Federated Identity, with a side of Scholar

Dr Ken Klingenstein,
Director, Middleware and Security, Internet2

INTERNET®

Topics

- Federated identity
  - Cleansing the palate with social identity
  - InCommon today
  - International R&E and US Gov federations
  - The next steps
    - Assurance
    - Its all about attributes
    - Interfederation
- A Side of Scholar
  - Research and Collaboration platforms, data set access, scholarly identity, aligning business processes, integration with LMS and library systems

Consumer marketplace update

- Several major “identity providers” (Google, Paypal, Yahoo) attempting to converge on a new standard, OpenId Connect.
  - OIX (Open Identity Exchange) is the hub
  - Technically Shibboleth++ redone in JSON
  - Uses SAML attributes and SAML metadata, allowing integration
  - Differs on discovery, marketplace vision, governance
  - Some are coupling with mobile operators for higher LOA, seeking federal certification
- Others sitting on sidelines – Facebook, Twitter

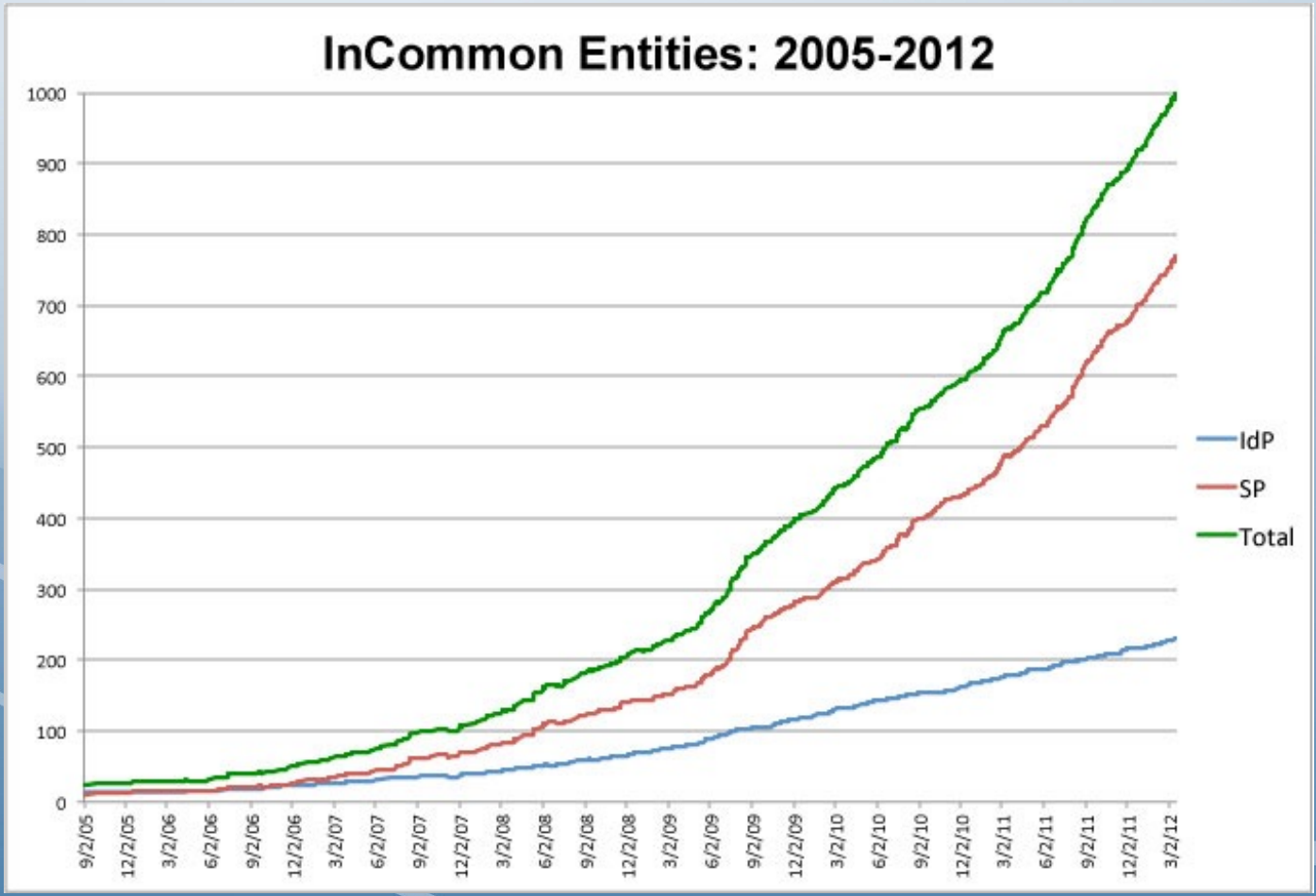
Integration of Internet identity: federation and social

- 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

InCommon today

- 290+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.

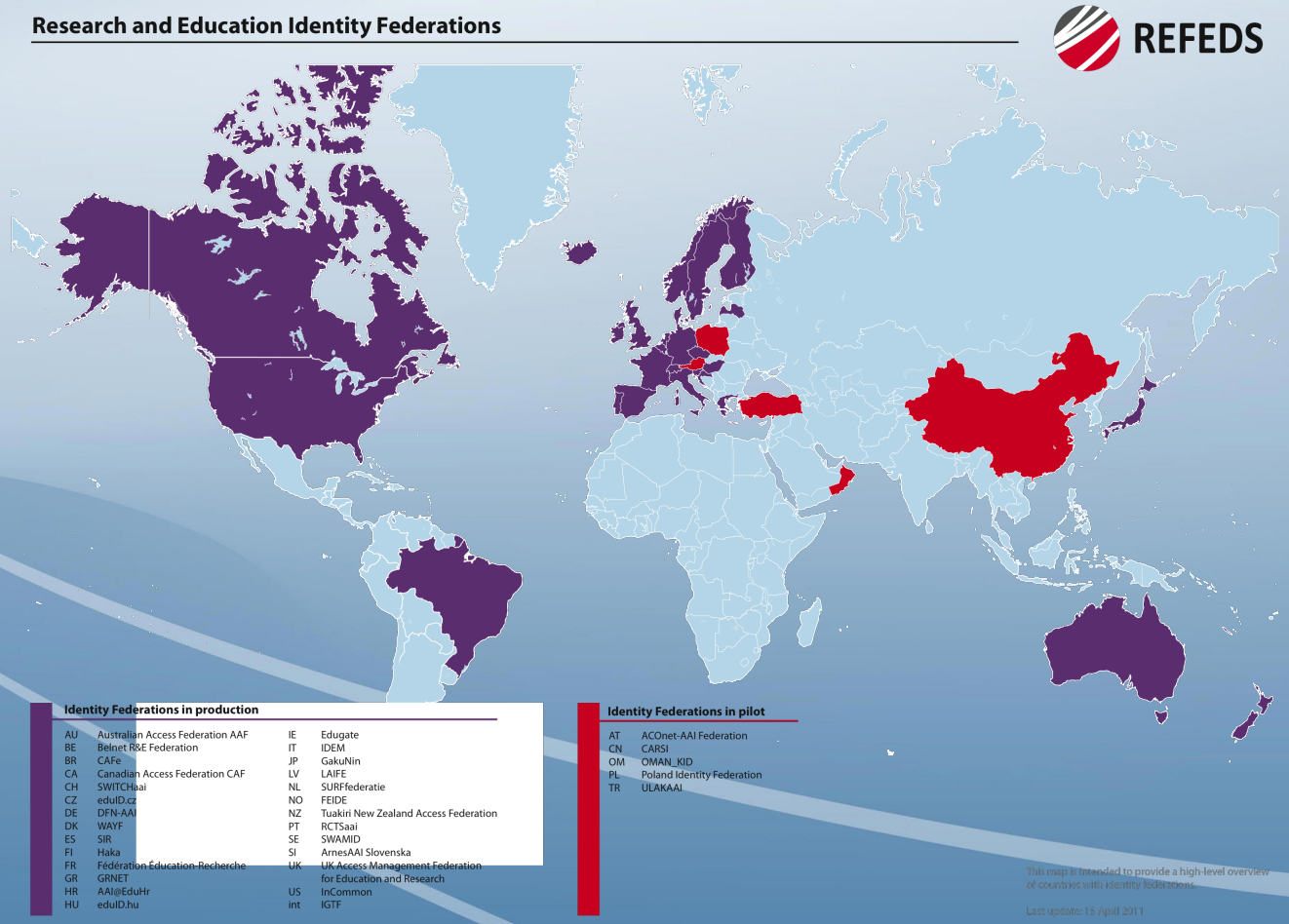
Growth


InCommon Entities: 2005-2012
1000
900
800
700
600
500
400
300
200
100
0
9/2/05
12/2/05
3/2/06
6/2/06
9/2/06
12/2/06
3/2/07
6/2/07
9/2/07
12/2/07
3/2/08
6/2/08
9/2/08
12/2/08
3/2/09
6/2/09
9/2/09
12/2/09
3/2/10
6/2/10
9/2/10
12/2/10
3/2/11
6/2/11
9/2/11
12/2/11
3/2/12
IdP
SP
Total

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

R&E federations



INTERNET2®

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

Grab File Edit Capture Window Help (95%) Mon 4:24 PM

Atlases – High Resolution Pathology Images

muni.cz https://atlases.muni.cz/en/index.html

Most Visited Getting Started Latest Headlines

OneView Internet Login | CNN.com – Breaking News, U.S.,... | Washington Dulles Internationa... | Program – 10th Symposium on... | Dashboard – Internet2 Wiki | Atlases – High Resolution Path...

Atlases - PATHOLOGY IMAGES

Collection of high resolution histological images

Lang:

Hypertext atlas of Dermatopathology

version 10.96, November 2010

Hypertext Atlas of Dermatopathology contains thousands of clinical and histological images of skin diseases. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Fetal Pathology

version 2.22, September 2010

Hypertext Atlas of Fetal Pathology contains clinical and histological images of various form of developmental anomalies. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Neonatal Pathology

version 1.11, September 2010

Hypertext Atlas of Neonatal Pathology contains clinical and histological images of various forms of neonatal pathology. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Bone Marrow Pathology

version 1.10, February 2010

Hypertext Atlas of Bone Marrow Pathology Pathology contains clinical and histological images of various forms of bone marrow diseases. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Rare Lymphomas

version 0.83, September 2010

Hypertext Atlas of Rare Lymphomas contains clinical and histological images of some rare hematologic/lymphatic malignancies of children. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Pathology

version 2.50, November 2010

Hypertext Atlas of Organ Pathology contains teaching materials for pre-graduate students. It is under construction and in full version so far available in Czech language only. The English version contains only chapters with images to enable image sharing (see bellow). The interface is similar to the Atlas of Dermatopathology. Many macroscopic and microscopic images are available, as well as images from CT and MRI scanners and endoscopes.

Demo pages of the Atlases

This page demonstrates technologies used in the Atlas on selected images (activation of arrows, sharpening, virtual microscope). This page does not require registration.

Contact us I Privacy I How to cite Atlases

CESNET

Registered users: 16229

In order to have an access to the **high resolution** images you have to **LOGIN** below:

If you have an account in one of the following **identity federation**, click on the logo.

eduID.cz
Log ind med WAYF
SIR
SWITCHaai
DFN
AAI EduHr
idem gerr aai
GakuNin
Renater
Australian Access Federation
arnes
cafe
Login KALMAR2

If you are not member of any listed identity federation, click on the button below:

Local account

Done

Next Steps for Federated Identity

- Patron systems and LMS as IdP's
  - Impacts on growth, on policies, on schema
- Silver – higher levels of assurance
- Attribute release bundles – the R&S bundle
  - Improved discovery everywhere…
- Non-web apps
- Interfederation
- Internet-scale access control

Bundles and Application Categories

- Attributes tend to travel in bundles
  - The R&S (research and scholarship) bundle
    - {name, email, authenticated identity, affiliation}
  - Applications are being vetted for minimal use and qualification for R&S
  - Attribute release “automatic” by IdP
- Several bundles are likely, e.g. {opaque-id, affiliation}, {authentication only}, privacy-preserving-personalization

Interfederation

- Connecting autonomous identity federations
- Critical for global scaling, accommodating state and local federations, integration across vertical sectors
- Several operational “instances” – Kalmar2 Union, eduGAIN
- Has technical, financial and policy dimensions
- Key technologies moving forward – PEER, MDX, metadata enhancements and tools, discovery

Value Added Services and Net+

- Demand aggregation is a very powerful tool
- Federation helps make demand aggregation much more viable
  - Single sign on
  - Automatic provisioning/deprovisioning
  - Groups for access control and close integration with institutional middleware
  - Negotiate once, use many times
  - Leverage existing contracts
- Remarkable savings – discounts of 60-98%

A Side of Scholar

- Attribute management for collaboration
  - The R&S bundle
  - Eduperson and the ORCID identifier
- Cyberinfrastructure
  - CIlogon - www.cilogon.org - bridging federated logon with national computational resources
  - Social to SAML gateways
  - Science Agency data set access controls
- Collaboration platforms
  - VO IdM + “domesticated applications”
  - Enrollment services
- Integration around the scholarly record
  - LTI, VIVO, etc.
- Leverage, leverage, leverage

Attribute management

- The R&S bundle is intended precisely for collaboration and scholarship
  - Hugely eases the boarding process for new apps by giving IdP's defaults for necessary attribute release
  - Qualified apps include most R&S services
- Eduperson normative university schema
  - Should it include the ORCID identifier?
  - If so, how would it be populated?
  - If so, how can it be leveraged?
- Others?

Data lifecycle access management

- Agencies call for research data management plans but neglect long-term access control issues
- Not all data is public – sensitive, PHI, international or private, etc.
- Access controls may change over time, by policy or sale or types of devices or …
- Access controls are needed
  - Scalable
  - Linkable identities

Integration around the scholarly record

- Campus scholarly systems, whether home-brew, emerging open-source or commercial product, needs enterprise authentication and basic access controls
- Trusted citations
- Integration of scholarly API's (e.g. LTI) with federated richness
- ScienCV

Opportunities

- For leverage
  - The value of a unique disambiguated identifier
  - Federation entity metadata
- For aligned biz processes
- For sustainability
  - What's the scholarly services Net+ package?

Some thoughts

- InCommon/I2 interest is not discovery of data, not content or taxonomies but access to content
- Future – rich metadata for discovery, ontology tools and mapping but not complex access controls on the data
  - Conservation of policies
  - Not a XACML in real life freak

- What we mean by metadata
  - End-entity services in the federation
  - Associated metadata – Incident handling, MDUI, Feh
- Using the metadata tools and trust, but operating separate repositories of metadata (by domains or clusters or…)

- Specific alignment of biz processes
  - Membership, subscription, delegation, etc
  - Contracts, liability and indemnification
- Scholarly net+ services – expansive in vision but select in choices