Covering the Rest of the Waterfront:

Ken Klingenstein, kjk@internet2.edu
Topics

• InCommon, eduGAIN, VO software, international attribute release traction, end-entity tags of value to R&E, Code of Conduct, schema harmonization follies, the state of LOA, distributing other trust authorities in metadata, Social2SAML identity, improving operational practices in data sharing, etc.

• InCommon and eduGAIN
• Social2SAML gateways
• Federated incident handling
• Attribute-based access control
• Needs for further harmonizations
• Attribute release and consent management
InCommon and eduGAIN

- InCommon has joined eduGAIN
  - Has a metadata service ingestion mechanism being tested
    - Starting dynamic metadata testing within InCommon
  - Exporting InCommon metadata into eduGAIN also in the plans
    - First IdP’s, then SP’s
    - Opt in/out sets of issues
- Exposes the next set of critical issues, some of which are almost showstoppers
  - Attribute release internationally
  - Inconsistent semantics of common attributes
Social2SAML Gateways and IdPoLR

• We make extensive use of Social2SAML gateways
  – Expands user base to students’ parents, contractors, alumni, etc.
  – Friendly commercial service works with campuses
  – Exposes next sets of issues – LOA, filtering out attributes, etc

• IdP of Last Resort (extensions of Commit)
  – Yet another way to serve a broader community that wants into our world
  – Slowly building an IdP to serve college admissions, and likely beyond
  – Business process takes the identities into high assurance
    • MFA
    • Identity vetting at College Testing services
Federated incident handling

- Concerns of major science service providers that if they go the federated route, they will be notified by IdP’s of compromised accounts relevant to the service provider.
- “Sir-T-FI” initiative to define and solve the problem
- Aligns well, surprisingly, with some innovative commercial sector thoughts
- Stay tuned
Identity, identifiers and attributes

- Identity is you and your account
- Identifiers are unique values tied to you, but often offering privacy instead of identity
  - Different identifiers give different type of privacy
    - (opaque but stateful, opaque and non-correlating, etc.)
- Attributes provide privacy, access control and scale
  - Attributes fall into two rough categories
    - Verified – by the identity provider, an attribute provider, a third party verifier, etc. e.g. Legal name, legal date of birth, over legal age, citizenship, student status, role in organization, is in Class X, walk-in-library-user, is PI of a NIH grant in oncology, etc.
    - Self-asserted – e.g. displayname, friends, interests, preferredlanguage and many from that might better be verified
Use cases and requirements for attribute-based access control

- Student in class Physics 1010
- Extension offices
  - "as a land-grant we must make all content available to anyone who is physically in the Library, regardless of . . ." or
  - " because of ADA, we must make public content not only available but accessible" or
  - or "because of the conditions of a gift on content X, we must make it available only to users in situation Y" or . . .
- Institutional repositories for complex interrealm sharing
- Alumni options for access
- Get rid of IP-address only options
- Research Data
  - is PI of a NIH grant in oncology, etc.
  - Progressive staged expansion from restricted access
  - What to do when the data is open but the tools that access them are copyrighted?
Needs for further harmonizations

- Semantics of common attributes
  - Fac/staff/student vs staff/student
- Licensing conditions
  - “Academic users”
  - Virtualization of reading rooms
- Code of conduct
  - Intra- EU vs EU-rest of the world vs *.*
- New end-entity tags
Attribute release and consent management

• Attribute release is the single highest barrier to use
• Key dimension of privacy
• Complex set of legal and technical and international and financial and ... issues
  – When and where and how to use is endless discussion
  – Initial and downstream are separate but very related topics
• Requirements list grows – informed, revocable, accessible, etc.
• Worst case are medical information
• The capabilities of the end user are limited
PrivacyLens privacy manager

Logged in to CMU's Calendar on 2014-05-05 22:10

Items sent:
- Andrew ID: "lujo"
- CMU affiliation: "faculty"

Next time you access CMU's Calendar, CMU should:
- Ask whether and what items to send to CMU's Calendar.
  - Send the following items automatically, but remind you that they are being sent:
    - Andrew ID (lujo) [1]
    - Credentials to access CMU services [1]
    - Full name (Lujo Bauer) [1]
    - Surname (Bauer) [1]
    - CMU affiliation (faculty) [1]

CMU will remind you what items are being sent...
Every 2 times you log into CMU's Calendar.
PrivacyLens as a paradigm

• Enabling effective and informed end-user consent
• Embraces a set of capabilities
  – Hierarchical information, fine grain control, bundling, revocation of consent, flexible notifications, etc.
• Embraces a style of presentation
  – Clear screens and slides
  – Optional display of values being sent
  – Affirmative user actions
• Embraces a variety of platforms and management approaches
  – Protocol-agnostic
  – Enterprise management consoles and management
  – Audit and security logs
Takeaways

- Open access is complex
  - Use cases are abundant and diverse
- There is an emerging infrastructure that meets all the requirements for delivering, with privacy and security, the information that users, content providers, research data stores, etc need to implement solutions
- IdP’s must plan to store and support external attribute authority attributes
- A bit of attribute-based access control thinking on the SP goes a long way
- The technologies are powerful and flexible. Don’t turn the knobs to generate policy; use the knobs to implement existing policy or, gasp, simplify it.