

## JISC e-Infrastructure Programme Project Document Cover Sheet Final Report

<b>Project Acronym</b>	CUCKOO Project	<b>Project ID</b>	
<b>Project Title</b>	Cardiff University Collaboration with KC-ROLO Organisational Objects		
<b>Start Date</b>	1 <sup>st</sup> April 2007	<b>End Date</b>	31 <sup>st</sup> March 2009
<b>Lead Institution</b>	Cardiff University		
<b>Project Director</b>	Ms Joan Wright		
<b>Project Manager &amp; contact details</b>	Graham Mason. Head of ICT, Kidderminster College. Market Street. Kidderminster. DY10 1LX. Tel 01562 512053 m: 07974351212		
<b>Partner Institutions</b>	Cardiff University, Kidderminster College		
<b>Project Web URL</b>	www.kidderminster.ac.uk/cuckoo		
<b>Programme Name (and number)</b>	e-Infrastructure VO Tools		
<b>Programme Manager</b>	James Farnhill & Chris Brown		

<b>Document Title</b>	Final Report		
<b>Reporting Period</b>	1 April 2007 to 31 March 2009		
<b>Author(s) &amp; project role</b>	Graham Mason, Project Manager; Ed Beddows Lead Developer; Joan Wright Project Director		
<b>Date</b>	March 2009	<b>Filename</b>	Cuckoofinalreport.doc
<b>URL</b>			
<b>Access</b>	Project, JISC General Dissemination		

<b>Version</b>	<b>Date</b>	<b>Comments</b>
0.1	03 March 2009	Draft text completed by GM & EB
0.2	13 March 2009	Amended at Project Executive
0.3	25 March 2009	JMW amendments
0.4	30 March 2009	GM & EB updates
1.0	31 March 2009	For submission to JISC
1.1	30 April 2009	Amended after JISC comments

Project Acronym: CUCKOO  
Version: 1.1  
Contact: Graham Mason  
Date: 30 April 2009

# CUCKOO Project

**Cardiff University Collaboration with KC-ROLO  
Organisational Objects**

## Final Report



**Joan Wright**  
Project Director

**Graham Mason**  
Project Manager



**JISC**

Contact:  
Graham Mason ([gmason@kidderminster.ac.uk](mailto:gmason@kidderminster.ac.uk))

## Table of Contents

### Contents

JISC e-Infrastructure Programme .....	1
Acknowledgements .....	4
Executive Summary .....	5
Background .....	6
Aims and Objectives .....	6
Methodology .....	7
Implementation .....	7
Outputs and Results .....	12
Outcomes and conclusions.....	15
Recommendations .....	17
References.....	17

## Acknowledgements

The CUCKOO Project was funded by The Joint Information Systems Committee (JISC) and was undertaken as part of the e-Infrastructure Programme focusing on researching, implementing and demonstrating Shibboleth Virtual Organisations (VO's) and on-line collaboration tools.

The Project was led by Ms Joan Wright Cardiff University (Project Director), Graham Mason (Project Manager) Edward Beddows, Rhys Smith (Engineering Consultant: Identity & Access Management), Anthony Williams and Andy Morris (Consultant). In the second year of the project, Rob Hebron (Identity Management consultant) contributed to the project.

The CUCKOO team would also like to thank the project sponsors and stakeholders for their advice, opinions and feedback. Thanks are also due to the colleagues at both Cardiff University and Kidderminster College who supported the project infrastructure and test environments.

FE Colleges in the initial stages Worcester Tech, Kidderminster and Shrewsbury  
RSC West Midlands: Jim Judges & Andy Morris

Assistance from the following individuals was also appreciated:

Brown University: James Cramton  
University of Chicago: Tom Barton  
Duke University: Klara Jelinkova  
SWITCH: Thomas Lenggenhager  
University of Newcastle GFIVO project: Caleb Racy  
University of Bristol: Gary Brown

## Executive Summary

The Cuckoo Project, which was funded as part of the "e-Infrastructure Programme", ran from 1<sup>st</sup> April 2007 until 31<sup>st</sup> March 2009 and had the following key aims:

- Research, implement and demonstrate Shibboleth Virtual Organisations (VO's) and on-line collaboration tools.
- Research into how Shibboleth 2.0 will affect these tools and solutions.

The project started with a survey of current Virtual Organisational tools and their use within the UK academic sector and elsewhere. The project decided to concentrate on the Internet2 tools, Grouper for group management and Signet for privilege management.

There is a good Grouper community, it has been in development since 2001 so has had a lot of input from institutions and individuals; because of this work, Grouper is fit for production level use. Research in the USA led us to James Cramton (Brown University), Tom Barton (University of Chicago) and Klara Jelinkova (Duke University), all doing work with "Grouper" within their institutions. Here in the UK, Gary Brown (University of Bristol) was leading Grouper within his University, with wider participation in the Grouper developments happening in the USA. We were also in contact with the [GFIVO](#) (Grouper to support Federated Identity for Virtual Organizations) project at Newcastle.

Signet was a less mature tool and our assessment was that it was less likely to be adopted by the community without considerable development. In October 2008, Internet2 ceased development and support of Signet. However there is a need for a privilege management tool to fill the gap and some institutions/projects are developing their own, such as [perMIT](#) from the Massachusetts Institute of Technology, and the [FLAME](#) (Federated Local Access Management Environment) Project at the LSE.

Kidderminster College, who had a particular interest in privilege management, built a Grouper and Signet demonstrator but, because of the limitations of Signet, did not bring this into production. A survey also suggested that for FE institutions, with a relatively small number of applications to manage, the overheads of these tools in terms of complexity would outweigh the benefit. The development of a Windows Installer and a guide and wizards to assist configuration would encourage the take-up of Grouper.

Cardiff University had a large number of applications and the requirement for a very large number of groups. Cardiff decided to adopt Grouper as its group management tool. The need for real-time provisioning of LDAP groups was fed back to the Grouper project. This was addressed in Grouper version 1.4 which provided "event hooks". Development work was undertaken at Cardiff to integrate it into the Identity Management system and, through code external to Grouper, to provide additional functionality. Cardiff also developed their own simplified UI, using the Grouper API, and this will be contributed to the Grouper project.

In an organisation with complex requirements, group management requires policies and procedures to be defined. Cardiff has set up a small Group Management Team, comprising Identity Management and MIS staff. Their role is to define the group hierarchy and prevent duplication of groups, to maintain comprehensive group descriptions using a consistent business vocabulary, to guide application owners on the definition of groups and to keep a register of applications which use groups.

During the second year of the project we also concentrated on Shibboleth 2.0. The benefits were demonstrated via a 2 day Project led Shibboleth 2 Install fest (funded by JISC) in Birmingham (Aston University) with Chad La Joie, Rhys Smith and Ed Beddows presenting. The materials are available to the wider community on the project website under the [documents section](#).

## Background

Core middleware services such as identity management, directory, and authentication provide a foundation for secure, manageable applications throughout an institution/federation. Members could belong to more than one real organisation; such as Foundation Degree students within the HE-FE environment, who would move in and out of the federated structure. Wishing to share resources across these HE-FE institutional boundaries often raises problematic security difficulties as VO membership may be more (or indeed less formal) in a HE-FE environment.

Federated access tools such as Shibboleth enable VO members to gain access to a resource using their home credentials. Cardiff University and Kidderminster College have been very active over the past three years in Shibboleth development and research.

Kidderminster College have been using Shibboleth software to allow single sign on into their applications for a number of years. Whilst this solution has solved the problem of users having to remember multiple passwords, it has not addressed the problem of centralised and delegated role and privilege management. Having this feature would allow an institution to free up application management time by providing a central place to make modifications to role and privilege modifications, instead of in every unique application.

Cardiff University has a mature Identity Management (IDM) system which is used to provision and manage user accounts. The recent introduction of a portal and development of Business Process Management created a need to manage a potentially very large number of groups and to integrate their management with the IDM system. During the course of the project, Cardiff decided to use Grouper for this.

## Aims and Objectives

The aim of the project was to research, implement and demonstrate Shibboleth Virtual Organisations (VO's) and on-line collaboration tools. The project wanted to build on and incorporate work already done with Shibboleth and Identity Management systems. The project had a number of objectives that would feedback into the HE & FE communities in the form of reports, lessons learnt and demonstrators.

- Review VO tools and concepts in place by other projects and catalogue the relevant data and findings of these projects
- Review the selection of Virtual Organisation Tools with particular emphasis on Grouper and Signet
- Highlight the difficult problems of tool selection
- Investigate the management of permission and access control in a HE-FE environment
- Create a demonstrator for JISC related events and documentation

Whilst most of the objectives remained largely unchanged, developments in technology over the two years of the project led to some changes in focus.

- After the initial discovery phase, we did not continue to investigate the ShARPE and MyVOCS projects as these did not focus on the VO tools we were researching. However data gained from these projects gave us a better understanding on real world VOs.
- The release of Shibboleth 2 did not affect the VO tools.

- Our initial assessment of Signet was that it was less likely to be adopted in the community than Grouper. This was reinforced when Internet2 ceased development and support of Signet in October of 2008.
- It proved difficult to encourage take-up of the tools in FE. However, Cardiff took the decision in 2008 to use Grouper for their group management solution. The emphasis of the project then moved to this production implementation in an HE institution.

## Methodology

The Research phase was mainly carried out online whereby we reviewed and collated past and present (JISC or other countries) related project reports or papers.

We also surveyed FE institutions within the West Midland area by a questionnaire. Previous Cardiff experience in the Identity Project showed that large surveys sent by email to FE institutions produce negligible response. The Cuckoo project kept the [questionnaire](#) very short. It was administered at one of the RSC regional events after a presentation which introduced the audience to the selection of tools available. This method we found beneficial as it gauged the audiences opinion during the meeting. However the representatives were IT staff. We have found that during some of our other JISC projects that we have been running parallel to this project, namely the FEAIMS & PAMS project, site visits and presenting to a wider audience (SMT, Librarians, IT and ILT) have been beneficial as you get a wider selection of institutional staff available, unlike a conference where normally only one or two staff would be released to attend.

Having selected the VO Tools that we would use throughout the life of the project, (namely "Grouper" & "Signet"), we built demonstrators of each separately as a proof of concept and then linked them together. Kidderminster took the decision that this did not provide a suitable solution for their requirements, due to the fact that the work required to set it up outweighed the benefits, Kidderminster already have most groups automatically created so the system would only benefit a very small number of ad hoc groups, it was felt this small number were better controlled in the small number of applications we have. Cardiff decided to adopt Grouper, but not Signet, and bring it into production

The technical research into Shibboleth 2 was made available to the community via an "install fest" training event run by JISC.

## Implementation

The project was managed by an "Executive Group" which met (in accordance with the Project Plan) either at Cardiff or Kidderminster

## Research phase

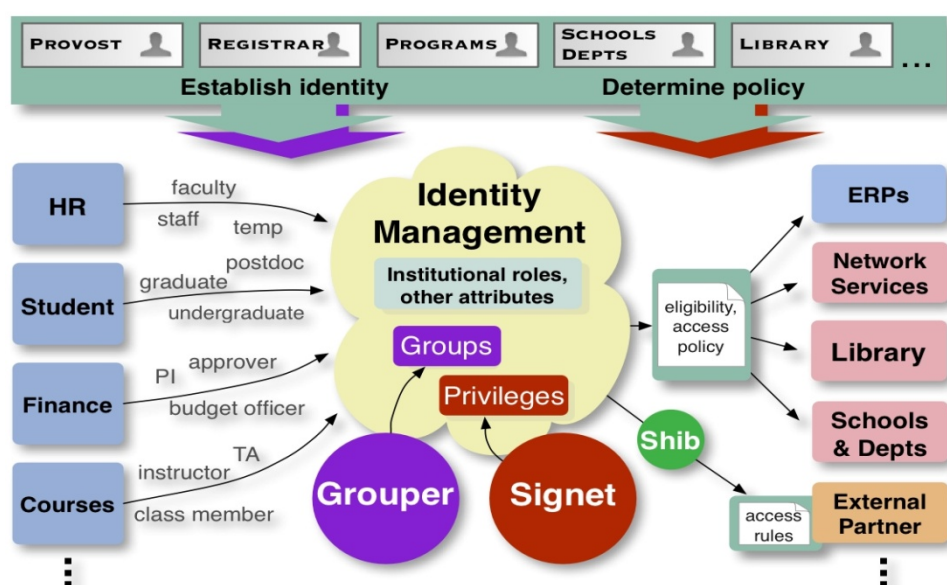
In the initial research stage, we wanted to build a picture of how organisations in differing sectors (UK or elsewhere) were using Virtual Organisations. This research was taken over a two month period concluding in a nine page research finding report which can be found on the project website.

To summarise the report, over 12 (quite recent) projects were researched relating to the research criteria we were interested in. Some projects gave us a more general view of VO's and not much information on VO Tools (although these projects gave us a better understanding of virtual organisations). Whilst other projects honed in on VO Tools and explained the contextual relationship they had within the organisation or research project. Highlighting this were two projects, namely: Tom Barton (University of Chicago), who gave an overview of VO Tools (Grouper & Signet) and how they can be integrated within an environment and James Cramton of (Brown University), presenting "Group Management", a view of Grouper within the IT systems at Brown University.

James and Tom were very helpful in our research into VO Tools and we contacted them for more information. Correspondence with Tom and James was via email or Skype and James kindly

presented via Skype (and webcam) during one of our executive meetings. His presentation is on the project website.

The next phase was to get a more in-depth knowledge of the tools we were going to use. At this stage we had decided to research Grouper and Signet as they appeared to be the most relevant to our requirements. Grouper development is led by Tom Barton and Blair Christensen at the University of Chicago. Tom Barton is Senior Director for Integration at the University of Chicago and is one of the lead MACE/Internet2 personnel working on the Grouper project. Signet development was lead by David Donnelly of Stanford University. The following diagram shows how Grouper and Signet can be integrated into an institution's existing identity management system to help with group and privilege management.



*Diagram showing how Grouper and Signet fit into an existing Identity Management System.  
 Source: Tom Barton, Chicago University*

Research correspondence with other projects that have been or are actively involved in Grouper and Signet within the UK has been particularly useful. We have been in touch with Caleb Racey from the University of Newcastle, Gary Brown (University of Bristol, in conjunction with U-Portal) and LSE with the FLAME project. Caleb Racey from the University of Newcastle uses Grouper with the Sympa mail list application. He is the project manager for the "GFIVO Project" whose aim is to develop a Grouper group management infrastructure to promote the formation, management of research based Virtual Organisations. We invited Caleb to one of our Executive Group meetings in which he presented a good overview of Grouper.

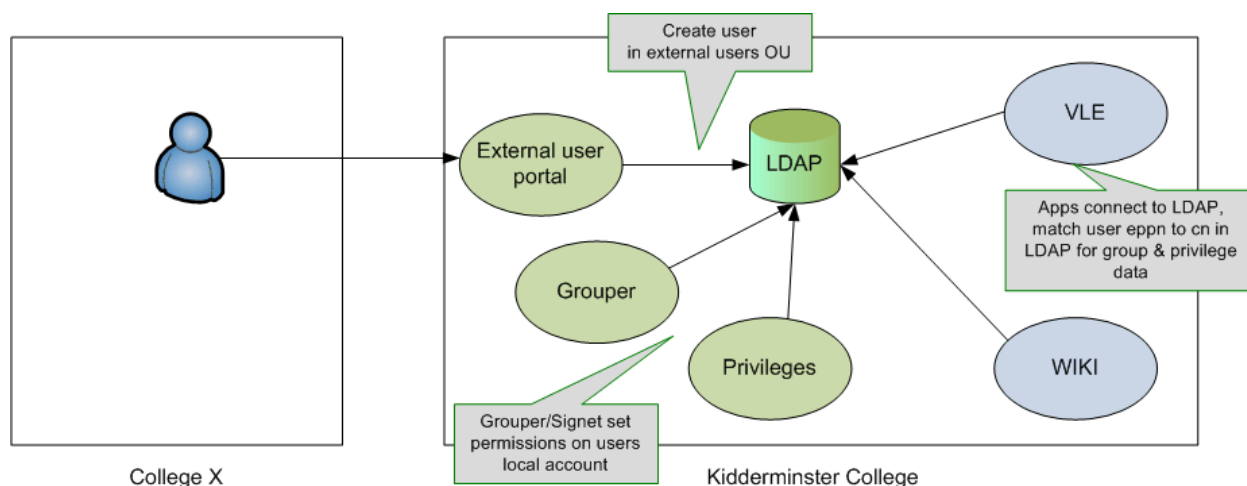
Correspondence and keeping up-to-date in what's happening in the Grouper and Signet communities has been helped by joining the Grouper & Signet mailing lists, which are very active. Klara Jelinkova (Duke University) has within her organisation been using Grouper for a number of years and helped with comments regarding Grouper's upgrade problems. James Cramton (Brown University) knows Grouper very well and was a good contact in the beginning of this research phase. His in-depth knowledge comes from his rollout of Grouper throughout his institution.

Project research into our neighbours in Europe did not get very far beyond the occasional email to a project contact in SWITCH. This was due in part to our key contact being unavailable through illness. SWITCH have developed their own Group Management Tool (GMT). Whilst this tool looked appealing at first, it became clear early on that it didn't provide group management for a central database of users (e.g. our LDAP server), but in fact creates groups in its own database, outputting .htaccess or Shibboleth XML access files. This solution would not suit our needs so was not looked at any further.

Functionality within the institution would play an important part. We conducted a survey within our West Midland RSC regional event (see questionnaire feedback on the Project Website).

## Grouper and Signet at Kidderminster

Kidderminster's goal was to test the viability of using Grouper and Signet to provision our Virtual Learning Environment (which consists of multiple Moodle's), a repository and a Wiki.



*Diagram of potential use of Grouper and Signet as a VO.*

We pointed Grouper to our Active Directory ([see report](#)) which would allow us to pull out all our staff and students via LDAP. This was relatively easy to do by looking at existing examples on the Grouper Wiki and other sites. We manually added a small number of test accounts into test groups using the Grouper UI. For proof of concept we created a simple scenario with 10 groups, each group representing a real course. These groups were created through the Grouper UI. For a real world scenario where hundreds or thousands of groups are present this would either be done through the API or directly into the grouper database.

Signet installation phase followed the Grouper install. We were looking to Signet to provide us with a central way to administer user privileges across all of our applications. In most cases this would be provisioning the user's eduPersonEntitlement attribute with the necessary privileges. As with Grouper, Signet provides us with the ability to delegate these tasks.

Signet was a less developed tool than Grouper and harder to install. However, the setup time of Signet was reduced due to the fact that some pre-requisites were installed as part of the Grouper installation.

As with Grouper, Signet pulls users from Active Directory (AD), and provisions it back into AD once permission information has been entered for users. Later on in the project we investigated Signet feeds directly from Grouper ([see report](#)). Due to the model of Moodle that we have running, we see these granular permissions as more suitable than those of group information, as they allow more control over what the user can do. As our AD is provisioned nightly from our MIS database, eduPersonEntitlement is already in place for our users. However with Signet set up these permissions would no longer be bound to the static permissions obtained from our MIS database giving us the ability to allow tutors or project leaders to delegate these permissions to users. This would reduce the burden on IT staff that are best placed doing administration at a lower level and do not know what groups users should be in.

Once both tools had been configured and tested independently of each other we began work on getting Signet feeding subject data from Grouper. After initial problems with configuring Signet to link with Grouper, further issues in Signet affected the viability of this solution in a production environment ([see report](#)). It was clear at this point Signet could not provide us with the necessary functionality to feed our users privilege data without a lot of design and development work.

It also became apparent during our Grouper research within the FE community and the survey finding, the consulted FE community felt that Grouper was only appealing to institutions that have lots of resources or applications to protect. Managing these resources and ownership was also seen as an issue - the more permission rules, the more administrative overhead.

Collaboration between the Learning Resource Centre (LRC), Information and Communication Technology Services (ICT) and Information Learning Technologists (ILT) may be lacking in some Further Education establishments. For example in the case of Kidderminster, ICT Services maintain control over the College IT infrastructure. This is not limited to network administration (users permission, Active Directory and attributes), but includes software (Federated content) and various associated task such as IT Security. The LRC have very little control over their users and resource/groups which have to be passed to ICT Services to be installed and allocated to the various users (the more groups the more administrative overhead). The LRC have no real way of giving permissions or setting-up applications for their target audience. We felt Grouper would be appealing to LRC's as it could give them some group control over their users accessing resources. Another appealing factor is that Grouper UI allows scalability for group's such as Power users, Librarians and administrators to access controlled applications. However feedback from the FE community found that small institutions or institutions with few resources (this was the case with Kidderminster) viewed that managing resources at a single point of access would be seen as an overhead and therefore would opt to directly manage the resource. For example to use a comment from our Survey *"Most institutions viewed the tools as a LDAP provisioning tool and felt that their ICT Services would manage resources via their Active Directory or the resources itself directly (such as Moodle). Although this approach would lose the group delegation functionality that is found in grouper"*.

With this in mind we felt it more beneficial that Grouper development was carried out at Cardiff University, with a view to implement it fully in a production environment.

## **Grouper at Cardiff**

Cardiff University identified the need for a potentially large number of groups for use by a wide variety of applications including IBM Websphere Portal, Collaboration Tools (Domino email service, blogs, wikis, social networking) and Business Process Management.

Three types of groups were required in both LDAP and the Domino email system:

- DA (Data Authority) groups = Centrally provisioned groups where data authorities, such as staff and student records, determine group membership. An example of such a group would be 'All staff in Biosciences'.

Because many University users have multiple roles, there was also the requirement to hold and implement variations to the rules which provision DA groups so that a user may be excluded from a group to which they would normally be provision and *vice versa*. For example, a member of staff in the Medical School might collaborate closely with Biosciences and need to be treated as a member of the 'All staff in Biosciences' group as well as 'All staff in Medicine'

- Ad Hoc groups = Centrally provisioned groups where the creation of the group and its membership are managed through a simple user interface. An example of such a group would be 'Staff who manage research grants'
- Application-only groups = Ad-hoc groups defined and managed within a specific application and not synchronised outside that application. An example of such a group would be a mailing list shared by only a small number of people. This type of group is not addressed in this report.

The users, both internal and external, who can be in groups are managed by Cardiff's IDM system. The IDM Rules and Routing Engine holds and applies the business rules and should also manage the rules for DA groups. A group management database was required to hold the variations for the DA groups and to hold the Ad-Hoc groups. A simple user interface was required to manage these.

In mid 2008, Cardiff evaluated Grouper version 1.3 which provided both a Group Management Database (GMD) and a Group Management Interface (GMI) and could be integrated with the IDM through the Grouper API. It was recognised that customisations would be required but these would be kept to a minimum.

- It was desirable that no changes should be made to Grouper Database or to the API
- Grouper 1.3 did not meet the requirement to provide outgoing real-time links to populate groups in LDAP and Domino directories. It was considered that triggers and log tables would need to be added to the database to achieve this, which would represent a change to the Grouper database. This was fed back to the Grouper developers. Grouper 1.4 provides event hooks which make it possible to invoke code to push a change out in real time. Grouper 1.4 was selected for use in Cardiff University
- The need to apply variations to DA groups is not directly available in Grouper. Instead we adapted "opt-in" and "opt-out" rights over groups to serve this purpose. The logic to calculate effective membership of DA groups is enclosed in code external to Grouper.
- Although the Grouper Web UI was initially seen as a strength of the product, further assessment raised concerns regarding the usability of the interface for both administrative staff and for end users. It was concluded that the level of customisation required to address these concerns meant that it would be more time and cost effective to develop an alternative UI in-house using the Grouper API.
- Cardiff has invested heavily in the WebSphere Portal, and it is considered highly desirable for web interfaces to be compatible with the environment. While it is possible simply to present a web application in an iFrame, it is more desirable to develop (or wrap) it as a JSR 168 Portlet, or make it accessible through Web Services for Remote Portlets (WSRRP). It was considered that either would be difficult to do with the existing Grouper UI. This requirement supported the decision to develop a UI in-house.

During the development of the prototype, it was found that there was a limit on the number of group members in Domino. Investigation of this delayed the project. It was decided that this work was lower priority than the provisioning of LDAP groups and to develop the prototype for LDAP groups only. Once this is complete, it is planned to introduce a subgroup layer that synchronises to Domino, although this may require arbitrary subgroups which are not meaningful to users.

The prototype system was completed in February 2009 and used to provision a small number of LDAP groups. In March a fuller-featured UI was developed in response to feedback. The focus now is on bringing the service to full production status and the policy and administrative arrangements for managing a large number of groups.

## **Shibboleth 2.0**

We also investigated Shibboleth 2.0 and explored its use alongside Grouper and Signet. Going to the install fest in America, enabling us to see the developers face to face, allowed us to update our understanding and documentation on Shibboleth 2.0.

Implementation of Shibboleth 2, i.e. installing and providing feedback to the Internet2 community, went well and the implementation guides produced by ourselves Internet2 and customised by ourselves were very useful for the community.

The best way we found for disseminating this knowledge was running a two day hands on workshop, the "install fest", inviting members of the community who have existing experience in the field to install the new software on their own virtual machine. Whilst there were a few technical issues at this event our goal of giving the community practical knowledge of Shibboleth 2 was fulfilled, giving all delegates useful examples that they could take away and implement. This event was organised and sponsored by JISC. The materials are available on the project website.

During this second phase Kidderminster College also upgraded their Identity Provider to Shibboleth 2.0 to help with the understanding of the software, and to aid us in our Grouper/Shibboleth 2 testing. The reasoning behind testing Grouper again with Shibboleth 2 was to see if SAML 2 could bring anything new to the table in terms of functionality.

We did not test Signet at this stage of the project as Signet development had been stopped and its relationship with Shibboleth 2 was not affected.

The last part of the project saw Cardiff continuing with the Grouper institutional rollout and development and Kidderminster finalising its Grouper and Signet demonstrators.

## Outputs and Results

The project reports are available at <http://www.kidderminster/cuckoo/documents.htm>.

At the start of the project we had identified two main tools for providing VO user management, these were Grouper and Signet. Like us, the FLAME project also thought of Grouper and Signet first when looking at Delegated Authority Management: "For DAM, the front runner is the combination of Signet with Grouper, both Internet2 tools designed to work with Shibboleth" (<https://gabriel.lse.ac.uk/twiki/bin/view/Projects/Flame/TaskT1>).

### Grouper

Grouper consists of a repository of data about groups and members of those groups, and an API to interact with the repository. In addition, a "Grouper shell", a web interface and web services interface are available. All of these use the Grouper API to interact with the repository. Data regarding the "subjects" who can be members of groups can be obtained through an interface to an LDAP directory or JDBC database. Groups and their memberships can be accessed through the API or exported using the Grouper Shell.

The following is a compilation of the known weaknesses found in Grouper by the CUCKOO and FLAME projects:

- Grouper will not use a combination of groups it does not manage (e.g. department information obtained from non-group attributes in the LDAP server) and groups it does manage
- Awkward user interface
  - Functionality considered vital by administrative users (such as bulk search and add operations, or copying of groups) was not obviously available.
  - End users generally require simpler workflows, with fewer options than administrative users
  - The need to add groups and subjects to a workspace before they could be managed was considered confusing.
- Some subjects need to be excluded from groups to which they would normally be provisioned as a member (and vice versa). This should be visible to administrators in the UI and so should be stored in the Grouper Database rather than externally. This requirement is not directly available within Grouper.

The FLAME project abandoned Grouper and Signet, at least for the short term (their reasons are listed among those in the issues above) to "develop an in house lightweight product". The key here is "lightweight", Grouper is by no means a lightweight solution, designed to fit into almost any infrastructure and plug into its existing systems; it's no surprise it does not just drop in and go.

Grouper does have a promising future thanks to its active community. Numerous features that were lacking have recently been implemented that will make Grouper more viable for production use, namely:

- Modifications to import/export tool make it easier to invoke
- Event hooks within Grouper make it possible to invoke code to (for example) push a change out in real time.
- Web Services
- User interface enhancements

This recent development work highlights that there is significant interest in Grouper as a solution for delegating group management, so an institution can be fairly sure if they choose Grouper that it will not go down the road that Signet recently has.

Cardiff University made the decision to implement Grouper to provision internal and external users into their correct groups. The following decisions were made regarding the rollout of Grouper at Cardiff:

- Grouper 1.4 would be used in the deployment of a group management solution in Cardiff University.
- The Grouper database and API would be used with minimal customisation. Customisation would be limited to attaching code onto event hooks within Grouper. This code would interface with the existing Identity Management system.
- The Grouper Web Service would not be used initially, but will be considered at a later stage.
- The Grouper API would be used to enable the existing Identity Management system to interface with Grouper.

Cardiff University have also developed a separate in house user interface to address the previously mentioned issues in this area.

- The main goal of this is to simplify the terminology and layout of the user interface
- The GFIVO project team have gone down a similar route, creating their own custom interfaces, including a vastly simplified interface for end users.
- This is clearly an area that is highlighted by many as a weakness, and as such is receiving a lot of attention by the community.
- Further enhancements/customisations by the likes of Cardiff University will be fed back to the community, making this tool an even more attractive solution in the future.

The roadmap for Grouper shows that version 1.5 (the next iteration of Grouper) will have Role & Privilege Management. The roadmap states "This is a placeholder for whatever initial implementation of grouper's support for Role and/or Privilege Management as may be decided upon". Mailing list discussions suggest this will not be as powerful as Signet; it will only provide a subset of its features. However, this subset could be enough privilege functionality for some institutions. Having Grouper take care of this instead of a separate application could speed up implementation time considerably.

Our main Grouper demonstrator is Cardiff University's implementation. This [report](#) on the project website highlights how Cardiff has integrated Grouper with their existing identity management solution. The project website also contains the [presentation](#) we made which explains the Kidderminster test Grouper/Signet/Shibboleth setup.

## Signet

Signet is a permissions control tool, but with a different emphasis compared to Grouper. Signet seeks to map permissions that are defined in a store such as Grouper. For example membership of one group may represent read permission over student records and write permission over an application such as a Wiki. Signet is intended to make it easier to map application specific permissions to facts about users' accounts, such as group membership. As part of this project we wanted to investigate whether Signet could provide a viable solution for FE and HE institutions.

- The Signet user interface as distributed is intended only as a demo and would need to be comprehensively rewritten to work with live data
- Signet cannot resolve group permissions to calculate individual user permissions (i.e. if a group is given a particular permission, the permission will not be extended to members of the group)
- Provisioning LDAP from Signet is in early phase of evaluation and was not possible until August 2008.
- Signet is no longer an active product.

As with Grouper, the usefulness of Signet would be greater as the number of applications you wish to protect increases. Some institutions may find Signet unnecessary, for example institutions that protect all their resources with groups. On the other hand, some institutions may find privilege management more useful than group management. Kidderminster College are an example of this; due to the way our identity management and VLE are setup, we thought Signet would be more useful for us. Groups are already taken care of in terms of courses students are on - when a student joins the college they are put in the correct group, this gets updated every night to ensure this is correct - so Grouper would only be useful for the ad hoc groups. Privilege management however, with its ability to provision the entitlements of users, is immediately useful to us. However due to the issues discussed in this document, Signet is not the tool to provide this.

Implementation of Grouper and Signet together encountered technical issues at various stages of the setup. Grouper installation went relatively well, Signet however caused a number of issues as mentioned. It became clear early on that Signet is not as developed as Grouper, which is no surprise as its user base is a lot smaller and there are no known production implementations.

Signet development has now ceased. Integration was hard with Signet, and never fully documented, which did not help Signet's uptake. If it were easy to bolt onto Grouper then its uptake would have been much greater due to the relatively large number of Grouper implementations. Part of Grouper's success may be down to the fact that institutions are already using groups in LDAP. Grouper therefore helped immediately with this by offering a better way to manage groups. It seems the community doesn't yet have a common idea on how to do privileges. In the end, Signet's demise came down to the fact that it didn't meet the needs of the community.

Since Signet's demise, the MACE-paccman (Privilege and Access Management) Working Group has been created with the intention to tackle issues of privilege and access management <https://spaces.internet2.edu/display/macepaccman/Home>. One possible outcome of this may be an alternative tool to Signet. Another possible replacement for Signet may be [perMIT](#), which is Massachusetts Institute of Technology's open source roles database. It has been in use for over 10 years. A project is underway at MIT to do a direct translation of the existing system into open source tools.

The COmanage suite of tools (Grouper + Signet) has now dropped Signet for its privilege management functionality; the project is currently running without this tool, using just Shibboleth and Grouper. The project website suggests they will be filling this gap shortly.

## **Shibboleth 2 with Grouper/Signet**

Tools to help manage Virtual Organisations interact with federated access in one main way – people can gain access to a resource used by the VO (for example, a wiki) using Shibboleth as a means of enabling federated access to that resource; these tools can then be used to manage these federated users. For example, the “Grouper” tool could be used to automatically place such users into different groups dependent on the attributes asserted about each user, and each group could then be given different access rights. Thus, the use of Shibboleth in these circumstances is to simply enable federated authentication to a particular resource, and the passing of attribute information to such VO management tools in order that they can make further use of various kinds of this information.

The fundamental principals between Shibboleth 1.x and 2.x remain unaltered; the difference is largely a technical one. Since Shibboleth is only used in the context of VOs as a method of enabling federated authentication and the passing of attribute information, and these fundamentals have not

changed between versions, then generally, the use of Shibboleth 2.x instead of Shibboleth 1.x does not affect tools that manage Virtual Organisations in any discernible major manner, either strategic or technical.

There is, however, a small positive effect in that given the increased flexibility of the Shibboleth 2.0 software – in terms of the fact that it can now “talk” multiple security languages (at least SAML 1.1 and SAML 2.0 to begin with) – then there is more potential for the organisations that constitute the virtual organisation to technically interact, no matter which software they themselves happen to be using.

Shibboleth 2 demonstrators are available on the project web site <http://www.kidderminster.ac.uk/cuckoo/documents.htm>. Kidderminster's production Shibboleth 2 IdP also serves as a demonstrator in dissemination events when explaining the technology.

## Outcomes and conclusions

When deciding whether or not to use Grouper, an institution needs to consider.

- Can your applications query group membership from a central store (LDAP or a database) and make use of this information?

Typical uses of group membership are for authorisation (e.g. access to a wiki, a portlet, course module with a VLE) or for role-based decisions (e.g within a business process, a service desk or a mailing list).

Applications that do not use group membership would require modification to benefit from Grouper. This may require significant effort, or be impossible, especially for commercial applications.

- How many applications which can query group membership do you have?

The benefits of having Grouper in an organisation are increased by the number of applications it serves. If you have only one application then having Grouper may not be of any benefit, as you could more easily use the application's internal user management

- Do you want to delegate group management (creation of groups and/or the assignment of users to groups) to non-IT staff such as teachers, librarians or administrators?

The Grouper user interface and API is specifically targeted at managing groups and may be more suitable for non-IT users than the built-in LDAP or database utilities, which manage a wider range of object classes. Both Cardiff and the GFIVO project have developed their own, more simplified, interface for such users. Grouper can also be used for end-user self-subscription to groups but the Cardiff implementation has not yet addressed this.

- Do your applications use groups held in many different stores?

Grouper can help by consolidating these into a central store, such as LDAP, and synchronising between the different stores, provided that there is a common definition of groups and their membership. Considerable effort could be required to import and export data, depending upon the APIs available.

- Do you have a central store of users?

A highly-devolved institution may have different directories for each college or department. A Grouper implementation would require extra effort to handle these.

- Do you need to hold group membership on users that are not in your directories?

An LDAP group can only contain users that are in that LDAP directory. Grouper can hold

membership information on external users provided there is a mechanism to import them into the user store that Grouper is configured to use.

Institutions with a small number of resources, or resources which are already centralised (for example they all use LDAP, and LDAP groups are provisioned via an IDM solution already) may find Grouper unnecessary, and actually increase administrative overhead. We feel there is room for a simplified tool in these circumstances, for example a simple web interface to allow users to connect straight to the LDAP server itself (whilst still providing limited delegation), as we feel the learning curve for Grouper is quite high for most FE institutions. This high learning curve can be justified by the fact that it has been written to operate in a heterogeneous environment where applications and user information may be stored in many different ways.

Cardiff has implemented a group management system which is in the process of entering full production. This was not part of the original objectives of the project. Cardiff's decision to use Grouper indicates that it is a useful tool for organisations with complex requirements. It has been possible to integrate it into the existing IDM infrastructure. This has meant that it is useful in a wider range of cases than if it were used as a stand-alone tool.

Cardiff had a mature IDM system and technical expertise in essential infrastructure such as Apache and Tomcat. For an institution without these skills, the development of a Grouper Installer would be desirable.

Technical implementation would be considerably easier if there were a guide to customising the configuration files. This would encourage take-up of Grouper.

Cardiff will make its simplified UI available to the Grouper project and also their use of event hooks to send data to other systems in real time.

We are keen to identify suitable dissemination events at which to present on the Cardiff implementation.

An organisation with complex group requirements needs to address not just technical but policy and administrative requirements. Cardiff has recognised the need for a small Group Management Team:

- To design the name hierarchy and ensure consistency in naming of groups.
- To prevent duplication of groups
- To ensure customers understand the exact meaning of DA groups. This requires an understanding of corporate data and the business rules and is best done by IDM or MIS staff.
- To ensure that comprehensive Descriptions of groups are maintained and use a consistent business vocabulary.
- To keep a record of the purposes for which groups are created and a register of other applications which use these groups. This requires the co-operation of IT staff in academic departments who write applications which use the LDAP service.
- To manage deletion of groups.

## Recommendations

- There is a need for a lightweight alternative to Grouper, this would be particularly useful for deployments in FE colleges where IT teams are smaller and sometimes less specialised. Funding for development of such a tool would be useful for the community. This development could leverage work on the in house alternatives that projects such as FLAME or perMIT are producing.
- As Grouper configuration is not particularly well documented or intuitive, we feel JISC funding could be used to improve this. A quick start guide would be useful, as well as configuration templates generated by “wizards”. Investment in making Grouper easier to configure could be a substitute to developing a lightweight alternative to Grouper. Researching the configurations required and writing an application that would guide the installer is estimated at 1 FTE for 6 months.
- A similar project to the Shibboleth Windows installer could also be considered, something that Microsoft only institutions would find very useful indeed. We estimate that the installer project would require 1 FTE for 3 months.
- The community needs a tool that fulfils the aims of Signet. The tool needs to be powerful, yet easy to implement to avoid the fate of Signet. JISC could be actively involved in this, perhaps working closely with the MACE Privilege and Access Management Working Group.

## References

Grouper - <http://grouper.internet2.edu/>

Signet - <http://signet.internet2.edu/>

The FLAME Project - <https://gabriel.lse.ac.uk/twiki/bin/view/Projects/Flame/WebHome>

GFIVO Project - <http://gfivo.ncl.ac.uk/>

Documents considered in the research phase are referenced on the project web site at <http://www.kidderminster.ac.uk/cuckoo/documents.htm>