

# Self Securing Dynamic Virtual Organisations

## Duncan Russell, Peter Dew and Karim Djemame

Informatics Institute, School of Computing, University of Leeds, Leeds, UK, LS2 9JT  
{duncanr, dew, karim} @comp.leeds.ac.uk

### Abstract

Business process integration can be complex when it spans organisations. Current grid technology aims to provide the capability to link processing between organisations, but does not presently provide manageable secure access to grid resources. In addition, existing workflow tools connecting grid services lack security for collaborative workflows. The DAME (Distributed Aircraft Maintenance Environment) is used to illustrate the collaborative use of grid services in diagnostics workflows. This paper shows that a Virtual Organisation (VO) policy needs be used to control access to a workflow executing collaborative services for different users from different organisations. The intention is to demonstrate mechanisms for securely sharing services instances using grid computers where the VO membership can change within minutes.

## 1 Introduction

The following text describes the combination of workflows with virtual organisations to form a collaborative problem-solving team. The example environment illustrates a requirement for many small dynamic teams involved in solving different problems. This environment is highly distributed from the perspective of both users and system components. These distributed system components take the form of aircraft with data logged by the aircraft engines in flight. This data has to be handled by the system for both immediate interpretation and for searching across historical records. With current Service Oriented Architectures (SOA) using web services to create distributed systems and the grid community creating stateful web services, there is a need for service level control to stateful services allowing for collaborative access to these service instances. In this case, the collaboration is a virtual organisation whose task is controlled by a workflow management system.

The example environment from which the virtual organisation requirements are derived is the Distributed Aircraft Maintenance Environment or DAME. This is a research project involving the Universities of Leeds, Oxford, Sheffield and York, supported by Rolls-Royce and Data Systems & Solutions. Its research is in systems for predictive maintenance diagnostics of aircraft engines on fleets of commercial aircraft.

Throughout this paper a Virtual Organisation (VO) is defined as a group of users and resources collaborating in one or many tasks across organisational boundaries, refining definitions given in [1, 2].

## 2 DAME

The motivation for the access control system is derived from the requirements of the DAME (Distributed Aircraft Maintenance Environment) project [3]. This project serves to demonstrate how a distributed architecture, such as grid computing, can provide a solution for aircraft engine diagnostics. The DAME project is supported by industrial partners Rolls-Royce, the aircraft

engine manufacturer and Data Systems & Solutions (DS&S), who provide IT support and maintain service contracts for engine leasing. To improve diagnostics and maintenance scheduling of aircraft engines an on-wing system has been designed to monitor vibration and performance parameters on aircraft engines whilst in flight. A ground-based system will analyse recorded data to monitor engine behaviour. This will be used to provide information on the condition of engines to the maintenance team at the airport for predictive maintenance. The DAME system is intended to be both an Expert System, providing diagnosis of known problems and a Decision Support System giving diagnostics support to experts to analyse problems not identified by the system. These experts reside within the organisations of both Rolls-Royce and DS&S.

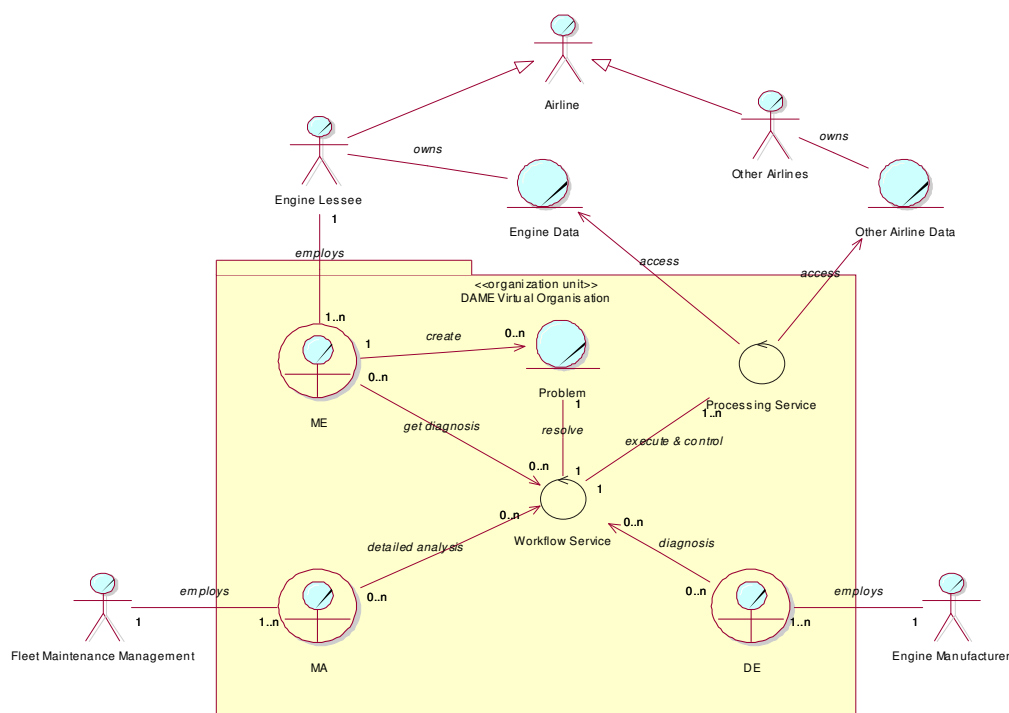


Figure 1 DAME Diagnostics Virtual Organisation

Figure 1 illustrates how the geographically distributed personnel collaborate on solving diagnostics problems. The diagram shows the personnel in the main diagnostics roles of the DAME project. They are the:

- Maintenance Engineer, based at the airport and physically works on the engine
- Maintenance Analyst, based at the diagnostics support centre (DS&S) where the airline's aircraft maintenance contracts are managed
- Domain Expert, based at the engine manufacturer's design centre and is an experienced aircraft engine designer

The mechanism to control the dynamics of the diagnostics team is provided by an escalation process. This process moves the main responsibility of investigation between members of the VO. The VO is created when out of parameter signals cannot be recognised by the initial DAME process. The Maintenance Engineer escalates the problem to the Maintenance Analyst linked to that airlines support contract. The Maintenance Analyst can involve further maintenance analysts and if needed escalate the problem to a Domain Expert. The Domain Expert can involve further Domain Experts.

Figure 1 shows the multiplicity of VO members linked by a single workflow and problem. The members of this team collaborate in a distributed environment, from different organisations and require differing access to common tools & data. The illustration does not highlight the possibility of multiple instances of the roles involved in a particular problem. Nor does it show

how the VO will evolve over time. In some cases, problems continue to be analysed by Domain Experts after the engine has been released, therefore the original Maintenance Engineer is no longer a member of the VO. It also illustrates the basic access to diagnostic services, which in turn access commercially sensitive data.

The benefits offered by grid computing to DAME can be summarised as:

- Geographically distributed data sources and users, every airport globally is a potential target for the DAME system
- Large amounts of transferred data, each engine will typically generate 35MB per hour
- Large amounts of stored data, increasing and possibly distributed
- Dynamically available resources to process each engine within a short period of time, e.g. aircraft turn around time
- System components are operated in different domains
- Requirement for strong security, due to commercially sensitive data and processing

### **3 Existing Solutions**

#### **3.1 Grid Security**

The current grid implementation of OGSA (Open Grid Services Architecture) by the Globus Alliance has some security restrictions for collaborative use of services. Firstly, only users already entered into the local list of identities can access secure services. Secondly, creating a secure environment to execute services requires a service factory per user identity. The DAME problem has multiple users managed by different organisations requiring access to sensitive services that are not managed by the users' organisation. Each organisation would maintain user identities with the role(s) a user can assume in DAME.

The current DAME implementation requires users to login to a portal, which then uses a single corporate certificate to access services and resources. This does not provide adequate protection for the large number of users, service instances and multiple VOs in the real environment. Therefore, each service needs further information to control access.

#### **3.2 Related Solutions**

There are a number of solutions for identity management in systems that cross organisation boundaries. The investigation into solutions for DAME has concentrated on those that use X.509 certificates. This is due to the ability of X.509 to delegate credentials by proxy to services [4] for single sign-on. Additionally, the credential allows users to be identified when accessing services.

The Globus Security Infrastructure (GSI) [4, 5] permits user access by mapping identities to local accounts, but is too restrictive to support DAME. The VOs require collaborative use of services and a more flexible user administration.

The Community Authorisation Service (CAS) [6], and the Virtual Organisation Management System (VOMS) [7] are certificate servers that attach user attributes to the user's certificate and can then be used to access authorised services with a VO. CAS attributes can specify access rights in low-level details such as local file permission. VOMS attributes are based on more general role and VO membership. Because all attribute information would be attached at the start of the workflow, either system would be difficult to maintain for a diagnostics process, where specific tools and data would not be known up front.

Shibboleth [8], a authentication system which precedes grid research, may provide a solution for requesting authentication and user attributes from trusted authorities. This can be combined with X.509 certificates to authenticate a user's identity and attach attribute assertions.

Policy decision engines such as Akenti [9] and PERMIS [10] use policies defined within the services against the user identity to provide an authorisation decision on an access request. Both of these use various technologies to incorporate multiple stakeholder policies. For DAME some policies will need to be dynamic, existing for the duration of a VO and its service instances.



addition, due to the Struts architecture, little administration is required to add new users and their corresponding role privileges. However, this does not fulfil the requirements for a deployed DAME system. Currently one portal exists and it manages the VO memberships and permissions. It is perceived that each organisation would have their own portal. Furthermore, there may exist multiple workflow engines, with workflow instances migrating between them. Consequently, the management of the VOs needs to move from the Portal and onto the grid. This is illustrated by the VO policy in the Access Control package in Figure 2. This VO policy would be a dynamic policy that contains not only permissions related to using the services but also permissions relating to managing the VO. The VO itself will have its own lifecycle and will be self-managing, by its user members.

To achieve the proposed solution for VO security there are a number of issues that will be investigated. These include:

- How to uniformly obtain and use user certificates across organisations with attributes, such as role or location of attribute repository
- How the VO secures itself with its own policy and self manages changes to the access permissions as the VO dynamically changes
- How to implement the separation of access control to service requests from access control to policy modifications
- How to synchronise simultaneous modifications to the VO policy
- What happens if a VO member is removed whilst requesting a service in that VO
- How is the policy implemented in the architecture:
  - As a single entity existing in one place on the network, or
  - As the emergent properties of each service in the VO, in separate policy files with service specific restrictions

Implications of the last point concerning how the policy is implemented are trade-offs in speed and manageability. For example, a single entity containing the policy for all services in the VO would be easy to manage and provide available visibility about the VO permissions. However, it would have a speed impact on service request authorisation if each request action needs to consult the policy before permitting access. Conversely, if the VO policy is distributed, with each service having a local VO policy segment, it would not impede policy decision time when accessing the policy, but would make management of the VO more complex. In both cases, a single entity would keep track of the services involved in the VO. This entity could be the workflow instance.

The implementation will be used to investigate mechanisms for embedding the security assertion sub-system within the services' hosting environment. This is intended to abstract the security implementation from the service implementation to reduce the burden on the service to include access control mechanisms and to allow different security models to be implemented without changing the underlying services. It is intended that this will involve filters in Apache Tomcat [12] running Globus Toolkit 3.2 [13], and future Globus incarnations of WS-RF [14]. The currently deployed demonstration of the DAME portal and diagnostics services has been deployed across the White Rose Grid (WRG) [15]. The enhancements to access control will also be deployed to the services on the WRG resources.

## Acknowledgements

This research is funded by the Engineering and Physical Sciences Research Council (EPSRC), e-Science Programme, Contract No. GR/R67668/01.

## References

- (1) Foster, I. and C. Kesselman, *The grid 2 : blueprint for a new computing infrastructure*. 2nd ed. San Francisco, Calif.: Morgan Kaufmann. 2003.
- (2) Foster, I. The anatomy of the grid: enabling scalable virtual organizations. in *Cluster Computing and the Grid, 2001. Proceedings. First IEEE/ACM International Symposium on*.

2001.

- (3) Austin, J. and et al., *Distributed Aircraft Maintenance Environment DAME: A GRID e-Science Full Proposal*, DAME Project, 28/06/2001.
- (4) Foster, I., et al. A Security Architecture for Computational Grids. in *Proc. 5th ACM Conference on Computer and Communications Security Conference*. 1998.
- (5) Welch, V., et al. Security for Grid Services. in *12th IEEE International Symposium on High Performance Distributed Computing (HPDC'03)*. 2003. Seattle, Washington: IEEE Press.
- (6) Cannon, S., et al. Using CAS to Manage Role-Based VO Sub-Groups. in *CHEP 2003*. 2003. La Jolla, California.
- (7) Alfieri, R., et al., *VOMS, an Authorization System for Virtual Organizations*, DataGrid Project, 2003. <http://grid-auth.infn.it/docs/VOMS-Santiago.pdf>.
- (8) Erdos, M. and S. Cantor, *Shibboleth-Architecture DRAFT v05*, 2002. <http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf>.
- (9) Thompson, M., A. Essiari, and S. Mudumbai, Certificate-based Authorization Policy in a PKI Environment. *ACM Transactions on Information and System Security*, 2003. **6**(4): p. 566 - 588.
- (10) Chadwick, D., A. Otenko, and E. Ball, Role-based access control with X.509 attribute certificates. *IEEE Internet Computing*, 2002. **7**(2): p. 62-69.
- (11) The Apache Jakarta Project, *The Apache Struts Web Application Framework*, The Apache Software Foundation, 2004. <http://jakarta.apache.org/struts/>.
- (12) The Apache Jakarta Project, *Apache Tomcat*, The Apache Software Foundation, 2004. <http://jakarta.apache.org/tomcat/>.
- (13) *Globus*, The Globus Project, 2003. <http://www.globus.org>.
- (14) Globus, *The WS-Resource Framework*, The Globus Alliance, 2004. <http://www.globus.org/wsrf/>.
- (15) Dew, P.M., et al. The White Rose Grid: practice and experience. in *UK eScience - All Hands Meeting*. 2003. Nottingham, UK.