

Project Acronym:  
Version:  
Contact:  
Date:



## JISC Final Report

Project Information			
<b>Project Acronym</b>	GridAPIv2		
<b>Project Title</b>	Authorisation interface V2 for the Grid		
<b>Start Date</b>	1 July 2005	<b>End Date</b>	30 November 2008
<b>Lead Institution</b>	University of Kent		
<b>Project Director</b>	David Chadwick		
<b>Project Manager &amp; contact details</b>	David Chadwick Computing Laboratory University of Kent Canterbury CT2 7NF  Tel: +44 1227 82 3221 Fax +44 1227 762 811		
<b>Partner Institutions</b>	None		
<b>Project Web URL</b>	None		
<b>Programme Name (and number)</b>	JISC Support of Research Committee		
<b>Programme Manager</b>	James Farnhill		

Document Name			
<b>Document Title</b>	Project Final Report		
<b>Reporting Period</b>	<i>Entire project</i>		
<b>Author(s) &amp; project role</b>	David Chadwick Project Manager		
<b>Date</b>	14 Feb. 09	<b>Filename</b>	finalreport.doc
<b>URL</b>			
<b>Access</b>	<input type="checkbox"/> Project and JISC internal		<input checked="" type="checkbox"/> General dissemination

Document History		
Version	Date	Comments
0.1	11 Feb. 09	First draft by DWC
1.0	14 Feb. 09	Incorporated feedback from JF

## Table of Contents

JISC Final Report.....	1
Table of Contents.....	2
Acknowledgements.....	2
Executive Summary.....	2
Background.....	2
Aims and Objectives.....	3
Methodology.....	3
Implementation.....	4
Outputs and Results.....	4
Outcomes.....	4
Conclusions.....	5
Implications.....	5
Recommendations.....	5
References.....	6

## Acknowledgements

The author would like to thank the UK JISC for funding this work.

## Executive Summary

The objectives of this project were:

- i) to be a joint chair of the OGSA Authzn working group
- ii) to be a joint editor of version 2 of the OGSA Authorisation protocol specification
- iii) to implement version 2 of the protocol in the PERMIS authorisation system
- iv) to add obligations to the PERMIS authorisation infrastructure (including the policy management GUI)
- v) to perform interworking tests with the future release of Globus toolkit that will support this protocol
- vi) to support validation tests with a still-to-be-determined UK or EGEE Grid project which finds it needs the features provided by this future specification and implementation.

All the objectives were achieved, except that the interworking tests in v) were not carried out solely with Globus Toolkit but rather with a series of implementations, since GT4 had not fully implemented all the protocol specifications by the time this project had completed.

## Background

Towards the end of 2002, the Globus team were just starting to define an authorisation interface for the Grid. At the beginning of 2003 the author put forward a proposal to work with them to define this interface as a Global Grid Forum standard, to implement the interface in PERMIS and to perform interoperability testing with an enhanced Globus toolkit. (The Globus team were to independently implement the interface in Globus toolkit during the same timeframe). This project successfully concluded in the spring of 2004 with the release of Globus Toolkit 3.3 and PERMIS 1.3, that both supported the GGF OGSA SAML authorisation interface, published as GFD 66[1].

During the next six months the integrated Globus-Permis implementation was rigorously tested at Glasgow University in the Bridges project. A deficiency in the GGF SAML specification was uncovered, namely, the inability to pass action parameters in the SAMLv1.1 protocol. Whilst PERMIS supports decision making based on action parameters, and these can be passed across its Java interface, the SAML protocol does not support it, and the GGF authors (wrongly as it turned out) thought that this feature was not necessary for the first version of GGF SAML specification.

Simultaneously with the Bridges testing, work at Virginia Tech in the USA determined that they needed obligations to be added to the GGF SAML specification. Again SAMLv1.1 does not support

Project Acronym:  
Version:  
Contact:  
Date:

the passing of obligations. Virginia Tech added their own extensions to the SAML specification for obligations.

At the March 2005 GGF 13 meeting, the OGSA Authorisation working group decided to publish the existing SAML specification as version 1 of the GGF OGSA authorisation protocol standard [1], since a) it worked, b) it was implemented in at least two independent implementations and c) the main technical work had been completed more than a year ago and all issues raised by the group had been successfully resolved. The meeting also decided that version 2 of the protocol should now be started as a new work item as soon as possible, to include action parameters and obligations, but also to look at replacing SAMLv1.1 with either the latest SAMLv2 or with XACML (a proposal made at the meeting by Frank Siebenlist). Since this would be a substantial piece of work and a major change to the current specification, it should not hold up publication of the existing specification.

This project is in line with the decisions of the GGF 13 meeting, and its objectives are specified below.

## Aims and Objectives

The objectives of the project were:

- vii) to be a joint chair of the OGSA Authzn working group
- viii) to be a joint editor of version 2 of the OGSA Authorisation protocol specification
- ix) to implement version 2 of the protocol in the PERMIS authorisation system
- x) to add obligations to the PERMIS authorisation infrastructure (including the policy management GUI)
- xi) to perform interworking tests with the future release of Globus toolkit that will support this protocol
- xii) to support validation tests with a still-to-be-determined UK or EGEE Grid project which finds it needs the features provided by this future specification and implementation.

The objectives remained the same throughout the project, except that the originally envisaged single protocol specification ended up being three protocol specifications, namely:

- Use of WS-TRUST and SAML to access a CVS [2]
- Use of XACML Request Context to access a PDP [3]
- Use of SAML to retrieve Authorization Credentials [4]

as well as a functional overview document [5].

## Methodology

The methodology for producing the protocol specifications was an iterative one. For specifications [2] and [3], the initial implementation in PERMIS was produced, based on [drafts of] existing OASIS specifications [6, 7, 8]. The OGF profile specifications were then written, based on the initial implementation, and these were reviewed by the OGSA-Authz working group. Revised specifications were produced as a result of comments and feedback, and these were then re-submitted to the working group. The PERMIS implementation was altered as necessary to keep in sync with the protocol specifications. Around 10 different versions of each of the OGF specifications [2, 3, 5] were produced during the three and a half years of this project. Specification [4] was rather different, in that this was the last of the specifications to be implemented and written, and was not originally included in the charter of the OGSA-Authz working group. The original draft was produced in 2007 by Tom Scavo and Valerio Venturi, who presented this to the OGSA-Authz working group for consideration and inclusion in the charter. The author took this document and revised it and published it as a working group draft. The charter of the OGSA-Authz working group was extended to include this specification. INFN in Italy implemented the server side of this protocol and Kent implemented the client side in PERMIS.

Once the protocol specifications were reasonably stable, and several implementations existed, a series of interworking demonstrations were performed at the OGF 22 meeting in Boston in February 2008. These tests were carried out by various combinations of GT4, PERMIS, VOMS, GP-BOX, and

Project Acronym:  
Version:  
Contact:  
Date:

Sun's XACML PDP. These demonstrations showed that the profile standards produced by the OGSA Authz working group were now maturing and were ready for wide scale adoption. The specifications were then prepared for public comment. The public comment periods were supposed to be completed by the OGF 24 meeting in Singapore in September 2008, but due to administrative errors by the OGF editor, their publication was delayed, so that the public comment periods had not all completed by the time of the meeting. Consequently by the close of this project, not all comments have been successfully resolved, and final versions of the specifications have still to be produced.

## Implementation

The initial implementation was performed in the PERMIS authorisation infrastructure, and the initial interworking tests were with our own implementation. We then used Sun's XACML PDP to perform interworking tests between PERMIS and the latter, based on [3]. As the project progressed other developers around the globe eventually started to use the XACML profile [3] and did their own interworking tests. They fed their results back into the OGSA-Authz working group, and these were incorporated into revised versions of the profile.

Unfortunately no other group implemented protocol [2] before this project completed.

Protocol [4] was initially implemented by INFN in Italy (server side), and we (and others) implemented the client side and did some successful interworking tests with this before the project completed. However, the specification still has a number of issues that need to be addressed at the completion of this project.

## Outputs and Results

The project has achieved the following tangible outputs.

1. It has produced 3 grid authorisation protocol profiles [2, 3, 4], when only one was envisaged at the start of the project, as well as an overview of the functional requirements of an authorisation infrastructure [5].
2. All three protocols have been implemented in the PERMIS authorisation infrastructure and have already been released as open source code
3. Two of the three protocols [3, 4] have been implemented in at least two other implementations around the globe, and a set of interworking tests have been successfully publicly demonstrated at OGF 22.
4. The work has led to further research funding and development work at Kent in the area of federated and grid authorisation.

## Outcomes

The project has achieved all the objectives that it originally set for itself, namely:

The objectives of the project were:

- i) to be a joint chair of the OGSA Authzn working group  
*This has been successfully carried out and the author intends to stand down as joint chair at the next OGF meeting (OGF 25) in March 2009.*
- ii) to be a joint editor of version 2 of the OGSA Authorisation protocol specification  
*This has been successful, in that 3 different protocol profiles have been specified. However, none of them have yet been published as OGF standards, and there are still some outstanding issues with them.*
- iii) to implement version 2 of the protocol in the PERMIS authorisation system  
*This has been successful as all three protocols have been implemented in PERMIS and released as open source code.*
- iv) to add obligations to the PERMIS authorisation infrastructure (including the policy management GUI)  
*This has been successfully completed and released as open source code.*

Project Acronym:  
Version:  
Contact:  
Date:

- v) to perform interworking tests with the future release of Globus toolkit that will support this protocol

*This has only been partially successful since GT4 has not implemented all 3 protocol specifications. Protocol [2] has currently only been tested between PERMIS implementations. Interworking tests with INFN in Italy have been successfully carried out for protocol [4]. Protocol [3] is the most widely tested of the three protocols.*

- vi) to support validation tests with a still-to-be-determined UK or EGEE Grid project which finds it needs the features provided by this future specification and implementation.

*Prof Richard Sinnott from the UK e-Science centre successfully performed validation tests of two of the three protocols [2 and 3] and we anticipate that validation tests of [4] will be completed later this year.*

One of the disappointing features of this project, was that at the outset the University of Kent was too far ahead of the rest of the grid world in its authorisation research, that we found it very difficult to generate sufficient enthusiasm and support from other groups to implement the authorisation profiles and perform interworking tests with us. Many grid implementers were still struggling with either application or authentication issues, and did not have the time or resources to concentrate on authorisation issues. At various times during the project it looked as if the OGSA-Authz working group might actually have to close prematurely due to lack of participation by members. It took a while before a second co-chair was appointed for the WG and the author had to chair several meetings himself for a while. Consequently this project had to be extended from its initial two year period, to nearly three and a half years. Interworking tests only really started to happen in the last year of the extended project, and we can honestly say that the project is still not fully complete, in terms of having a final set of OGF specifications fully published as standards and implemented by multiple groups around the globe.

One of our biggest disappointments was with the EEEG project, which never sent participants to the OGSA-Authz working group meetings, and when invited to participate in the standardisation work and be a joint editor in the protocol specifications, they refused the offer. Instead they did their own thing in their project, wrote their own internal protocol profiles, and then shortly before the OGSA-Authz specifications were due to go out for public comment, they tried to halt the process in order to not invalidate their in-house specifications through the availability of OGF standards. Fortunately they did not succeed in stopping the process, and they did provide a significant set of comments on [3] which have been addressed in a revised version of [3]. However it was not possible to perform any interworking tests with the EGEE project.

## Conclusions

Standardisation work is long and hard, time consuming and sometime tedious. Its benefits to end users are obvious, but it is not obvious if the cost/benefit ratio is sufficiently positive to researchers for them to consider it worthwhile to participate in their production. Indeed, it would appear from this project that many researchers do not consider it worthwhile to participate.

## Implications

It is no good one country or one organisation funding standardisation work. It needs to be a global effort, with multiple countries funding multiple organisations to participate in the same standardisation effort at the same time. In the previous project we were lucky that JISC funded Kent at the same time as the NSF funded the Globus team, and so the specification, implementation and testing of [1] went relatively smoothly. But in the current project there was a significant period of time when Kent was the only organisation funded to do this work and the only organisation driving the standards in the OGSA-Authz working group. Consequently there were not the synergies available to drive the work forward at a reasonable pace, and this project had to be nearly doubled in timescale. At its close, the work was still not fully completed, in terms of having OGF standards published.

## Recommendations

1. The work that still needs to be done in order to ensure that the 3 documents can be published as OGF standard profiles is as follows:

Project Acronym:  
Version:  
Contact:  
Date:

- a. Get international consensus from the OGSA-Authz working group as to how all the public comments should be resolved;
  - b. Produce revised versions of the 3 protocol specifications;
  - c. Submit the revised versions to the OGF editor for either GFSG final review or a second public review, depending upon the extent of the changes. If the latter then repeat from step 1a. again
2. Enhance the PERMIS implementation to conform to the final versions of the OGF standards.
  3. As a general recommendation to JISC, it is proposed that JISC does not fund standardisation work unless it is known that other international groups have similar funding to participate in the work. It is appreciated that this can be logistically difficult to achieve, but nevertheless, without international cooperation and participation, any such standardisation work is bound to be slow, and reaching international consensus is bound to be time consuming and difficult, as this project has adequately shown.

## References

- [1] Von Welch, Rachana Ananthkrishnan, Frank Siebenlist, David Chadwick, Sam Meder, Laura Pearlman. "Use of SAML for OGSi Authorization", GFD.66. March 2006,
- [2] David Chadwick, Linying Su. "Use of WS-TRUST and SAML to access a CVS". OGF OGSA-Authz WG draft, 18 September 2008
- [3] David Chadwick, Linying Su, Romain Laborde. "Use of XACML Request Context to access a PDP", OGF Authz WG Draft, 14 September 2008
- [4] V. Venturi, T. Scavo, D.W. Chadwick, "Use of SAML to retrieve Authorization Credentials", 7 April 2008
- [5] David Chadwick. "Functional Components of Grid Service Provider Authorisation Service Middleware", OGF OGSA-Authz WG draft, 6 April 2008.
- [6] OASIS, "WS-Trust 1.3", OASIS Standard, 19 March 2007
- [7] OASIS "eXtensible Access Control Markup Language (XACML)" v2.0, 6 Dec 2004, available from [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)
- [8] OASIS. "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005