The Future of Federations

Future of Federations

- Background
  - Where we are today
  - Where we'll be later today
- Future technology issues – Ian Young
  - Improvements in federation operations
  - Interfederation technology issues
- Future policy issues – Nicole Harris
  - Harmonization
  - Interfederation policy issues
- Working across sectors – David Simonsen
  - A small country going far… David Simonsen,
  - A large country going NSTIC Ken Klingenstein

Where we are today

- R&E Federations
- Social Identity Interactions
  - Note the Social2SAML (and SAML2Social) work
- Major governmental initiatives
  - NSTIC, Stork, eID, T-Scheme
- Unusual situations – UCLA in Denmark
- Cross and con federation
  - Kalmar Union 2
  - eduGain
  - Paul Caskey's desktop

Where we'll be later today

- Other verticals beginning full multilateral federations
  - Learning about metadata
  - Soon to learn about common attributes for payloads
- Early pilots of key interfederation technologies
  - PEER and REEP
- Buckets of bi-lateral metadata sharing

Scalable Privacy:
An NSTIC grant for the Identity Ecosystem

Scalable Privacy

- Grant Basics
- Key deliverables
- How the pieces fit together and create infrastructure

Basics

- Part of the Identity Ecosystem initiative (NSTIC)
  - Governance
  - Pilots to inform and advance the ecosystem
  - Scoped to US but with global implications
  - http://nist.gov/nstic/
- Two year grant (second year pending) for $3.4 M
- Emphasis on major infrastructure elements for privacy, but with second factor authentication added in

Key deliverables

- Promotion of two factor authentication
  - Good privacy begins with good security
- Schema for common use
  - A user-manageable but broadly useful set of attributes
- Privacy managers
  - For users to control the release of attributes
  - Putting the informed into informed consent
- Implementing anonymous credentials at scale
  - Engineering into infrastructure privacy protecting technologies
- Metadata strategies to support the above
- Significant pilots and testbeds
- Several policy thickets
  - Any new and good technology presents major policy issues

Promotion of multi-factor authentication (MFA)

- Good privacy begins with good security
- A variety of second factor alternatives are now viable – USB devices, NFC devices, cell phones, certificates, etc and technology can bridge across them.
- Grant will support wide-scale deployments at three lead schools (MIT, Utah, Texas) with harvesting of planning processes
- Facilitation will support a cohort of additional schools with their deployments, leveraging the lead school activities.

Privacy foundational elements

- Common attributes and schema
- Privacy managers
  - Controls the release of personal attributes
  - Spans user contexts
  - Relies on the trusted metadata for informed consent
- Trusted meta-data
  - About the relying party and the IdP
  - Vetted by the federation and by third-parties
- Anonymous credentials
  - Integrated at key junctions into the ecosystem, leveraging existing infrastructure
  - In software, use of metadata, and user experience
- Pushing policy issues

Big Picture Slide

- IdP's
- SP's
- Attribute authorities
- Third parties, portals, etc.
- Application auditors
- Federation operators
- The user

What Flows Within the Big picture

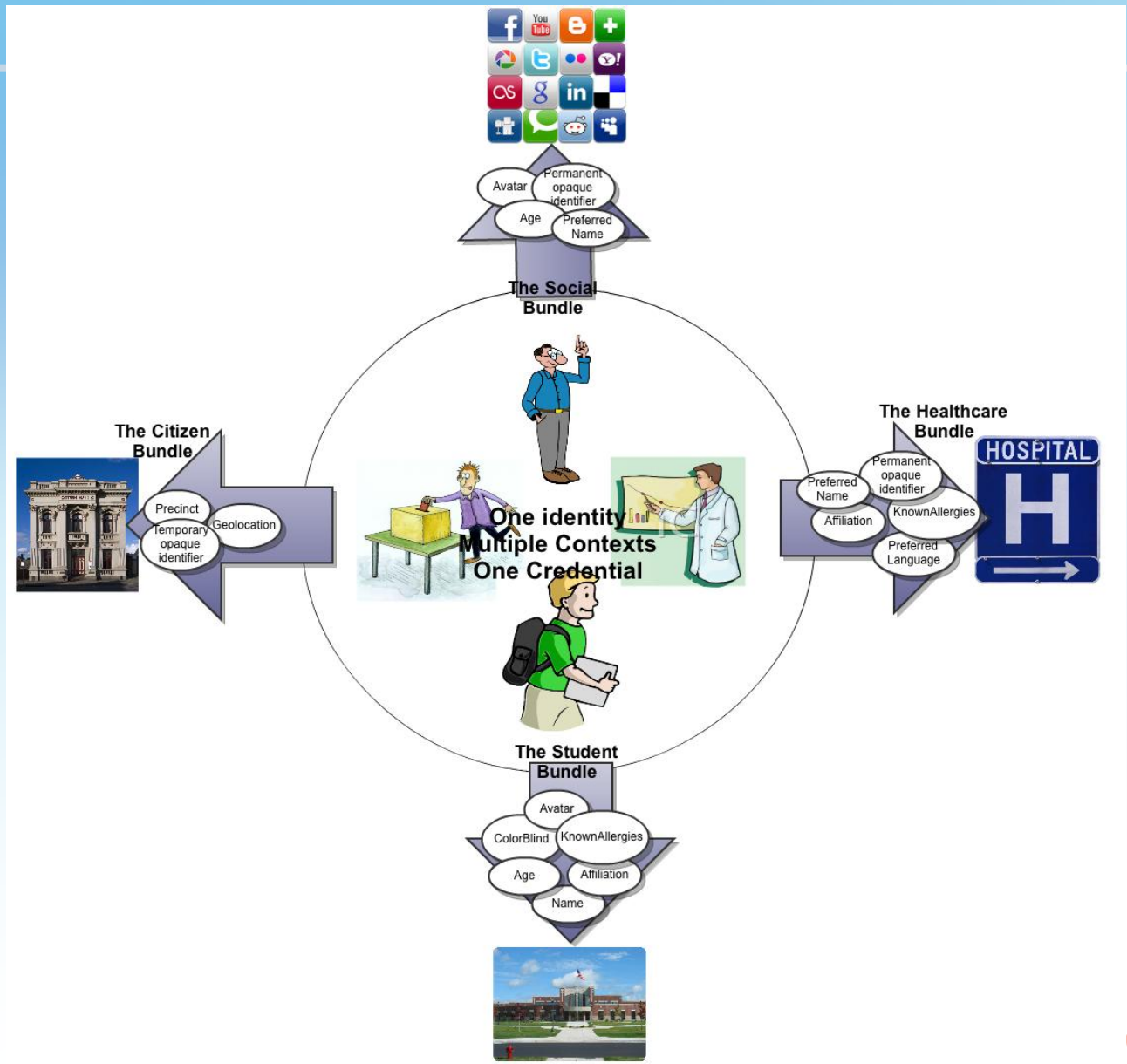
- Attributes
  - May be externally asserted (e.g. student, citizenship), self-asserted (e.g. preferred language), third party asserted (e.g. resident of a town), etc.
- Management of attributes
  - Trust, vetted application information, user consent flows, etc.

The User and Contexts

- A person operates in one of several contexts when on-line:
  - As a citizen
    - At local, state and national levels
  - As a worker-employee
    - With other businesses, with governments, with consumers
  - As a consumer
  - As a physical entity
    - Geolocation, age, personal preferences, etc
  - Maybe one or two others
- In managing their privacy, what parts of the user experience should be consistent between contexts and what may be different?

Common attributes, schema and bundles

- A small set of attributes, organized into schema and bundles, that span the needs of a broad range of applications
- Primarily "citizen" oriented, but with significant value to many other contexts, including consumer and business.
- Intended to be user-manageable
  - Through privacy managers
  - With informed consent
  - Leveraging existing and emerging trust and security infrastructure


Avatar
Permanent opaque identifier
Age
Preferred Name
The Social Bundle
The Citizen Bundle
Precinct
Geolocation
Temporary opaque identifier
The Healthcare Bundle
Preferred Name
Permanent opaque identifier
Affiliation
KnownAllergies
Preferred Language
HOSPITAL
One identity
Multiple Contexts
One Credential
The Student Bundle
Avatar
ColorBlind
KnownAllergies
Age
Affiliation
Name

Privacy managers (Carnegie-Mellon Univ)

- Consoles to help users manage the release of attributes
- Can leverage trust, informed consent, default settings and preferences, etc.
- Must be carefully engineered
  - Across the variety of contexts
  - Across a variety of credential types
  - In ways that are user-effective
- Similar, less leveraged approaches are successfully deployed in a few settings.

Attribute authorities

- Entities that generate additional attributes about an individual (but do not provide other identity services)
- Examples include: Agencies (grant information, security clearances, etc) identifier services (ORCID, SSN, Driver's licenses, etc), auditors and compliance organizations, etc
- Many open issues exist:
  - Linking between attribute authority and {IdP, RP, third party, etc}, including LOA
  - Uni-directional or bi-directional, One time vs regular vs upon-change
  - Policy and contractual frameworks

Anonymous Credentials (Brown University)

- Special credentials issued by attribute authorities
  - Encrypted at rest; reduces privacy spills
  - When queried by RP, will do minimal disclosure of encoded attributes
    - E.g. Over 18, True/False on specific sets of attributes, such as citizen, medical, IMBY discussions, etc.
  - Can be done so that IdP does not know either the values being released or the RP's requesting information
- Need infrastructure to support deployment at scale
  - Delivering credentials to user and storing, scalable query controls, audit, policy issues, integrating with privacy management

INTERNET 2

Metadata and trust implications

- At scale, there needs to be ways to establish and convey trusted information about applications and services to users
  - Implies "vetting" or auditing processes for services
  - Implies metadata that can convey this information in real time to users
  - Implies trust in the metadata
- Dynamic metadata services
  - Work is already underway on this in other places
- Federation operations need to evolve
- Auditing applications
  - For "privacy-preserving" approaches (minimal attribute requests, informed consent, proper handling and disposal, etc.), for COPA compliance, for …
  - Prototype approaches are successful; market needs to grow

Significant pilots and testbeds

- Intent is to facilitate significant deployments through:
  - Three partially supported leadership deployments of MFA at MIT, Texas, and Utah
  - Focus testing of privacy managers through development cycles
  - Identify and leverage existing IdM consortia to pilot, with active support and facilitation, both privacy managers and anonymous credentials
  - Create a broader cadre of observing institutions that participate in the planning and deploys, including attribute/schema development
- Work actively with related communities, from registrars to researchers, to help them understand the issues and opportunities

Policy thickets

- Anonymous credentials
  - How to deploy? How to choose acceptable attribute providers? How much to audit? Legal exposures?
- Privacy
  - Retention of attribute releases? Portability?
- Application privacy assessment “marketplace”

How it all fits together

- A user, in their context as a university student, uses a privacy manager to release their institutional affiliation to student discount services
- A user, in their context as a citizen, uses a privacy manager to release sufficient residence information that allows them to then anonymously post to the neighborhood-only wiki.
- A user, in their context as a consumer, uses a privacy manager to manage the release of preferences (e.g. zip code, preferred language, geolocation, etc) to customize commercial services while preserving privacy
- A user, in their context as a worker, uses a privacy manager to release anonymous credentials (such as security clearances and personal medical information) to third party contractors.
- A parent uses a privacy manager to manage their children's on-line privileges to COPPA compliant applications

Thank you! For more information,
please visit www.internet2.edu

Thank you! For more information,
please visit www.internet2.edu