AuthZ Interoperability
Status and Plans

June 12, 2007
Middleware Security Group Meeting

Gabriele Garzoglio
Computing Division, Fermilab

Overview

- Motivations & Collaboration
- Informal Requirements
- Open Issues
- Conclusions

Motivations

- Modern middleware development requires the integration of software with grid authorization layers.
- Each grid has a different authorization infrastructure. Authorization call-out protocols are not standardized.
- Example: SRM/dCache is integrated with the OSG AuthZ infrastructure but not with EGEE. Deployment must still rely on legacy AuthZ mechanisms.
- Discussion started in Oct 2006 to address authorization interoperability.

Collaboration

- OSG (VO Services Project)
  - Keith Chadwick, Ted Hesselroth, Gabriele Garzoglio, Igor Sfiligoi, Steve Timm, Valery Sergeev, John Weigand
  - John Hover, Jay Packard
- EGEE (Site Authorisation and Enforcement Services)
  - David Groep, Oscar Koeroo
  - Yuri Derchenko, Joni Hahkala
- The Globus Toolkit
  - Rachana Ananthakrishnan, Frank Siebenlist, Dan Fraser

A window of opportunity

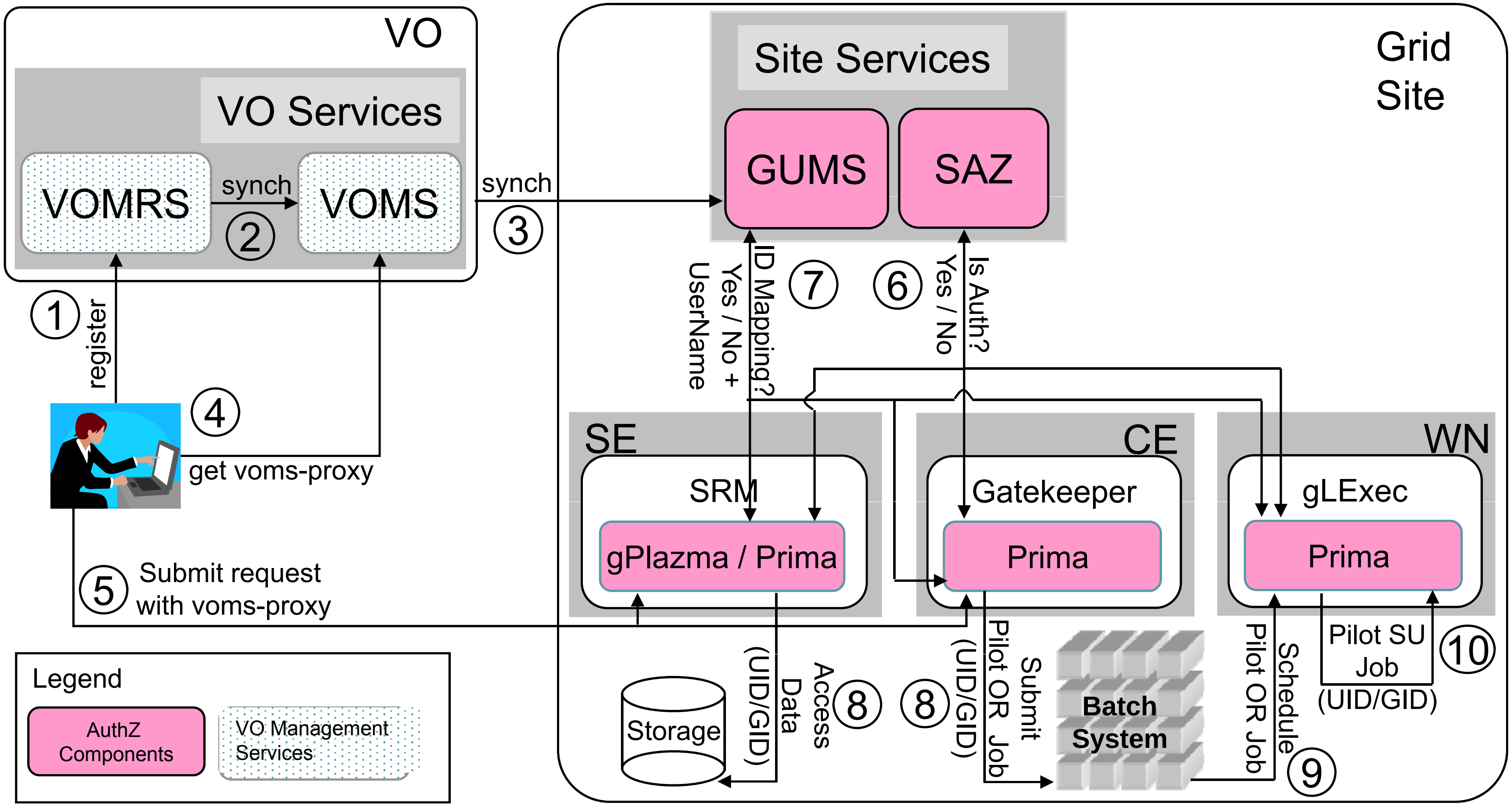
- Globus is in the process of developing a new pluggable AuthZ call-out infrastructure for GT4
  - OSG and EGEE can contribute in defining real-life use cases
- EGEE is considering to make the LCMAPS system accessible as a network service
  - The group needs to decide soon what network protocol to use
- VO Services project is finishing Phase II on Summer 07
  - Effort becomes available for Phase III of the project

Open Science Grid

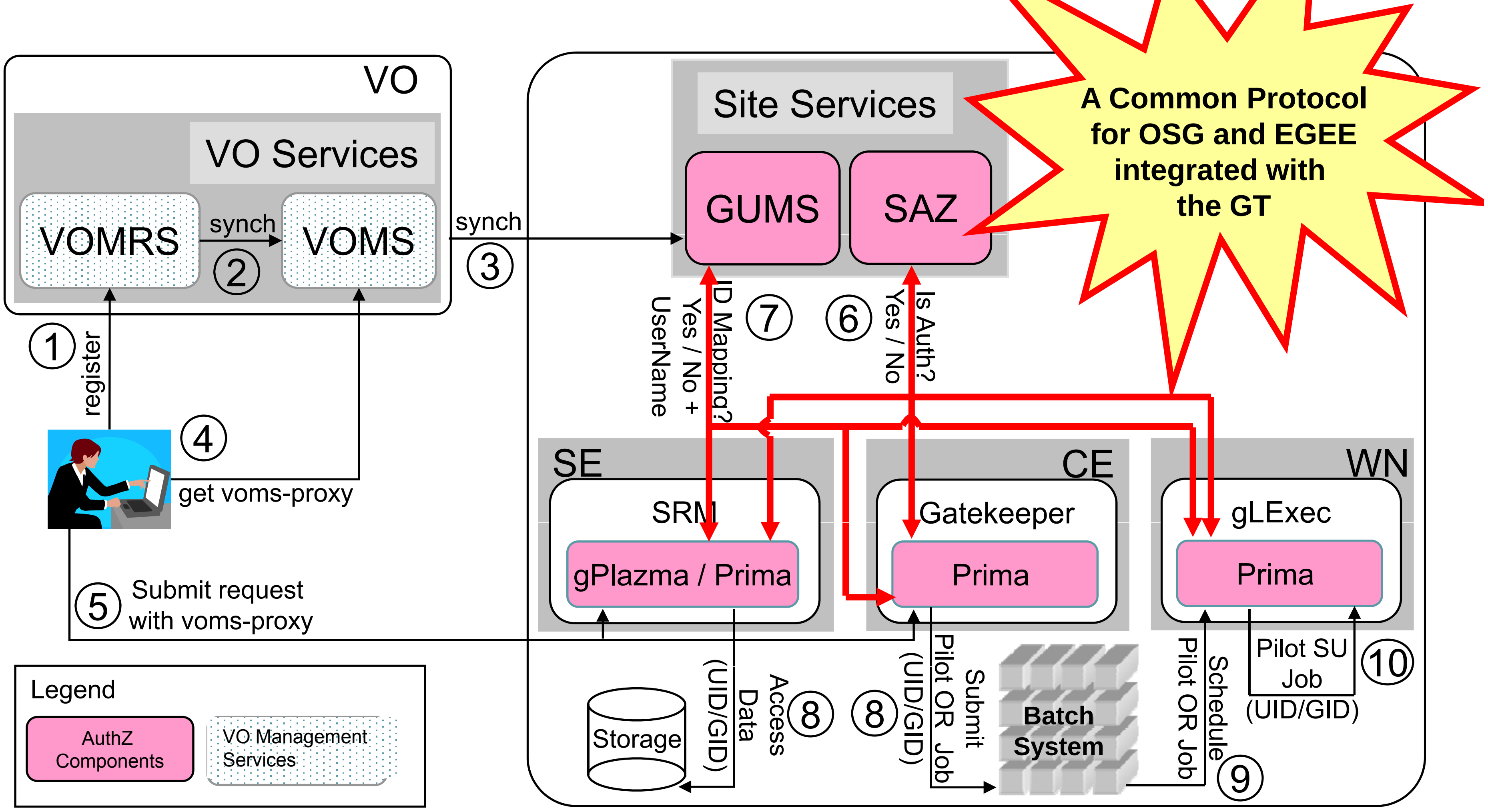
Meetings History

- Oct 2006: http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=239
- Feb 2007: http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=323
- Mar 2007 (discussions at the MWSG 11) http://indico.cern.ch/conferenceDisplay.py?confId=12654
- Apr 2007: http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=333
- May 2007: http://cd-docdb.fnal.gov/cgi-bin/DisplayMeeting?conferenceid=338

Architecture (the OSG case)



Architecture (the OSG case)



A Common Protocol for OSG and EGEE integrated with the GT

Overview

- ✓ Motivations & Collaboration
- ➢ Informal Requirements
- Open Issues
- Conclusions

Open Science Grid

Background

- Globus has a prototypical implementation of an authorization call-out library
  - Developed in collaboration with IBM
  - Based on XACML 2 / SAML 2
- The library is going to be integrated with GT4.x

Informal Requirements

- The library should be usable outside of the Globus Toolkit framework
  - However, the GT4 PEP are natively integrated
- The library should support remote or local attribute validations
  - The library should support sending signed assertions through the wire
  - We will need to standardize the attribute names used in the assertion, to have a consistent semantics across implementations

Informal Requirements

- The library should allow signing assertions with different certificates
  - For example host cert, user cert, pilot admin cert, etc.
- The library should be able to send some of the PEP context to the PDP
  - For example: job description parameters, RSL, etc.
  - The information could be passed to the PDP as a standardized XACML attribute.
- The library should support arbitrary information from the PDP
  - Using XACML Obligations…

XACML Obligations (PDP Output)

- OSG and EGEE use cases are almost the same
  - Return set of UID/GID (CE), Root Path, Priority, Quotas (SE)
- EGEE wants support for more general structures
  - “Authorization Tickets” to enable session management
  - Discussed the use case of AFS tokens
- Clients should be able to declare what obligations they can support
  - We can use a standardized tag of the "environment" element
  - Allows “upgradability” of the clients
- Handling of obligations should be implemented via external handlers
  - Handlers will be associated to standardized obligation ids.

Open Science Grid

Overview

- ✓ Motivations & Collaboration
- ✓ Informal Requirements
- ➢ Open Issues
- Conclusions

Open Science Grid

Language Support

- The languages of interest for the library are C and Java
- The prototype is in Java
- Server-side: is Java enough?
  - It might for OSG (both GUMS and SAZ are in Java)
- Client-side: must support C:
  - We can generate WSDL bindings in C, **but** this will lack support for obligations
  - We can try JNI, **but** similar attempts (CABig group) have been done outside of the GT4 framework
  - We can translate the Java library in C, **but** it will required longer timelines

Open Science Grid

Open Issues

- What are the EGEE time constraints ?
- What is the schedule of Globus to provide
  - support for parsing/manipulating obligations
  - support for a C library

  (tentatively: α-version by the end of July)
- What features of the C library are essential to write client software ?

Conclusions

- The window of opportunity to develop an interoperable authorization system is now
- Globus, OSG & EGEE have laid the groundwork for a successful collaboration
- For this phase, we still need to
  - Agree on a common plan and timeline
  - Formalize requirements
  - Understand what standards are needed