Internet2 Middleware: The Big Picture Gets Bigger

RL “Bob” Morgan
University of Washington
Internet2 Spring Member Meeting
April 2007
Topics

• The societal function of HE middleware
• Internet2 Middleware software projects
• Internet2 Middleware-related services
• The extended community
Some philosophical inspiration

THE OPEN SOCIETY AND ITS ENEMIES

by KARL R. POPPER

Volume I

THE SPELL OF PLATO
Internet2 Middleware: The Open Infrastructure and Its Friends

RL “Bob” Morgan
University of Washington
Internet2 Spring Member Meeting
April 2007
Closed vs Open Societies

• Closed
  • caste-based, taboo-based, state-oriented, no distinction between natural law and custom, no outside influence, stable, change only via revolution

• Open
  • non-"organic", socially mobile, law-based, humanitarian, incrementally changing, unstable
“Abstract Society”

“Conceive of a society in which men never meet face to face -- in which all business is conducted by individuals in isolation who communicate by typed letters or by telegrams, and who go about in closed motor-cars... Such a society might be called a “completely abstract or de-personalized society.” (p. 174)

• De-personalization?
  • in the sense of “laws, not men”, or “policies, not personalities”
The unbearable burden of openness

• Open society
  • not “organismic”, constant ferment, seeking satisfaction in abstraction and rationality
  • benefits are: freedom, criticism, ability for incremental change

• Utopianism vs “piecemeal engineering”
  • piecemeal is many small experiments, correcting mistakes, seeking small correctable improvements
Institutions

• “Institution” (defined)
  • “a significant practice, relationship, or organization in a society or culture; an established organization or corporation (such as a bank or university)”

• Institutions exist to create and maintain trust
  • in their areas of business, by acting predictably, absorbing risk, producing reliable work
  • business of R&HE is creation and dissemination of knowledge, via practice of intellectual collaboration
Infrastructure and trust

• The reliable knowledge business
  • who created that knowledge, who reviewed it, who checked the bona fides of creator and reviewer, who published it, stored it, indexed it, etc
  • this is now overwhelmingly online and digital
  • tying knowledge processes to fundamental institutional infrastructure is a requirement to maintain our status as institutions
Infrastructure for trust

• Identity management
  • who are the people involved, what are their roles, what processes established this

• Access management
  • who can create, update, view; who set policies

• Federation
  • how all the above is made available to a world of partners
Shibboleth Project

• Shibboleth 1.x very successful
  • ~12 state/national Shib-based R&HE federations, commercial and government partners, many other deployments, opensaml use in products
  • put privacy on the federation map, via emphasis on attribute-based access control
  • put scalability on federation map, via emphasis on partner configuration via metadata
Shibboleth 2.0

• 2.0 syndrome?
  • maybe; team is now bigger, focused on release

• key new features
  • multi-vendor interop via SAML 2.0
  • improved discovery
  • self-contained SSO, hooks for non-Shib SSO
  • focus on attribute-handling in both IdP and SP
  • fully compatible with Shib 1.3
More Shib 2.0

- more features
  - customizable/pluggable throughout
  - modular multi-protocol support
  - attribute encryption
- beyond 2.0
  - EZ-Install IdP for small shops
  - WS-*, Liberty for non-web-SSO usage
  - Information card support (funding by Microsoft)
Grouper Project

• now at release 1.1
  • production use at several HE sites, evaluation at many more, incorporated into caBIG cancer research infrastructure
  • performance/UI/import-export improvements
  • site integration via Subject API (shared with Signet)
Grouper Futures

- integrated Grouper+Signet “quickstart”
- change history
- incremental/event-based provisioning
- standard “people picker” UI on Subject API
- protocol interfaces
- rule-based aging, deactivation, reactivation
- long-term sustainability model
Signet Project

• now at release 1.0.1
  • pre-production and evaluation use at many sites
  • new 1.2 release shortly

• Futures
  • improved delegation
  • bulk privilege assignment, revocation
  • XACML support
  • long-term sustainability model
InCommon Federation

- 50 participants (35 HE, 15 sponsored)
- working groups driving new use cases
  - TeraGrid integration for science-site access
  - Student-process use cases
    - admissions, student 3rd-party services, transcripts, enrollment verification; active registrar participation
  - Library-services adoption
  - iTunesU integration
InCommon and US Gov Federation

- InC collaborating with E-Auth for quite a while
  - E-Auth recently revised participation rules, revising CAF/LoA based on NIST revisions due date June
  - InC and EAuth expect to sign interfed MoA in June
  - Dept of Ed applications looming
  - InC working separately with NIH on federated access to several NIH resources
USHER CA

• Root PKI certificate authority for US higher ed
  • now open at usherca.org
  • issues certs to HE institutions and sponsored partners
  • same institutional vetting process as InCommon
  • defined lightweight “expected practices”
  • first certs issued shortly ...
Middleware Initiative and MACE

• MACE stable (maybe too stable)
  • looking forward to Internet2/NLR denouement
  • dealing with some member job changes
• Initiative
  • seeking new round of NSF funding
  • exciting new middleware staff ...
  • new product presentation focus
MACE-Dir and eduPerson

• continued focus on attribute use in SAML
  • agreeing on common approaches for providing authorization-useful attributes to widely-used service providers

• eduPersonScopedAffiliation
  • a new look at affiliation values: what's the useful level of detail and precision, internationalization

• eduPersonEntitlement
  • useful commonly-defined values, patterns?
Collaborative Applications Scalability

- the modern app environment
  - many users, many orgs, many collaboration tools, many collaborations using many kinds of apps, many kinds of existing infra
  - deployers must manage application suite access
  - some work but state of art is poor
  - Advanced CAMP conference on this topic, Portland, Oregon, June 27-29 (please attend!)
International middleware

• Many EU/AU initiatives
  • eduRoam: federated wireless network access
    • work to add SAML for attribute-based access
  • eduGAIN: interfederation approach
  • ECAM: Euro MACE-like group
  • SCS commercial PKI root
  • all-federations work with key service providers
  • JISC federation animation ...
Collateral activities

• EDUCAUSE Identity Management Constituent Group
  • active useful email list re IdM deployment

• ITANA
  • “MACE-like” IT Architecture activity
  • itana.org
  • first face-to-face in NYC May 22 (please attend!)
Internet Identity

• Information cards
  • Microsoft CardSpace 1.0 in Vista, XP
  • other identity selectors, IdPs, RPs happening
  • support in Shibboleth starting up

• OpenID
  • lots of buzz, success still in “consumer” areas
  • may help apps to externalize
  • can community hold together to extend it?
Summary

- Middleware world grows based on incremental extensions, focusing on core notions of institutional and personal credibility and control
- We're still having fun ...