Identity Meets Reality

RL “Bob” Morgan
University of Washington
CAMP Shib, Burlington, VT, June 2006
Topics

• Federation and interfederation
• Beyond WebSSO
• Identity, society, universities
"The Phantom slowly, gravely, silently approached. When it came, Scrooge bent down upon his knee; for in the very air through which this Spirit moved it seemed to scatter gloom and mystery."

- Dickens, A Christmas Carol
trust federation for US Higher Education
  and our partners
  HE institutions are members, others sponsored
  operated by Internet2
currently based on SAML technology
  specifically Shib, but others possible
  other technologies as needed, e.g. RADIUS
low barrier to entry
• slow steady growth, lessons learned
  • setting the bar at the right height
    • even simply documenting practices can be a struggle
  • legalities for open-ended services are hard
  • maturing technical specs, e.g. re attribute use
  • adding an “open” IdP, maybe two or three
  • new focus on interfederation with US E-Auth
  • relationship to HE federations, both US- and non-
• chartered to support e-government, run by GSA
• access to US government apps for citizens, employees, contractors, etc
  • agencies obliged to operate apps in EAI federation, IdPs can be gov agencies and non-gov companies
• standard levels of assurance
  • 1 - 4, low to high, SAML+passwords to PKI certs
• assessment frameworks for IdPs, apps
• legal participation agreement (93 pages ...
EAI technology

- SAML for levels 1 - 2, client certs for 3 - 4
  - approved SAML product list, compliance-tested
- EAI-specific X.509 certification authority
- EAI portal used for all signon flows
- mandated operational features
  - security/uptime probing, user acceptance, loggin/reporting, branding, etc
• access to USG apps for HE members
  • grants management, Dept of Ed, research collabs
• alignment project active now
  • agreement, pilot by end of 2006
• many problems to overcome
  • certs, role of portal, assurance, liability, privacy, ...
• implies new InCommon levels of membership
  • matching EAI level 1, 2 ; who will do auditing?
Global (inter)federation

- European HE federations leading the way
  - natural fit for national R+E networks (NRENs)
  - some SAML/Shib-based, some not
  - leveraging existing arrangements with content publishers, pushing those relationships forward
  - interfederation more compelling
    - eduGAIN project developing SAML-based interfed tech
    - also applies to interfed with US?
Internet scale federation

- IdP discovery
  - WAYF is weakest link of current SAML-based ops
  - is it the SP's problem? some SPs don't want it ...
  - client (i.e. browser) improvements to the rescue?
- dynamic trust
  - DNS-style SAML metadata lookup?
  - from trust federations to reputation?
It's the apps, stupid

• when will apps be federated OOtB?
  • many popular apps (blogs, wikis) being webSSO-enabled now, hence Shib-enabled for simple authn
  • vendor apps starting to talk about it
  • key HE apps: Sakai, BB, outsourced providers
  • e-science/Grid: GridShib component
    • alignment with PKI-based environments
brave new WS-world

- new apps, interfaces are “web services”
  - meaning SOAP, usually
  - how are these secured? especially in multi-tier scenarios, ie operations invoked by web app; does SAML apply?
  - WS-Security and friends are one approach
  - Liberty WSF alternative likely more realistic
  - you can help define Shib support ...
• vast convergence of identity interests
  • the phishing problem
  • ordinary people as resource owners: blogs, wikis, photos/music, RSS, social networks, blogspam
  • personal privacy, personal control: institutions of all kinds are the bad guys (including us)
  • many technical solutions being promoted: two examples: OpenID, information cards
OpenID

• see http://openid.net/
  • developed in fight against blogspam
  • user identifier is your URL (you have one, right?)
  • mechanism/assurance similar to email signup
  • operations crypto-protected, trust management is up to you (aka “reputation”)
  • spreading through blogspace
  • Shib support? no plans ...
Information cards

• Microsoft-promoted, much industry uptake
  • formerly InfoCard, aka “identity metasystem”
  • MS “identity selector” is CardSpace, in Vista
• identities visible to users as “cards”
  • user-generated or third-party provided
  • typical signon, credit card purchase cases
• supported by WS-Trust protocol
• Shib support? we hope so
Whither institutional identities?

- the compliance factor
  - high-security, high-trust, high-value, high-cost, institutionally-controlled and -licensed, audited ...

- the community factor
  - a valuable and popular player in identity communities, easily obtained, portable, low-barrier, adaptable, multi-protocol ...

- can we do both?