the globus alliance
www.globus.org

Identity Federation for Virtual Organizations: GridShib and MyProxy

APAN Middleware Workshop
Jan 22nd, 2006
Toyko, Japan

Von Welch
vwelch@ncsa.uiuc.edu

NCSA

Outline

- GridShib
- MyProxy
- Future plans: Shibboleth/MyProxy/GridShib integration

What is GridShib

- NSF NMI project to allow the use of Shibboleth-issued attributes for authorization in NMI Grids built on the Globus Toolkit
  - Funded under NSF NMI program
- GridShib team: NCSA, U. Chicago, ANL
  - Tom Barton, David Champion, Tim Freemon, Kate Keahey, Tom Scavo, Frank Siebenlist, Von Welch
- Working in collaboration with Steven Carmody, Scott Cantor, Bob Morgan and the rest of the Internet2 Shibboleth Design team

Motivation

- Many Grid VOs are focused on science or business other than IT support
  - Don’t have expertise or resources to run security services
- We have a strong infrastructure in place for authentication in the form of Grid PKIs
- Attribute authorities are emerging as the next important service

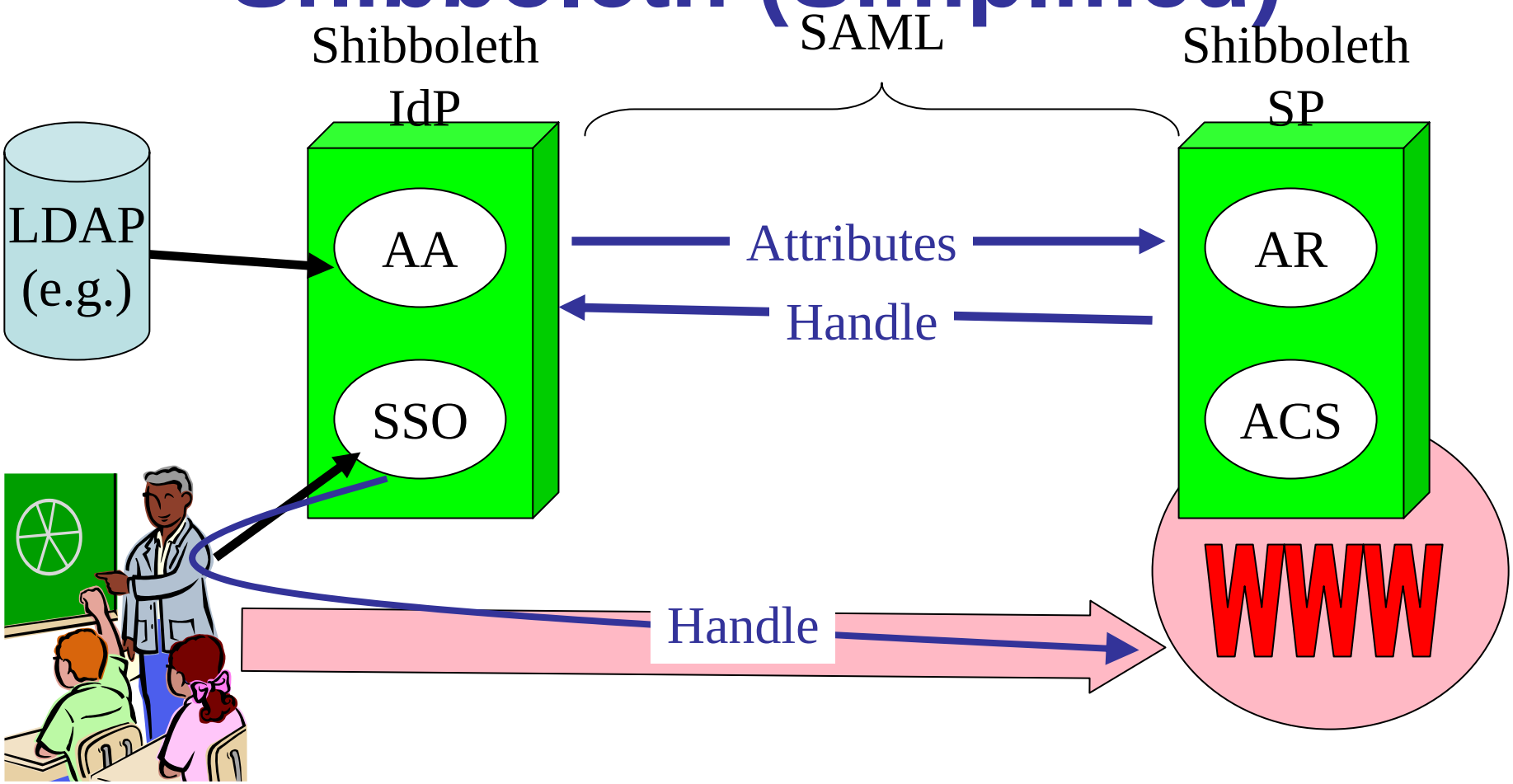
Shibboleth

- http://shibboleth.internet2.edu/
- Internet2 project
- Allows for inter-institutional sharing of web resources (via browsers)
  - Provides attributes for authorization between institutions
- Allows for pseudonymity via temporary, meaningless identifiers called ‘Handles’
- Standards-based (SAML)
- Being extended to non-web resources

Shibboleth

- Identity Provider composed of single sign-on (SSO) and attribute authority (AA) services
- SSO: authenticates user locally and issues authentication assertion with Handle
  - Assertion is short-lived bearer assertion
  - Handle is also short-lived and non-identifying
  - Handle is registered with AA
- Attribute Authority responds to queries regarding handle

Shibboleth (Simplified)



Globus Toolkit

- http://www.globus.org
- Toolkit for Grid computing
  - Job submission, data movement, data management, resource management
- Based on Web Services and WSRF
- Security based on X.509 identity- and proxy-certificates
  - Maybe from conventional or on-line CAs

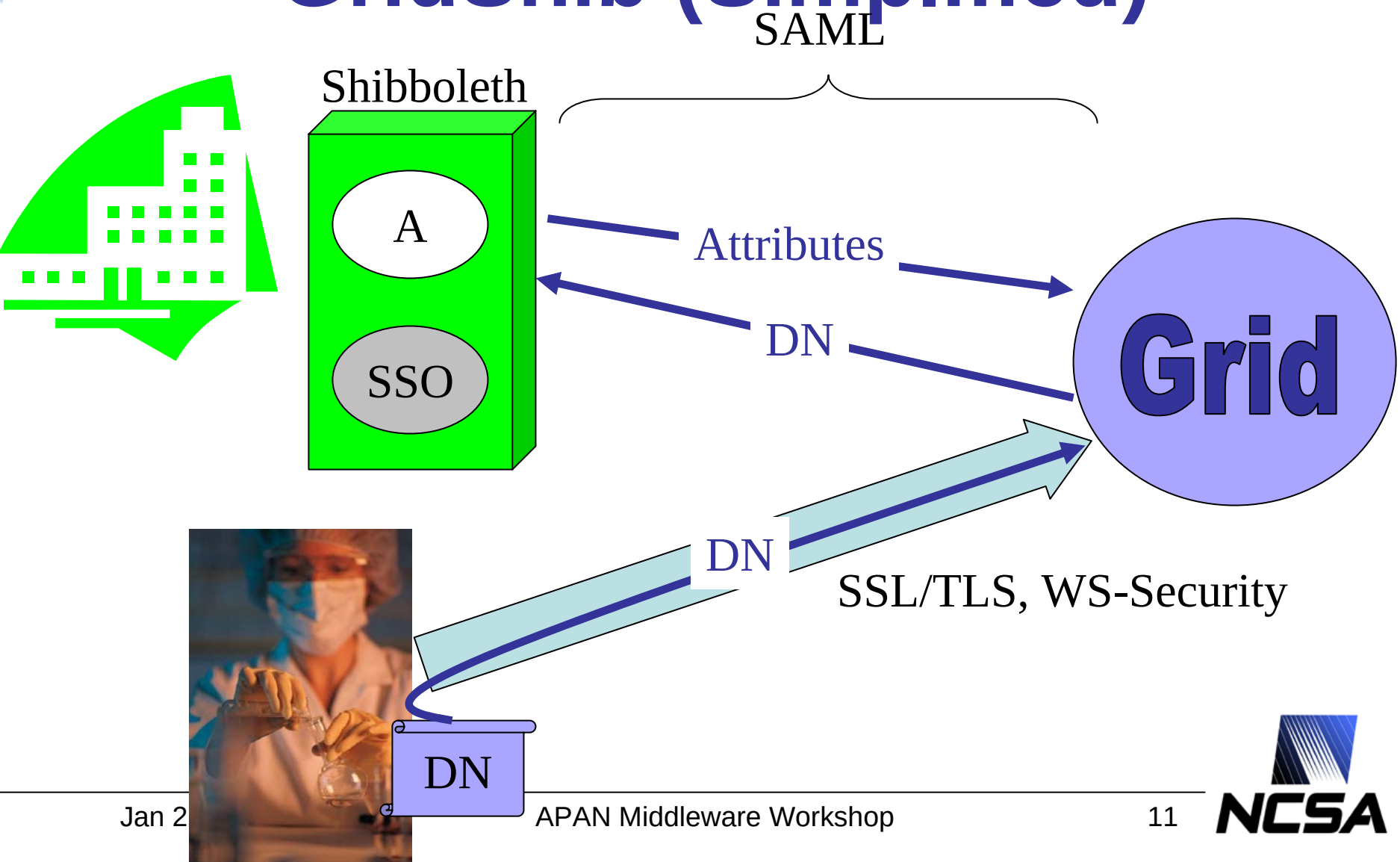
Grid PKI

- Large investment in PKI at the international level for Grids
  - Dozens of CAs, thousands of users
- International Grid Trust Federation
  - http://www.gridpma.org

Integration Approach

- Conceptually, replace Shibboleth's handle-based authentication with X509
  - Provides stronger security for non-web browser apps
  - Works with existing PKI install base
- To allow leveraging of Shibboleth install base, require as few changes to Shibboleth AA as possible

GridShib (Simplified)



Authorization

- Delivering attributes is half the story…
- Currently have a simple authorization mechanisms
  - List of attributes required to use service or container
  - Mapping of attributes to local identity for job submission

Globus Authorization Framework

- Authorization framework in Globus Toolkit
  - Siebenlist et. al. at Argonne
  - Pluggable modules for processing authentication, gathering and processing attributes and rendering decisions
- Work in OGSA-Authz WG to allow for callouts to third-party authorization services
  - E.G. PERMIS
- Convert Attributes (SAML or X509) into common format for policy evaluation
  - XACML-based

GridShib Status

- Beta release publicly available
- Drop-in addition to GT 4.0 and Shibboleth 1.3
- Project website:
  - http://gridshib.globus.org
- Very interested in feedback

What is MyProxy?

- Project led by Jim Basney @ NCSA
- A service for managing X.509 PKI credentials
  - A credential repository and certificate authority
- An Online Credential Repository
  - Long-lived private keys never leave the server
- An Online Certificate Authority
  - Issues short-lived X.509 End Entity Certificates
- Supporting multiple authentication methods
  - Passphrase, Certificate, PAM, SASL, Kerberos, Pubcookie
- Open Source Software
  - Included in Globus Toolkit 4.0 and CoG Kits
  - C, Java, Python, and Perl clients available

MyProxy Authentication

- Key Passphrase
- X.509 Certificate
  - Used for credential renewal
- Pluggable Authentication Modules (PAM)
  - Kerberos password
  - One Time Password (OTP)
  - Lightweight Directory Access Protocol (LDAP) password
- Simple Authentication and Security Layer (SASL)
  - Kerberos ticket (SASL GSSAPI)
- PubCookie

MyProxy Online Credential Repository

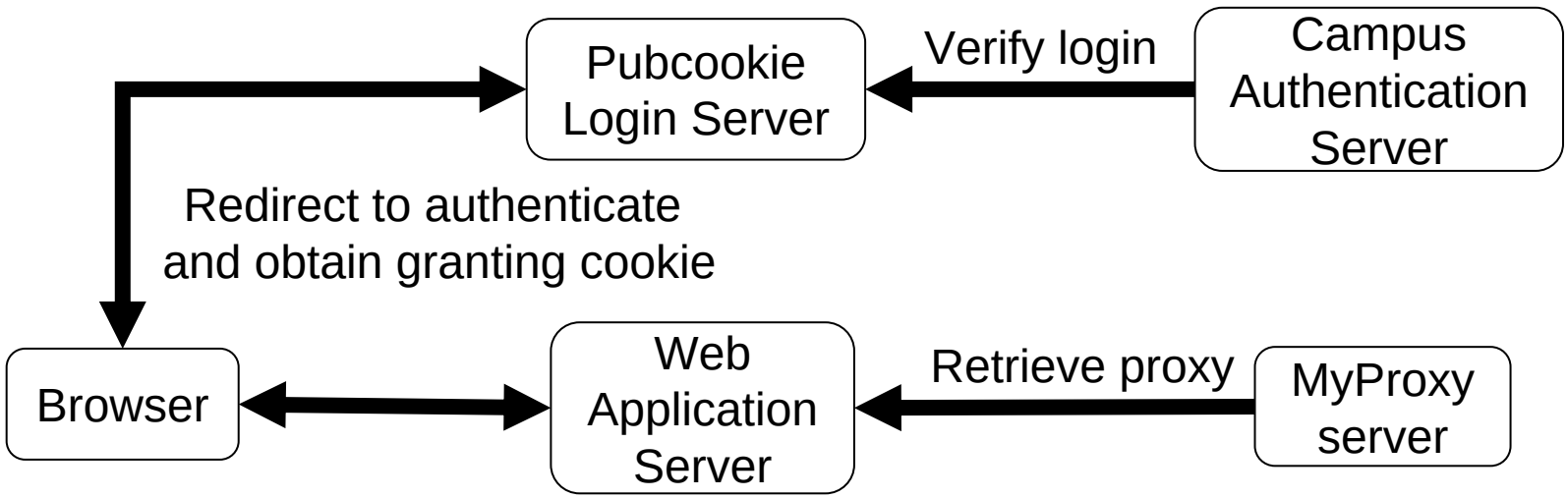
- Stores X.509 End Entity and Proxy credentials
  - Private keys encrypted with user-chosen passphrases
  - Credentials may be stored directly or via proxy delegation
  - Users can store multiple credentials from different CAs
- Access to credentials controlled by user and administrator policies
  - Set authentication requirements
  - Control whether credentials can be retrieved directly or if only proxy delegation is allowed
  - Restrict lifetime of retrieved proxy credentials
- Can be deployed for a single user, a site, a virtual organization, a resource provider, a CA, etc.

MyProxy Online Certificate Authority

- Issues short-lived X.509 End Entity Certificates
  - Leverages MyProxy authentication mechanisms
  - Compatible with existing MyProxy clients
- Ties in to site authentication and accounting
  - Using PAM and/or Kerberos authentication
  - “Gridmap” file maps username to certificate subject
    - LDAP support for mapping
- Avoid need for long-lived user keys
- Server can function as both CA and repository
  - Issues certificate if no credentials for user are stored

MyProxy and Pubcookie

- Combines web and grid single sign-on
  - Authenticate to MyProxy with Pubcookie granting cookie



Jonathan Martin, Jim Basney, and Marty Humphrey, "Extending Existing Campus Trust Relationships to the Grid through the Integration of Pubcookie and MyProxy," 2005 International Conference on Computational Science (ICCS 2005), Emory University, Atlanta, GA, May 22-25, 2005.

Example: TeraGrid User Portal

- Use TeraGrid-wide Kerberos username and password for portal authentication
  - Obtain PKI credentials for resource access across TeraGrid sites via portal & externally
- \

Example: LTER Grid Pilot Study

- Build a portal for environmental acoustics analysis
- Leverage existing LDAP usernames and passwords for portal authentication
  - Obtain PKI credentials for job submission and data transfer
  - Using MyProxy PAM LDAP authentication

LTER

Long Term Ecological Research Network Information System

Example: NERSC OTP PKI

- Address usability issues for One Time Passwords
  - Obtain session credentials using OTP authentication
- Prototyping MyProxy CA with PAM Radius authentication
  - ESnet Radius Authentication Fabric federates OTP authentication across sites

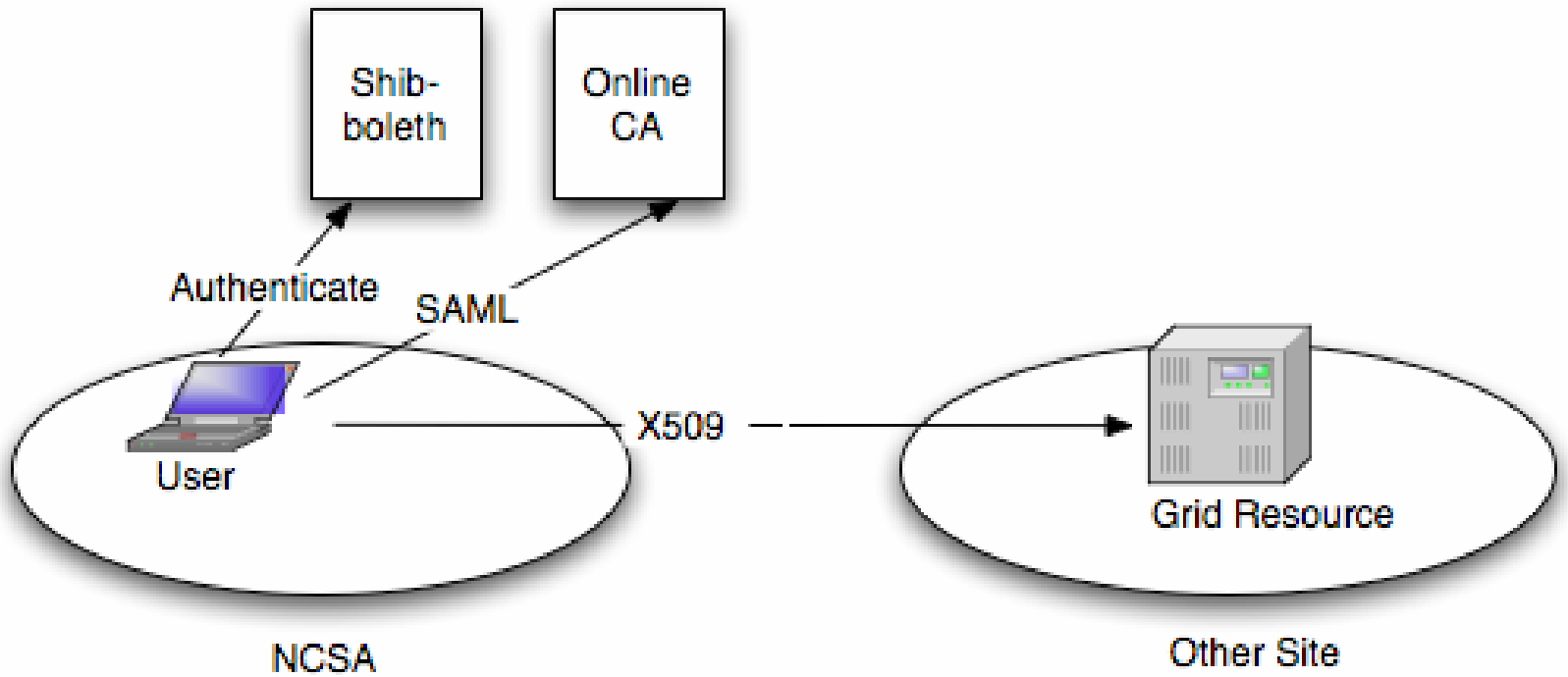
Example: NCSA OTP & Kerberos PKI

- Can use either OTP or Kerberos password to obtain X509 credentials
- PAM configurations tries both in turn and returns X509 credentials if either suceeds

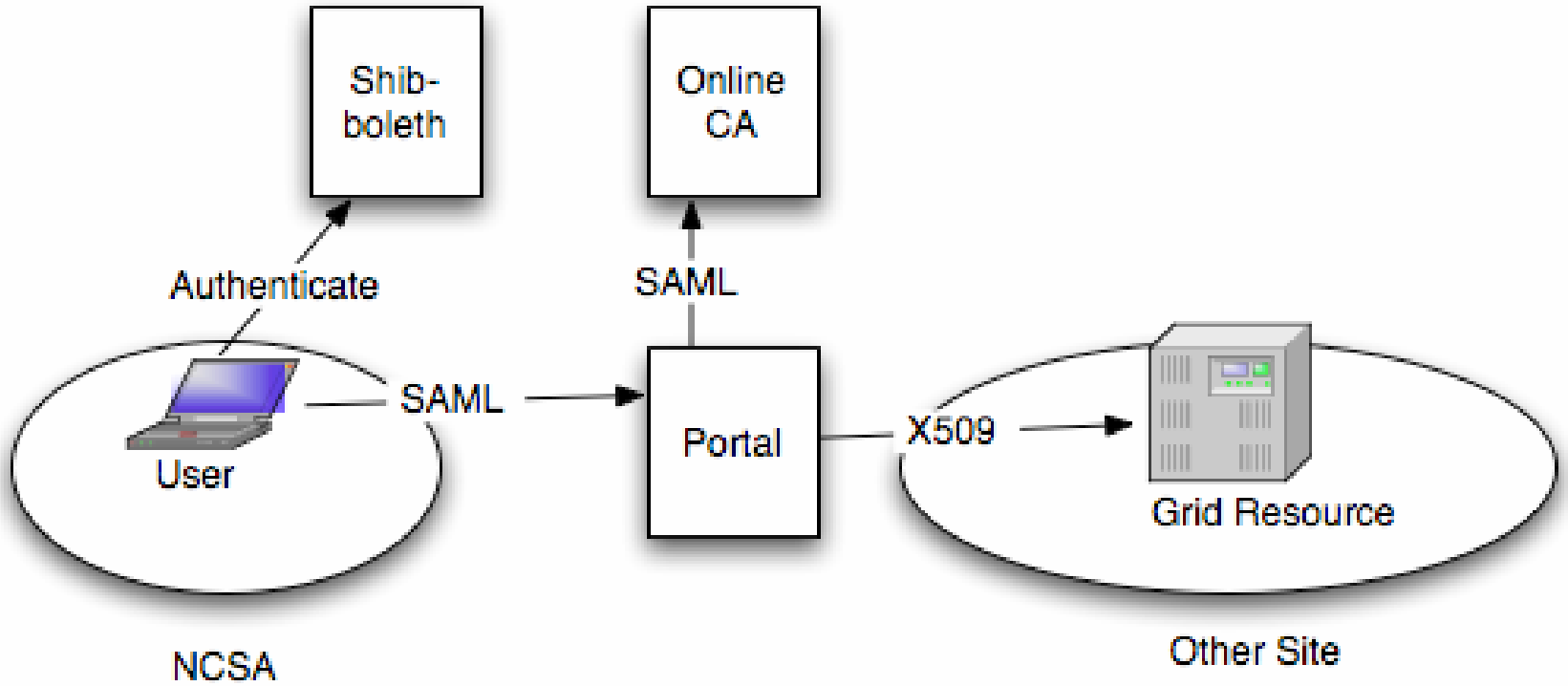
Future Plans: GridShib/MyProxy Integration

- Allow for leveraging of Shibboleth SSO for Grids
  - Need to convert Shib SAML into X509
- Accomplish by adding SAML authentication support to MyProxy
  - Ala Pubcookie
- Continue to use current GridShib work for Shibboleth-issued attributes to Grid resources
- Two motivating use cases…
  - Command-line users
  - Portal users

GridShib/MyProxy Integration



GridShib/MyProxy Integration



GridShib/MyProxy Integration

- Challenge is one of name management
- User's local name must be mapped to X509 DN and then back to name meaningful to attribute authority
- Is algorithmic approach better or can we assume database of mappings?
- Who should do the mappings?

Thank You

- My email:
  - vwelch@ncsa.uiuc.edu
- GridShib
  - http://gridshib.globus.org
- Shibboleth
  - http://shibboleth.internet2.edu/
- Globus Toolkit
  - http://www.globus.org/
- MyProxy
  - http://myproxy.ncsa.uiuc.edu/