

Updates on Internet Identity

Topics

- Consumer marketplace update
 - The big consumer players – OIX - and the other big consumer players – Facebook, Twitter
 - National Strategy for Trusted Identities in Cyberspace
- Federated identity update
 - InCommon and international federations
 - Non web apps – OAuth and Moonshot and ECP
 - Social2SAML and other bridges
- InCommon update, including certs, silver, NSF, uApprove
- Collaboration management platforms and work with VO's
- Federated identity and ABAC
- Implications for GENI and its projects

Internet Identity in the last few years...

- Internet identity has become pervasive, in two flavors
 - A rapidly growing, but still maturing federated identity infrastructure, particularly in the R&E sector globally.
 - A set of theoretically interoperable social identity providers serving large masses of social and low-risk applications
- Federated uses vary by country and sector
 - In some countries, 100% of citizens, using for government, research, educational and other uses
 - In the US, R&E and extensive federal/state government use
 - Verticals (medical, real estate, etc) building federated corporate identities

Social Identity

- Large scale phenomenon beginning around 2007
- A number of major players currently sharing a set of non-interoperable deployments of weak protocols
- Convergence beginning around a new, common variant (OpenId-Connect) that uses many of the federated strategies but adoption is unproven.
- Integration of federated and social approaches emerging, including Social2SAML gateways, etc.
- Efforts to build a proper marketplace challenged by {Google, Yahoo, Paypal, MSN} vs Facebook vs Twitter vs...

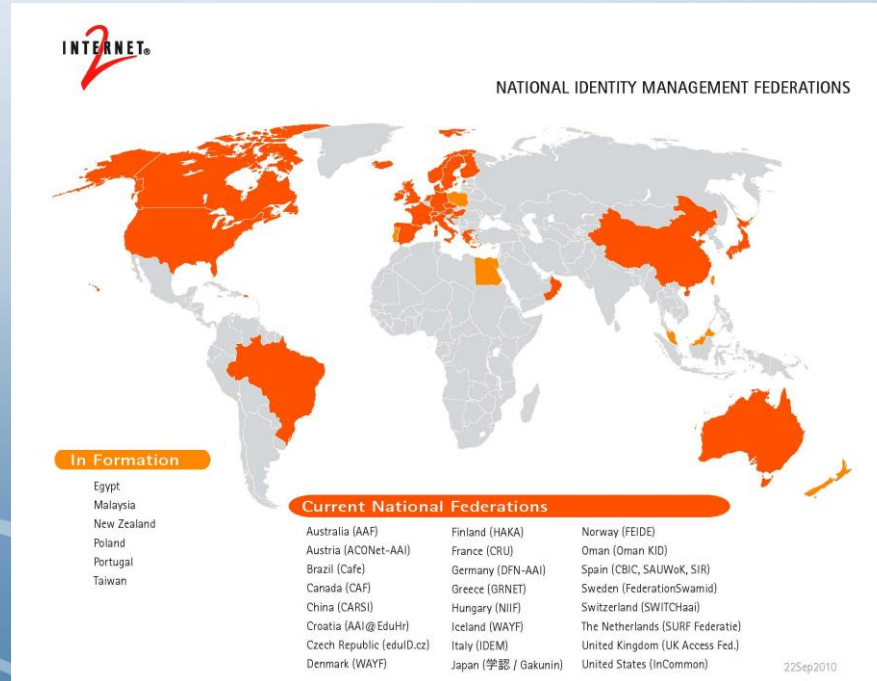
NSTIC

- National Secure Transactions in Cyberspace – major White House Initiative on citizen-gov security/privacy
- Serving the government and anchoring a commercial marketplace
- www.nist.gov/nstic
- Three workshops in progress– on governance, privacy and technology
- Works well with SAML and R&E federations
- A lot of drivers from the government, but uncertain acceptance from the big consumer players
 - The Facebook ToS, the limited revenue opportunities
- Will this Federal effort finally succeed?

Federated identity is still a work in progress

- Still immature
 - Not all institutions are in a federation
 - Not all institutions populate all base-level attributes
 - User-managed attribute release beginning
- Still gaps being worked
 - Non-web apps just getting addressed
 - Interfederation
 - Developing the attribute ecosystem

SAML federations worldwide - scope



InCommon today



- 250+ universities, 450+ total participants, growth still 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, UHC, Mayo, etc.
- Certificate services bind the InCommon trust policies to new applications, including signing, encryption, etc.
- FICAM provisionally (privacy to be worked) certified at LOA 1 and 2 (Bronze and Silver).

Important New Services

- Research.gov
 - Includes NSF Fastlane
- Electronic grants administration from NIH
- Cilogon (cilogon.org)
- Mayo Clinic, UHC, National Student Clearinghouse
- IEEE, Educause
- NBCLearn, Desire2Learn, PeopleAdmin, Qualtrics
- UniversityTickets, Students Only Inc, StudentVoice

Research.gov

POWERING KNOWLEDGE AND INNOVATION

Home Contact Us Site Map Help

July 23, 2011

LOGIN AS

- NSF Visitor
- NSF User
- NSF Staff
- USDA User
- InCommon

> Who We Are

> Service Offerings

> News

> SEE Innovation

APPLY FOR GRANTS

Grants.gov

NSF FastLane

NASA Nspires

FEEDBACK

Tell Us What You Think

Want to use your Institution ID to log in to Research.gov?

Join the InCommon integration!

Click here for more information >>


Alerts

Research.gov will be unavailable Sunday, July 24, 12:01 AM to Sunday, July 24, 8 AM for scheduled maintenance. For assistance, contact the National Science Foundation Help Desk -7 AM to 9 PM- at 1.800.381.1532 or at rgov@nsf.gov.

You may experience system errors while conducting searches using Research.gov. We are working to correct this error. For additional assistance, contact the NSF Help Desk- 7 AM to 9 PM - Eastern Time, Monday through Friday at 1-800-381-1532 or by emailing rgov@nsf.gov.

Our Services

Welcome to Research.gov! We have a new look and feel and exciting new and enhanced services. Select a service from the list below to find out more.




Research Spending & Results

Find Recovery Act Awards made by NSF. Also find information about how NSF and NASA grant award dollars are being spent, what research is being performed, and how the outcomes of the research benefit society.



Science, Engineering, and Education Innovation (SEE Innovation)

Provides the public, scientific community, and policy makers with quick, dynamic access to information about NSF investments at the forefront of science, engineering, and education.



Policy Library

An electronic library that consolidates federal and agency-specific policies, guidelines and procedures for use by federal agencies and the research community. Agency-specific documents are available for Research.gov partner agencies.

Print Page Adjust Font Size: A A A



RECOVERY.gov

Learn More About the American Recovery and Reinvestment Act of 2009.

[Learn More](#)

▼ Events

September 14 - 16, 2011
[FDP Meeting Conference](#)

October 17 - 18, 2011
[NSF Regional Grants Conference](#)

October 22 - 26, 2011
[SRA 2011 Annual Meeting Conference](#)

[View All Events](#)

▼ My Weather

My NCBI - Home

http://www.ncbi.nlm.nih.gov/sites/myncbi/

NCBI Resources How To

My NCBI Sign In

My NCBI

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

[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 >](#)

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

Crab File Edit Capture Window Help

Mozilla Firefox

Research.gov - Homepage x // Select your identity provider x http://www.ncbi.nlm.nih.gov/sites/myncbi/7cmd-expandedList x

http://www.ncbi.nlm.nih.gov/sites/myncbi/7cmd-expandedList

Most Visited Latest Headlines Bookmarks

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 x // Select your identity provider x +

terena.org https://login.terena.org/way//module.php/disco/power/disco.php?entityID=https%3A%2F%2Fterena.org%2Fsp&return=https%3A%2F%2Flogin.terena.org%2Fway%2Fmodule.php%2Fsam%2Fsp%2Fdiscoresp.php%2F... Google

Most Visited Latest Headlines Bookmarks

SELECT YOUR IDENTITY PROVIDER

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



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

[Login at Internet2](#)

All Nordic countries Spain UK eduGAIN Guest providers Miscellaneous

808 entries

Incremental search...

- 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

InCommon – a work in progress

- Growth and managing growth
- Silver – higher levels of assurance
- uApprove – end user attribute management
- Solidifying member participation
- Social2SAML coordination
- Personal certificates
 - Powerful old technology for authentication, signed email, signed documents, encryption, etc.
 - Soon to be a major user of federated identity

Silver

- Higher assurance profile to deal with access of a financial or valued resource
 - Electronic grants administration, Teragrid, OSG, medical records, etc.
- A careful walk between what's feasible on campuses and what agencies would like
- Includes some type of audit by InCommon (possibly review of exceptions to common practice)
- Fresh baked, unpriced yet
- <http://www.incommon.org/assurance/>

When to do Consent

- Not at all – part of an existing contractual relationship
- At the point of collection of information
 - “We intend to use what you give us in the following ways”
- At the point of release of information
 - “I authorize the release of this data in order to get my rubber squeeze toy...”
 - Per transaction or persistent for some time

User interface - uApprove

- Provide users with control, and guidance, over the release of attributes
 - Includes consent, privacy management, etc.
- Basic controls (uApprove) now built into Shibboleth, but largely untapped in deployments.
- Additional technical developments would help scalability
- 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.

Cancel

Confirm



Non-web apps

- A variety of approaches are being developed to address these large families of apps
 - Challenges are discovery, trust anchors in the clients, attribute release and privacy management
- Three categories of approaches
 - Moonshot - GSS over Radius (and maybe SAML)
 - Oauth and OpenId-Connect
 - SAML ECP (extended client profile)
- Lots of hope but no turn-key deployments yet

Social2Saml

- Operational gateway now in Sweden for many social id providers.
- Deployment strategies could include a federation service or a campus/org service
- LOA likely 1, identity needs to be mapped
- Addresses outreach and low-security needs

Collaboration Management Platforms

- An integrated “collaboration identity management system”
 - Provides basic group and role management for a group of federated users
 - Plugs into federated infrastructure to permit automatic data management
- A growing set of applications that derive their authentication and authorization needs from such external systems
 - Collaboration apps – wikis, lists, calendaring, netmeeting
 - Domain apps – instruments, databases, computers, storage
 - <https://wiki.surfnetlabs.nl/display/domestication/Overview>

CMP

- Next generation portal/gateways
- Intended for federated users and multi-domain applications
 - plumbed into the infrastructure
- More secure, more powerful, more privacy preserving, more application possibilities, more...

From the collaboration perspective

Scalable actions expected (or at least hoped for) in a CMP:

- Create and delete/archive users, accounts, keys
- Group management on an individual and CMP-wide scale
- Permit or deny access control to wiki pages, calendars, computing resources, version control systems, domain apps, etc.
- Domesticated applications to meet the needs of the VO
- Usage reporting
- Metering and throttling

CMP from the technical perspective

- A combination of enterprise tools refactored for VO's
 - Shib, Grouper, Directories, etc
- A person registry with automated life-cycle maintenance
 - Includes provisioning and deprovisioning
- A place to create, maintain local attributes
 - Using Groups and Roles
- A place to combine local and institutional attributes for access to applications
- A place to push/pull attributes to domesticated applications
 - Collaboration apps – wikis, lists, net meetings, calendars, etc
 - Domain apps – SSH, Clusters, Grids, iRods, etc.
 - Attributes delivered via SAML, LDAP, X.509, etc

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, metadata enhancements and tools, discovery

Issues for MAGIC participants

- What is broken now? What might not be met in the emerging infrastructure?
- How can agencies and directorates inform their communities about these new opportunities?
 - How can they incent?
 - What is the agency's ROI? What is the VO ROI?
- What do agencies need to do together and what can they do independently? What needs to be consistent across agencies (at least appear to be to the federated partners)
- What pieces of infrastructure should the agencies be providing? How?