Federated Identity, InCommon and the Science Agencies

Dr Ken Klingenstein
Director, Internet2 Middleware and Security

INTERNET®

Topics

- Federated identity basics
- InCommon update
- Levels of assurance (LOA)
  - ICAM - Bronze, Silver and Gold
  - Assessing the domain and collaboration apps
  - Assessing the research adminsitration apps
- InCommon and the science agencies
  - NIH
  - NSF
  - Dept of Energy

Basics of federated identity

- Leverages institutional identity and authentication for inter-institutional use
- Based on SAML software, such as Shibboleth
- Industry tends to think of bilateral federated identity, e.g. for outsourcing; R&E does multilateral federations for collaborations and research and …
- Provides privacy and security
- Extra value in passing attributes for access control

kjk@internet2.edu

Growth of Federated Identity

- InCommon continues exponential growth, greater than 4M users, 200 major universities, research centers, and companies
- Internationally, growth is even more rapid; 25+ countries representing > 100M users
- Typical organization (Penn State) does 70,000 transactions a day with trust based on InCommon; reduces help desk cost by 85%
- Used for financial transactions, scholarly content access, access to national scientific resources, collaboration tools, social networking, etc.

kjk@internet2.edu

Hypertext atlas of Rare Lymphomas, version 0.51 January 2010

Hypertext Atlas of Rare Lymphomas contains clinical and histological image
histological images available in very high resolution. The Atlas is available ir

Hypertext atlas of Pathology, version 1.80 January 2010

Hypertext Atlas of Organ Pathology contains teaching materials for pre-grad
contains only chapters with images to enable image sharing (see bellow). Th
well as images from CT and MRI scanners and endoscopes.

Demo page of the Atlas

This page demonstrates technologies used in the Atlas on selected images

Tool for sharing images of this atlas in your HTML documents

Images from our atlases can be (for teaching purposes) shared in your HTM
HTML documents. The functionality of the atlas (arrows, virtual microscope)

Discussion forum for users of the atlases

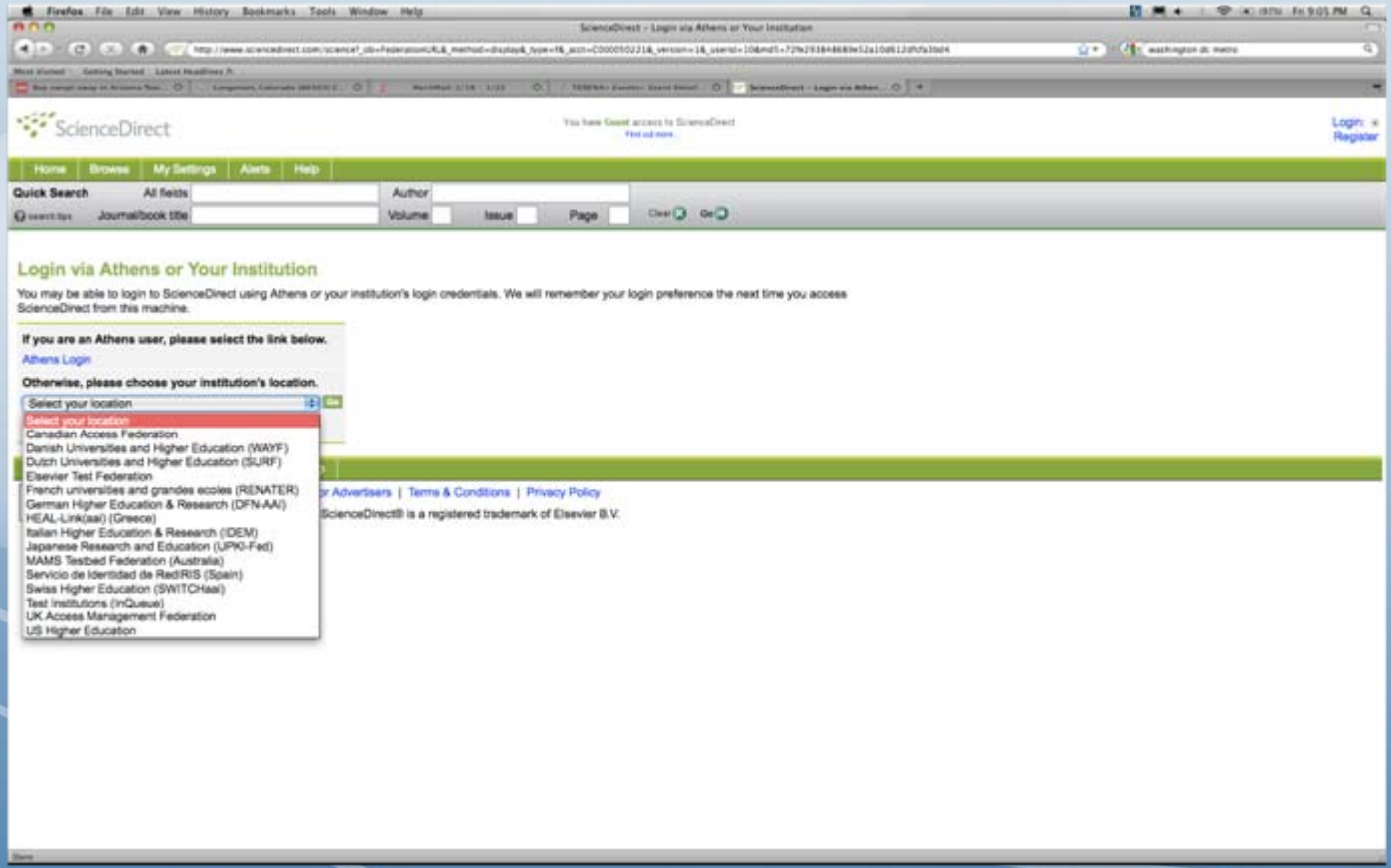
Registered users can discuss individual atlases (contents as well as technic

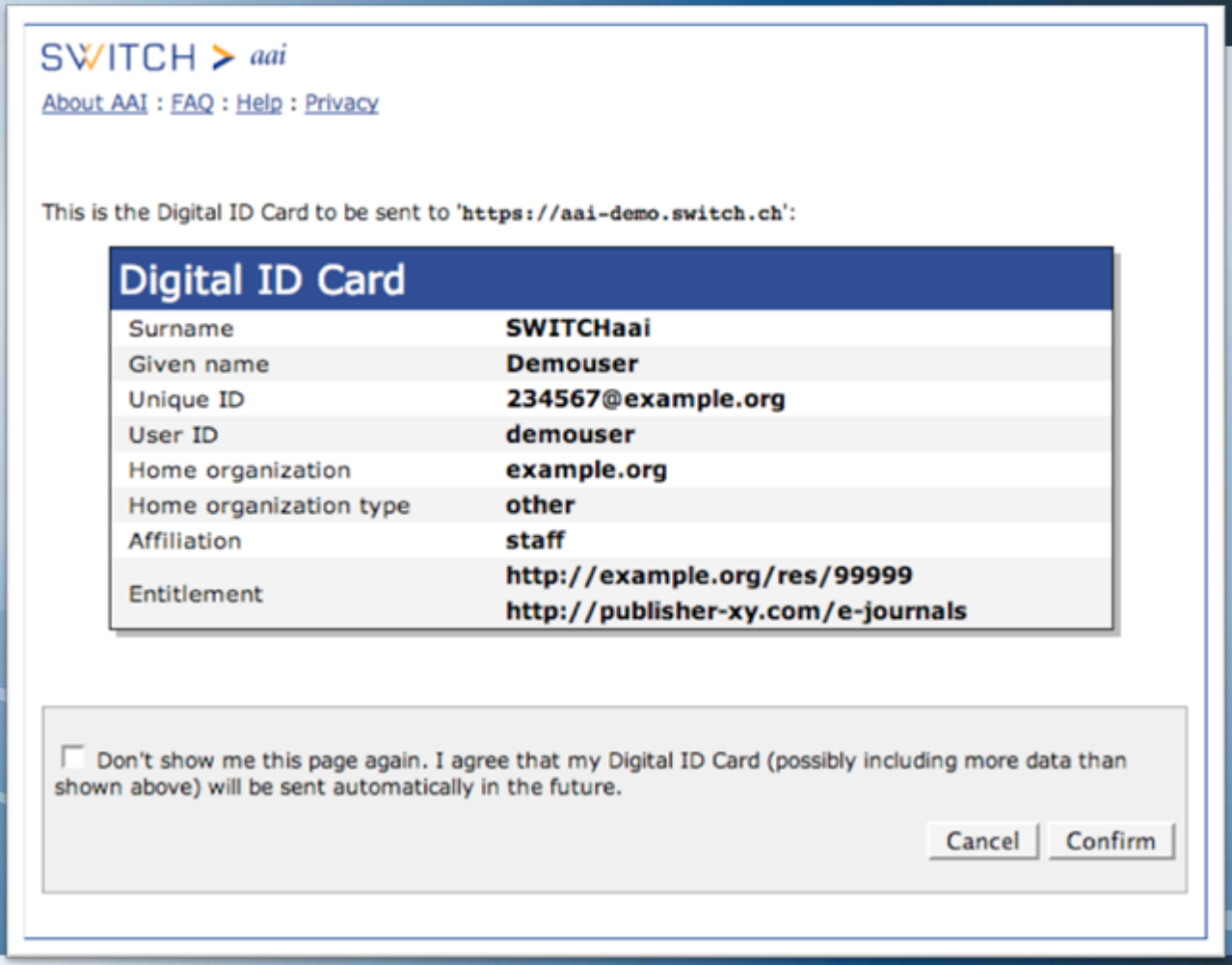
Please select the language: ◉English ○Czech

Free registration is required to use the atlases. If you are not registered

Atlases are accessible also through the identity federations. If you have an a

- eduID.cz — Česká národní federace identit
- WAYF Denmark
- SIRIS — Servidor de Identidad de RedIRIS - SIR Spain
- DFN — DFN AAI Germany
- AAI@EduHr Croatia
- SURFfederatie Netherlands
- IDEM GARR AAI Italy
- UPKI Japan
- Renater France
- cafe — Comunidade Acadêmica Federada (CAFe) Brasil


ScienceDirect
Home
Browse
My Settings
Alerts
Help
Quick Search
All fields
Author
Journal/book title
Volume
Issue
Page
Clear
Go
Login:
Register
Login via Athens or Your Institution
You may be able to login to ScienceDirect using Athens or your institution's login credentials. We will remember your login preference the next time you access ScienceDirect from this machine.
If you are an Athens user, please select the link below.
Athens Login
Otherwise, please choose your institution's location.
Select your location
Select your location
Canadian Access Federation
Danish Universities and Higher Education (WAYF)
Dutch Universities and Higher Education (SURF)
Elsevier Test Federation
French universities and grandes ecoles (RENATER)
German Higher Education & Research (DFN-AAI)
HEAL-Link(aai) (Greece)
Italian Higher Education & Research (IDEM)
Japanese Research and Education (UPKI-Fed)
MAMS Testbed Federation (Australia)
Servicio de Identidad de RedIRIS (Spain)
Swiss Higher Education (SWITCHaai)
Test Institutions (InQueue)
UK Access Management Federation
US Higher Education
Terms & Conditions
Privacy Policy
ScienceDirect® is a registered trademark of Elsevier B.V.


SWITCH aai
About AAI : FAQ : Help : Privacy
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.
Cancel
Confirm

Multiple levels of assurance

- Defines the risks of an incorrect authentication to an application and identifies appropriate technologies and business processes for mitigating the risk
  - LOA 1 for wikis, outreach, etc
  - LOA 2 for grant administration
  - LOA 3/4 for sensitive data and apps
- Step-up processes to integrate user experience

ICAM

- Current initiative by US Government to leverage external credentials for government apps, by officials, institutions and businesses and consumers
- Best but still fragile in a long list of such government efforts
- Will formalize much of the federated activities now underway
- Progress succeeds steadily in the meantime

kjk@internet2.edu

InCommon LOA

- InCommon – today's federation
- Bronze - A campus researcher uses their campus account to access an NIH clinical trial wiki
- Silver – A sponsored research accountant uses their secure campus account to modify documents on NSF Fastlane
- Gold - A campus security officer could use their local two factor authentication to participate in a Teragrid security incident

kjk@internet2.edu

InCommon and NIH

- Pioneering work started with federated access to controlled wikis
- CTSA wikis piloted with six institutions; now up to 75, all user driven
- Help desk calls drop dramatically
- NIH staff starting to use their identities externally
- Silver applications now moving forward –
  - eRA – 22 applications
  - caBIG and BIRN

InCommon and NSF

- Centerpiece is research.gov
- Uses:
  - Grant submission
  - Grant management
- Teragrid
  - CI login
  - Federated incident handling

InCommon and Energy

- Starting an aggressive program to federate labs and layer trust and services on top of InCommon
- Will likely add stronger levels of authentication, maybe some additional attributes/schema
- One additional focus is the citizen science capabilities