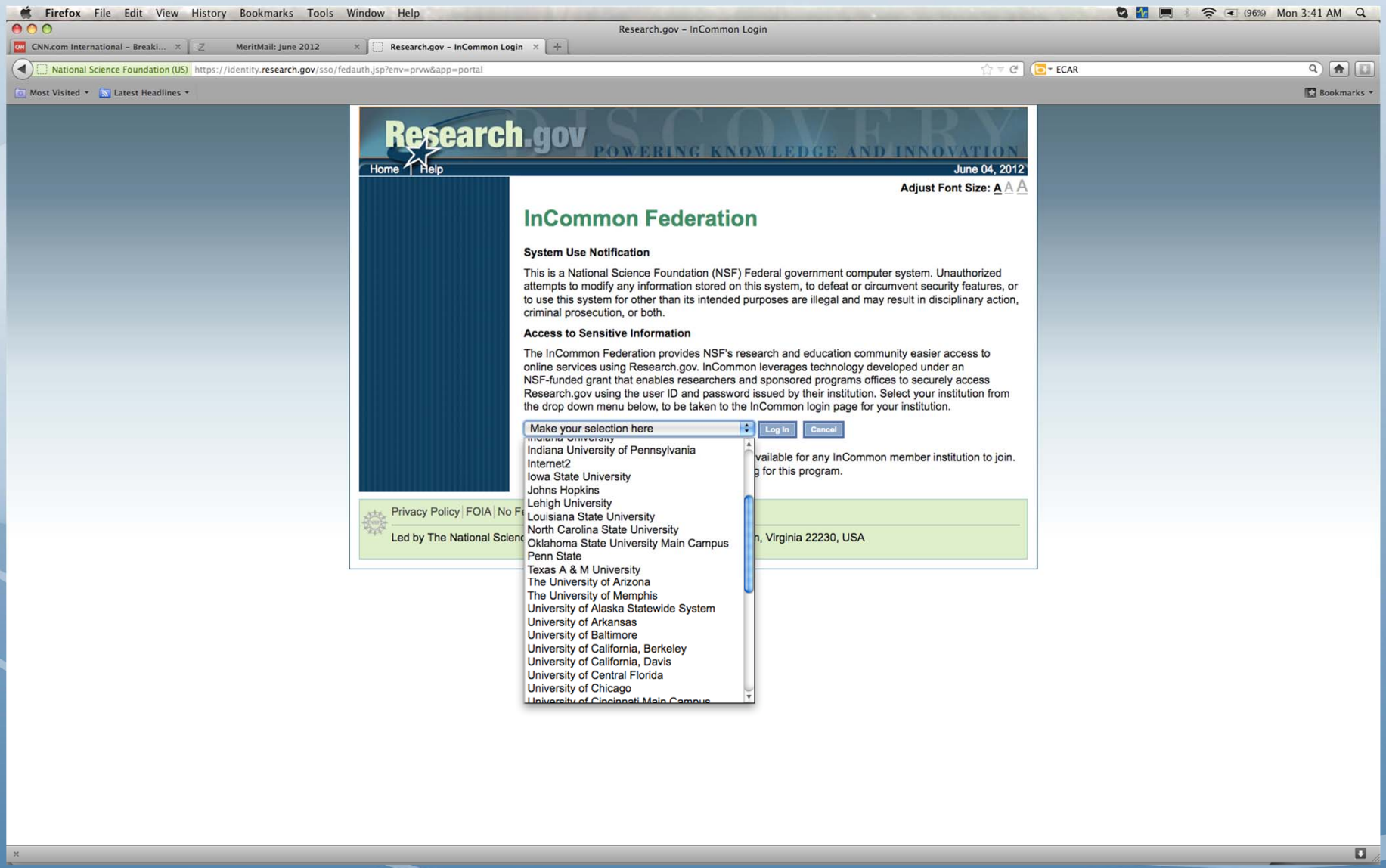
- > 100M users across >30 countries
- Coverage in several countries is 100%, and extensive in many others.
- Generally part of a national network but associated with another org or independent in a few
- Frequently linked to several government activities, in research, education, governance, health, etc.
- Some interfederation activities, including the Kalmar2 union and eduGAIN.
- www.refeds.org



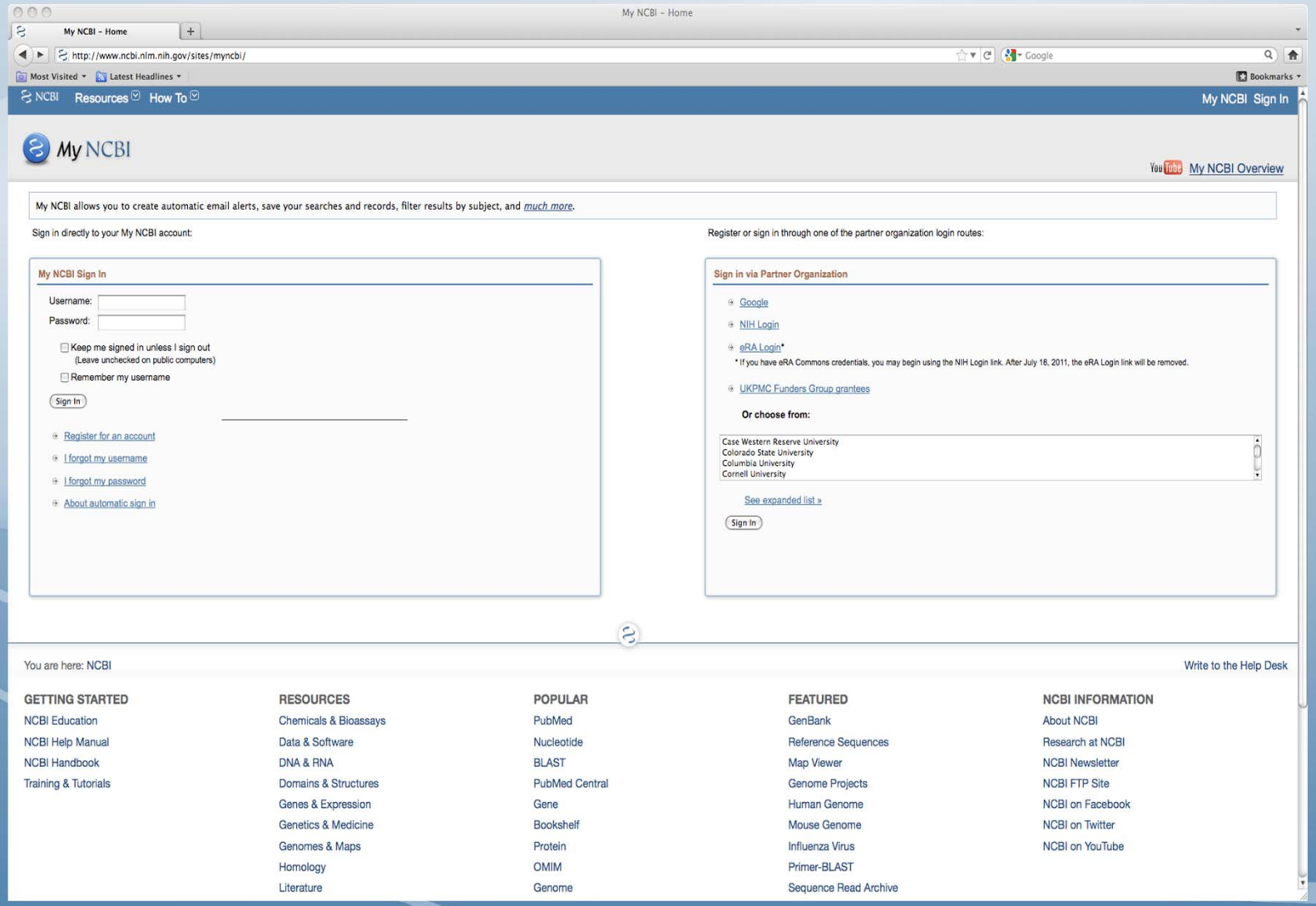
kjk@internet2.edu



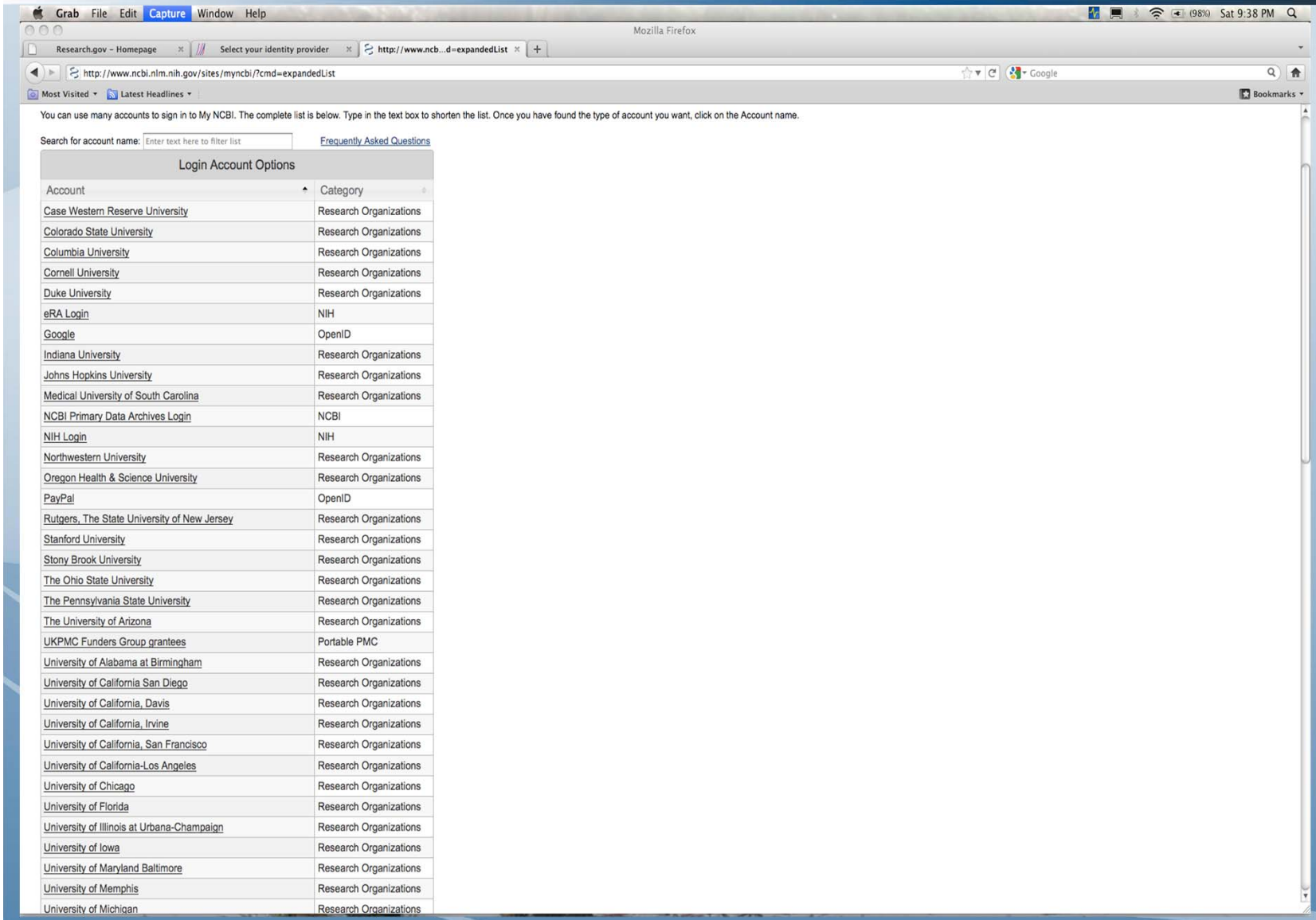
kjk@internet2.edu



kjk@internet2.edu



kjk@internet2.edu



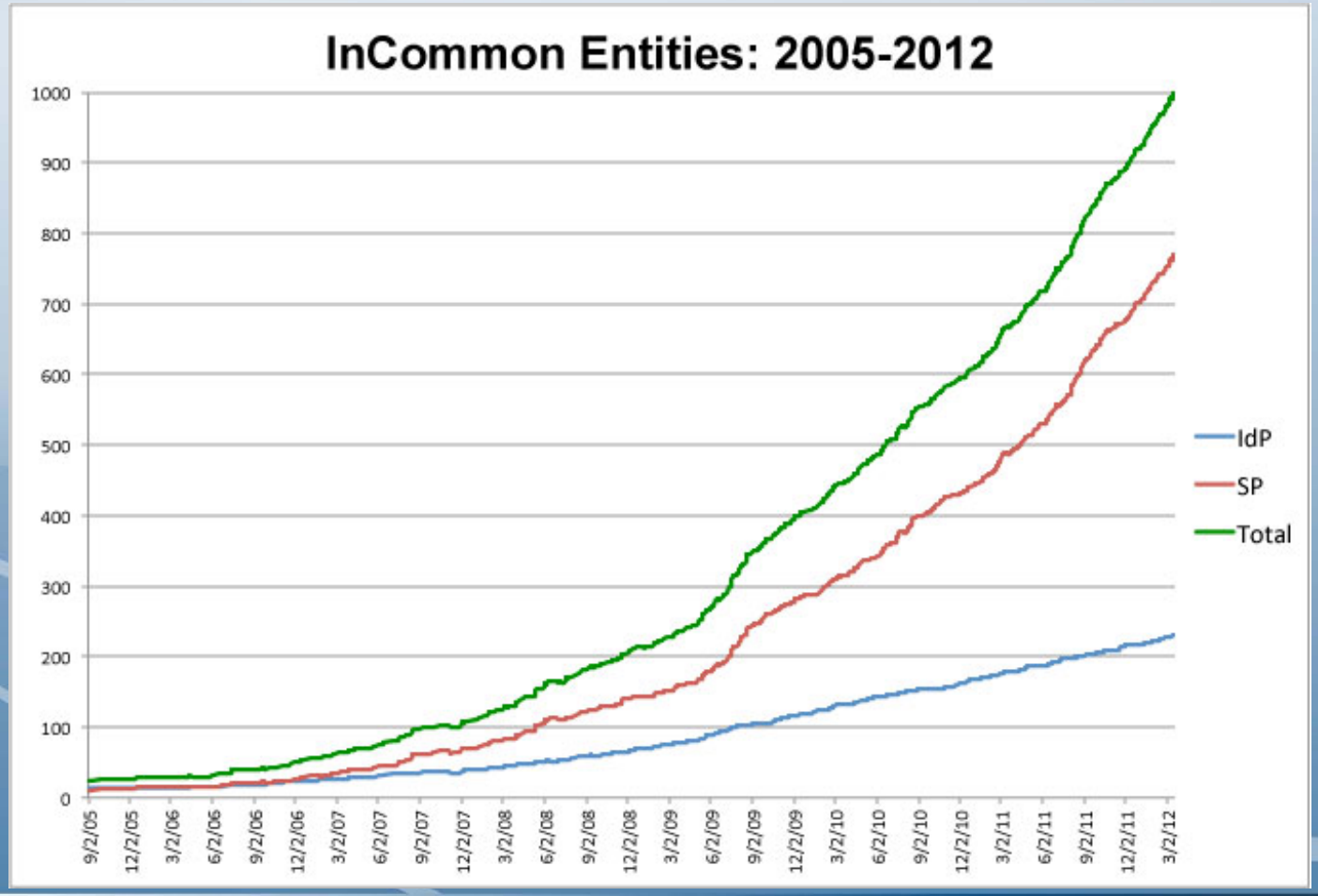
kjk@internet2.edu

InCommon today

- 300+universities, 450+total participants, growth continues rapid
- > 10 M users
- Traditional uses continue to grow:
    - Outsourced services, government applications, access to software, access to licensed content, etc.
- New uses bloom:
    - Access to wikis, shared services, cloud services, calendaring, command line apps, medical, etc.
- FICAM certified at LOA 1 and 2 (Bronze and Silver).
- Certificate services bind the InCommon trust policies to new applications, including signing, encryption, etc.

kjk@internet2.edu

InCommon Growth



kjk@internet2.edu

Types of services connected by InCommon

- R&E Centric
  - 300+ Universities providing services to students, staff, alumni, external users, K-12, etc.
  - NSF, NIH, National Supercomputing and DataBases, National Labs, GSA, Education, Veterans, etc.
- With outsourced content and service providers
  - OCLC, JSTOR, Travel management, Testing Services, HR systems, Loan providers, Parking management, NBCLearn, Elsevier, IEEE, ATT, Box, etc.
- With related business partners
  - Particularly health care – NIH, Mayo Clinic, UHC, VA
- With markets selling to students, etc.
  - Student Universe, UniversityTickets, National Student Clearinghouse, SAT's

kjk@internet2.edu

A typical enterprise-InCommon use profile

- Academics use it to get to Elsevier journals, OCLC holdings, IEEE, etc
- Staff use it to get to the cloud and do their employee/payroll entry
- Students use it to take on-line class tests at an outsourced test service
- Researchers use it to get to Grants.gov and Fastlane
- Researchers use it to get to CIlogon and use the Teragrid , Open Science grid, etc.
- Researchers use it to get to the Clinical Trial wikis at NIH, PubMed, etc.
- Many collaborators and administrators use it to get shared wiki space at Internet2, Educause, the CIC, the UC system, the UT system…
- Students are using it for student tickets, software at Microsoft, etc

kjk@internet2.edu

South – Social Identity

- A very large and fragmented marketplace
- Some key players are more on the sidelines – Facebook, Twitter, etc
- Most other key players engage in OIX (OpenId Exchange) – Google, Yahoo, Microsoft
  - Evolving protocol settling into OpenIdConnect
  - Looking at partnerships for higher LOA, e.g. with mobile, postal service, etc.
- Exploring what the marketplace is
  - In a landscape where each vendor wants to own it…

kjk@internet2.edu

Key Directions in Social Identity

kjk@internet2.edu

Social Identity – Key Directions

- Getting technical interoperability, including those not yet in
  - Dealing with the new complexities, needs for profiles, etc
- Alliances for better LOA and attributes
  - Mobile and IdP/email provider
  - Banks and IdP/email provider
- Getting a proper marketplace for identity
- Marketplace for attributes - Monetization

kjk@internet2.edu

A Proper Marketplace for Identity

- Who pays for services
  - The service provider, the user directly, the user indirectly (perhaps through tracking and advertizing)
- Who competes to provide services
  - Monopoly, big dogs, a marketplace
  - Will set directions for interfaces, discovery, innovation, low barriers to entry
- Who sets the rules
  - About security and privacy of data
- And what does it cost?

kjk@internet2.edu

A Proper Marketplace for Attributes

- Some attributes can have broad monetary value, e.g. verified postal address, over legal age, current location
- Who owns these attributes? How are they verified? When is consent necessary to release them? What form does consent take?
- Who can “buy” them? What are the rules of use? Who makes money?
- First markets being tested now…

kjk@internet2.edu

Integration of Internet identity: federation and social

- Ability to deploy a variety of identity types to solve a use case
- Gateways and other approaches to credential conversion
  - PIV in federation
  - Social2SAML gateways
  - SAML2Social gateways
- Integration opportunities increase with OpenId Connect

kjk@internet2.edu

What's coming

- Privacy managers
- Interfederation
- Anonymous credentials

kjk@internet2.edu

Interfederation

- PKI is globally scalable
  - Unfortunately, its not locally deployable…
- Federation is locally deployable
  - Can it scale globally?
- Inter-federation
- Like BGP, only 1000 times harder

Interfederation

- Connecting autonomous identity federations
- Critical for global scaling, accommodating local federations, integration across vertical sectors
- Has technical, financial and policy dimensions
- Several operational instances – Kalmar2 Union, eduGAIN, ad hocs (UC Trust, Texas)
- Use cases now numerous, across sectors, within sectors
- Short-term and long-term approaches
- If its called the Internet, shouldn't the marketplace start talking about "interfederated identity"

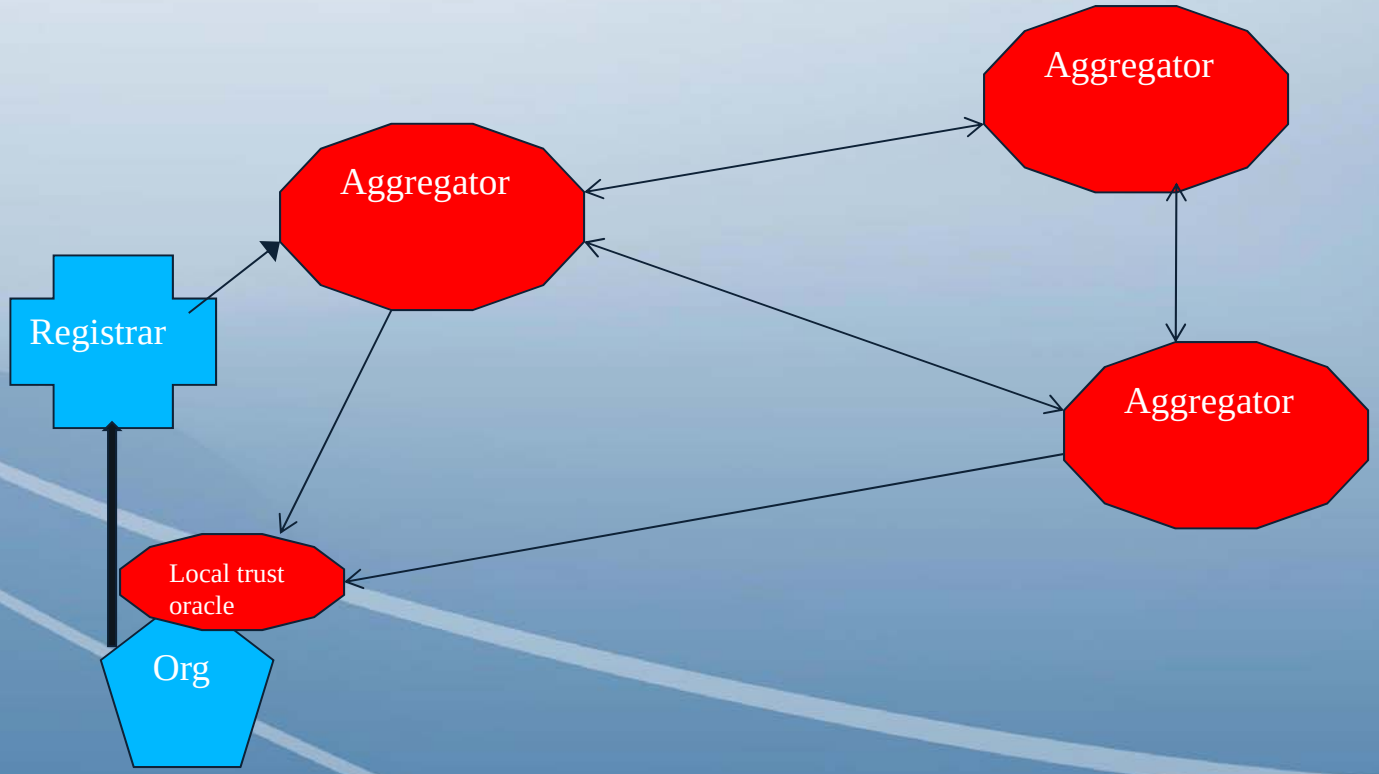
kjk@internet2.edu

Buckets of interfed issues

Both short-term and long-term approaches must address:

- Exchange, and massage, of metadata
- Policy alignment
- Alignment of payloads (attributes)
- Operational issues – error handling, incident handling, legal and contractual, etc

Future metadata flows in Interfederation



kjk@internet2.edu

Emerging key software and protocols

- MDA – metadata aggregator
- PEER – metadata registry management software
  - There may be multiple PEER services instances
- MDX – the query protocol(s) to request metadata; return via normal publishing protocols
- Improved discovery services – accountchooser, discojuice, embedded discovery services
- End-entity categories – an important new type of metadata, allowing for certified apps and IdP's.

Interfed policy areas

- Federation operations
  - Legal status and bone fides
  - Operational issues – signing key and metadata protection, incident handling, etc
- Federation to member relationships
  - Contractual
  - Vetting of members and delegation of metadata
- Community standards
  - LOA
  - End-entities and vetting values
  - Attribute bundles
- IdP-SP direct relationships
  - What issues do they work directly? If they have a contract? If they don't

kjk@internet2.edu

Is interfederation getting harder?

- Or, as Ian says, do we just understand the problem better?
- In the old days, just exchange signing keys
- Now, do you understand my metadata? My attribute bundles? My application categories and how I assess apps? My policies
- And do I understand yours?
- And with more use cases every day…

User Contexts

- Individuals do trusted Internet transactions in a variety of contexts
  - The enterprise/federated use of identity well-established; may be enhanced with roles
  - Consumer
  - Citizen
  - Geo-temporal
  - Personal “wallet” – preferred language, accessability, etc
  - Others?
- Same identity; different roles; different policies and governance on privacy, etc

kjk@internet2.edu

Scalable privacy

- Small spanning set of attributes
  - Extensible but end-user manageable
  - Use of bundles to minimize complexity
- Rich metadata for trusted dialogue
  - Defaults, learning to minimize dialogues
  - Putting the informed into informed consent
- End user privacy manager with quality UI, some out of band consent, getting the defaults right
- Integration of federated and anonymous credentials

At the center, integration

- Across user contexts
- Across devices and platforms
- Across millions of users and sites
- Across federated and anonymous credentials
- Through portals and gateways
- Leveraging the common business processes
- Making the market

kjk@internet2.edu

Impacts

- A true global layer on top of the original Internet
  - Connecting people, not machines
  - Close to the wetware, so lots of policy
- Number of users >> 1 billion
- Moving towards 2-factor authentication
- Exposes inconsistencies in policy, behavior, etc.

kjk@internet2.edu

A personal comparison

- The original Internet was massively consequential but relatively technically thin
  - Intentionally kept the technology simple
  - Most of the work was in making the marketplace of equipment, applications and users, and businesses.
- This Internet identity stuff is very, very important but relatively rich in issues
  - A result of working so close to the wetware, connecting people not machines
  - How much work will making the marketplace be?

kjk@internet2.edu

kjk@internet2.edu