DELOS
NETWORK OF EXCELLENCE ON DIGITAL LIBRARIES

Joint DELOS-NSDL
Summer School

NSDL
THE NATIONAL SCIENCE DIGITAL LIBRARY

Distributed Service & Identity Management

David Millman
NSDL Core Integration
Columbia University
May 2007

DL Site Components (review)

- store content
- discovery, navigation, tag, relate
- cite, reuse

DL Site Components (review)

- store content
- discovery, navigation, tag, relate
- cite, reuse

- identity management

Identity Components (1)

- prove identity (authentication)
  - login
  - userid/password, email/password
- obtain profile/demographic/personal data
- DL system decision to act based on user data (authorization)

NB: these may, or may not be supplied by user

Planning--Why identity?

- access restrictions
  - levels of participation (editor, moderator, contributor, administrator, cataloger, “security”)
  - content (license, copyright, dark archive)
- personalized functions
- evaluation, usage metrics

Relation to goals can determine requirements

- license: what terms?
- personalize: need to know how much? legal restrictions?
- evaluation: individual or aggregate data?
- open access: balance w/ other goals?

Identity Components (2) (questions)

- prove identity (how do you know it's accurate?)
  - I made my own
  - or, an organization gave me one (Member of Community)
  - organization follows a procedure (good enough?)
- obtain profile data (where does it come from?)
  - I fill out a registration form
  - and/or, an authority asserts data about me
- DL authorization decision
  - enforce DL policy

Dimensions of Trust ("Trust Fabric")

- value/risk of service
  - of dissemination of . . .
  - of impersonation of . . .
- privacy
- relationships
  - partners
  - users

Trust-in-Action

- For example, tension across goals: want to allow blog post from senior research faculty in Chemistry while maintaining anonymity
- For example, trust management tool: Level of Assurance standards process

Level of Assurance (LOA)

- Formal specifications to assess strength of identity assertion
- For example,
  - self-registered
  - identity assigned by my teacher
  - identity assigned by an officer of the institution
  - identity assigned after an in-person visit, presenting government-issued identification

[Tangent]

- Trust, value, risk and assurance methods in identity management are similar to authenticity & attribution of content.
- Authentication of people vs. authentication of documents or digital objects.
- See also digital signatures.
- See also “diplomatics.”

DL Planner Summary (1)

- Have clear goals and requirements
- Use appropriate identity technology
- Interoperate with partners

DL Planner Summary (1)

- Have clear goals and requirements
- Use appropriate identity technology
- Interoperate with partners

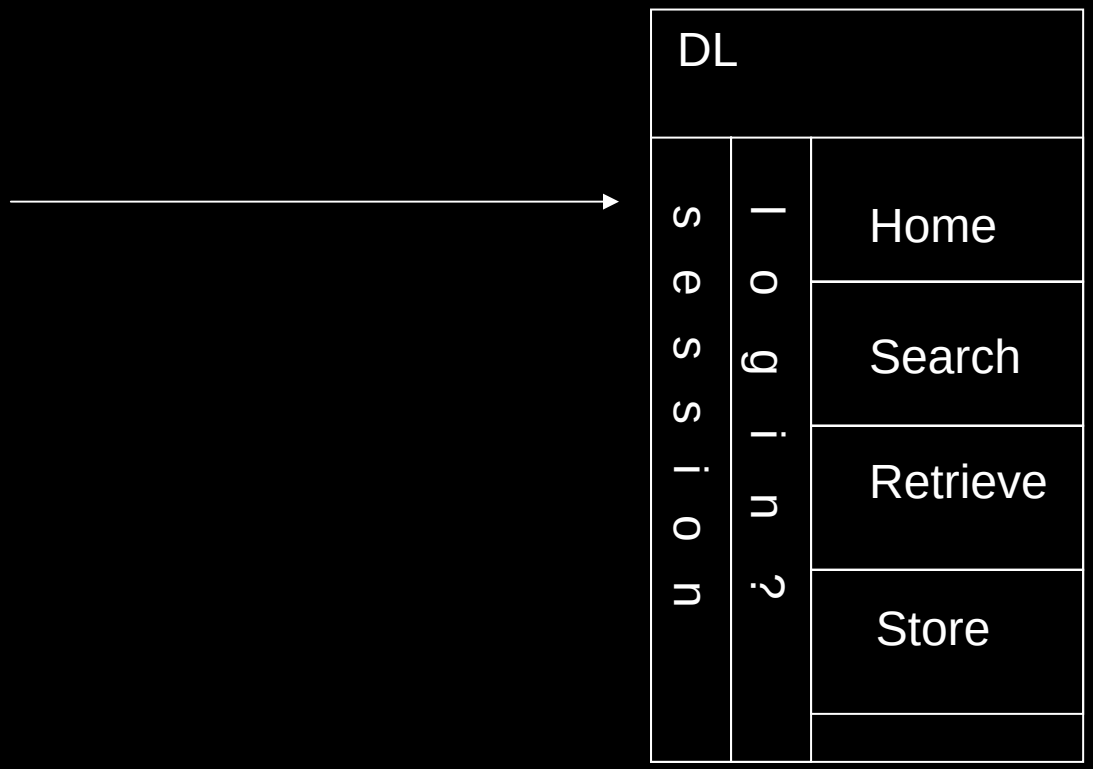
- How to interoperate with partners?

Interoperation

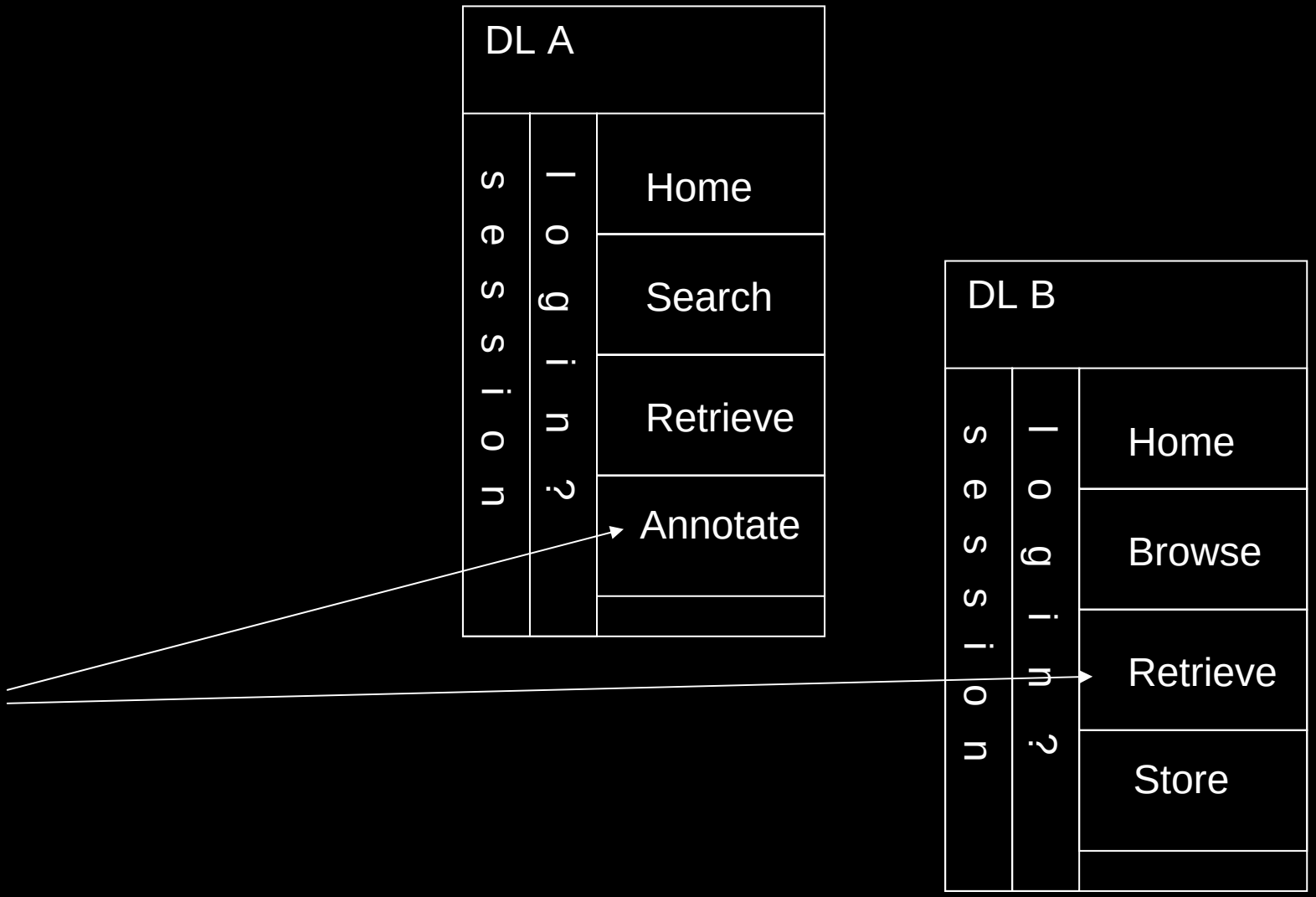
- Internal -- relationships, context, navigation, discovery
- External -- partners
- What are our responsibilities to partners?
  - offer standard metadata
  - offer standard interfaces
  - share identities across functions

Traditional Site Architecture

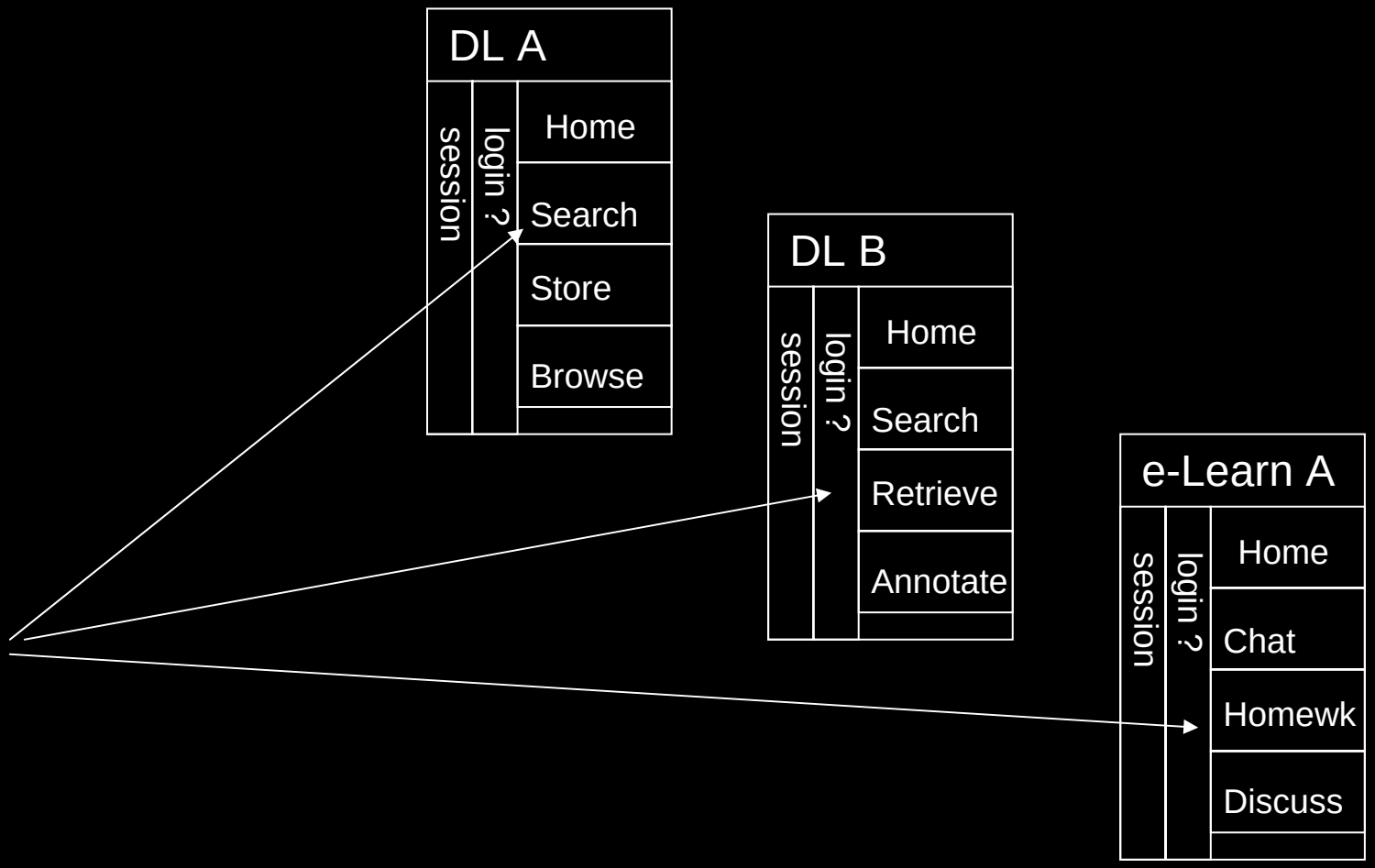
Alternative: login independent of function



Sharing Functionality



Sharing Functionality



Scaling Identity

- Prove identity
  - establish login and user management services with clear policy, not dependent on other DL site functions.
  - join others with similar policies
- Profile data
  - agree on vocabularies, authority control, definition of attributes with partners
  - many parallels with other kinds of metadata standardization
- Authorization decision
  - use maximum partner-agreed profile data; will create most seamless user experience

Scaling Identity

- Prove identity
  - establish login and user management services with clear policy, not dependent on other DL site functions.
  - join others with similar policies
- Profile data
  - agree on vocabularies, authority control, definition of attributes with partners
  - many parallels with other kinds of metadata standardization
- Authorization decision
  - use maximum partner-agreed profile data; will create most seamless user experience

FEDERATION

Example: NSDL

- Small number of identity-proving sites; moving to harmonize policies.
- Active profile attribute standardization process.
- Legal MOU (memorandum of understanding) among partners. Establishes “federation” of agreed policy and attribute definitions, and expectations for authorization decisions.

DL Planner Summary (2)

- Click to add text

David Millman
dsm@columbia.edu