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
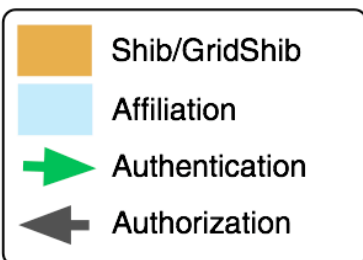 - GridShib for GT at the resources

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

- Set-up of Shibboleth IdPs at the participating C3 partners
  - Federation membership in DEMOaar, DFN-AAI
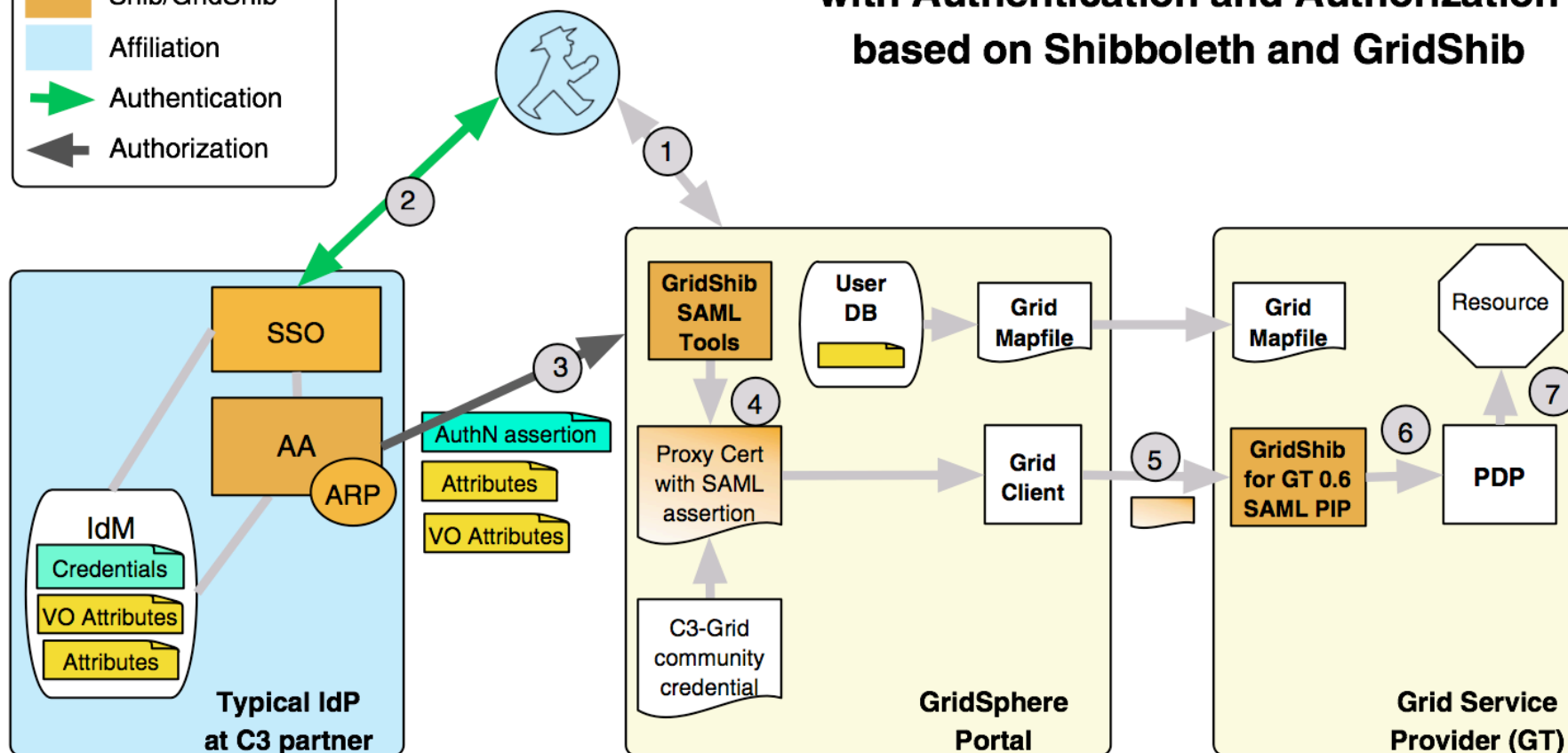- AWI provides simple test SP

- 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

- **Integration of GridShib solution for TeraGrid Science Gateways**

- **GridShib SAML Tools**
  - Binding of SAML assertions into X.509 proxy certifikates

- **GridShib for GT**
  - SAML PIP for Globus Toolkit
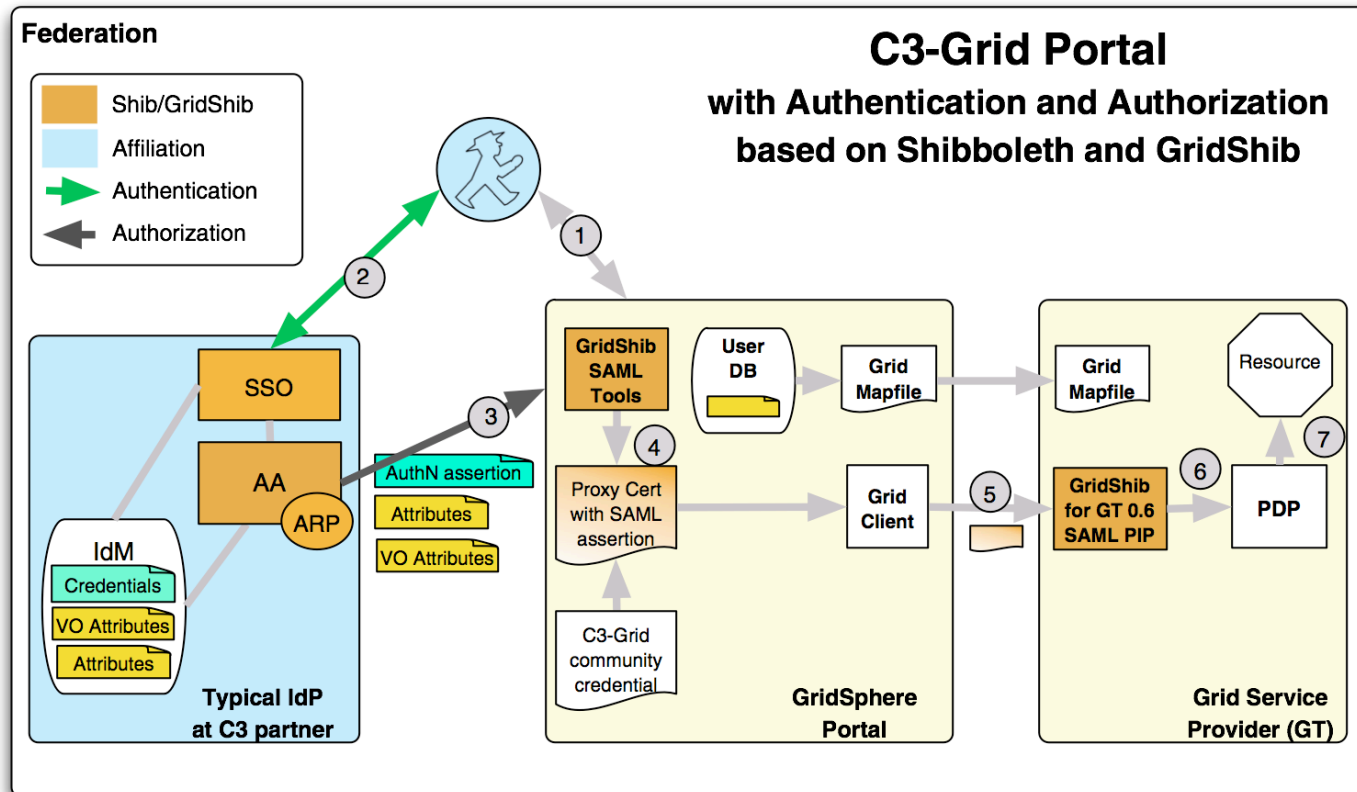 - For Globus 4.0.x and above

- **Roadmaps C3 and GridShib „match"**

Step 3: Architecture

Federation

Legend:
- Shib/GridShib
- Affiliation
- Authentication
- Authorization

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

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

GridSphere Portal:
- GridShib SAML Tools
- User DB
- Grid Mapfile
- Proxy Cert with SAML assertion
- Grid Client
- C3-Grid community credential

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

AWI 2007

S. Makedanz   **Design Shibboleth AuthZ C3-Grid**   2nd D-Grid Security WS, 27 March 07

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/

- GridShib Roadmap:
  http://dev.globus.org/wiki/GridShib_Development_Roadmap

- GridShib Science Gateway:
  https://spaces.internet2.edu/display/GS/TeraGrid und
  https://spaces.internet2.edu/display/GS/NanoHUBTestbed

- DEMOaar Federation: http://aar.vascoda.de/test/demo.php

- IVOM: http://dgi.d-grid.de/index.php?id=314

- C3-Grid: http://www.c3-grid.de/

End

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

- Thanks!
- Questions?