Trust, Identity Management and GENI

Dr. Ken Klingenstein,
Senior Director, Middleware and Security, Internet2
Technologist, University of Colorado at Boulder
Topics

• Internet identity update
  • Technology updates
  • ISOC, IETF “Identity, Trust and the Internet”
• R&E identity federations
• Some thoughts on federation and trust
Internet identity

- Federated identity
  - Enterprise centric, exponentially growing, privacy preserving, rich attribute mechanisms
  - Requires lawyers, infrastructure, etc
- User centric identity
  - P2P, rapidly growing, light-weight
  - Marketplace is fractured; products are getting heavier to deal with privacy, attributes, etc.
- Unifying layers emerging – Cardspace, Higgins
Federated identity

- Convergence around SAML 2.0 – even MS; increasing use of Shibboleth as the interoperability standard.
- Exponential growth in national and international R&E sectors
- Emerging verticals in the automobile industry, real-estate, government, medical
- Policy convergence for LOA, basic attributes (eduPerson), but all else, including interfederation, remains to be developed
- Application use growing steadily
- Visibility is about to increase significantly through end-user interactions with identity selectors and privacy managers
User-centric identity

• Driven by social networking {Facebook, MySpace, etc} and {Google, AOL, MSN}, growing rapidly
• Relatively lightweight to implement for both application developers and identity providers
• Separates unique identifier and trust (reputation systems, etc.)
• Fractured by lack of standards, vying corporate interests, lack of relying parties, etc.
• OpenId, Facebook Connect, Google Connect, AOL
Unifying the user experience

- Among various identity providers, including P2P, self-issued, federated
- Need to manage discovery, authentication, and attribute release
- Cardspace, Higgins, uApprove, etc.
- Consistent metaphors, somewhat different technical approaches
- Starting to deploy
- Integrating enterprise and social identity
Trust, Identity and the Internet

- Acknowledges the assumptions of the original protocols about the fine nature of our friends on the Internet and the subsequent realities
- ISOC initiative to introduce trust and identity-leveraged capabilities to many RFC’s and protocols
- First target area is DKIM; subsequent targets include SIP and firewall traversal (trust-mediated transparency)
Privacy

• A broad and complex term, like security, encompassing many different themes

• In the GENI case, at least several instances
  • Protection of research data and collaborative materials
  • Consent for personal data release for access controls, particularly in international collaborations
  • Likely others

• International federations have already explored some of the privacy issues.
Federation Update

- R&E federations sprouting at national, state, regional, university system, library alliance, and elsewhere
- Federated identity growing in business
  - Many bilateral outsourced relationships
  - Hub and spoke
  - Multilateral relationships growing in some verticals
R&E Federation Killer Apps

• Content access – Elsevier, OCLC, JSTOR, iTunes
• Government access – NIH, NSF and research.gov
• Access to collaboration tools – wikis, moodle, drupal, foodle
• Roaming network access
• Outsourced services – National Student Clearing House, student travel, plagiarism testing, travel accounting
• MS Dreamspark
• Google Apps for Education
International R&E federations

• More than 25 national federations
• Several countries at 100% coverage, including Norway, Switzerland, Finland; communities served varies somewhat by country, but all are multi-application and include HE
• UK intends a single federation for HE and Further Education ~ tens of millions of users
• EU-wide identity effort now rolling out - IDABC and the Stork Project (www.eid-stork.eu)
• Key issues around EU Privacy and the EPTID
• Some early interfederation – Kalmar Union and US-UK
InCommon

• Over 123 members now
• More than two million “users”
• Most of the major research institutions
• Other types of members
  • Non usual suspects – Lafayette, NITLE, Univ of Mary Washington, etc.
  • National Institute of Health, NSF and research.gov
  • Energy Labs, ESnet, TeraGrid
  • MS, Apple, Elsevier, etc.
  • Student service providers
• Steering Committee chaired by Lois Brooks of Stanford;
  Technical Committee chaired by Renee Shuey of Penn State
InCommon Update

• Growth is quite strong; doubled in size for the fifth year straight…
• Potential size estimates (pre-interfederation) could grow > 5,000 enterprises; revenue stream….
• Overarching MoU for federal agencies to join may happen
• Silver profile approved
• Major planning effort on the future of InCommon now underway, including governance, community served, pricing and packaging principles, business models
NIH

- Driving agency for much of our government activity
- Several types of applications, spanning two levels of LOA and a number of attributes
  - Wikis, access to genome databases, etc
  - CTSA
  - Electronic grants administration
- “Why should external users have internal NIH accounts?”
- Easier stuff – technology, clue at NIH
- Harder stuff – attributes (e.g. “organization”), dynamically supplied versus statically-supplied info
Federation Soup

- Within the US, federations happening in many ways – state, university system, library, regional, etc
- Until we do interfederation, and probably afterwards, federations will form among enterprises that need to collaborate, regardless of their sector
- Common issues include business models, legal models, LOA and attributes, sustainability of soup
- Overlapping memberships and policy differences creates lots of complexity in user experience, membership models, business models, etc.
- One workshop in, so far…
- https://spaces.internet2.edu/display/FederationSoup/Home
Examples of federation soup

• Texas: UT, Texas TACC/Digital library, LEARN
• North Carolina – the MCNC federation
• California – UCOP, Cal State, State of Cal, etc…
• New Jersey - NJEdge
A point in time

- We’re about ten years into federated identity
  - Much has been accomplished – strong use cases, SAML 2.0, national level R&E federations, redirection of government efforts, corporate deployments, etc.
  - Many positive if unexpected outcomes (secrecy, revenue)
- There are significant gaps to fill in
  - Building a real global Internet identity layer
  - Nothing looks technically intractable; policies are harder
  - Integration of enterprise and social identity
Federated what...

• Not all things federated fit together well
  • E.g. federated search meets federated identity is an uneven fit.
  • Federated resources may not overlap with federated users and identities
• The hardest part of federation is the policy space.
• What parts of the existing policy space should/must GENI use?
Even in identity federation…

- Which federation(s) to be in
- The alignment of resource owners to federations
- Levels of LOA
- Common schema
  - For people
  - For almost everything else – devices, measurements, etc
Virtual Organizations and Federations

- VO’s can leverage peered federations
  - Use local authentication, integrate local and external privileges, etc.
  - Improve end-user experience, create a layer of privacy, better security
- A VO, or a cluster of VO’s sharing an IdM or a CA, can be considered a federation
- COmanage might be a useful tool.
Access control

• Web versus web services vs other protocols
  • Shib is web right now, with some web services extensions and a few non-web buried instances
  • SAML can be bound to almost any protocol, but hasn’t been yet
• Sources of authority for privileges on all sorts of things…
• Using groups
• Using privileges
Externalizing identity management from the management apps

• [http://groups.geni.net/geni/wiki/GeniServices](http://groups.geni.net/geni/wiki/GeniServices) is not federated…
• The collaboration apps
• The domain apps
• The admin users
Trust-mediated transparency

• Security is not just threats; it is also opportunities
• The biggest problem, for the R&E community, is the TDA’s (traffic disruption appliance) – firewalls, NAT’s, packetshapers, etc
• A deeply layered problem, with vicious feedback loops
• Dave Clark talked (~2003) about trust-mediated transparency as an essential aspect of the next-gen Internet...