Project Closure Report

VO Services Project Phase III

Table of Contents

1. Approvals

Customers and Sponsors	**Signature:**	(approved)
	Print Name:	Mine Altunay
	Title:	For OSG
	Date:	Jun 23, 2009
	Signature:	(approved)
	Print Name:	Ian Fisk
	Title:	For USCMS
	Date:	Jun 25, 2009
	Signature:	(approved)
	Print Name:	Michael Ernst
	Title:	For USAtlas
	Date:	Jun 19, 2009
Project Manager:	**Signature:**	(approved)
	Print Name:	Gabriele Garzoglio
	Title:	Application Developer and System Analyst
	Date:	Jun 18, 2009

2. Document Change Log

Revision	Date	Change Description	Prepared By	Approved By
v0.1	04/07/09	Initial text	Gabriele Garzoglio	
v1.0	06/18/09	Finalized the text	Gabriele Garzoglio	

3. Project Abstract

The VO Services Project (formerly, the VO Privilege Project) provides software solutions for Virtual Organization (VO) user registration and fine-grained authorization for access to Grid-enabled resources. The infrastructure assists VO and site administrators with user account assignment and management at Grid sites, reducing the associated administrative overhead. Authorization is linked to membership of users to VO-defined groups and roles. User-to-account mapping is flexible, dynamic, and based on both VO group/role and least privilege access.

The project is sponsored by US CMS, based at Fermilab, US ATLAS, based at Brookhaven National Laboratory, and the Open Science Grid. The project started in 2003 to build, extend, and integrate elements within the grid authorization architecture developed by the Grid2003 team. The project is composed of a comprehensive suite of software services, maintained in part by the project team and in part by close

collaborations with partners Grid Middleware groups, including EGEE, INFN, and Globus. Such suite of services include software project for Virtual Organization management (VOMRS and VOMS), for Authorization Call outs (PRIMA, PRIMA-WG, gPlazma, gLExec), and for authorization policy decisions (GUMS).

4. Project Documentation

This section provides links to project definition documents and initial plan.

Project web page:
http://www.fnal.gov/docs/products/voprivilege/

Minutes and material from all collaboration meetings:
http://www.fnal.gov/docs/products/voprivilege/atwork.html

Presentations and documentation:
http://www.fnal.gov/docs/products/voprivilege/doc.html

5. Supporting Documentation

This section lists the documentation developed during the definition and execution of the project. The following link provides context and support for closing the project.

Specific documentation on activities carried under the VO Services project umbrella
http://www.fnal.gov/docs/products/voprivilege/focus.html

Links to individual components documentation pages:
http://www.fnal.gov/docs/products/voprivilege/software.html

Link to the closing report of the Authorization Interoperability project, a major effort under the VO Services umbrella: CD docdb 3238

6. Reason for Closing the Project

The project coordinated development activities amongst the multiple components under its umbrella. All components performed functions in the domains of access authorization and user registration. The project contributed expertise in these domains and coordinated the end-to-end delivery of functionalities for its stakeholders.

The main development activities, identified in the WBS for Phase III, have closed down. Potential follow up activities will benefit from new project structures. Development of functionalities confined within individual components is being delegated to other projects: gPlazma to the dCache project; gLExec to the GlideIn WMS project; GUMS remains with the GUMS project. The Authorization Interoperability project, a major effort under the VO Services umbrella, has also closed down. The project on the convergence of VOMRS and VOMS-admin is managed at CERN; Tanya Levshina acts as direct liaison for VOMRS from Fermilab; the VO Services coordination umbrella is not needed anymore. See project Deliverable for details on all closing activities.

7. Project Deliverables

This section lists high-level deliverables for the projects.

Planned Deliverables	Actual Deliverables
OSG / EGEE Authorization Interoperability	A profile and implementation in C and Java of a common authorization call-out protocol. Resource gateways integrated include pre-WS and WS Globus Gatekeeper, GridFTP, SRM/dCache, gLExec. Available policy decision points include GUMS and SCAS. See Authorization Interoperability closing document for a list of limitations and further details (CD docdb 3238).
Support Storage Groups in Defining Next Generation Storage Authorization Models	As part of the AuthZ Interop project, we worked with the dCache project to define authorization attributes and obligations for the storage authorization use cases. The most relevant of these attributes and obligations have been implemented in a library, part of the AuthZ Interop deliverables, and are used by dCache / gPlazma and are being integrated by BeStMan.
Convergence of VOMS-admin 2.5 with VOMRS	Defined the convergence project. Identified a list of missing VOMS-admin features in order for it to support all use cases currently supported by VOMRS. Defined five VOMS-admin releases / phases that include progressively growing capabilities. Phase I is currently being tested and it is due for EGEE certification; phase II is scheduled for early 2010; phase III-V for afterwards. Identified the project management structure to execute the project as the gLite Engineering Management Team.
Investigate Mechanisms to Define and Enforce VO and Site AuthZ Policies (SBIR w/ TechX)	Worked with TechX to provide a prototype of the policy infrastructure as an SBIR Phase I grant. The prototype was delivered together with a study of the feasibility of this approach to handle VO and Site policies. Laid down the work for the consolidation of the infrastructure as an SBIR Phase II.
Enable VOMS-signed Attribute Certificate Validation at OSG Resource gateways	Attribute Certificate (AC) Validation has been delivered for SRM / dCache only. Other gateways have not been integrated at this point. The authorization interoperability project provides the pre-requisites to adopt the gLite resource gateway authorization modules (L&L + SCAS client), which enable AC Validation out of the box. We have not provided an in-house implementation of AC validation in our modules, considering more cost effective integrating the gLite infrastructure in the future. This integration can be managed as a separate project, if this issue is still relevant to OSG in the near future.
Provide a validation tool to check the conformance of the authorization infrastructure configuration at sites with the OSG	The project has developed an RSV probe to compare the local GUMS configuration with a reference GUMS instance at the GOC. RSV probes are the mechanism used by OSG to check the status of provided services. The RSV framework was not capable of properly handling error conditions from the probe. Integration was delayed until Mar 2009, when a new version of RSV was made available. By that

authorization template.	time, GOC was not maintaining a reference GUMS instance anymore. More development work has been scheduled to lift the reliance on a reference GUMS instance (information is transformed from a reference GUMS configuration template provided via the web). This item is handed over to the STG to complete the end-to-end delivery of the functionality.

Change Requests	**Impact**
Provide a validation tool to check the conformance of the authorization infrastructure configuration at sites with OSG authorization templates.	The request was made by the OSG PI / Facility Manager and endorsed by the OSG Security officer in Feb 2008. The request did not cause major disruption in the schedule, but is not completed yet, because of the schedule of other related projects (RSV framework). The GUMS developers and the STG are working together to provide the end-to-end delivery of this functionality.
GUMS usability functionalities	Requested by OSG and US CMS. Requests were minor enough that they could be fit into the normal software improvement schedule.

8. Project Schedule

This section discusses the schedule of major milestones (or "Project Phases" as per the table below).

Project Phases	**Planned Completion Date**	**Actual Completion Date**
Started Phase III: Opening Phase III, reassessing WBS and establishing quarterly stakeholders' meetings.	-	Nov 2007
Closed SVOPME (Policy Management) Phase I SBIR: TechX provided a prototype of the SVOPME infrastructure and related documentation.	Mar 2008	Mar 2008
Change Request (Validation Tool): The request was made on Feb 08. A prototype was made available by Apr 2008. The prototype, however, could not be deployed in production because of a deficiency of the RSV framework.	Apr 2008	Incomplete
Opened SVOPME Phase II SBIR: TechX received financing for the production quality implementation of the infrastructure.	Sep 08	Sep 08
Change Request (GUMS usability functionality): Minor improvements in the behavior of GUMS: (1) Allow disabling of gridmap-file creation, to avoid full pool-account mapping instantiation.; (2) Reorganize logs so that "critical" faults send emails.	Sep 2008	Sep 2008
Closing of the Authorization Interoperability Project: See project closing document for details: CD docdb 3238	Nov 2008	May 2009
Closing of the VO Services Project: Transitioned development of components to	Jun 2009	Jun 2009

maintenance or to other projects. Managed final communications with stakeholders. Closing down project.		

9. Project Team

The team was composed by members from FNAL and BNL (shaded in grey).

Name	Project Role	Ramp-down Plan	Timeframe
Gabriele Garzoglio	Project Coordinator (FNAL)	Coordinate remaining tasks, having meetings monthly, then only occasionally.	Jun 2009
Igor Sfiligoi	VO Services developer for PRIMA and gLExec (FNAL)	Move to maintenance of PRIMA. Maintenance and development of gLExec will be coordinated through the dCache project.	May 2009
Jay Packard	VO Services developer for GUMS (BNL)	Maintain focus on GUMS, assuming responsibilities for end-to-end delivery of GUMS features,	May 2009
Ted Hesselroth (externally budgeted in CD by Data Movement and Storage)	dCache developer for gPlazma (FNAL)	Maintenance and development of gPlazma will be coordinated through the dCache project.	May 2009
Dave Dykstra	VO Services developer for PRIMA and gLExec (FNAL)	Move to maintenance of PRIMA. Maintenance and development of gLExec will be coordinated through the GlideIn WMS project.	May 2009

10. Budget and Financial Information

M&S budget did not require additions to the regular development platforms used by the development team.

S&W budget:

- Budgeted effort in FY08 was 1.6 FTE, of which 0.6 paid by CD (Garzoglio and Levshina), 0.5 by USCMS (Sfiligoi), and 0.5 by OSG (Packard). Other experts working with the projects included Hesselroth (storage), Weigand (testing) and Hover (GUMS expert). Most of the effort was spent in the Authorization Interoperability project. Nominal effort was within budgeted effort.
- Budgeted effort in FY09 was 1.35 FTE, of which 0.45 paid by CD (Garzoglio and Levshina), 0.40 by USCMS (Sfiligoi and Dykstra), and 0.5 by OSG (Packard). Hesselroth was budgeted at 0.25FTE by Data Movement and Storage and paid by CD to work on storage authorization. Weigand and Hover occasionally helped with the project. In an effort to finish the Authorization Interoperability project, nominal effort was higher than budgeted in the first quarter of FY09, especially for storage (0.45 FTE vs. budgeted 0.25); with the effort on storage ramping

down to almost 0 in the last quarter of FY09, we envision an average yearly effort as budgeted.

Financial advantages of the project:
With the authorization interoperability project, the project successfully reduced maintenance effort by reusing authorization call-out code with gLite and the Globus Toolkit. Future developers' effort to adapt middleware to the OSG and EGEE authorization infrastructures will also be virtually null, since the new interoperability modules work in both environments.
The VOMRS / VOMS-admin convergence project will allow the reduction of the maintenance cost for VOMRS to CD. The budget of 0.15 - 0.2 FTE dedicated in the past 3 years was enough to maintain the infrastructure, but not to address new user requests.

11. Outstanding Risks

The following section describes risks with the software produced by this project.

- Oversubscription of the STG in managing the end-to-end delivery of authorization-related features. STG has oversight over GUMS (developed at BNL) and over the RSV authorization validation probe. Being very busy, the group might delay proper attention to these projects, resulting in additional support load for sites and developers.
- Missed convergence of VOMRS / VOMS-admin. gLite has not funded the INFN effort to develop features of VOMS-admin necessary for the convergence, despite a request by INFN. The effort is an in-kind contribution and the uncertainty on the schedule of Phase III-V reflects the uncertainty on funds. Should VOMRS and VOMS-admin fail to converge, the Fermilab CD is committed to the maintenance of VOMRS for the foreseeable future. This corresponds to a minimum of about 0.15 FTE, with possible spikes necessary to modernize the infrastructure.
- Deviation from agreed interoperability standards as the structure of the forum becomes more relaxed (see also AuthZ Interop closing document: CD docdb 3238). In particular, with the raise of the EGEE Authorization Service, the foreseen convergence of the EGEE and OSG authorization call-out infrastructure might be delayed or stopped. This will result in the need for continued maintenance of our infrastructure (roughly at 0.35 FTE/month) or new development effort to adopt new solutions.

12. Operations and Support

With the closing of the VO Services project, responsibility for individual components has been transitioned to other projects or organizations. Operations, maintenance, and support for each component rest with these projects and organizations. The sections below describe operations, support, and maintenance for the VO Services components.

12.1 Operations

The VO Services components are distributed through VDT and operated in the context of large organizations, such as OSG, US CMS, and US Atlas. Operational documentation for individual components is maintained as OSG technical documentation and updated during the ITB release cycles as necessary.

12.2 Maintenance and support

Maintenance responsibilities are assigned as follows:

1. **PRIMA**: This module implements the authorization call-out for middleware developed in C. It depends on the SCAS libraries and is used by the GT pre-WS gatekeeper, gridftp, and gLExec. It was developed and maintained by the VO Services project. Dave Dykstra (dwd@fnal.gov) is the main contact. Support can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org).
2. **gLExec**. This executable command implements a POSIX UID-switching tool. It depends on PRIMA and the LCAS/LCMAPS framework (maintained by Oscar Koeroo, Nikhef). It is used by job management systems, such as GlideIn WMS and Panda. It is developed and maintained by Nikhef. The main developer and contact person is Oscar Koeroo (okoeroo@nikhef.nl), who can be contacted via the mailing list grid-mw-security@nikhef.nl or by opening a Global Grid User Support (GGUS) ticket (helpdesk@ggus.org / https://gus.fzk.de/pages/ticket.php). Support for OSG has transitioned to the GlideIn WMS project. The OSG contact person is Dave Dykstra (dwd@fnal.gov). Support for OSG users can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org)
3. **gPazma**. This module implements the authorization call-out for SRM/dCache. It depends of privilege.jar. It is developed and maintained by the dCache project. The contact developer is Ted Hesselroth (tdh@fnal.gov). Support can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org) or through the dCache support channels.
4. **GUMS**. This server implements a Policy Decision Point and is deployed in OSG as a user mapping service. It depends on privilege.jar. It is developed and maintained by BNL, under the umbrella of the VO Service project. The contact developer is Jay Packard (jpackard@bnl.gov). Support can be solicited by opening a Grid Operation Center (GOC) ticket (goc@opensciencegrid.org).
5. **Site configuration validation tool**: the OSG Software Tool Group has taken responsibility for the delivery of this feature, in collaboration with the RSV and GUMS teams. Alain Roy (roy@cs.wisc.edu) and Mine Altunay (maltunay@fnal.gov) are leaders of the group. Support can be solicited by opening a GOC ticket.
6. **VOMRS / VOMS-admin convergence:** gLite Engineering Management Team has taken responsibility for this work; Maria Dimou (Maria.Dimou@cern.ch) is managing the project. For maintenance and support questions on VOMRS, we recommend opening a Fermilab Service Desk ticket, which will be handled by Tanya Levshina (tlevshin@fnal.gov). Questions on VOMS-admin should be directed to the INFN-BO developers through the Global Grid User Support (GGUS) ticket (helpdesk@ggus.org / https://gus.fzk.de/pages/ticket.php).

13. Next Steps

- Maintaining the communication channels / forum for occasional communication on Authorization and User Registration.
- Gabriele Garzoglio agreed to triage requests from stakeholders, while the new organization becomes more widely known.
- For the next steps of Authorization Interoperability see CD docdb 3238.
- Attribute Certificate Validation at the gateways and integration with LCAS & LCMAPS (L&L) / SCAS. The adoption of a common protocol for authorization (delivered by the Authorization Interoperbility project) allows for the introduction of a common EGEE/ OSG implementation of the call-out modules. We envision that this common implementation could be the gLite L&L framework with the SCAS module (this plan is

contingent on the deployment schedule of the new EGEE Authorization Service). The L&L framework supports AC validation out-of-the-box. See also “Attribute Certificate Validation in OSG”, OSG docdb 756

- VOMRS / VOMS-admin convergence. With more and more of the VO membership registration use cases supported in VOMS-admin, we envision to start asking VO administrators to migrate away from VOMRS towards the end of 2010. This will free up resources currently involved in the support and maintenance of VOMRS.

14. Lessons Learned

- An umbrella project that coordinates a diverse range of activities, each potentially centered at different institutions, needs to be back up by an appropriate funding structure. Relying solely on in-kind contributions may not grant sufficient authority to the project manager to conduct a cohesive program of work.
- In order to coordinate a diverse range of activities in the US with the equivalent efforts in the EU, we found that meeting in person regularly at least twice a year was of crucial importance. The Middleware Security Group (MWSG) played such a role for the authorization and registration efforts, convening four times per year. Alternating the hosting of such venues between the EU and the US was critical to guarantying attendance.
- Despite the different focus of operational security and authorization, we found beneficial exposing the personnel of the two groups to each other’s activities / concerns.
- See also the lessons learned from the Authorization Interoperability project (CD docdb 3238).