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](http://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
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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td>SWITCHaai</td>
</tr>
<tr>
<td>Given name</td>
<td>Demouser</td>
</tr>
<tr>
<td>Unique ID</td>
<td><a href="mailto:234567@example.org">234567@example.org</a></td>
</tr>
<tr>
<td>User ID</td>
<td>demouser</td>
</tr>
<tr>
<td>Home organization</td>
<td>example.org</td>
</tr>
<tr>
<td>Home organization type</td>
<td>other</td>
</tr>
<tr>
<td>Affiliation</td>
<td>staff</td>
</tr>
<tr>
<td>Entitlement</td>
<td><a href="http://example.org/res/99999">http://example.org/res/99999</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://publisher-xy.com/e-journals">http://publisher-xy.com/e-journals</a></td>
</tr>
</tbody>
</table>

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.
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.surfnetslabs.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?