U.S. Department of Energy Office of Science
Scientific Discovery through Advanced Computation Solicitation 01-06 and LAB01-06
National Collaboratories and High Performance Networks

Security and Policy for Group Collaboration

A DOE SciDAC Collaboratory Middleware Project

Final Report

For the period May 1, 2001 – September 31, 2006

Principal Investigators

Ian Foster
Mathematics and Computer Science Division, Argonne National Laboratory
Argonne, IL 60439
Tel: 630 252 4619 Fax: 630 252 5986
Email: foster@mcs.anl.gov

Carl Kesselman
Information Sciences Institute, University of Southern California
4676 Admiralty Way, Suite 1001
Marina del Rey, CA 90292-6695
Tel: (310) 448-9338 Fax: (310) 823 6714
Email: carl@isi.edu

Other Senior Personnel

Jim Basney	National Center for Supercomputing Applications
John Bresnahan	Mathematics & Computer Science Division, Argonne National Laboratory
Doug Engert	Electronics & Component Technologies Div., Argonne Natl Laboratory
Jarek Gawor	Mathematics & Computer Science Division, Argonne National Laboratory
Miron Livny	Dept of Computer Science, University of Wisconsin Madison
Laura Pearlman	Information Sciences Institute, University of Southern California
Frank Siebenlist	Mathematics & Computer Science Division, Argonne National Laboratory
Von Welch	National Center for Supercomputing Applications

Table of Contents

Abstract

“Security and Policy for Group Collaboration” was a Collaboratory Middleware research project aimed at providing the fundamental security and policy infrastructure required to support the creation and operation of distributed, computationally enabled collaborations. The project developed infrastructure that exploits innovative new techniques to address challenging issues of scale, dynamics, distribution, and role. To reduce greatly the cost of adding new members to a collaboration, we developed and evaluated new techniques for creating and managing credentials based on public key certificates, including support for online certificate generation, online certificate repositories, and support for multiple certificate authorities. To facilitate the integration of new resources into a collaboration, we improved significantly the integration of local security environments. To make it easy to create and change the role and associated privileges of both resources and participants of collaboration, we developed community wide authorization services that provide distributed, scalable means for specifying policy. These services make it possible for the delegation of capability from the community to a specific user, class of user or resource. Finally, we instantiated our research results into a framework that makes it useable to a wide range of collaborative tools. The resulting mechanisms and software have been widely adopted within DOE projects and in many other scientific projects. The widespread adoption of our Globus Toolkit technology has provided, and continues to provide, a natural dissemination and technology transfer vehicle for our results.

A. Narrative

A.1. Introduction

This SciDAC project has developed software and tools to enforce required security policies in DOE's major distributed science projects.

Scientific advances today are almost exclusively the result of large collaborative teams. The Department of Energy SciDAC program contains many examples of such collaborative teams:

- *High energy physics*: Particle physics experiments, such as BABAR, CMS, and ATLAS, are designed and conducted by large, multinational teams. Subsets of the team might be responsible for the design of the detector, various pieces of software for on-line data collection, data preprocessing and event detection. Team members use shared data sets for analysis and may use community wide compute resources for data analysis.
- *Earth System Grid (ESG):* Scientists studying global climate change perform extensive post-simulation analysis in order to attempt to understand the results of a simulation. While a small team may develop the simulation code, separate groups may configure and run the code to generate data about a specific phenomenon. At this point, the simulation data becomes a community resource that has a variety of uses.
- *National Fusion Collaboratory (NFC)*: This community has for over a decade utilized remote monitoring and control of select instruments. Magnetic fusion experiments are conducted at three large experimental sites, which distribute large amounts of data to a theoretical and simulation community, which works with the experimental team to create realistic 3D plasma models.

These examples illustrate four essential properties of collaborative work:

- *Geographical and organizational distribution*. Participants in a collaborative activity are distributed, both geographically and organizationally, as are the tools and resources used to perform the work of the collaboration (e.g., computers, data sets, storage devices, simulation programs).
- *Large and dynamic scale*. Collaborations can scale in size from a few individuals to literally hundreds or thousands of participants, which is the case of many high-energy physics experiments. Furthermore, the membership of participants of a collaboration is not static, but frequently varies over the lifetime of the collaborative task. Participants may join or leave, and resources may be added or removed
- *Diverse roles*. Collaborations may span areas of expertise, with members filling different roles within the collaboration. The role of a member may be fixed for the duration of the collaboration, or it may change during its lifetime. For example, in the case of climate modeling there are distinct roles with associated specific rights of the simulation writer, the simulation runner, and the consumer of simulation data.
- *Community resources*. The work of the team is enabled by providing team members with access to a variety of resources including computers, storage systems, datasets, applications, and tools. Thus in a real sense, a collaboration is not just the group of individuals participating in the activity, but the resources that can be used by members of the collaboration to conduct their work.

In order for such collaborations to succeed, participants must have means to perform the work of the collaboration: e.g., mechanisms for annotating and cataloging information so that it may be understood by members of the collaboration, electronic notebooks for sharing what processes had been followed, interfaces that make computing resources available for use, methods for discovering and initiating simulation codes, etc. Most work on collaboration tools focuses on the development of these tools.

In order for the collaboration to be effective, its participants must also have mechanisms for establishing and maintaining the structure of the collaboration. Users and resources are rarely fully devoted to any particular collaboration, but instead remain bound by policies and technologies that are in place at their home organization and in other collaborations of which they are a part.

The foundation of these mechanisms for collaboration structure is the ability to identify the collaboration members (authentication) and determine what their specific roles and privileges are (authorization). This process of authentication and authorization is non-trivial due to the number of parties that contribute policy to authorization process – the collaboration, the resource sites, the resource managers, and the users are all examples of entities, which have a stake in the authorization process. The complexity of combining these different policies is increased by several factors:

The policies to be combined may be dynamic and diverse. The collaboration may need to change its policy as users or contributed resources change, when its goals change, or the collaboration may begin with only a rudimentary idea of what its policies should be and formulate more appropriate policies over time. Policies from the site or other parties may similarly change. This requires mechanisms for forming the combined policy must be capable of acquiring and combining these policies in real-time as the policy is applied.

Policies and the attribute and identity credentials they depend on, come in a variety of forms. Unfortunately we have many standards for expressing policies and attributes. Different sites and collaborations have in the past, and will continue in the future, continue to select different mechanisms (e.g. X.509 attribute certificates, SAML assertions, LDAP) for legitimate reasons. A system that supports the combining of policies and attributes from multiple sources must be capable of dealing with different formats.

Policies vary in granularity. In some cases policy will need to be fine-grained, e.g., expressing access to individual files, while in other cases they will be rather coarse-grained, e.g., only users with DOE Grids identity certificates may use this service. This requires that the enforcement system for the resulting policy be flexible. For example, a system designed to only enforce access control to a site may not be capable of differentiating between what file is being referenced in a request

Policies cover a wide range of resources. Collaborations are not concerned with only a single type of resource (e.g., computation, data storage, visualization, instruments), but with a wide range. This requires the policy and enforcement systems to be broadly applicable.

A.2. Project Summary

At the time that this project began, GSI provided simple mechanisms for authentication, authorization, and delegation. During the course of this project, we have designed and developed software components to facilitate adding users to a collaboration, managing policies within a collaboration, evaluating and enforcing policy information, and managing delegated credentials. We have also integrated our security framework with applications for the Earth Systems Grid (ESG) project and remained active in standards activities, both in terms of adopting emerging standards in our components and in participating in standards activities.

1. Adding users to a collaboration. We have developed the *Portal-based User Registration System* (PURSE), which simplifies the process of adding users to a collaboration by providing an easy-to-use Web interface for potential users of an application to “register” themselves and request sign-in credentials. Administrators receive requests and decide whether to grant them. When a user is registered, a Grid credential is created on his behalf and used “behind the scenes” whenever he uses the application.

PURSE combines the Simple CA and MyProxy components with a back-end database and a web portal to automate user registration requests. The registration interface solicits basic data from user, including a desired ID/password combination. Requests are forwarded by email to an administrator and the data from the requests are stored in a database. The administrator uses administrative functions in the web portal to process requests. Users receive email notification when their accounts are ready for use.

Key benefits of this approach are:

- Users never have to see or manage their Grid credentials.
- The MyProxy service is automatically populated with user credentials which can be retrieved either from web portal interfaces or from desktop systems using the MyProxy client tools.
- A database is automatically populated with basic information about all application users.
- The registration service, user credentials, and MyProxy service can be re-used in other applications.

We successfully integrated the PURSE system in the Earth System Grid (ESG) portal (Figure 1) as the primary authentication infrastructure service, which is in full production mode without any major issues.

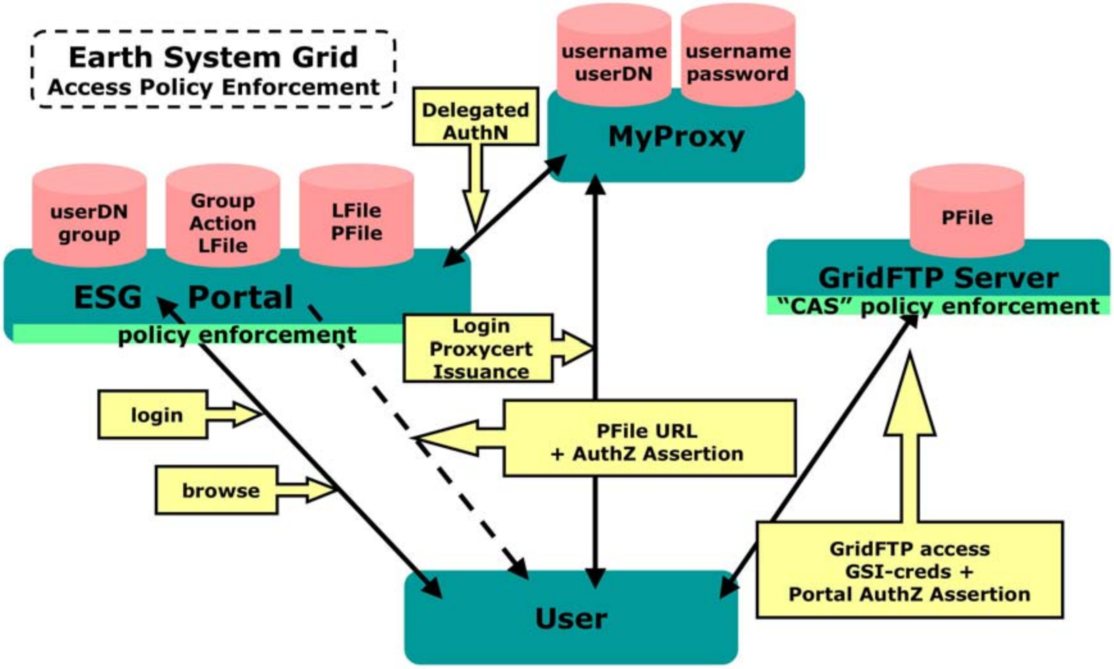

Figure 1. Earth System Grid Security

2. Managing policies within a collaboration. We have developed the *Community Authorization Service* (CAS: Figure 2) to manage VO-wide policies regarding resources distributed across multiple sites.

Clients interact with a CAS server to obtain a SAML authorization assertion that is signed by the CAS-associated authorization authority. The client then presents the assertion to the application server, which, to the extent that it trusts the authorization authority that signed the assertion, will use that policy information to evaluate the client's access rights. The signed authorization may be embedded in the client's proxy certificate as a non-critical extension or pushed to the server using an application-specific mechanism; alternatively, the application server may query the CAS server directly using our standardized SAML authorization query interface.

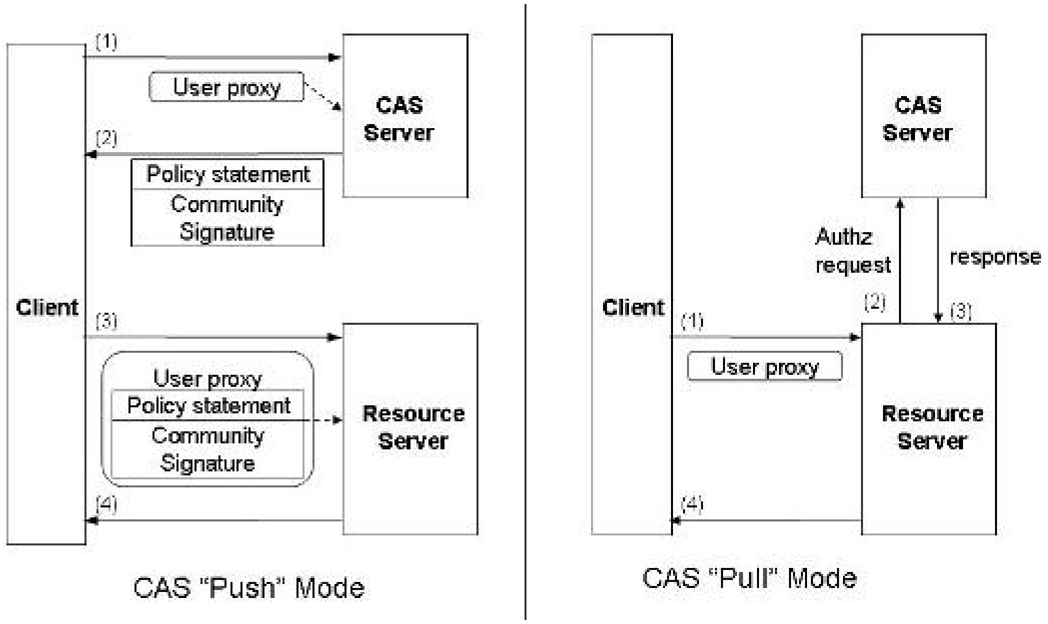

Figure 2: CAS server requests

Over the course of this project, the CAS server has evolved in response to developing standards and user requirements. CAS was implemented first using an XML-RPC based protocol before becoming an OGSI-based, and finally a WSRF-based service. Its policy assertions were initially expressed in an ad-hoc policy language, then in SAML.

3. Evaluating, combining, and enforcing policies from multiple sources. We have designed and implemented a generalized authorization framework and attribute collection framework, which provide extensible mechanisms to evaluate policy and attribute information from multiple heterogeneous sources.

The *Globus Authorization Framework* (Figure 3) is an extensible runtime module that evaluates external policies and assertions via a plugin interface and combines the results to make authorization decisions in a consistent and policy-driven way. More and more DOE deployments use sophisticated authorization models requiring that the policy enforcement point either make callouts to external authorization servers or handle pushed authorization assertions in different formats.

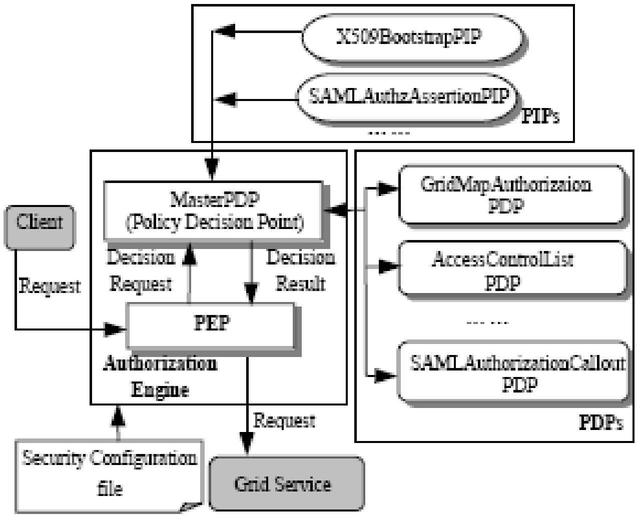

Figure 2: Globus Authorization Framework

In this framework, an authorization engine gathers attribute information from Policy Information Points (PIPs), queries Policy Decision Points (PDPs) to determine whether the request would be allowed under one or more policies, and combines the result to make a final access control decision for each client request. Since the Globus Toolkit's runtime includes natural policy enforcement points, the Authorization Engine is called at those points to provide access control decisions before any application code is called. The Authorization Framework provides plug-in interfaces for PDPs and PIPs, which are configurable at run time. This code is part of the Globus Toolkit core.

As most DOE deployments are moving or have expressed desire to move towards an attribute-based authorization policies, support for the consistent and generic processing of the different attribute assertions is required. The attributes are expressed in different formats, such as X509 Attribute certificates and SAML, are either pushed by the clients or retrieved from attribute services, and have to be presented to the subsequent policy decision point where the policy expressions are evaluated that rely on the attribute values. With the lessons learned from our GridShib experiences, we have designed and implemented an attribute collection framework that collects, validates and standardizes the attributes before they are handed hoff to the authorization-processing phase. Together with the before mentioned authorization processing functionality, this working code is currently being validated for correctness and is expected to become part of the Globus Toolkit core.

4. Management of delegated credentials. Grid applications often need to delegate user credentials to servers, in order to allow those servers to access other grid resources on the user's behalf. GSI has long supported a mechanism for delegation, but this mechanism has two limitations. First, it requires that a new key pair be generated for each delegation, which can be a somewhat computationally-expensive process. Second, if the delegated credential expires, there is no way to renew it, which means that users who (for example) use grid services to spawn long-running jobs must be able to predict in advance how long their jobs will take, or run the risk that their delegated credential will expire before their job has completed. Users can work around the expiring-credential problem by delegating long-lived credentials, but by doing so they subject themselves to increased risk that those credentials will be compromised. To address these issues, we have implemented a *Delegation Service*, which provides a mechanism for users to delegate credentials to services and to refresh previously-delegated credentials. The caching provided by the Delegation Service provides performance enhancements, by reducing the number of (relatively expensive) delegation options performed when several service invocations are made by the same user within a short period of time. The credential refresh mechanism enables users to ensure that long-running jobs will continue to have the credentials they need to access grid resources without incurring the risk associated with delegating a long-lived credential.

5. Integration with ESG applications. While users interact through ESG's portal application to browse and select files for download, ESG's group/role-based authorization system determines the user's access to its local and remote resources. The associated authorization decisions are translated in so-called SAML authorization assertions, which are digitally signed tokens that state that the ESG portal as an authorization authority allows the subject to transfer certain file(s). By using a format of these tokens identical to those generated by CAS (Community Authorization Service), we are able to leverage the CAS-enable GridFTP servers "out of the box." The result is that the GridFTP servers will honor the ESG's authorization decisions. The required code changes in our SAML-associated authorization code have been completed and delivered to ESG and the data-mover clients are expected to deploy the issued SAML assertions shortly for GridFTP.

ESG requires that multiple files often must be transferred from the same GridFTP server, while at the start of the GridFTP session not all the authorization decisions have been received yet. The standard CAS / GridFTP clients embed authorization assertions in the proxy certificate used to authenticate to the GridFTP server, which limits the authorization assertions that can be used in a GridFTP session to those available at the time the session is created. We have designed and implemented an alternative mechanism that enables clients to communicate new authorization assertions to the server over the GridFTP control channel at any time during a session.

6. Standards. Our new components are, to the extent possible, based on established or emerging standards – for example, CAS is a WSRF service that issues assertions expressed in SAML. We have also been active in community standards activities:

- The OGSA Authorization working group's "Use of SAML for OGSI Authorization" and "OGSI Authorization Requirements" drafts have passed the public comment period in the Global Grid Forum; no issues are identified.
- The X.509 Proxy Certificate Profile became an Internet RFC (RFC 3820) in June 2004.
- The OGSA's working group's "OGSA, WSRF Basic Profile 1.0 ", "OGSA Basic Security Profile 1.0 – Core" and "OGSA Basic Security Profile 1.0 – Secure Channel" have progressed and have been submitted for review.
- The Web Service Security V1.1 and the XACML V2.0 specifications, with our contributions, have been promoted to standards in OASIS.
- We continued to participate in Web services security standards work in OASIS, namely, XACML, SAML, Web Service Security, and Web Services Secure Exchange.
- We helped organize a well-received workshop at GGF15 in Boston in October, 2005. This workshop is documented in "Report for the GGF 15 Community Activity: Leveraging Site Infrastructure for Multi-Site Grids".
- We continued our activities to ensure smooth operation of the DOE Grids CA by participating as a member of its policy management authority.

A.3. Overall Assessment

The impact of the project on both computer science and DOE science has been tremendous. The project has produced authentication and authorization algorithms and software that have been adopted by hundreds of major distributed science projects and form the basis for the vast majority of science grid deployments. Thousands of scientists access remote data and computational services securely thanks to Grid Security Infrastructure. These projects and scientists have in turn profited from the availability of high-quality secure authentication and authorization mechanisms to achieve significant advances in distributed science. The following are just three examples:

- The DOE Earth System Grid (ESG) data portal has used Grid Security Infrastructure (GSI) mechanisms to register over one thousand climate researchers as users during the past year. These users have downloaded tens of terabytes of data from ESG sites and produced 250 publications from International Panel on Climate Change (IPCC) data alone.
- The Fusion Collaboratory uses GSI mechanisms to provide secure remote access to advanced fusion codes, increasing by an order of magnitude the number of simulations performed relative to past practice.
- Participants in the DOE Particle Physics Data Grid (PPDG) collaboration have used GSI mechanisms to enable not only high energy and nuclear physicists but also biologists and chemists to harness computers and storage at 50 sites across the U.S. for large-scale distributed data analysis. This work has reduced significantly the time required to produce analyses of data from physics and biology experiments.

A.4. Future Directions

We want to work with the members of an NSF-funded effort to integrate our Globus Toolkit with Internet2's Shibboleth, which will allow us to leverage Shibboleth/SAML attribute services for our

CAS/XACML authorization. Many of the ideas for the generic attribute collection framework were a result of our collaboration, and the expectation is that the SciDAC community will benefit from sophisticated attribute services in the policy enforcement within their collaboratories.

We want to make the PURSE, CAS/SAML-libraries, enhanced GridFTP and CAS features, and attribute collection and authorization framework available to other SciDAC DOE projects. In addition, many NSF projects (LSST, GEON) are planning and working to leverage various of these components. This wider adoption provides us with further sources of feedback and experience.

We want to continue to collaborate with the DOE National Collaboratories to define future directions for information technology within the DOE's research agenda. The CET SciDAC proposal "Security for Open Science" from ANL, LBNL, NERSC, ESnet, NCSA, PNNL, UofWisconsin, UofDelaware, and UofVirginia, provides a roadmap to implement the security-related features to address the critical issues for secure collaboration in DOE as stated by Open Science Grid (OSG), Earth System Grid (ESG), FusionGrid, NERSC, NLCF. The proposed program of work are in four interrelated areas:

- Auditing and Forensics: Services to enable sites, communities, and application scientists to determine precisely who did what, where and when.
- Dynamic Host Firewall Port Management: Services to open and close ports dynamically for applications while enforcing site policy.
- Identity Management: Services to seamlessly manage identity and access control across sites and collaborations, and to allow for rapid response to security incidents.
- Secure Middleware: Services to proactively find and fix software vulnerabilities and guarantee deployed security software is current and correctly configured.

B. Publications

Conference Proceedings:

1. Von Welch, Ian Foster, Carl Kesselman, Olle Mulmo, Laura Pearlman, Steven Tuecke, Jarek Gawor, Sam Meder, Frank Siebenlist, "X.509 Proxy Certificates for Dynamic Delegation", paper for PKI04, April 2004.
2. Liang Fang, Samuel Meder, Olivier Chevassut, and Frank Siebenlist, "Secure Password-Based Authenticated Key Exchange for Web Services", ACM XML Security Workshop, Aug 20, 2004.
3. Frank Siebenlist, Takuya Mori, "Grid-Centered Position Paper for the W3C Workshop on Constraints and Capabilities for Web Services", W3C Constraints and Capabilities workshop, Sep 3, 2004.
4. Von Welch, Tom Barton, Kate Keahey, Frank Siebenlist, "Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration", 4th Annual PKI R&D Workshop: "Multiple Paths to Trust", April 19-21, 2005, NIST, Gaithersburg MD
5. Liang Fang, Dennis Gannon, Frank Siebenlist, "XPOLA - An Extensible Capability-based Authorization Infrastructure for Grids", 4th Annual PKI R&D Workshop: "Multiple Paths to Trust", April 19-21, 2005, NIST, Gaithersburg MD
6. Stephen Langella, Scott Oster, Shannon Hastings, Frank Siebenlist, Tahsin Kurc, Joel Saltz "Dorian: Grid Service Infrastructure for Identity Management and Federation", 19th IEEE Symposium on Computer-Based Medical Systems (CBMS 2006) - Grids for Biomedical Informatics, Jun 22-23, 2006, (accepted Mar 9, 2006)
7. A Community Authorization Service for Group Collaboration. L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke. IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

8. K. Keahey, V. Welch, S. Lang, B. Liu, S. Meder. Fine-Grain Authorization Policies in the GRID: Design and Implementation. 1st International Workshop on Middleware for Grid Computing, 2003.
9. V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke. Security for Grid Services. Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), IEEE Press, June 2003.
10. Shane Canon, Steve Chan, Doug Olson, Craig Tull, and Von Welch. Using CAS to manage role-based VO sub-groups. Computing in High Energy Physics 03 (CHEP '03), 2003.
11. Ian Foster, Carl Kesselman, Laura Pearlman, Steven Tuecke, and Von Welch. The Community Authorization Service: Status and Future. Computing in High Energy Physics 03 (CHEP '03), 2003.
12. V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder, F. Siebenlist. X.509 Proxy Certificates for Dynamic Delegation. 3rd Annual PKI R&D Workshop, 2004.

Reports and specifications:

1. Frank Siebenlist, contributor "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", OASIS Standard 200401, 2004.
2. Jim Basney, Von Welch, Frank Siebenlist, "A Roadmap for Integration of Grid Security with One-Time Passwords", white paper, Apr 2004.
3. Foster, D. Berry, A. Djaoui, A. Grimshaw, B. Horn, H. Kishimoto, F. Maciel, A. Savva, F. Siebenlist, R. Subramaniam, J. Treadwell, J. Von Reich, "The Open Grid Services Architecture, Version 1.0", GGF GWD-I, June 2004.
4. Frank Siebenlist, contributor "Section: Next-Generation Security Capabilities" of the "National Collaboratories Horizons" Report of the, National Collaboratories Program Meeting Conducted by the Office of Advanced Scientific Computing Research of the U.S. Department of Energy Office of Science, ANL, IL, Aug 10-12, 2004 ,"http://www-fp.mcs.anl.gov/nc2004/NCReport041116b.pdf"
5. Ian Foster and Veronika Nefedova, "Data Access Control for the Earth System Grid", internal ANL-ESG report, Nov 4, 2004
6. Von Welch, Rachana Ananthakrishnan, Frank Siebenlist, David Chadwick, Sam Meder, Laura Pearlman, "Use of SAML for OGSA Authorization", GGF GWD-R, Nov, 2004.
7. Frank Siebenlist, contributor "eXtensible Access Control Markup Language (XACML) Version 2.0", OASIS final draft Dec 2004
8. Foster, I., Frey, J., Graham, S., Tuecke, S., Czajkowski, K., Ferguson, D., Leymann, F., Nally, M., Sedukhin, I., Snelling, D., Storey, T., Vambenepe, W. and Weerawarana, S. Modeling Stateful Resources with Web Services, www.globus.org/wsrf, 2004.
9. Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson. RFC 3820, IETF, June 2004
10. Co-Investigators, Frank Siebenlist, Ian Foster "Security for Open Science" DOE SciDAC Center for Enabling Technology proposal for the period July 1, 2006 – June 30, 2011, U.S. Department of Energy Office of Science Solicitation LAB06-04, Mar 9, 2006
11. Von Welch, Rachana Ananthakrishnan, Frank Siebenlist, David Chadwick, Sam Meder, Laura Pearlman, "Use of SAML for OGSI Authorization", GGF GWD-R (proposed), Aug 15, 2005.
12. Von Welch, Frank Siebenlist, David Chadwick, Sam Meder, Laura Pearlman, "OGSI Authorization Requirements", GGF GWD-I (proposed), Jan 14, 2006.
13. Frank Siebenlist, Takuya Mori, editor "OGSA Basic Security Profile 1.0 – Core", GGF GWD-R Draft, Global Grid Forum, Feb 9, 2006.
14. Frank Siebenlist, Takuya Mori, editor " OGSA Basic Security Profile 1.0 – Secure Channel", GGF GWD-R Draft, Global Grid Forum, Feb 9, 2006.

15. Frank Siebenlist, contributor "Report for the GGF 15 Community Activity: Leveraging Site Infrastructure for Multi-Site Grids", GGF GWD-I Draft, Global Grid Forum, Oct 6, 2005.
16. Frank Siebenlist, Ian Foster, contributor "OGSA, WSRF Basic Profile 1.0", GGF GWD-R Draft, Global Grid Forum, Sep 22, 2005.
17. Frank Siebenlist, contributor "OGSA - Grid Security Infrastructure Message Specification", GGF GWD-I Draft, Global Grid Forum, Feb 24, 2006.
18. Frank Siebenlist, contributor "eXtensible Access Control Markup Language 2 (XACML), OASIS Standard, 1 Feb 2005
19. Frank Siebenlist, contributor "SAML 2.0 profile of XACML v2.0", OASIS Standard, 1 February 2005
20. Frank Siebenlist, contributor "Core and hierarchical role based access control (RBAC) profile of XACML v2.0", OASIS Standard, 1 February 2005
21. Frank Siebenlist, contributor "Privacy policy profile of XACML v2.0", OASIS Standard, 1 February 2005
22. Frank Siebenlist, contributor "Multiple resource profile of XACML v2.0", OASIS Standard, 1 February 2005
23. Frank Siebenlist, contributor "Hierarchical resource profile of XACML v2.0", OASIS Standard, 1 February 2005
24. Frank Siebenlist, contributor "XML Digital Signature profile of XACML v2.0", OASIS Standard, 1 February 2005
25. Frank Siebenlist, contributor "Web Services Security X.509 Certificate Token Profile 1.1", OASIS Standard, 1 February 2006
26. Frank Siebenlist, contributor "Web Services Security Username Token Profile 1.1", OASIS Standard, 1 February 2006
27. Frank Siebenlist, contributor "Web Services Security Kerberos Token Profile 1.1", OASIS Standard, 1 February 2006
28. Frank Siebenlist, contributor "Web Services Security: SOAP Message Security 1.1", OASIS Standard, 1 February 2006
29. Frank Siebenlist, contributor "Web Services Security: SOAP Messages with Attachments (SwA) Profile 1.1", OASIS Standard, 1 February 2006
30. Frank Siebenlist, contributor "Web Services Security: SAML Token Profile 1.1", OASIS Standard, 1 February 2006
31. Frank Siebenlist, contributor "Web Services Security: Rights Expression Language (REL) Token Profile 1.1", OASIS Standard, 1 February 2006