Outsourcing Trust

Internet2 Spring 08 Membership Meeting

Asbed Bedrossian
University of Southern California
April 22, 2008
Align IT with the university’s policy and business

Prove alignment with a process that is

- Sound (technology, security, interoperability, standards-based)
- Transparent (comprehensible, documented, repeatable)
- Accountable (auditable, consistent, comprehensive)
- Charged (endorsed at highest attainable level of leadership)
One picture… one thousand words…

- SIS
- Payroll
- iVIP
- USCard
- mu
- Person Registry (PR)
- Business Rules
- GDS LDAP
- Shib
- Legacy LDAP
- AD
- Kerberos
- Library Svcs
- myUSC
- Blackboard
- Web Reg
- ePay
- Advisement
- Roster
- White Pages
- Legal Waivers
- HIPPA Waivers
- Google Apps
- Email
Back in IT heaven

- SIS
- Payroll
- iVIP
- UCard
- mu

- Person Registry (PR)
- Business Rules
- GDS
- LDAP
- GDS COMMITTEE
- Library Svcs
- myUSC
- Blackboard
- Web Reg
- ePay
- Advisement
- Roster
- White Pages
- Legal Waivers
- HIPPA Waivers
- Google Apps
- Email

DATTEAM

Shib
The Governance cloud

- **The GDS Exec committee**
  - Focuses on prioritization, technical and IAM roadmapping issues
  - Attended by Systems of Record (SORs) and the GDS team

- **The Data Committee**
  - Focuses on issues of data output and integrity from the PR and GDS
  - Attended by SORs, GDS team and Data Stewart business specialists

- **The Directory Steering Committee (DSC)**
  - Focuses on issues of data management policy, data import into the IAM cloud, and data release to sponsored services
  - Attended by leaders in policy and technology from schools and departments, data stewarts, CIAO, CIO reps.
  - Expecting a high level appointment and charge for this committee
The liabilities

- Privacy
  - Email, online white pages, LMS, grades, etc.

- Compliance
  - HIPPA, FERPA, Financial

- Financial
  - Money matters, graduation assurance

- Branding
  - PR presence online
The university has charged and trusts its data stewards and SORs with the protected data and identities of its members.

Locally, we ensure that level of trust floats to the IdP, and all the way out to the service provider.

Serving roughly 15K faculty and staff, 35K students. About 50,000 members.
But what about 10K affiliates

300K pre-student recruits, inquirers, prospects, with a requirement to keep 2 years, 600K worth of them

250K alumni…

…and 100 million Trojans not yet born?

Do we have a Y10K problem?
The case for OpenID…

- Serve large constituencies
  - Increase scalability
- Leverage existing online identities
  - Reduce cost
- Meet low risk service requirements
  - Reduce risk
...and the case against

- No Trust in the IdP
  - Who are they?
  - What is the vetting process?
  - What is the physical security environment?
  - What is the IT security environment?

- No Trust in the process
  - Who or what is the IdP?

- Relativistic identity frame of reference
  - No anchor. Or not anchored to the institution’s frame of reference.
  - How do you define a level of assurance on an assertion? an identity?
A use case

Managing relationship with “pre-students”

- The good: features are low risk
  - Admission application
  - Request for Information
  - Search/response
  - Campus tour and event registration
  - Application document management
  - Financial aid planner
  - Notification communication
  - Online certification

- The bad: self-registration required, needs to open university ID generating code to the public. Possibly more.

- The ugly: wanna a USCID?