AuthZ Interoperability
Requirements, Plans, and Milestones

Overview

- Goals

- Where are we? An assessment.

- WBS and Schedule

- Concerns: a New Development Team

Dec 6, 2007
Middleware Security Group Meeting

Gabriele Garzoglio
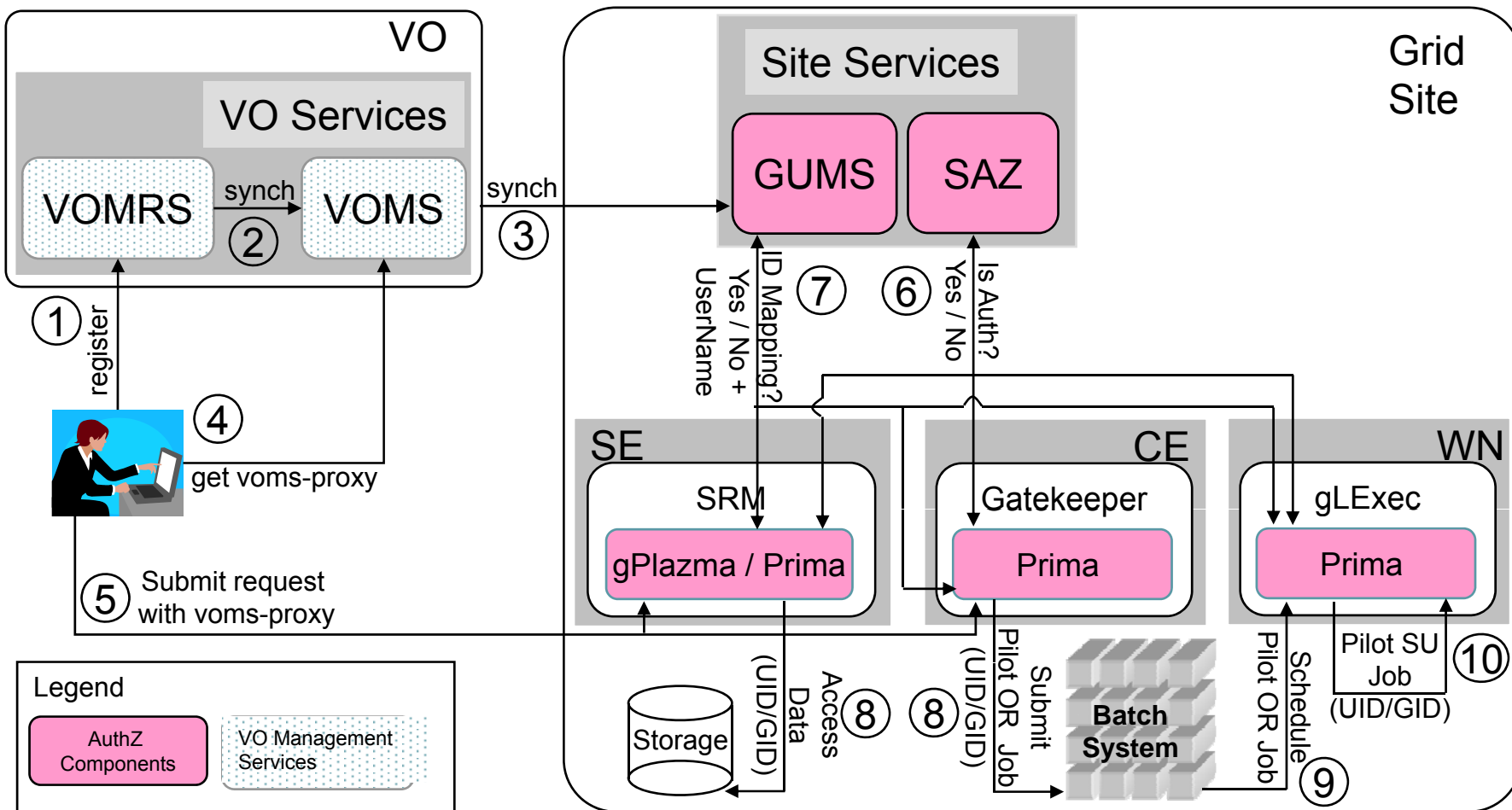**Computing Division, Fermilab**

Goals

1. Reviewing all fundamental areas of the work (even the ones settled or not discussed in several months) and reassuring ourselves that we are still on the same page everywhere

2. Discuss the scope and release schedule for the development work in OpenSAML 2. The goal is gathering enough information to update our plans. After the MWSG, we will need to carefully evaluate if these changes of scope and schedule make the joint project still cost effective.

3. Discuss communication channels w/ new development team and its management; discuss expectations for participation, response time, quality, etc.
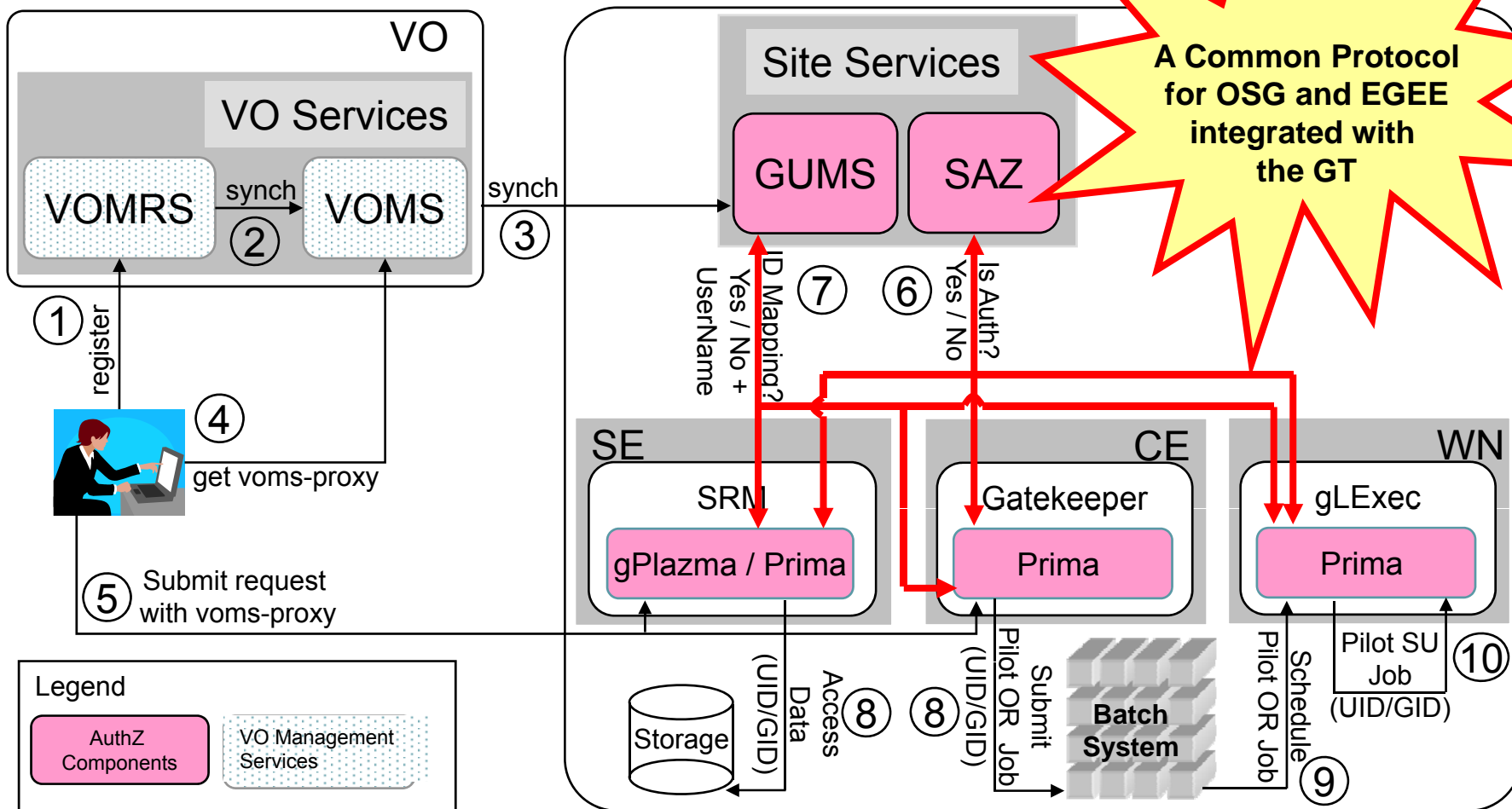
Architecture (the OSG case)

Architecture (the OSG case)

Open Science Grid

VO

VO Services

VOMRS --- synch ② ---> VOMS --- synch ③ --->

① register

④ get voms-proxy

⑤ Submit request with voms-proxy

Site Services

GUMS   SAZ

A Common Protocol for OSG and EGEE integrated with the GT

ID Mapping? Yes / No + UserName ⑦

Is Auth? Yes / No ⑥

SE

SRM

gPlazma / Prima

CE

Gatekeeper

Prima

WN

gLExec

Prima

Access Data (UID/GID) ⑧

Submit Pilot OR Job (UID/GID) ⑧

Schedule Pilot OR Job ⑨

Pilot SU Job (UID/GID) ⑩

Storage

Batch System

Legend

AuthZ Components

VO Management Services

Overview

✓ Goals

➢ Where are we? An assessment.

• WBS and Schedule

• Concerns: a New Development Team

Gabriele Garzoglio

Where are we? An assessment

- Collaboration is very active and meets approx. biweekly
  - Collaboration has representatives from EGEE and affiliated groups, Globus, and VO Services project / OSG
  - Meetings material is available from the FNAL DocDB
  - Meetings, Software, Documentation is indexed at http://home.fnal.gov/~garzogli/privilege/AuthZInterop/info.html

- Globus has been responsible for the Java and C implementation of the XACML/SAML 2 specs. Very positive collaboration:
  - Globus has demonstrated sensitivity to our schedule (α-version of the SAML lib was released on the agreed date)
  - They actively participated to our group meetings, gathering and providing input
  - Fixing bugs in the α-version of the lib was appropriately timely

Main Activities

- The Group has been working on 2 main activities

  1. Defining an interoperability profile for authorization requests and responses

  2. Working with Globus to provide input and test the implementation of the XACML library

Activity Overview

1. Actively working on XACML Interoperability profile
   – Standardization of request and response contexts.
   – Agreed on <obligations> and <subject> context.
   – Discussing <action>, <resource>, <environment>
   – See Oscar's talk for more

2. Testing the XACML lib with stateful (GUMS / LCMAPS) and stateless (GPBox, gJAF) PDP
   – Learning if XACML lib is sufficiently complete to write relevant XACML policies.
     • E.g. α-version of GT was missing data types.
   – Learning what types to use for the XACML Interop. profile.
     • E.g. Is "secondary GID obligation" composed by a list of attributes of type integer OR by a single attribute of type integer list ?
   – See Håkon's talk for more

Informal Requirements (Jun'07)

- 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 (Jun'07)

- 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…

Informal Requirements (Jun'07)

- 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.

- Interoperability profile should be used to generate test classes for the library (new)
  - Check that our contexts (obligation structures, data types, etc.) do not break the wire representation

Overview

✓ Goals

✓ Where are we? An assessment.

➢ WBS and Schedule

• Concerns: a New Development Team

Gabriele Garzoglio

WBS

1. Manage transition of development team
   1. Establish communication channels w/ development team and its management
   2. Agree on expectations for participation, response time, quality, etc.
   3. Adapt plans and scope to new product qualities
2. Project Oversight
   1. Organize periodic phone meetings and agenda, record decisions
   2. Maintain publicly accessible information (project web page)
   3. Prepare presentation material (MWSG and other conferences)
   4. Maintain communication with stakeholders

WBS

Open Science Grid

3. Define Interoperability XACML Profile
   1. Write Interoperability XACML Profile document
      1. Define XACML response profile (obligations)
      2. Define XACML request profile (subject, action, resource, environment)
   2. Interact with other bodies interested in Authorization (e.g. OGF)

4. Develop XACML/SAML library
   1. Agree on scope and development plan
   2. Release alpha version
   3. Release beta version
   4. Release v1 version
   5. Add tests on the wire to library for Interoperability Profile

WBS

5. Test XACML / SAML library with different infrastructures

    1. Test each release with XACML engine, using typical policies, obligations, etc. (gJAF, GPBox)

    2. Use alpha release with mock client/servers to test library with statefull PDP (LCAS/LCMAPS, PRIMA/GUMS, SAZ, gLExec)

6. Integrate XACML/SAML library with existing infrastructures (PRIMA, GUMS, gLExec, LCAS/LCMAPS, …)

    1. Develop parser for attribute certificates (PIP) according to Interop. XACML profile

    2. Integrate beta release with key client/servers to expose integration difficulties

    3. Integrate v1 release with production version of all components

    4. Packaging , deployment, and user documentation

WBS

6. Test interoperability

    1. Attempt deployment of SRM/dCache with same authz call-out on OSG and EGEE AuthZ infrastructures

7. Project closure activities

Schedule (to be revised)

- Feb 07: beginning of the project
- Aug 07: release α-version of lib: *met*
- Nov 07: test α-version of lib against PDP: *approx. met*
- Dec 07: release β-version of lib: *suspended*
- Jan 07: test β-version of lib against PDP: *suspended*
- Feb 08: complete Interop. Profile doc: *on track*
- Feb 08: develop PIP as per Interop. Prof. doc
- Feb 08: integrate β-version of lib w/ PEP/PDP: *???*
- Apr 08: release v1 of lib: *???*
- Jun 08: integrate v1of lib w/ PEP/PDP: *???*
- Aug 08: demonstrate interoperability: *???*
- Aug 08: package and prepare for deployment: *???*

Open Science Grid

Overview

✓ Goals

✓ Where are we? An assessment.

✓ WBS and Schedule

➢ Concerns: a New Development Team

Gabriele Garzoglio

Concerns

- EGEE proposes to take over development responsibilities for XACML / SAML 2 library from GT

- Concerns:

  1. Scope: some features we relied on might be out of scope now. How much more work is this for us ?

     - GT agreed to develop a series of helper classes to facilitate development (obligation handling framework, message composition API, …)

     - GT agreed to implement tester classes using definitions from the Interop. Profile

Concerns

- Concerns:
  2. Consistency of the JAVA and C development
     - Java libraries are developed by EGEE, C by GT
  3. Ability to collaborate
     - Need to establish communication channels w/ development team and its management
     - Agree on expectations for participation, response time, quality, etc.
     - Adapt plans and scope to new product qualities

Conclusions

- The Authorization Interoperability project is a promising future direction for GT/EGEE/OSG authorization infrastructures

- Project has good momentum and collaboration is working effectively on high priority issues

- Change in development team requires reassessment of the costs/benefits.