Middleware Activities Update

Internet2 Membership, with coordination provided by Internet2 et al. presentation by Renee Woodten Frost.

Internet2 and the University of Michigan CNI Fall Task Force Meeting December 2000

Internet2 New Initiatives

A brief introduction to new initiatives launched at the Internet2 Fall Member Meeting:

- End-to-End Performance
- Expanded Access

End-to-End Performance Initiative

Goal: To create a ubiquitous, predictable, and well supported environment in which Internet2 campus network users have routinely successful experiences in their development and use of advanced Internet applications.

Components:
- distributed, coordinated Performance Evaluation and Response Teams (PERTs), information resources, and mechanisms for access to experts
- a persistent, proactive, and widely deployed performance measurement infrastructure, including tools and instruments for detection and resolution
- ongoing outreach, tech transfer, and dissemination of best practices to the Internet2 membership, and beyond.

Timeline:
- planning cycle now through late January, 2001
- RFP published late January to identify small set of partner campuses for second phase
- second phase begins early April

Expanded Access - Sponsorship

- One or more member universities may sponsor a networked aggregate of educational organizations (e.g., a state education network) in the same state.
- In states with multiple state education networks (e.g., distinct K-12, CC, and 4-year college networks), one or more sponsors can work with the same Abilene Connector to aggregate these networks' traffic.
- Upon approval of the Participant, the Connector assumes fiscal and operational responsibility for the Sponsored Education Group Participant to both UCAID and the Abilene NOC.

Expanded Access - Sponsored Education Group Participation

- Effective January 15, 2001, a networked aggregate of educational institutions may gain access to Abilene as a Sponsored Education Group Participant.
- designed primarily to accommodate existing and emerging state-based education networks (Regional GigaPoP proposal – June, 2000)
- reflects modified Abilene CoU (approved by UCAID Board – October, 2000)
- This new class of Abilene participation supplements the existing classes of Member Participant, Collaboration Site, and Sponsored Participant
- Sponsored Participation remains a viable option for individual colleges and school districts
- Applications will be accepted commencing December 1, 2000
Along a middleware path...

Identifier mapping (prerequisite)
EduPerson - an objectclass for higher education
Directory of directories - large-scale directory interactions
Shibboleth - inter-realm authentication and basic authorization

Applications integration
  • H.323
  • Jabber - an instant messenger
  • WWW

Other Middleware Sessions
Internet2 Fall Meeting

Identifier Mapping
Getting the house in order
Establishing enterprise names spaces and ids
Obtaining an institutional OID
http://middleware.internet2.edu/earlyadopters/identifier-mappings/

eduPerson
A directory objectclass to support inter-institutional applications
Contains suggested attributes for instructional, research and administrative inter-institutional use
Fills gaps in traditional directory schema
Intends to integrate with Grid, IMS, and other upper-middleware
Has parent classes of iNetOrgPerson and Person; states good practices for those attributes
Specifies several new attributes and controlled vocabulary to use as values.
Provides suggestions on how to assign values, but it is up to the institution to choose.
Version 1.0 almost done; one or two revisions anticipated

Issues about Upper Class Attributes
eduPerson inherits attributes from person, iNetOrgPerson
Some of those attributes would benefit from syntactic conventions about controlled vocabulary (e.g. telephones)
Some of those attributes need ambiguity resolved via a consistent interpretation (e.g. email address)
Some of the attributes need standards around indexing and search (e.g. compound surnames)
Many of those attributes need access control and privacy decisions (e.g. jpeg photo, email address)

New eduPerson Attributes v1.0
  • eduPersonAffiliation
  • eduPersonPrimaryAffiliation
  • eduPersonOrgDN
  • eduPersonOrgUnitDN
  • eduPersonPrincipalName
  • eduPersonGivenName
  • eduPersonName
Some Possible v1+ Attributes

- eduPersonSchool/CollegeName
- eduPersonPrimarySchool/CollegeName
- eduPersonJobClassification
- eduPersonFERPAFlag
- eduPersonAthlete
- eduPersonResearchInterest
- eduPersonNotEnrolledMailAddress

eduPersonAffiliation

Multi-valued list of relationships an individual has with institution

- Controlled vocabulary includes: faculty, staff, student, alum, member, affiliate
- Applications that use: DoD, white pages

eduPersonPrimaryAffiliation

Single-valued attribute that would be the status put on a name badge at a conference

- Controlled vocabulary includes: faculty, staff, student, alum, member, affiliate
- Applications that use: DoD, white pages

eduPersonPrincipalName

userid@securitydomain

EPPN may look like an email address but it is used by different systems.

- One must be able to authenticate against the EPPN
- Intended for inter-realm authentication such as Shibboleth
- In some situations it can be used for access control lists; if used, a site should make sure that the identifier is unique

eduPerson Next Steps

Led by Keith Hazelton, Wisconsin

version 1.0 by Dec 15.

Check with web site for additional changes
http://axle.dot.wisc.edu/~haz/mware/eduPerson01113doc.html

Participate: mace-dir@internet2.edu

A Directory of Directories

An experiment to build a combined directory search service for higher education

- To show the power of coordination
- To show the existing barriers to cooperation
  - standard object classes
  - standard display formats
  - standard meta-data
- To investigate load and scaling issues - on the clients and the servers
- To suggest the service to follow
**D o’ D Next Steps**

Michael Gettes, Georgetown project manager
SUN to provide equipment and directory software
Two different experimental regimes to be tested
- centralized indexing and repository with referrals
- large-scale parallel searches with heuristics to constrain search space
Will interact with EU directory work
Target is 5,000,000 entries among 100 institutions by March, 2001
http://middleware.internet2.edu for ongoing information

---

**Shibboleth**

A word which was made the criterion by which to distinguish the Ephraimites from the Gileadites. The Ephraimites, not being able to pronounce sh, called the word sibboleth. See –Judges xii.
Hence, the criterion, test, or watchword of a party; a party cry or pet phrase.
- Webster’s Revised Unabridged Dictionary (1913):

A catchword or formula adopted by a party or sect, by which their adherents or followers may be discerned, or those not their followers may be excluded.

1638 E. Notice, New Gospel 3: His followers sequestering themselves to such as were their own way...gave themselves to mirth and jollity...as if it were the only Shibboleth whereby to be discerned from the miserable Legalists that held mourning and sorrow for sinne.

-OED

**Shibboleth Discussion Outline**

- Model and Basic Approaches
- Assumptions
- Campus and Resource Requirements
- Deliverables
- Operation
- Design Issues
- Project Status/Next Steps

---

**Why Is Shibboleth Needed?**

There is a strong and growing demand for this functionality
Vendors haven’t (yet) addressed it;
When there is a solution, campuses will need an “open” solution
Isn’t This What PKI Does?

End-to-end PKI fits the Shibboleth model, but other forms of authentication do as well. Uses a lightweight certificate approach for inter-institutional communications - uses the parts of PKI that work today (server side certs) and avoids the parts of PKI that don’t work today (eg client certs). Allows campuses to use other forms of authentication locally. May actually have benefits over the end-user to target-site direct interactions...
Assumptions
Disturb as little of the existing campus infrastructure as possible
Encourage good campus behaviors
Be deployable soon
Engineer with PKI in mind
Require no new client software
Do not provide session management software for the target application
Create a marketplace and reference implementations
Accommodate push and pull authorizations

Campus and Resource Requirements
Campus-wide identifier space
Campus-wide authentication service
Campus-wide web single sign-on service
DNS that supports SRV records
LDAP-based web access controls
Implementation of EduPerson objectclass

Deliverables
Architecture and open standards
Apache module on the web server to redirect authentication requests and then accept authentication requests (that have passed the weblogin phase) and then process authorization steps
Reference implementation of a weblogin server
A "where from" service and a key exchange service (static at first, then perhaps dynamic)

Operational Steps
Many alternatives for implementation
Off-the-shelf will use redirects, URLs to contain transaction certs
"Where from" service
Public key exchange service

Design Issues
Transport of requests and credentials
Security of authentication requests and replies
If PKI, distribution of public keys
"Where from" service implementation - central service, distributed within security domains, distributed within web servers
Securing personal identity
Extensibility of credentials
Push authorization - forwarded credentials contain rights of user
Pull authorization - resource provider requests rights of user

What Phase I Will Not Do
Addressing the 3-tier problem
Formal trust management between domains
Authorization beyond htaccess
Implementing pseudonymous identity
What Phase I May Do

Reference web single signon implementation

Discovery process for important applications (e.g., classes, affiliations)

Discussants

Campuses
Internet2
IBM
Industrial cabal
Terena
The Athens replacement project (UK)
Libraries (DLF, CNI, EBSSCO)

Shibboleth
Project Status/Next Steps

Analysis largely complete; proposed architecture under discussion
IBM and Mace-Shibboleth are refining architecture and evaluating issues
IBM intends to develop an Apache web module (perhaps an extension of auth_ldap)
Internet2 intends to develop supporting materials (documentation, installation, etc.) and web tools (for htaccess construction, filter and access control, remote resource attribute discovery).
Testbed target start-up - March 1, 2001
Release - Summer 2001
Deployment - Fall 2001

Architectural Closure

Are the basic boxes and flows right?

Are there any boxes or flows that contain “show-stoppers”, or do we think we can work each out, perhaps with shims, scope limitations, static first steps, etc.?

Do we know of at least one way today, however ugly, that establishes the viability of the architecture?

Protocol Specifications

Define the units of information for the flows

Define the APIs that interface with the flows

Define the alternatives for service locations

Protocol Implementations

Apache modules

Proprietary implementations among web single signon vendors
Interested? Concerned?

Led by Steven Carmody (Brown) and RL "Bob" Morgan (Washington)

http://middleware.internet2.edu/shibboleth

mace-shibboleth@internet2.edu

Applications Integration

Many "killer apps" are stalled in deployment by lack of identifiers and associated authentication

Examples include
- H.323 (desktop video) (both direct client authentication and MCU-mediated)
- Instant messaging
- Distributed file systems

Strategies may include working with open source versions to include EPPN-based authentication

Opportunities for Volunteers

Nature of work - participating in bi-weekly calls, reviewing documents and specifications, seeking campus counsel, speaking one's clue

Mace-dir - working on eduPerson refinements, the directory-of-directory, directory aspects of Shibboleth, etc.

Mace-shibboleth - working on inter-realm authentication

Mace-med - working on issues in the integration of enterprise and academic medical middleware

HEPKI TAG and HEPKI PAG - PKI policy and technology issues, including mobility, profiles, etc.