Carnegie Mellon University

Low Level of Assurance Identities & OpenID

Russell J. Yount <rjy@cmu.edu>
Systems Architect

Shibboleth & InCommon Federation

The Identity Solution for U.S. Higher Education

- Shibboleth
  - OS Neutral Solution (Windows/Linux/Unix)
  - Open Source/Community Supported
  - Code has been widely reviewed for security
- InCommon Federation/Local Compus Federations
  - Federation framework enables trust in identities
    - InComon POP – Participant Operating Practices
    - Level Of Assurance (LOA) - InCommon Silver/Bronze
  - Enables single rather than multiple identities (accounts) for individuals
    - No need for second for collaborative researchers sharing resources
    - No need for second for cross registered student access
    - Vendor software as a service (SAS) solutions use existing identities
    - An academic visitor can use home identity for local service access

Shibboleth & InCommon Federation

The Identity Solution for U.S. Higher Education

- We have embraced it because accounts are expensive
  - Registration process
    - Requires coordination with account holder
    - Identity proofing issues
  - Password maintenance
    - Initial password
    - Forgotten password

- Solution for population directly affiliated with U.S. Higher Education
  - Students
  - Faculty
  - Staff

Other Populations We Care About?

There are other population we often are requested to service

- People with distant relationships with university
  - Parents, guardians, spouses, embassy consulate
  - Alumni
  - Principals/Guidance Counselors
  - Prospective Students (preadmission)
  - Donors

- Non-academic visitors to campus
  - People involved in campus events (presenters, associates, media)
  - Family/friends visiting students
  - Corporate sponsors

Other Population We Care About?

There are often very expensive to service with traditional accounts

- Impractical to handle as normal accounts
  - Short notice of need
    - Tomorrow, Today, Now
  - Short lifetime
    - Weeks, Days, Hours
  - Identity proofing is impractical
    - Likely just vouched for by others

The account requirements of these population are often

- Identities only require a Low Level of Assurance (LLOA)
- Identities limited to use with small number of services
- Identities are vouched for by other campus identities as identity proofing

OpenID

OpenID has matured in the past few years

- OpenID 2.0 and associated standards have matured
  - Attribute release
  - Documented standards
  - http://Openid.net
- U.S. Goverment Federal Identity Credential & Access Management (ICAM)
  - http://www.idmanagement.gov
    - OpenID Providers
    - InCommon
  - ICAM OpenID 2.0 Profile
- Open Identity Exchange – OIX
  - http://openidentityexchange.org
  - Goals of trust establishment similar to federations

OpenID

OpenID has a large number of users

- Some of the larger Identity Providers such as
  - Google
  - Yahoo
  - MSN
  - AOL
  - MySpace

- Many smaller Identity Providers
  - MyOpenId
  - ClaimId

- OpenID identity providers service the “Other populations we care about”
  - Confirmed by email addresses known to our student information system

OpenID & Shibboleth on Campus

Desire to operate Shibboleth only service providers

- Work to migrate to Shibboleth from Pubcookie is enough for service owners
  - Complexity and expense of Shibboleth/OpenID configuration is too much
  - Service provider want to develop services not SSO systems

Provide an OpenID to Shibboleth Proxy for Local Federation

- Can make OpenID integration easier for service providers
  - Discovery Service treats OpenID gateway part of local CMU federation
    - Pittsburgh Campus
    - Qatar Campus
    - Department Identity Providers
    - OpenID

OpenID & Shibboleth on Campus

OpenID gateway technical issues

- Should not use OpenID identities directly
  - What if in the future someone sponsors Google as part of InCommon?
  - Seems just wrong to assert non-CMU namespace
  - Translate OpenID identity to internal user@openid.cmu.edu namespace
- OpenID identities are not always email addresses
  - Sponsor or voucher likely can know users email address but not OpenID
  - Registration service invites by email for people register
  - Registrant chooses OpenID provider to use to register
  - Plan to collect some additional contact information on registration
    - Maybe via OpenID attributes

OpenID & Shibboleth on Campus

OpenID to be presented to service owners as

- For use in Low Level of Assurance access to services
  - Weak identity proofing
  - OpenID generally not as cryptographically secure
- Service must obtain email address of OpenID account holder
- Service requests to IDM an invitation be sent to OpenID account holder

Pilot use case for OpenID gateway

Student Information System Billing

- Currently students can have copy of bill sent to Parents, Guardians, Spouses, Embassy Consulate
- Plan to phase over viewing of bills to OpenID access Q3 2011
- Will also accept InCommon Identities
  - Only for Low Level of Assurance Access due to identity proofing issues