DE-FG02-04ER25601

Identity Federation & Policy Management Guide

PI: Marty Humphrey

University of Virginia

8/15/2004 – 8/14/2007
(with 8/15/2007 – 8/14/2008 no-cost extension)

Final Report

Contents

Annual Report: Aug 15, 2004 -- Aug 14 2005 2
Annual Report: Aug 15, 2005 -- Aug 14 2006 5
Annual Report: Aug 15, 2006 -- Aug 14 2007 9
Annual Report: Aug 15, 2007 -- Aug 14 2008 (no-cost extension)..... 11
Summary of Overall Project Accomplishments 13

Annual Report: Aug 15, 2004 -- Aug 14 2005

1. Technical progress during the current budget period

The goal of this 3-year project is to facilitate a more productive dynamic matching between resource providers and resource consumers in Grid environments by explicitly specifying *policies.* The first problem being addressed in this proposal is the lack of an Open Grid Services Architecture (OGSA)-compliant mechanism for expressing, storing and retrieving user policies and Virtual Organization (VO) policies. The second problem being addressed in this proposal is the lack of tools to resolve and enforce policies in OGSA. The goal is to make all policies explicit (e.g., virtual organization policies, resource provider policies, resource consumer policies), thereby facilitating policy matching and policy negotiation. Significant proposed contributions over the 3-year project include:

- *MyPolMan,* an add-in tool suite to MyProxy, a widely-available on-line Grid credential manager, that creates the ability for a Grid user to centralize (where appropriate) and manage his/her policies
- *VOPolMan,* in which the policies of the Virtual Organization are expressed, managed, and dynamically consulted

1.1 Participant individuals

Marty Humphrey, PI
Sang-Min Park, 1st-year Graduate Student
Yuliyan Kiryakov, 1st-year Graduate Student

1.2 Activities and findings

In the first year of this project, we have focused on getting two new two Graduate Students (Sang-Min Park and Yuliyan Kiryakov) started. Because the funding for this project did not get established until approximate October, 2004 (which was toward the end of the semester), the Graduate Students were initially consumed by classes (projects and finals). During this time, the Graduate Students met with PI Humphrey and began background reading on material related to the project, including documents on OGSA, Globus, and MyProxy.

Starting in January, the Graduate Students were able to devote more time on the research problems identified in the project. Specifically, Sang-Min Park has been focusing on the remote execution scenario for Virtual Organizations by adding new capabilities for security (and security policy). Yuliyan Kiryakov has been focusing on developing and expressing polices on individual services so that these services can dynamically modify Quality-of-Service (QoS) provided to potential consumers. For example, if a particular service is capable of executing in two different "modes" (e.g., "emergency" and "normal"), then this capability must be expressed and attached onto the individual service via some policy document. This will provide the basis for explicit policy management that is the subject of this project.

Since October, 2004, PI Humphrey has been directing the two Graduate Students in this project. Support from this project has also enabled PI Humphrey to:

- Participate in GGF-related activities
- Collaborate with two DOE scientists (Mary Thompson and Keith Jackson) on an overview of Grid Security, published in the *Proceedings of the IEEE* (see below).

- Contribute to two security-based submissions relevant to the DOE mission (papers 2 and 4, below)
- Collaborate with numerous DOE scientists (or DOE-sponsored projects) on the development and evaluation of WSRF-based services (paper 4, below -- submitted to HPDC 2005)

In the remainder of the first year (April 4, 2005 -- Aug 15, 2005), PI Humphrey will continue to direct the two grad students' activities:

- Sang-Min Park will use his experience with developing support for secure remote execute as the basis for creating user-specific policies (based on WS-Policy). Mr. Park will make modifications to individual OGSA-based remote execution services such that they contain these XML-based policies and are able to offer these XML-based documents to potential clients (this will be in coordination with Mr. Kiryakov). Mr. Park will then hand-create user-specific policies and begin to modify MyProxy to act as a repository for these policies. This will allow us to run Experiment #1 ("*Upload and/or modify user policy in MyPolMan add-in to MyProxy*") from the proposal on-schedule.
- Yuliyan Kiryakov will focus on the policies of the Virtual Organization as a whole by designing and implementing *VOPolMan.* Specifically, Mr. Kiryakov will create Client-side GUI-based tools for constructing policies to be uploaded to VOPolMan. Mr. Kiryakov will also create ways in which services may contact VOPolMan to retrieve relevant policies (which may cause the services to change their behavior to be consistent with these VO-wide policies).

1.3 Publications partially supported by this project

1 M. Humphrey, M. Thompson, and K.R. Jackson. Security for Grids. *Proceedings of the IEEE (Special Issue on Grid Computing)*, vol 93, No. 3, March 2005. pp. 644 -- 652.

2 D. Del Vecchio, J. Basney, N. Nagaratnam, and M. Humphrey. CredEx: User-Centric Credential Selection and Management for Grid and Web Services. Submitted for publication.

3 J. Wang, D. Del Vecchio, and M. Humphrey. Extending the Security Assertion Markup Language to Support Delegation for Web Services and Grid Services. Submitted for publication.

4 M. Humphrey, G. Wasson, K. Jackson, J. Boverhof, M. Rodriguez, J. Gawor, S. Lang, I. Foster, S. Meder, S. Pickles, and M. McKeown. State and Events for Web Services: A Comparison of Five WS-Resource Framework and WS-Notification Implementations. Submitted for publication at HPDC 2005.

2. Plans for the coming year (Aug 15 2005 -- Aug 14 2006)

By the beginning of Year 2 (Aug 15 2005), we expect to have the basis of MyPolMan and VOPolMan created so that, respectively, the user can specify his/her specific requirements and policies and the VO can express its policy as a whole (both via XML-based documents). The focus on year 2 will be the expansion of these capabilities as well as their integration.

Sang-Min Park, centered on the MyPolMan research and development, will:

- Develop and harden appropriate User Interface (UI) mechanisms by which a user can upload and/or inspect the policy-specific aspect of MyPolMan.
- Develop and harden mechanisms by which general services can locate and interact with the appropriate MyPolMan to determine the requester's policies.
- Prototype service-specific interpretation of policies retrieved from MyPolMan. This will form the basis of per-service policy resolution (that will be continued in Year 3 of this project).

Yuliyan Kiryakov, focused on VOPolMan research and development, will:

- Create appropriate call-out mechanisms by which the VOPolMan can begin to monitor the services to determine if the policies of the VO are being adhered to.
- Design and implement mechanisms by which services can be modified (in a generic manner) to be more consistent with the overall goals of the VO. Determining *which* services should be modified to achieve *what* behavior is particularly challenging (if, for example, the approach is to be scalable).

We have identified two specific experiments to be accomplished over this next year:

- **Experiment 1 (Approx. Jan 1 2006):** *User engages Grid service; Grid service retrieves policy from appropriate MyProxy server in order to complete the client request according to a balance between the service's policy and the user's policy.* The goal is to ensure that the correct MyProxy server can be easily found, the relevant policy or policies can be retrieved from the MyProxy server, the Policy Decision Point (PDP) mechanism can be properly invoked, and the Policy Enforcement Point (PEP) mechanism can comply with the results of the PDP mechanism.
- **Experiment 2 (Approx. May 31 2006):** *Experiment 1 + policy retrieval from the VOPolMan.* This is a relatively straightforward extension of experiment 1 so that VO-wide policies can be reconciled with the policies of the VO. This experiment and Experiment 1 will be designed so that there may require a non-trivial reconciliation of policies, but the reconciliation *can* be performed on-line via automated conflict resolution.

We plan to submit one paper this year based on Sang-Min Park's work and one paper based on Yuliyan Kiryakov's work. The planned venue is HPDC.

Annual Report: Aug 15, 2005 -- Aug 14 2006

1. Technical progress during the current budget period

The goal of this 3-year project is to facilitate a more productive dynamic matching between resource providers and resource consumers in Grid environments by explicitly specifying *policies.* The first problem being addressed in this proposal is the lack of an Open Grid Services Architecture (OGSA)-compliant mechanism for expressing, storing and retrieving user policies and Virtual Organization (VO) policies. The second problem being addressed in this proposal is the lack of tools to resolve and enforce policies in OGSA. The goal is to make all policies explicit (e.g., virtual organization policies, resource provider policies, resource consumer policies), thereby facilitating policy matching and policy negotiation. Significant proposed contributions over the 3-year project include:

- *MyPolMan,* an add-in tool suite to MyProxy, a widely-available on-line Grid credential manager, that creates the ability for a Grid user to centralize (where appropriate) and manage his/her policies
- *VOPolMan,* in which the policies of the Virtual Organization are expressed, managed, and dynamically consulted

1.1 Participant individuals

Marty Humphrey, PI
Jun Feng, 4th-year Graduate Student
Sang-Min Park, 2nd-year Graduate Student
Weide Zhang, 2nd-year Graduate Student
Zachary Hill, 1st-year Graduate Student

1.2 Activities and findings

In the second year of this project, we have continued the first year's work on policy-based remote execution (graduate student Sang-Min Park) and a general policy management framework (graduate student Jun Feng). Additionally, we have expanded the activities to include policy-based auditing (graduate student Weide Zhang) and the application of policy-based computing in the Open Science Grid, particularly CMS (graduate student Zachary Hill). We now describe these activities and findings in more detail.

Fourth-year graduate student Jun Feng has taken over the work being pursued last year by Yuliyan Kiryakov, who was leading the design and implementation of MyPolMan and VOPolMan. (Mr. Kiryakov has been moved to another project entitled "Dependable Grids"). On April 17, 2006, Mr. Feng successfully culminated a productive research year by presented his PhD Proposal based on this work ("Explicit Resource Usage Policy Management and Enforcement in Grid Computing"). Mr. Feng has prototyped MyPolMan and VOPolMan, based on XACML and WS-Policy. Mr. Feng has had two papers accepted this year based on this work (Grid Workshop 2005 and ICPADS 2006, publications #5 and #3, below, respectively).

As in year 1 of this project, second-year graduate student Sang-Min Park has been focusing on the remote execution scenario for Virtual Organizations by adding new capabilities for security (and security policy). Mr. Park has completed a technical report on this work ("Policy Resolution and Enforcement of Privileges in a Grid Authorization System Based on Job Properties"), which is the basis for his newly-

completed Master's degree. (Mr. Park is continuing on this project for his PhD research). This work is novel because, instead of basing remote execution on the *identity* of the submitter of the job, this work takes into account the intended actions of the job as the basis for authorization (in addition to identity). In combination with sandboxing techniques, this will allow for more secure execution.

Second-year graduate student Weide Zhang has created new flexibility for logging/auditing of distributed services this year. In his prototype system, data owners can specify the explicit fine-grained policy by which to create logs (for example, "write the following data if/when Bob Smith attempts to read foo.txt…."). We believe that this creates a more secure distributed computing environment that is possible today. This work (publication #2, below) has been submitted to the 2006 Grid Computing conference, to be held in Barcelona, Spain. We believe this work has broad impact and applicability to DOE researchers.

First-year graduate student Zachary Hill began working with this project in January 2006. At that point, we wanted to make sure that this research effort was well-grounded in the operational requirements of DOE science, so we have asked Mr. Hill to install the Open Science Grid code, with particular focus on CMS. Mr. Hill has been studying OSG/CMS to determine how we might best integrate our general policy framework.

In this year of this project, PI Humphrey has:

- Directed the 4 graduate students identified above
- Participated in GGF-related activities
- Collaborated with numerous DOE scientists on a vision for security for Open Science (this is the basis of a SciDAC-2 proposal, led by PI Deb Agarwal, LBNL)
- Presented this project status at the September 2005 "DoE High-Performance Network Research PI Meeting" at Brookhaven National Lab
- Directed an undergraduate's senior thesis on a directory service for policies in distributed computing based on UDDI (IPDPS 2006, publication #4 below)
- Co-authored a Supercomputing 2005 paper on the architecture of OGSA-based Grids (publication #6, below)

We accomplished the two experiments we had planned for this year:

- **Experiment 1 (Planned date: Jan 1 2006; actual date: March 2006):** *User engages Grid service; Grid service retrieves policy from appropriate MyProxy server in order to complete the client request according to a balance between the service's policy and the user's policy.* The goal is to ensure that the correct MyProxy server can be easily found, the relevant policy or policies can be retrieved from the MyProxy server, the Policy Decision Point (PDP) mechanism can be properly invoked, and the Policy Enforcement Point (PEP) mechanism can comply with the results of the PDP mechanism.
- **Experiment 2 (Planned date: May 31 2006; actual date: June 2006):** *Experiment 1 + policy retrieval from the VOPolMan.* This is a relatively straightforward extension of experiment 1 so that VO-wide policies can be reconciled with the policies of the VO. This experiment and Experiment 1 will be designed so that there may require a non-trivial reconciliation of policies, but the reconciliation *can* be performed on-line via automated conflict resolution.

1.3 Publications partially supported by this project

1) S-M. Park, G. Wasson, and M. Humphrey. Policy Resolution and Enforcement of Privileges in a Grid Authorization System Based on Job Properties. University of Virginia Department of Computer Science Technical Report. May 1, 2006. *Submitted for publication.*

2) W. Zhang, D. Del Vecchio, G. Wasson, and M. Humphrey. Flexible and Secure Logging of Grid Data Access. University of Virginia Department of Computer Science Technical Report. April 24, 2006. *Submitted for publication.*
3) J. Feng, L. Cui, G. Wasson, and M. Humphrey. Policy-Directed Data Movement in Grids. *12th International Conference on Parallel and Distributed Systems (ICPADS 2006)*, Minneapolis, MN, July 12-15, 2006.
4) E. Benson, G. Wasson, and M. Humphrey. Evaluation of UDDI as a Provider of Resource Discovery Services for OGSA-based Grids. *2006 International Parallel and Distributed Processing Symposium (IPDPS 2006),* Rhodes Island, Greece, April 25-29, 2006.
5) J. Feng, L. Cui, G. Wasson, and M. Humphrey. Toward Seamless Grid Data Access: Design and Implementation of GridFTP on .NET. Proceedings of the *2005 Grid Workshop (Associated with Supercomputing 2005)*. Nov 13-14, 2005. Seattle, WA.
6) M. Humphrey, G. Wasson, Y. Kiryakov, S-M. Park, D. Del Vecchio, N. Beekwilder, and J. Gray. Alternative Software Stacks for OGSA-based Grids. *Proceedings of Supercomputing 2005*, Seattle, WA, Nov 12-18, 2005.

2. Plans for the coming year (Aug 15 2006 -- Aug 14 2007)

In year 2 of the project, we accomplished our main goals of designing and implementing the main pieces of the policy management framework via separate sub-projects (e.g., policy-based remote execution, policy-based logging, prototyped MyPolMan and VOPolMan). In the third year of this project, we will both continue to develop and harden these individual sub-projects as well as integrate these projects. Furthermore, we will use OSG/CMS to guide the further development and evaluation of the work. It is planned that Jun Feng, Sang-Min Park, and Zachary Hill will devote some/all of their time to this project in this third and final year of this project.

More specifically, in year 3 of this project our plans include the following:

- The policy-based remote execution system and the policy-based logging system will, at run-time, utilize policies stored in MyPolMan and VOPolMan. To date, these policies have been stored locally, with the respective Grid services.
- The GUI currently being developed for MyPolMan and VOPolMan will be extended to allow the construction of policies for use in the policy-based remote execution system and the policy-based logging system.
- We will extend the current limited policy resolution engine to be able to handle broader policies. To date, it can only resolve very simple policies.
- We will create appropriate call-out mechanisms by which the VOPolMan can begin to monitor the services to determine if the policies of the VO are being adhered to.
- We will design and implement mechanisms by which services can be modified (in a generic manner) to be more consistent with the overall goals of the VO. Determining *which* services should be modified to achieve *what* behavior is particularly challenging (if, for example, the approach is to be scalable).
- We will integrate our policy framework with the core OGSA execution service: Basic Execution Service (BES). This will ensure applicability to OGSA.

In year three, we have two specific experiments planned:

- **Experiment 4 (Approx. Aug 30, 2006):** *Experiment 3 + irreconcilable policy conflict.* The goal of this experiment is to inform the principals (the VO, the Grid Service, and the Grid user) that the automated conflict resolution has failed (for example, one policy might be that "Service 1

cannot be used" and another policy might state that "Service 1 must be used"). The mechanism used to inform the participants might be email. In any case, this experiment will be the motivation for ensuring that out-of-band policy conflict resolution can be performed.

- **Experiment 5 (Approx. Aug 1, 2007):** *VOPolMan deploys new policies to select Grid Services to re-focus the short term behavior of the VO.* The goal of this experiment is to ensure that the VO can identify and inform certain principals of the VO that their policies must be modified in order to achieve the long-term goals of the VO. This is primarily a test of the measurement and enforcement capabilities of the VOPolMan and the Grid infrastructure.

We plan to continue to disseminate this work through high-quality conference publications (e.g., HPDC), Global Grid Forum (GGF) meetings, and personal meetings with DOE researchers (e.g., at Supercomputing 2006).

Annual Report: Aug 15, 2006 -- Aug 14 2007

1. Technical progress during the current budget period

The goal of this 3-year project is to facilitate a more productive dynamic matching between resource providers and resource consumers in Grid environments by explicitly specifying *policies.* The first problem being addressed in this proposal is the lack of an Open Grid Services Architecture (OGSA)-compliant mechanism for expressing, storing and retrieving user policies and Virtual Organization (VO) policies. The second problem being addressed in this proposal is the lack of tools to resolve and enforce policies in OGSA. The goal is to make all policies explicit (e.g., virtual organization policies, resource provider policies, resource consumer policies), thereby facilitating policy matching and policy negotiation. Significant proposed contributions over the 3-year project include:

- *MyPolMan,* an add-in tool suite to MyProxy, a widely-available on-line Grid credential manager, that creates the ability for a Grid user to centralize (where appropriate) and manage his/her policies
- *VOPolMan,* in which the policies of the Virtual Organization are expressed, managed, and dynamically consulted

1.1 Participant individuals

Marty Humphrey, PI
Jun Feng, 5th-year Graduate Student
Sang-Min Park, 3nd-year Graduate Student
Weide Zhang, 3nd-year Graduate Student
Zachary Hill, 2st-year Graduate Student

1.2 Activities and findings

In the third year of this project, we have made significant progress on a number of different aspects of policy management in Grids.

Jun Feng has been very productive in this first year since he defended his PhD Proposal ("Explicit Resource Usage Policy Management and Enforcement in Grid Computing"). He has continued work on developing the policy language that is the basis of MyPolMan and VOPolMan. He has also worked on the policy resolution logic, expanding the support for different types of resources and different resolution mechanisms. He expects to submit a paper on this work in the coming year.

Sang-Min Park has had a paper accepted (publication #1, below) on remote execution based on the policy of recognizing certain job properties as being more important than the identity of the submitter. He has spent the majority of this year developing his PhD proposal that is based in part on this work.

Weide Zhang has produced a paper accepted to *Grid 2006* on policy-based access for GridFTP, which is used by a large number of DOE researchers. We have found that this new flexibility enables finer-grained access of information – above and beyond the typical identity-based control.

Zach Hill has studied OSG/CMS and used many of the insights for research into general policy-based grid management.

In this year of this project, PI Humphrey has:

- Directed the 4 graduate students identified above
- Participated in OGF/GGF-related activities
- Co-authored a Supercomputing 2006 paper on the security of Grid portals (many of which are used by DOE collaboratories, see publication #2 below)

1.3 Publications partially supported by this project

1) S.-M. Park, G. Wasson, and M. Humphrey. Authorizing Remote Job Execution based on Job Properties. *2nd IEEE International Conference on e-Science and Grid Computing*. Dec 4-6, 2006, Amsterdam, Netherlands. pp. 29 – 38.
2) D. Del Vecchio, V. Hazlewood, and M. Humphrey. Evaluating Grid Portal Security. *ACM/IEEE International Conference for High Performance Computing, Networking, Storage, and Analysis (Supercomputing 2006)*, Tampa, FL, Nov 11-17, 2006. pp. 114 – 127.
3) W. Zhang, D. Del Vecchio, G. Wasson, and M. Humphrey. Flexible and Secure Logging of Grid Data Access. *7th IEEE/ACM International Conference on Grid Computing (Grid 2006),* Sept 28-29, 2006, Barcelona Spain. pp. 80 – 87.

2. Plans for the coming year (Aug 15 2007 -- Aug 14 2008)

We have requested (and been granted) a 1-year no-cost extension to complete this project. We plan to continue to make enhancements to the basic framework, so that users, resource providers, and resource consumers can better express the policies and obligations for OGSA-based Grids.

Annual Report: Aug 15, 2007 -- Aug 14 2008 (no-cost extension)

1. Technical progress during the current budget period

The goal of this 3-year project is to facilitate a more productive dynamic matching between resource providers and resource consumers in Grid environments by explicitly specifying *policies.* There are broadly two problems being addressed by this project:

1) The lack of an OGSA-compliant mechanism for expressing, storing and retrieving user policies and VO policies.
2) The lack of tools to resolve and enforce policies in OGSA.

The goal is to make all policies explicit (e.g., virtual organization policies, resource provider policies, resource consumer policies), thereby facilitating policy matching and policy negotiation. Significant proposed contributions over the 3-year project include:

- *MyPolMan,* an add-in tool suite to MyProxy, a widely-available on-line Grid credential manager, that creates the ability for a Grid user to centralize (where appropriate) and manage his/her policies
- *VOPolMan,* in which the policies of the Virtual Organization are expressed, managed, and dynamically consulted

1.1 Participant individuals

Marty Humphrey, PI
Jun Feng, 6th-year Graduate Student
Sang-Min Park, 4th-year Graduate Student
Zachary Hill, 3rd-year Graduate Student

1.2 Activities and findings

In this final year (no-cost extension), we have successfully completed the project, thereby greatly expanding the ability to perform general policy-based access to resource and information. Our efforts in this year were centered on three integrated research projects.

First, in the previous year of this DOE project, we created new policy-based access for GridFTP. We found that while this provided new capabilities for policy-based access to information, the actual policy language was not as flexible and as expressive as we needed in certain use-cases. To remedy this situation, we collaborated with Microsoft Research, applying their security language called SecPAL with our approach for GridFTP. This paper was accepted and presented at *Grid 2007*.

Second, Jun Feng wrapped up his work on MyPolMan and VOPolMan, and summarized the overall effort in his *Grid 2007* paper entitled "Resource Usage Policy Expression and Enforcement in Grid Computing". In many ways, this paper represents the overall summation of the results of this DOE project.

Third, we leveraged the successful completion of this DOE project to create a more comprehensive framework in which all resources are dynamically managed via a policy-based, and specifically for dependability/performance (publication #2 below) and for dependability/intrusion detection (publication #3 below).

1.3 Publications partially supported by this project

1) M. Humphrey, S.-M. Park, J. Feng, N. Beekwilder, G. Wasson, J. Hogg, B. LaMacchia, and B. Dillaway. Fine-Grained Access Control for GridFTP using SecPAL. *8th IEEE/ACM International Conference on Grid Computing (Grid 2007)*, Austin, TX, Sept 19-21, 2007.
2) Z. Hill, J. Rowanhill, A. Nguyen-Tuong, J. Basney, G. Wasson, J. Knight and M. Humphrey. Meeting Virtual Organization Performance Goals through Adaptive Grid Reconfiguration. *8th IEEE/ACM International Conference on Grid Computing (Grid 2007)*, Austin, TX, Sept 19-21, 2007. .
3) J. Rowanhill, G. Wasson, Z. Hill, J. Basney, Y. Kiryakov, J. Knight, A. Nguyen-Tuong, A. Grimshaw and M. Humphrey. Dynamic System-wide Reconfiguration of Grid Deployments in Response to Intrusion Detections. *High Performance Computation Conference 2007 (HPCC 2007),* 26-28 September 2007, Houston, TX.
4) J. Feng, G. Wasson, and M. Humphrey. Resource Usage Policy Expression and Enforcement in Grid Computing. *8th IEEE/ACM International Conference on Grid Computing (Grid 2007),* Austin, TX, Sept 19-21, 2007.

Summary of Overall Project Accomplishments

The goal of this 3-year project was to facilitate a more productive dynamic matching between resource providers and resource consumers in Grid environments by explicitly specifying *policies.* There were broadly two problems being addressed by this project. First, there was a lack of an Open Grid Services Architecture (OGSA)-compliant mechanism for expressing, storing and retrieving user policies and Virtual Organization (VO) policies. Second, there was a lack of tools to resolve and enforce policies in the Open Services Grid Architecture.

To address these problems, our overall approach in this project was to make all policies explicit (e.g., virtual organization policies, resource provider policies, resource consumer policies), thereby facilitating policy matching and policy negotiation. Policies defined on a per-user basis were created, held, and updated in *MyPolMan,* thereby providing a Grid user to centralize (where appropriate) and manage his/her policies. Organizationally, the corresponding service was *VOPolMan,* in which the policies of the Virtual Organization are expressed, managed, and dynamically consulted. Overall, we successfully defined, prototyped, and evaluated policy-based resource management and access control for OGSA-based Grids.

This DOE project partially supported 17 peer-reviewed publications on a number of different topics: General security for Grids, credential management, Web services/OGSA/OGSI, policy-based grid authorization (for remote execution and for access to information), policy-directed Grid data movement/placement, policies for large-scale virtual organizations, and large-scale policy-aware grid architectures. In addition to supporting the PI, this project partially supported the training of 5 PhD students.