

Internet Scale Identity, Collaboration and Research & Education

Ken Klingenstein
RL “Bob” Morgan
September 2007

Topics

- Internet Scale Identity
 - Federated identity
 - R&E federations, US activities and Shibboleth
 - User centric identity
 - Hybrids and integration
- The Bloom of Collaboration Tools
- Putting the Parts Together
 - For new Internet services
 - For human collaboration

Requirements for Internet identity

- Fewer Internet sign-ons, fewer passwords
- Preservation of privacy, especially across international boundaries
- Several layers of assurance of identity, to deal with low-risk to high-risk applications
- Ease of deployment (consistent with risk)
- Ease of use
- also see Kim Cameron's "Laws of Identity"

Styles of Internet identity

- Federated
 - Leveraging enterprise identity for inter-realm purposes
 - Authentication and attributes (identifiers, affiliations, memberships, entitlements) are the common payloads
 - Privacy, security and trust are the critical issues
 - Is hard to set up
- “User-centric”
 - Originally PGP, now Infocard and OpenID
 - Emphasize self-asserted scenarios (but not only those)
 - Ubiquity is key issue
 - Is easy to set up
- Both are growing at exponential rates

Federated Identity

- Enterprises exchanging assertions about users
 - Often identifier-oriented but can provide scale and preserve privacy through the use of attributes
 - Real time exchanges of standardized attribute/value pairs
- Basis for trusting the exchanged assertions via common policies, legal agreements, contracts, laws, etc.
- Federations offer a flexible and largely scalable privacy preserving identity management infrastructure

Shibboleth (a sidebar)

- Shibboleth is 1.3 the widely deployed base in R&E
- OpenSAML libraries widely built upon
- Shibboleth 2.0 now in beta
- “Shib 2.0 will interoperate with other SAML 2.0 products better than they interoperate with each other.”
- Apache-licensed; contributor base broadening; Google and Microsoft among project supporters
- Support services businesses developing in the US and overseas

The rise of federations

- Federations are now occurring broadly, and internationally, to support inter-institutional and external partner collaborations
- Almost all in the corporate world are bi-lateral; almost all in the R&E world are multilateral
- They provide a powerful leverage of enterprise credentials
- Federations are learning to peer (aka inter-federate)
- Internal-to-organizations federations also proving useful

Technical Aspects of Federations

- Federating protocol and profiles
- Enterprise signing keys
- Metadata management and distribution
- IdP discovery service
- Participant name management

Policy Aspects of Federations

- Participant operational practices
 - Enterprise identity management practices
 - Service provider privacy policies
- Agreement between federation and members
 - Dispute resolution, liability, termination, governance ...
- Standardized attributes
 - e.g., eduPerson schema
 - Levels of Assurance (LOA)

International R&E federations

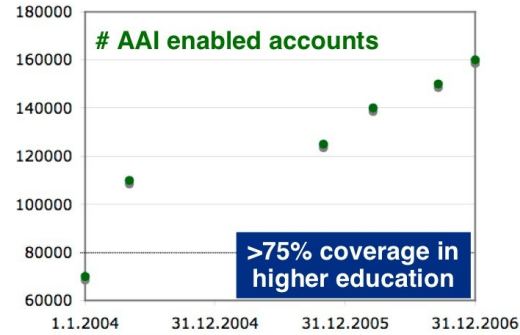
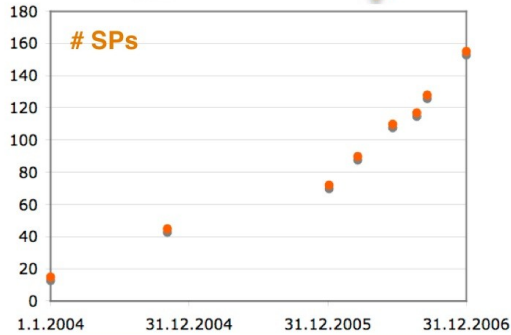
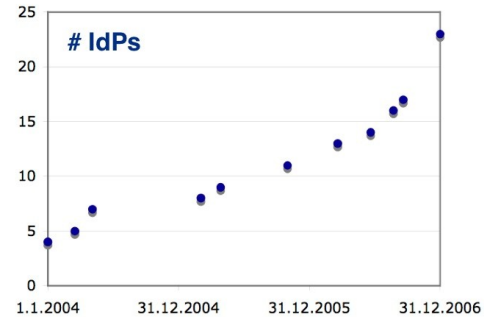
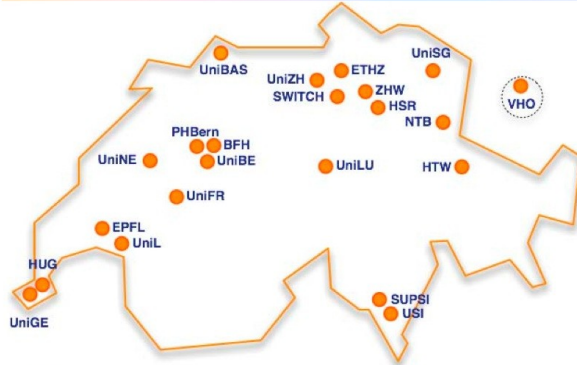
- Mature federations in many countries, including UK, Norway, Switzerland, US, Australia, France, Denmark, Finland, Spain, Germany, Netherlands, etc.
- Most are Shib based; some use other federation products.
- Scope of membership usually higher ed, but some are broader, e.g. UK, Spain, Netherlands
- Use cases range from content access to collaboration support to learning management systems to wireless roaming to...

An adoption curve

SWITCH Hai Federation End of 2006

SWITCH

The Swiss Education & Research Network



InCommon



- US Research&Education Federation, a 501(c)3
- Addresses legal, LOA, shared attributes, business proposition, etc issues
- Members are universities, service providers, government agencies
- Over 60 organizations and growing steadily; 1.3 million user base now, crossing 2 million by the end of the year
- Uses range from popular and academic content access to wiki and list controls to access NIH applications to ...
- Almost all use is transparent to users (it's middleware) but that is about to change
- www.incommonfederation.org

Key aspects of InCommon

- Federating software
 - Shib 1.3 (other possibilities in the future)
- Shared attributes and schema
 - eduPerson based
 - <http://www.incommonfederation.org/attributesummary.htm>
- Levels of authentication
 - POP (participant operational practices) for LOA-today
 - InCommon Bronze and Silver will map to LOA 1 & 2
- Governance/Management
 - Steering committee of members IT executives
 - Operations staffed by Internet2

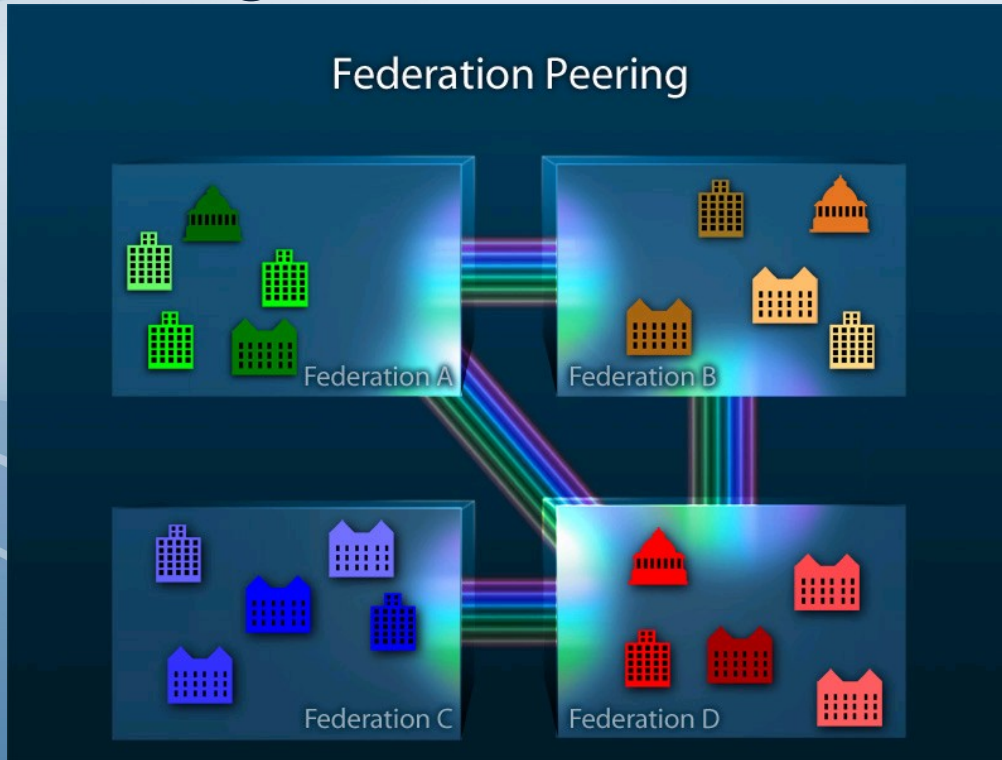
The complex nature of privacy

- Shift from no one knows to “I control who knows”
- Most users want the defaults to work
- International exchange deeply compounds
 - Differing policies
 - A US citizen using a Swiss IdP
 - A roaming network user from Australia in the EU.
- User consent matrix not well understood
- Legal considerations and log files
- Paradigm clashes happen, e.g. federated identity meets federated search

Relationships among federations

- Peering (membership sharing)
- Confederation
 - Presumes peering, adds multi-federation support
- Leveraged (distinguished subset)
 - Specialized federations that extend a common base federation – e.g. the University of California system and InCommon
- Intersecting

Peering Parameters



Parameters:

- **LOA**
- **Attribute mapping**
- **Legal structures**
 - **Liability**
 - **Adjudication**
- **Metadata**
 - **VO Support**
- **Economics**
- **Privacy**

Some inter-federation key issues

- Multi-protocols
- Sharing metadata
- Aligning policies
- IdP discovery functionality
- Dispute resolution
- Virtual organization support

Prague Meeting on Inter-federation

- 15-20 International R&E federations (5 continents) plus Liberty Alliance and a few others
- Prague, September 3 2007
- Lots of topics: Attribute mapping, Privacy Policies, Dispute resolution, Financial considerations, Technical direction setting
- Next steps:
 - UK drafting an analysis of International Peering needs, opportunities, etc.
 - Discussions with Liberty EGov SIG (e.g SAML 2.0 profiles, attribute schema)

User-centric Identity

- Semi-grassroots alternative to federation-style identity
- PGP in the old days, now OpenID, Infocard
- Initial use cases include blogs and wikis, social networking
- Very active development – Cardspace in MS Vista, Higgins and the Bandits, OpenID, OAuth, etc.
- Several layers
 - Globally unique identifiers
 - Provider mobility
 - User interface, consent, control, manipulability
 - Reputation, not static trust

User-Centric Identity 2

- Many things to many (marketing) people, but mostly ...
- User “owned”
 - not @facebook.com
hence: externalized from a particular app
 - not @google.com, not @washington.edu
hence: not the property of some big organization
- User control of information flow
 - no (or limited) backchannels
 - consent for release

Infocard: Yes

- Smart client extends dumb browser
 - no more IdP discovery
 - hooks for real crypto, hardware support
 - proper, identity-specific UI
 - self-asserted and org-asserted in one scheme
- Unfortunately: just a little complicated
 - bugs in CardSpace 1.0, other impls slow to appear
 - support in Shibboleth in 2008 (planned)

OpenID: eh

- as easy and secure and ubiquitous as ... email
 - can be secured, at the expense of its “easy” appeal ...
 - will 2.0 see adoption? non-http-URL ID instances?
- it's the use cases, stupid, not the technology
 - promiscuous interactions between many IdPs and RPs
 - eliminate account sign-up barrier at most RPs
 - userid potentially independent from IdP
 - are these R&E use cases? yes ...

Example: R&E and academic work

- R&E collaboration is the original “social networking”
 - find peers worldwide based on publishing specialized interest profiles
 - self-organized fiercely-maintained reputation systems
 - cross-disciplinary linkage
- in support of the development and dissemination of knowledge, the mission of R&E
 - for R&E, this serious business involving real resources, often expensive and restricted

Example: Lifelong Learning / Tracking

- student's e-portfolio
 - everything (that's wanted) from a whole academic career, across multiple institutions
 - all transcripts, complete with course syllabi etc
- outcome tracking
 - judge success of teacher training based on life success of all students of that teacher ...
- these are serious societal identity problems

User-Centric vs Enterprise-Centric

- OpenID fits as subprime level of assurance
 - and low-assurance use cases **are** important
- Mixed, chained, proxied, leveraged scenarios useful but must be treated with caution
 - educating users, partners on implications of choices
 - must get much better at risk assessment
 - identity management systems must provide support
- **Ensuring applications are identity-agile is key**

Identity integration goals

- First, of federated and p2p identity
 - Many levels of integration – tokens, GUI, privacy management paradigm, trust fabrics...
- Then, of identity, group and privilege management
 - Assignment and management of permissions to users by those with authority to grant such access
 - Addresses the static aspects of the authorization space, with audit, delegation, prerequisites, etc.
 - Permissions can be enterprise or virtual organization

A Bloom of Collaboration Tools

- An over-abundance of new tools that provide rich and growing collaboration capabilities (aka Web 2.0)
- Do you
 - Wiki, blog, moodle, email, sakai, IM, Chat, videoconference, audioconference, calendar, flickr, netmeeting, access grid, dimdim, listserv, webdav, etc
 - Share files among workgroups, access Elsevier, work with the IEEE, etc
- No uber-app – limits invention and community of users
- Use of 3 - 4 apps is manageable, but more per user is hard
- Leads to the need for management of collaboration

Collaboration Tools and Identity Management

- Deeply enriches collaboration tools
 - Fine-grain access control and wikis
 - spaces.internet2.edu
 - “member of the community” processes
 - Transparently shared file stores
 - Collaboratively visible calendaring
 - Embedded VO IM channels in campus portals

Relieving the Pain of Rich Collaboration Management

- Commonly manage which identities and which attributes can use the capabilities of the collaboration tools
- Can offer delegation, privacy management, maybe even diagnostics
- CO-Manage

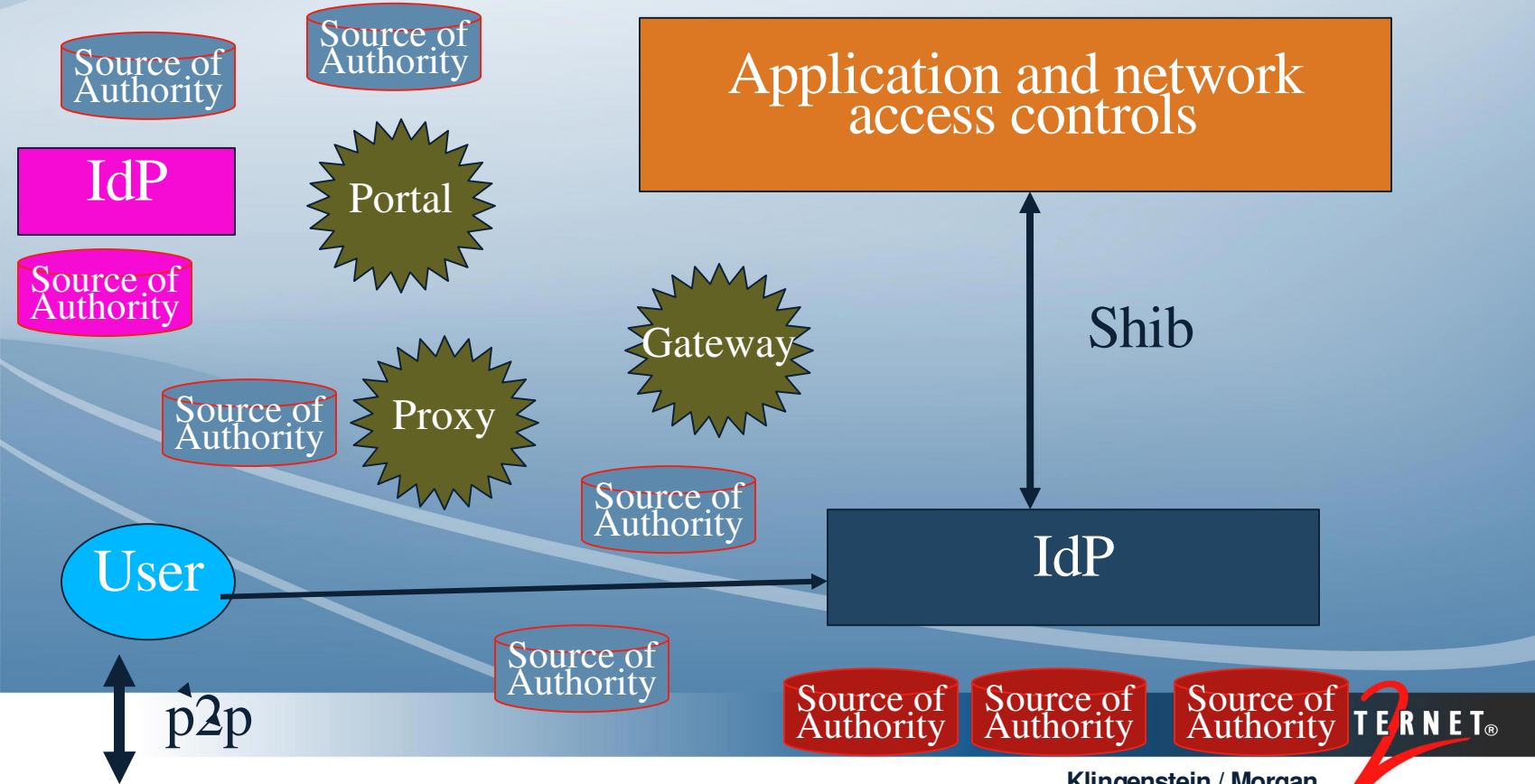
Collaboration Tools and Identities

- Enterprise, VO, and P2P persona are in all of us – our day job, our second job, the rest of our life...
- When and how we integrate the persona needs to be carefully done – legal, ethical, personal issues
- The abundance of communication and collaboration devices makes this harder

Putting It All Together

- Real life and the attribute ecosystem
- “Internet-scale” collaboration
- CO-Manage

Real life and the attribute ecosystem



Attribute Ecosystem

- Many sources of authoritative user info
 - but only one IdP per user sign-on (presumably)
 - many strategies for gathering/caching
 - who-can-say-what is the big issue
 - transformers/gateways often useful
 - sometimes called “claims-based architecture”

CO-Manage

- Management of collaboration a real impediment to collaboration, particularly with the growing variety of tools
- Goal is to develop a “platform” for handling the identity management aspects of many different collaboration tools
 - Platform includes a framework and model, specific running code that implements the model, and applications that take advantage of the model
 - This space presents possibilities of improving the overall unified UI as well as UI for specific applications and components.

CO-Manage 2

- Leverages federated identity and the attribute ecosystem heavily
- Uses Grouper to manage groups and Signet to manage privileges
- Built completely on open protocols, using open source components
- Open and proprietary applications can be plumbed to work with it

CO-Manageable applications

- Already done
 - Sympa list manager, Federated wikis, Asterisk (open-source IP audioconferencing), Dim-Dim (open-source web meeting)
- Immediate targets
 - Rich access controlled wikis
 - Web-based file shares

CO-Manage dimensions of growth

- In the applications that can be driven by it
 - Collaboration and domain science prime areas
 - Largely a function of the application's respect for middleware
- In the areas being managed
 - Diagnostics? Others?
- In the identities being managed
- In the coupling of autonomous and diverse instances
 - Deployment instances may be at many layers of organization and shift as it matures
 - Underlying stores may be db, directory, or other

Research & Education is an interesting sector

- A driver for advanced collaborative approaches
 - TCP/IP and the Internet
 - SAML and Federated identity
 - Collaboration management
- We engage deeply with government agencies and in international research activities
- We also educate the next gen user, and many of those in this room...