Mapping the Use Cases

- Identity
- Interoperability

Use cases:
- User
- Business
- Government

User:
- Play
- Buy
- Work

Business:
- Customer facing
- Employee services
- IT and app integration
- Value and supply chain

Government:
- Tax
- Benefits
- Regulatory
- Law Enforcement

Value and supply chain
Use Cases – Seem like Islands?

User-centric Territories

- Play
- Buy
- Work

Federated Spaces

- Customer facing services
- Employee services
- IT and app integration
- Value and supply chain

Identity Interoperability

User

Use cases

Business

Government

Land of PKI

- Tax
- Benefits
- Regulatory
- Law Enforcement

Value and supply chain
State of the Market

- Federated identity adoption is expanding
  - Enterprises with many federation partners, trying to scale
  - Multi million user deployments underway
  - Community federations: higher education, telecommunications, automotive, government, pharmaceutical, financial services, petroleum…
- Many commercial products support SAML 2.0
  - Vendors have moved quickly to support converged standard; still some growing pains
  - Enterprises implementing multiprotocol scenarios
- Yet divergence continues - between federated and user-centric spaces, and between some of the vendors
State of the Market

• Adoption of federated identity in business growing, but not universal
  • Deployment barriers
    • Standards and tools that work for 10s or 100s of partners still to hard to scale when deploying 1000s of partners
    • Partners not ready, or unwilling
    • Difficult for small business to deploy
    • Application service providers don’t focus on identity
    • Relative high cost for some implementers
    • Concerns about risk, liability, and audit
    • Difficult to build business agreements

Trust is the elephant in the road
Federations in R&E: Current Soup and Future Bread
Topics

• The Research and Education Sector
• Shibboleth
• InCommon and international R&E federations
• Next Steps
  • Inter-federation soup
  • Collaboration management platforms and the attribute ecosystem
The Research and Education Sector

- Intense need to collaborate
  - For both research and education
  - Inter-institutional and international
- Historic roles
  - Innovator in networking
  - Technology transfer
  - Shaping a new generation of consumers
R&E Engagements

- TCP/IP, first as a technology and then as a market-maker
- SAML/Shibboleth, first as a technology and then as a market-maker
- Collaboration tools and collaboration management platforms
Shibboleth

- Deployments > 10,000; countries > 20
- Shib 2.0 release ~ Mar 4, 2008
- Landmark release; strong platform for years to come, on which considerable enhancements will be broadly provided
- “More interoperable with commercial SAML systems than they are with each other”
- OpenSAML 2.0 already heavily used by Verisign, Tata, etc.
- It is suggested that federations migrate to 2.0 sooner than later.
Shib and OpenId

• Shib 2.0+ containing an OpenId provider under discussion
• Shib 2.0++ may contain more clever and useful integration of federated and ad hoc identity management
• The OpenId platform within Shib will have a warning reminding applications to use caution in their consumption of external identities.
• UK leading development, with broad conversation, but OpenId is generally a US concern.
Missing pieces

• End-user attribute release management
  • InfoCard?
  • Attribute release editors within Shib
• Dynamic metadata (not dynamic trust)
• N-tier tokens
InCommon

- Approximately 80 members and growing steadily
- More than two million “users”
- New types of members
  - {St. Mary’s of the Plains}
  - National Institute of Health
  - Student service providers
  - Energy Labs
  - MS, Apple
- On third generation of Steering Committee
- Has less value right now than it will...
The DreamSpark Nightmare

- Microsoft delivery of developer kits, source code, etc to students
- Shows how far down you can bury federation in the user experience (and way under a LiveId and custom WAYF)
- A learning experience for us all
- Showed the value in implementing the full features of Shib (such as the ePTId generator)
- [http://www.pcworld.com/article/id,142597-c,software/article.html](http://www.pcworld.com/article/id,142597-c,software/article.html)
- [https://downloads.channel8.msdn.com/](https://downloads.channel8.msdn.com/)
- Asserting “studentness” is highly useful
InCommon Next Steps

- New members
  - MS, Apple, Michigan, University of Mary Washington, William and Mary, Lafayette, Emory, Richmond
  - Pending – MIT, Google, student service companies, medical consortia, 1200 institutions from the National Student Clearinghouse

- InCommon Silver
  - LOA-2
  - Not hard but lots of thought upfront – profiles, audit guides, etc.
  - Rich new set of applications from NIH
  - Intended to be ultimately revenue neutral
  - Remarkable barn-raising experience so far…
Federations

- Almost everywhere now
  - Internationally – UK (2-3 new members a day), Spain, France, Sweden, Finland, Switzerland, Netherlands, Germany, Denmark, Norway, Australia, Brazil, Japan, Canada, etc.
  - State university systems
  - Community college libraries
  - Medical associations
  - DoJ and DoD
- All do SAML; most are Shib
- Limited interfederation interactions – Kalmar Federation, UK-Australia, MS, Elsevier
International federation highlights

• Several countries at 100% coverage, including Norway, Switzerland, Finland
• Community 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
• Real use cases involving international team science now driving interfederation peering urgency
International Activities

  - A summary of discussions among R&E networks, including a survey of national efforts
- [http://www.jisclegal.ac.uk/access/](http://www.jisclegal.ac.uk/access/)
  - Excellent policy analytics, especially around international issues of privacy, peering, and attributes
  - TransEuropean activities in IdM for use among citizens, governments, and businesses
IDABC

- IDABC stands for Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens.
- Final recommendations due soon.
- Federated approaches are likely; open source standards may be identified
Interfederation

- We used to know more…
  - We thought there was primarily peering and we could do that
  - Things changed…
- A rich mix of emerging relationships – nested, leveraged, peered, orthogonal, etc.
Peering

• Efforts between InCommon and EAuth collapsed a while ago
  • We got close, but EAuth priorities changed
• International Peering
  • UK Feasibility analysis
  • Attribute Alignment
  • Privacy due out in May
  • Peering drafts to follow
Some of the bases to touch in peering

• Typical issues -
  • Problem resolution and adjudication, liability and indemnification, financial considerations, impact on member agreements, etc.

• New issues -
  • Metadata exchange
  • Attribute mapping
  • Transitive trust
Peering Parameters

Parameters:

• LOA
• Attribute mapping
• Legal structures
• Liability
• Adjudication
• Metadata
• VO Support
• Economics
• Privacy
Federation Soup

• Workshop to held early June, with NSF support requested
• Bringing together all manners of federation to figure out federation relationships
  • InCommon, JISC, state federations, library federations, university system federations, grid federations, etc.
  • Topics include alignment of policies, technologies, attributes, metadata, etc.
• Approaches include peering, nested, leveraged, and a whole lot of ad hoc
• Outputs may include best practices, multi-homing, etc.
Emerging key themes

• Privacy and consent
• Privacy and the aggregation of attributes
  • The glory of ePTID
• Support of collaboration and virtual organizations
• Complexity
  • Lack of federal law coupled with state laws
Future issues

• Filling in some of the missing policy pieces
• Dynamic metadata, maybe dynamic trust
• End-user experience – wayf and privacy manager
• Attribute mapping
• Federations as trusted metadata sources
• Inter-federation
• Collaboration management platforms and the attribute ecosystem
IDTrust Observations

- When you get the right topic, the crowd more than doubles (OASIS helps too)
- Most federation work, regardless of sector, faces similar issues
  - What to do about everyone else
  - Attributes
- There’s a reasonably good handle on authentication
  - OpenId was there, real but rational
- Next year’s theme “It’s the Attributes, stupid”
More IDTrust

- [http://middleware.internet2.edu/idtrust/2008/program.html](http://middleware.internet2.edu/idtrust/2008/program.html)
- [http://www.oasis-idtrust.org/node/55](http://www.oasis-idtrust.org/node/55)
- Open reputation systems, discovery protocols for OpenId
- Research community springing up
- Importance of Card Space type services
A few interesting talks

- **A Client-Side CardSpace-Liberty Integration Architecture**
  University of London
- Identity Interoperability, Standards, and the State of Adoption, Dan Blum, Sr. VP and Principal Analyst, Burton Group
- **Panel: Open Reputation Management Systems**
  - Panel Moderator: Abbie Babir, Nortel
  - Drummond Reed, Cordance Corporation
  - Tony Nadalin, IBM
  - Chris Hagenbuch, SafeTSpace
  - Rakesh Radhakrishnan, Sun Microsystems