Design of Shibboleth-based Authorization in C3-Grid

Siegfried Makedanz

Computer Center
Alfred-Wegener-Institut
givenname.lastname [at] awi.de
Introduction

- Use Case
  - Portal-based data access
  - Initially for C3-Grid
  - Eventually for Earth Science Community
Technologies

- Grid middleware: Globus TK 4
- AAI: Shibboleth
- Portal: GridSphere
  - With Shibboleth Plugin
- GridShib
  - SAML Tools at the portal
  - GridShib for GT at the resources
Roadmap (2007 - 2008)

- **Step 1 (April 2007)**
  - Participating C3 partners set Shib IdP up

- **Step 2 (June 2007)**
  - „Shibbolized“ GridSphere
  - Portal-based trust
  - Simple VO management

- **Step 3 (December 2007)**
  - GridShib „Science Gateway“
  - Access control at the resource providers

- **Step 4 (April 2008)**
  - „Real“ VO management based on IVOM findings
Step 1 (April 2007)

- Set-up of Shibboleth IdPs at the participating C3 partners
  - Federation membership in DEMOaar, DFN-AAI
- AWI provides simple test SP
- Integration of Shibboleth-based authentication and authorization at the Portal (GridSphere)
- Simple VO management
  - Distributed at the IdPs
  - eduPersonEntitlement: c3-member
- Resource providers trust the Portal
- Mapping on a **single** C3 user at the providers
- Required component: „Shib-enabled“ GridSphere
Step 3 (December 2007)

- Integration of GridShib solution for TeraGrid Science Gateways
- GridShib SAML Tools
  - Binding of SAML assertions into X.509 proxy certificates
- GridShib for GT
  - SAML PIP for Globus Toolkit
  - For Globus 4.0.x and above
- Roadmaps C3 and GridShib „match“
Step 3: Architecture

C3-Grid Portal with Authentication and Authorization based on Shibboleth and GridShib

Federation
- Shib/GridShib
- Affiliation
- Authentication
- Authorization

Typical IdP at C3 partner:
- IdM: Credentials, VO Attributes, Attributes
- AA: AuthN assertion, Attributes, VO Attributes
- ARP

GridShib SAML Tools
- User DB
- Grid Mapfile

Proxy Cert with SAML assertion
- Grid Client
- GridSphere Portal

C3-Grid community credential

GridShib for GT 0.6 SAML PIP
- PDP
- Grid Service Provider (GT)

Resource

AWI 2007

Design Shibboleth AuthZ C3-Grid
Step 4 (April 2008)

- „Real“ VO management system
  - VO self-administration
  - Sub-VOs
- Will be based on findings of IVOM project
  - IVOM: „Interoperability and Integration of VO Management Technologies in D-Grid“
Links

- Shibboleth: http://shibboleth.internet2.edu/
- eduPerson: http://www.educause.edu/eduperson/
- GridShib: http://gridshib.globus.org/
- DEMOaar Federation: http://aar.vascoda.de/test/demo.php
- C3-Grid: http://www.c3-grid.de/
- Thanks!
- Questions?