Integrating Grid and Enterprise Infrastructures: Toward Scalability and Flexibility

http://arch.doit.wisc.edu/keith/cans/

Keith Hazelton, University of Wisconsin

Internet2 Middleware Architecture Committee for Education (MACE)

Identity & Access Management (IAM) Reality

- Each person's online activities are shaped by many Sources of Authority (SoAs)
  - Human resources system (payroll, etc.)
  - Student information system (registrar, etc.)
  - Resource managers
  - Program/activity heads
  - Other policy making bodies
  - Self

Identity & Access Management (IAM) Reality

- Shared, campus-wide middleware infrastructure should be operated centrally
  - Then departments/programs/activities do not have to build their own core middleware
- Management of the information it conveys should be distributed among the SoAs
  - Feed information from all of those Systems of Authority into the middleware infrastructure

Middleware becoming crucial to network and Grid communities

- QoS, Authenticated network access and network service ALL require IAM suite of functions
- In addition, Grid services need support for multiple-institution virtual organizations (VOs)
- Middleware becomes crucial for
  - Scalability (DeRoest: 300,000 users)
  - Flexibility (Many VOs, frequent changes)

Middleware becoming crucial to network and Grid communities

- Campus-wide infrastructure includes
  - Directory
    - Contains attributes about people (their “digital identity”)
  - Support for federated identity and access management
    - Project Shibboleth (open source, community-developed and supported SAML implementation from Internet2)
    - Being widely deployed internationally

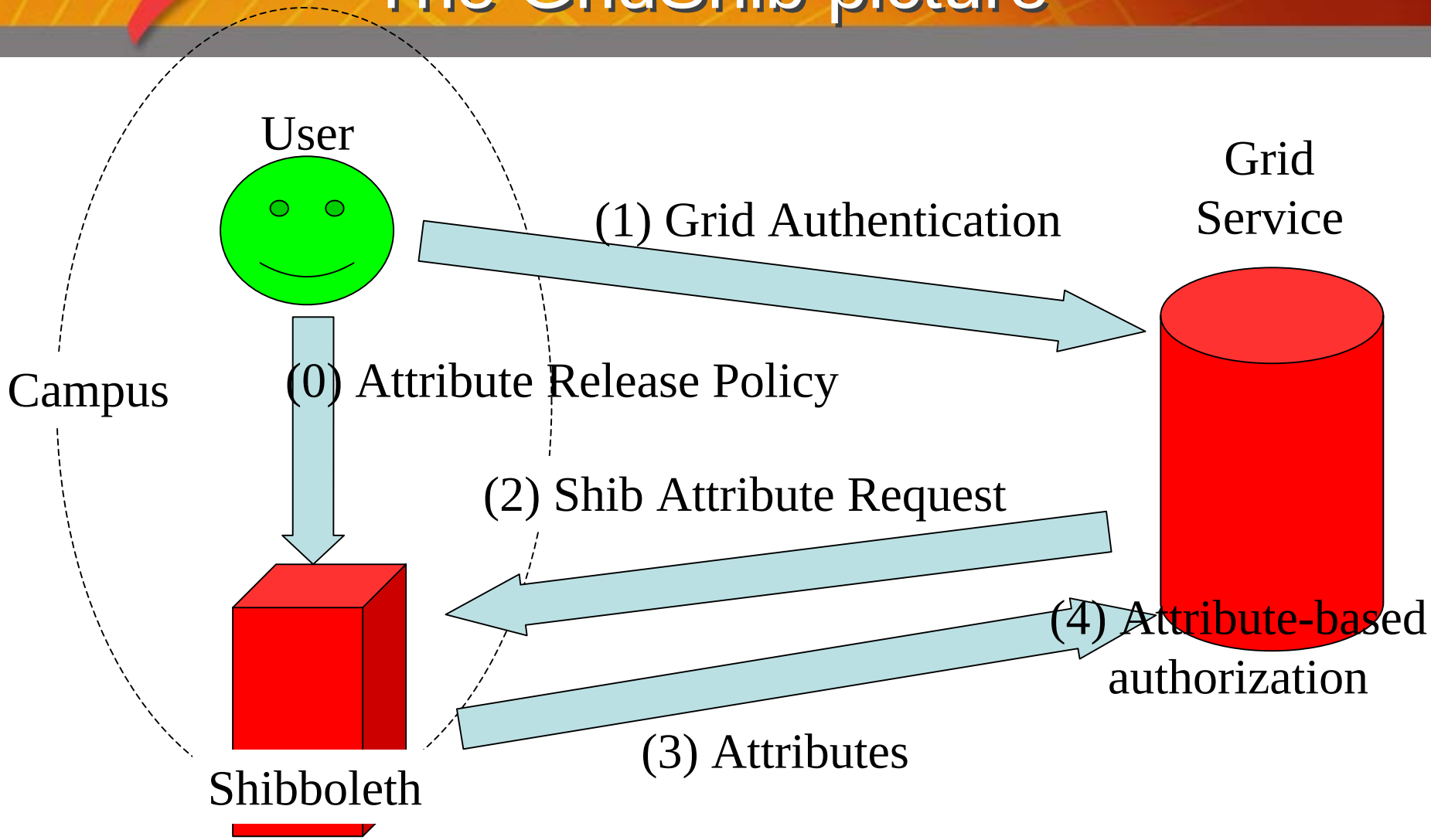
What is GridShib?

- NSF Middleware Initiative (NMI) Grant: “Policy Controlled Attribute Framework”
- Allow the use of Shibboleth-transported attributes for authorization in NMI Grids built on the Globus Toolkit v4
- 2 year project started December 1, 2004
- Participants
  - Von Welch, UIUC/NCSA (PI)
  - Kate Keahey, UChicago/Argonne (PI)
  - Frank Siebenlist, Argonne
  - Tom Barton, Uchicago
  - And many others

Why GridShib now?

- Attribute-based authorization has shown itself to be useful in large grids with far-flung participants in several types of roles
  - Identity-based approach scales poorly
- Shibboleth is well supported and becoming widely deployed
- SAML is used in the larger identity federation world, not just Shibboleth. Integrating SAML support into Grids opens the door to leveraging this large technology space

The GridShib picture



Infrastructure - Grid convergence

- What are likely paths of collaboration and convergence?
- SAML and WS* and PKI interoperability
  - to bring institutional IAM and Grid IAM into alignment
  - Project GridShib & JISC Project ShibGrid
- IAM infrastructures at departmental in addition to institutional levels

GridShib Integration Principles

- No modification to typical grid client applications
  - Modifications only to Grid Services and security clients (e.g. grid-proxy-init)
- Leverage shibboleth's attribute marshaling capability and release policies
- Leverage strategic investment that campuses make in Identity Management operations

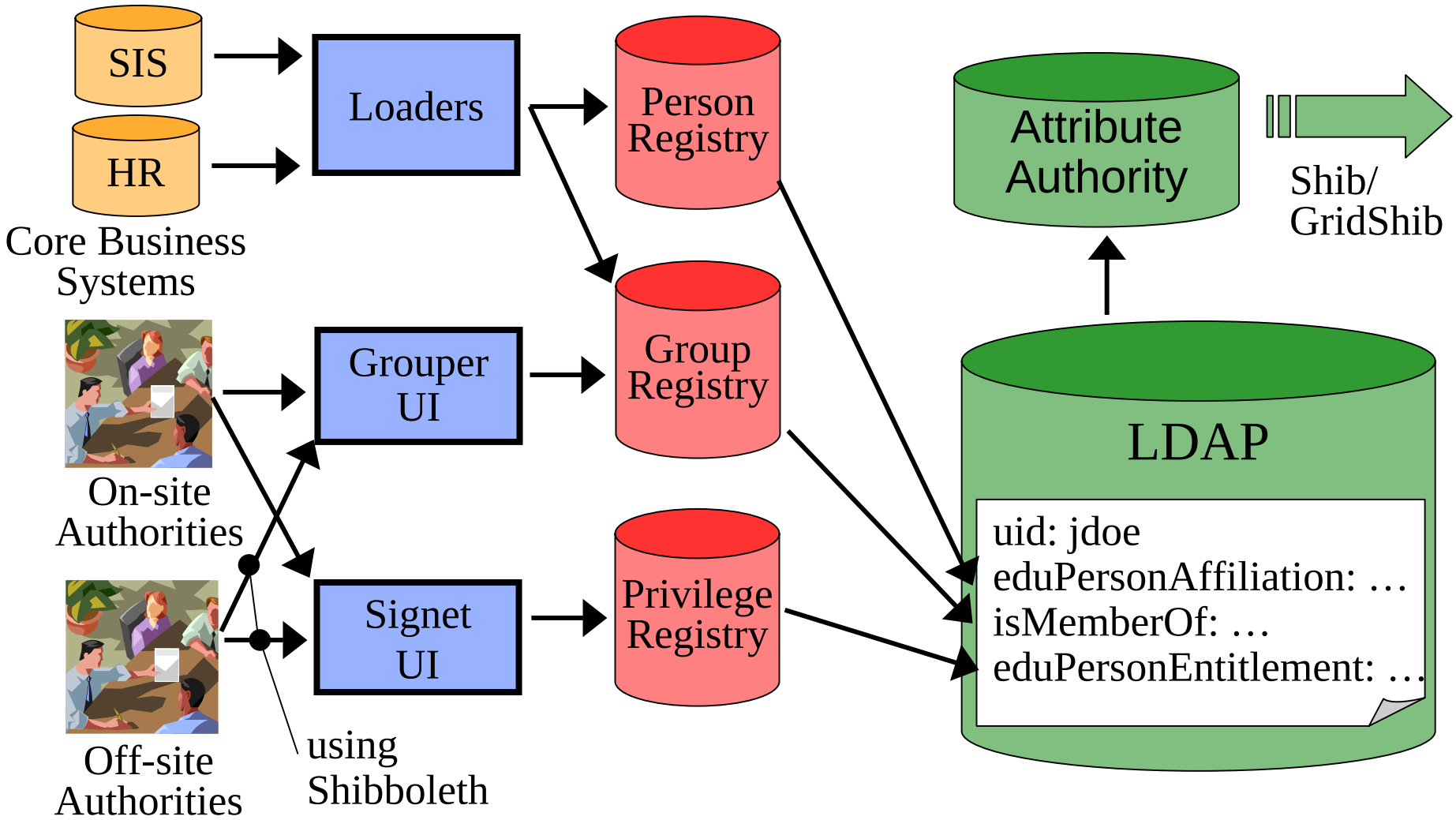
GridShib Progress

- Developers hired February 2005
- Grid - Shibboleth integration
- Shibboleth Identity Provider plugin
  - Maps externally-issued X.509 identity certificates to local identifiers
- SAML attribute marshaling in GT4 runtime

GridShib Progress (cont'd)

- Common attribute format internal to GT4 runtime to support access policies spanning SAML and X.509 PMI attribute sources
  - Uses XACML Request Context
- Initial GridShib release in beta testing
  - Based on GT 4.0 and Shib 1.3

Getting Attributes into a Site's Attribute Authority



Collaboration Opportunities

- Participate in beta testing of middleware components like GridShib to get your requirements into development stream
  - Email hazelton@doit.wisc.edu
- Participate in middleware-enhanced VO trials
- Others???

Q & A

- http://middleware.internet2.edu
- http://shibboleth.internet2.edu
- http://grid.ncsa.uiuc.edu/GridShib
- http://middleware.internet2.edu/dir/groups/grouper
- http://middleware.internet2.edu/signet
- http://www.incommonfederation.org
- hazelton@doit.wisc.edu