

Access Control for Dynamic Virtual Organisations

Duncan Russell, Peter Dew, Karim Djemame

Informatics Institute, School of Computing, University of Leeds, LS2 9JT
duncanr@comp.leeds.ac.uk

Abstract

Business process integration can be complex when it spans organisations. Existing grid technology aims to provide the capability to link processing between organisations, but does not presently provide manageable secure access to grid resources. Furthermore, current 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 can 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 service instances using grid computers in a diagnostics environment.

1. Introduction

The following text describes the combination of workflows with VOs 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. Some of these distributed components take the form of aircraft engines with vibration and performance data logged 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 of stateful services allowing for collaborative access to these service instances. In this case, the collaboration is a VO whose task is controlled by a workflow management system.

The context from which the VO 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, in collaboration with Rolls-Royce and Data Systems & Solutions. Its research is in systems for predictive maintenance diagnostics of aircraft engines on fleets of commercial aircraft.

The VO as defined in [1, 2] is a group of users and resources collaborating in one or many tasks across organisational boundaries. In this paper, the VO is a problem solving team involved in the diagnostics of aircraft engine.

The team will typically be short lived, existing only for the duration of a diagnosis.

2. DAME

The motivation for the access control system is derived from the requirements of the DAME (Distributed Aircraft Maintenance Environment) project. 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. Between the two partners, they manufacture, sell and lease aircraft engines to commercial airlines. When leasing engines they also provide contracted maintenance servicing. The trend in aircraft leasing is using a costing model of 'power by the hour' and keeping aircrafts in service is a major issue for airlines, especially for low cost airlines where they demand high use of the aircraft stock. To improve diagnostics and maintenance scheduling 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 detect wear of components, foreign object damage (e.g. ingestion of birds) and other out of parameter signals.

The main aim is 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 by using diagnostics support tools for experts to analyse problems not identified by the system. These experts reside within the organisations of both Rolls-Royce and DS&S. The distributed nature of parties involved in DAME is shown in Figure 1. The aircraft maintenance teams are based at the airports across the globe served by the airline, the organisation employing the maintenance team.

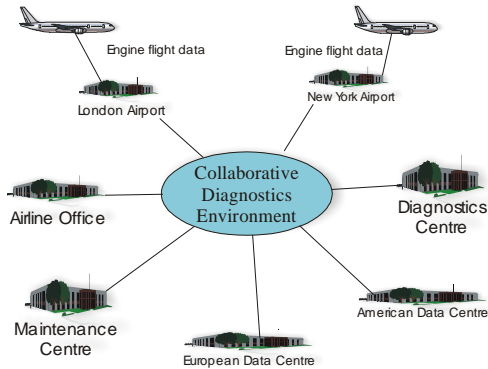


Figure 1 DAME Operational Scenario

The appropriateness of grid computing to DAME [3] 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.

2.1 DAME Architecture

The DAME project is aimed at demonstrating a distributed diagnosis service for the support of engine diagnosis for the scenario shown previously in Figure 1. A range of computation services is required to support the diagnosis.

Figure 2 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 manufacturers design centre and is an experienced aircraft engine designer.

On landing at the airport the data is downloaded from the engines into the local Ground Support System, which is connected to the grid. On receiving new engine data, DAME automatically executes a range of tools and produces a prognosis on the condition of the engine, shown in Figure 3 as 'Brief Diagnosis / Prognosis'. There are three main outcomes from the decision process 'Check Diagnoses':

- No Faults Found
- Known Condition Detected
- Unknown Condition.

The 'No Faults Found' and 'Known Condition Detected' outcomes provide the Maintenance Engineer with sufficient information to continue with maintenance procedures and the release of the aircraft.

If the initial diagnosis produces an 'Unknown Condition' then the problem is escalated. The Maintenance Engineer would escalate to the Maintenance Analyst, based at fleet management, who can look at the output from the diagnostics stages and possibly provide a diagnosis. Then, if the Maintenance Analyst cannot provide a sure diagnosis, the problem can be escalated to the Domain Expert who has access to a further range of tools enabling deeper analysis of the problem.

During this escalation process, the task-based problem or workflow forms a VO consisting of its distributed members. The members of this team collaborate in a distributed environment, from different organisations and require differing access to common tools & data. Figure 3 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.

Further security issues contribute to requirements:

- In some cases, the engine data is owned by the airline operating the aircraft
- Engine data is commercially sensitive and should be protected from access by parties not involved in using DAME or any access outside of DAME

- Pattern matching and case based reasoning tools use previous engine data and diagnosis history, so there may be restrictions on detailed access to diagnosis output, depending on role and organisation attributes of the user
- Similar issues may occur when using provenance data compiled from DAME operations in case based reasoning for workflow advice.

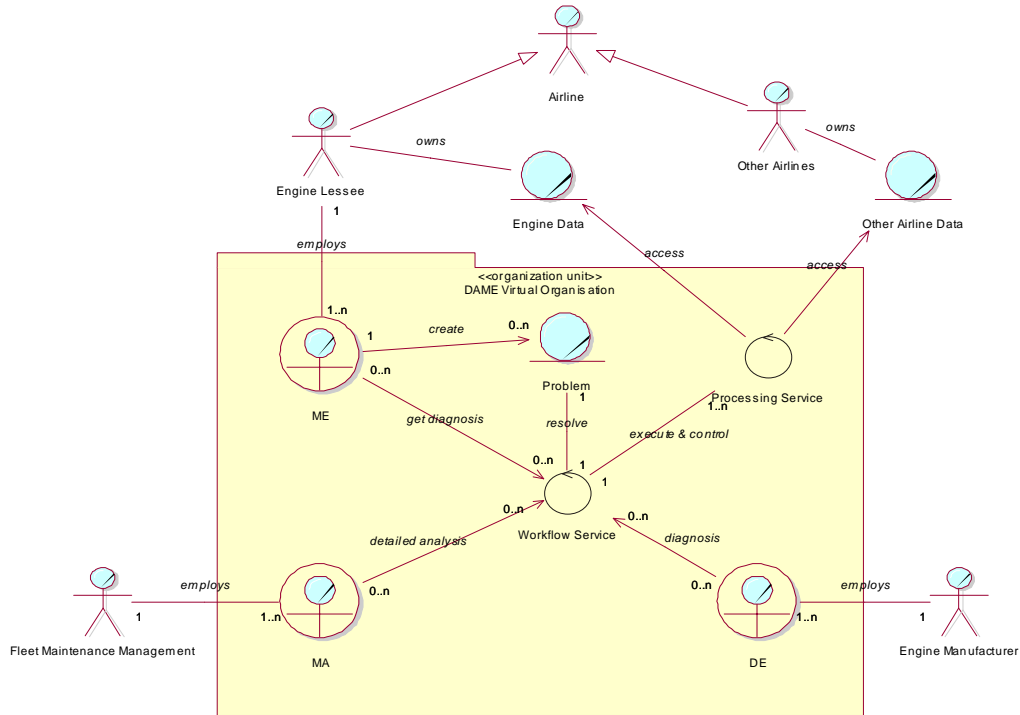


Figure 2 DAME Diagnostics Virtual Organisation

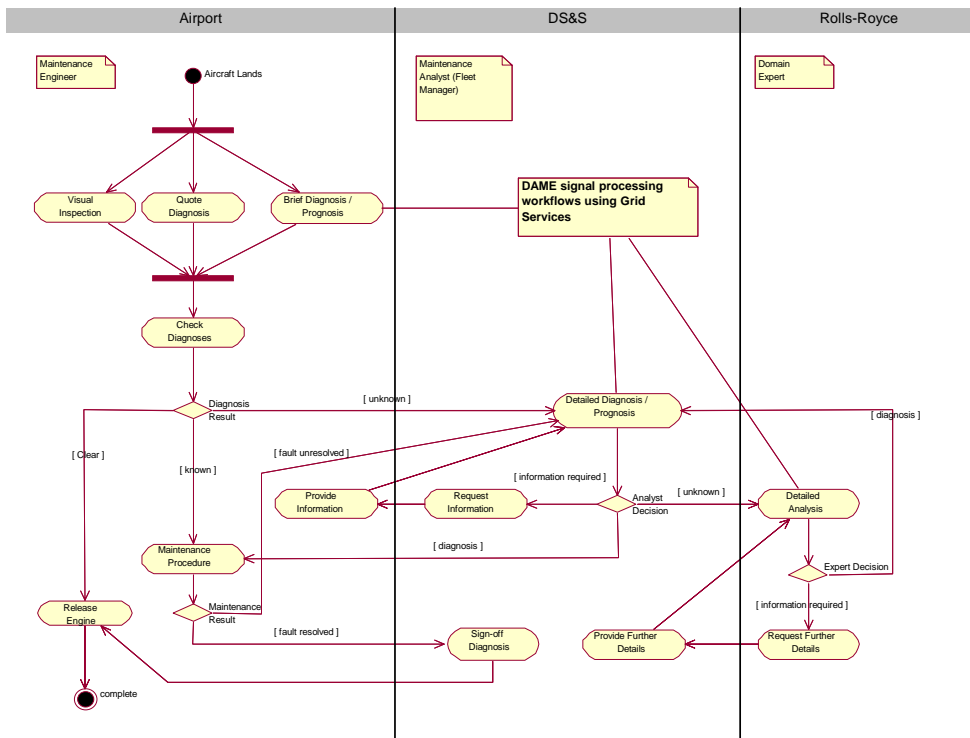


Figure 3 DAME Business Process

2.2 Grid Security

The current grid implementation of OGSA (Open Grid Services Architecture) by the Globus Alliance has some security restrictions. Firstly, access to secure services can only be made by users already entered into the local list of identities. Secondly, creating a secure environment to execute services requires a service factory per user identity.

The first problem manifests itself when using grid resources that are outside the organisational boundaries of the user; this even includes federated grid resources. The DAME problem has multiple users from different organisations requiring access to sensitive services that are not managed by the users' organisation.

The OGSA implementation Globus Toolkit 3.2 [4] requires the user identity to match an entry in the grid-map-file to permit access. This is too restrictive for DAME with such a large user base across many organisations. To maintain a distributed style of administration, each company would maintain user identities that would be attributed to the organisation; it would also contain attributes as to the role(s) the user can take in DAME. Company trusted services would provide identity attribute assertions that would permit access by role to use the services.

The current DAME implementation uses a single corporate certificate to access services and resources. This certificate provides unrestricted access to the DAME services and service instances. Access control takes place in higher-level components providing workflow services and portal login. This is insufficient to log users access to services, since the delegation by the user to the workflow service then uses a different identity for the services accesses and subsequently for further delegate services. It does control the access of a VO to the set of service instances, but works in a centralised manner for known identities accessed by the workflow management system.

3. Problem Overview

This section highlights the issues faced with implementing a solution that meets the potential requirements for the DAME system when commissioned across different organisations.

3.1 DAME System Summary

User Population is:

- Across a large number of sites (at least every international airport)

- Across many organisations (Rolls-Royce, DS&S and each airline)
- Dynamic; changes will occur within organisations, independent of DAME.

Resource Pool is:

- Large, commodity resources may contain many processing nodes. Small processing nodes may be located at major airports
- Dynamic, availability of resources will change over time, especially when using commodity resources. Desirability of locations may change due to local pricing policies for peak usage.

An individual user's identity on any resource must be recorded for accountability and traceability.

The system components are service based and use commodity-computing resources. It would be very difficult to impose fine-grained access control for every user in the system. Adding and subtracting users would be impossible without information about the users attributes.

3.2 DAME Problem Summary

The Problem of:
Providing and restricting access to commercially sensitive data and services in distributed systems where system resources, services and users belong to different organisations. Users collaborate in task based problem solving, from geographically distributed locations.
Affects:
Owners of data and authors of services that allow access to parties on a need to know basis avoiding conflict of interest.
The impact of which is:
<ul style="list-style-type: none"> • No sensitive data should be read or modified by unauthorised users or services • No service should be instantiated by unauthorised users or services • No service instance should be accessed by unauthorised users or services • The workflow of the collaboration should not be restricted in access to resources/services to resolve problems, in its normal flow of execution • Access to data should be restricted by conflict of interest mechanisms • For information that is sensitive to security level, the access control policy should restrict read and write access • Access policy mechanisms should not impede the workflow time frame when authorising security assertions.
A successful system would be:

A system that supports single sign-on by users and permits access to all resources/services allowed without detrimental time or execution overheads. It will react to changes in policy or collaboration membership before unauthorised access can occur. It will support the workflow dynamics of a problem solving VO using identities, roles and policies created by multiple organisations.

The system must be managed from multiple locations, with each organisation able to impose policies on aspects under their own interest. There should be visibility of available services and resources and the impact of policies imposed. Access to services should be logged under fine-grained detail, with security exceptions clearly identified.

There should be a means of recording access to services in a manner that is non-repudiable to support auditing. This includes intruder detection whether access has been gained or not, and auditing for economic reasons.

The workflow should manage its own access control policy to itself and the service instances currently being used. This may or may not be triggered by user intervention.

3.3 Standards

Conformance to standards is important for the adoption of this framework. It also allows the solution to be integrated into systems such as Globus Toolkit and the emerging web services standards. Among the significant developing security standards is WS-Secure Conversation [5], which comes from Globus Security Infrastructure (GSI) Secure Conversation [6, 7], and includes WS-Security [8].

Two important security standards are SAML [9], Security Assertion Markup Language, and XACML [10], eXtensible Access Control Markup Language. SAML is designed for the communication of assertions about user attributes and decisions on access permission. XACML is used to describe access policies, although there is some overlap in capabilities between SAML and XACML.

This project also requires the upper services layers of Globus Toolkit. Currently version 4.x is being developed to the WS-Resource Framework (WS-RF) [11] standard.

Other important considerations are the integration into workflow technologies. The workflow language BPEL4WS [12] is being used by the major players Microsoft and IBM. This is rapidly dominating commercial web service workflow systems and may be important when considering how to integrate security

services and policy requirements into DAME business procedures.

3.4 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. These allow delegation by proxy to services [13], for single sign-on and the credentials allows users to be identified when accessing services.

GSI [6, 7] maps user identities to local user accounts, where access permissions are defined by the local system administration. This is shown to be too restrictive to support VOs in collaborative use of services [13]. The Globus Project has produced a Community Authorisation Service (CAS) [14, 15], which uses a push model to provide access permissions using X.509 extensions. The certificate extension contains attributes that detail a user's permissions to grid resources, including such low level details as to read/write file permissions. This micro management would be very difficult to maintain across a large grid and almost impossible across organisations. However, this low level detail does resolve issues in the Globus toolkit [16] when executing processes in a shared account or container. Otherwise account or container privileges are automatically inherited by executing processes.

Another push model system is the Virtual Organisation Management System (VOMS) [17]. Similar to CAS, the user connects to the VOMS server and supplies the user with an extended X.509 certificate. In this case, VOMS extends the certificate with role and group attributes. The resource authenticating this certificate then needs to know the access policies for the roles and groups in order to make authorisation decisions.

CAS and VOMS are frameworks to managing and distributing attributes about authorisation. Akenti [18, 19] is a policy engine providing a decision on a users' request. It uses a pull model to obtain policies to ascertain permissions based on a users' identity. A resource is protected by a Policy Enforcement Point (PEP), which connects to a Policy Decision Point (PDP) that uses the access policy certificate for that resource. The policy certificate can contain links to stakeholder policies, which are retrieved when deciding on access permission. The PDP locates and verifies all relevant certificates, then evaluates them and returns the access decision.

The PERMIS system [20] is another decision engine. It obtains user attributes and policies by both push and pull methods. PERMIS provides an application gateway that holds access control policies according to role. Service requests are first parsed by the gateway, which verifies access permission to the target service before passing the legitimate request to the service. This service can contact multiple LDAP (Lightweight Directory Access Protocol) directories that contain various policies, from multiple organisations.

Both Akenti and PERMIS use LDAP for policy certificate management. Although the structure is defined for both systems, it has the disadvantage of difficult deployment across organisations and incorporating future changes. Better methods proposed for attribute and policy exchange are the XML standards of SAML [9], Security Assertion Markup Language, and XACML [10], eXtensible Access Control Markup Language. Both Akenti and PERMIS are in the process of modification to use parts of the above standards.

Another access control system is Shibboleth [21], which precedes grid research. This system was designed on web browser based access to underlying data and processing. It describes a way to federate access permissions across multiple organisations. The groundwork for this can be used to apply attribute based policies to grid service and resource sharing. By using policy assertion mechanisms that exchange authorisation via services, rather than certificates, an assertion can be trusted without knowing from whom the request is attributed. This is an example of pseudonymous access; a third party can identify permissions of a user, but not obtain the user's identity. This system may be useful for DAME. However, most services require a non-repudiable log of the action attributed to the user.

Some of the systems described are able to work together, such as CAS and Akenti. However, all of these are focused on supporting large static communities and static resources. The problem DAME described contains a large number of users, but restricted to well defined, static roles. Within a collaborative group, the roles may be defined in a policy. A fine-grained access control policy is required for service instances that are shared between group members. The policy needs to specify user identities of the respective roles and must be dynamic. By the nature of DAME services, the access control policy for the group is an emergent property of the distributed policies for service instance access. The mechanisms

described above do not provide the means to control the distributed policy across services and across organisations. Each problem in DAME is a VO with its own access policy, which presents a scalability issue with the large numbers of individual problems to manage.

A system utilising both SAML and XACML for assertions on distributed policies is Cardea [22]. It is designed to separate the authorities responsible for users from those responsible for resources, particularly applicable to dynamic resources. Whilst DAME uses dynamic resources, it is unclear how the Cardea system can respond to dynamic policies.

4. Research Directions

The conceptual system diagram in Figure 4 describes the security architecture of the DAME portal and workflow management system. The packages Portal, Workflow and Grid reflect the current state of implementation. The Portal uses the Apache Struts [23] framework and links in access control by mapping users to roles at login, which then restricts the views and actions available to that user. In addition, the Workflow sub-system uses role-based access control to restrict user requests at the workflow level. The Grid services are factory based with message level security, access currently restricted to the known certificates using Globus Grid Resource Identity Mapper (GRIM) [7] security mechanisms.

To achieve the desired solution for VO security there are issues that will be investigated. These include:

- Dynamic connection of user session in portal to workflow manager so that a different role may be used without logging out
- Obtaining and using user certificate with attributes, such as role
- User certificates with attribute containing location of trusted attribute repository, so that a remote system can be contacted for user attributes, such as role or permissions
- How the VO secures itself with its own policy and self manages the access permissions as the VO dynamically changes
- How to define a self modifying policy:
 - Separate access control to service requests from access control to VO policy modifications
 - Synchronisation issues with simultaneous modifications to VO policy
 - What happens if an identity is blocked access whilst requesting a service in a VO
 - How to specify restrictions by role and ID in the VO policy

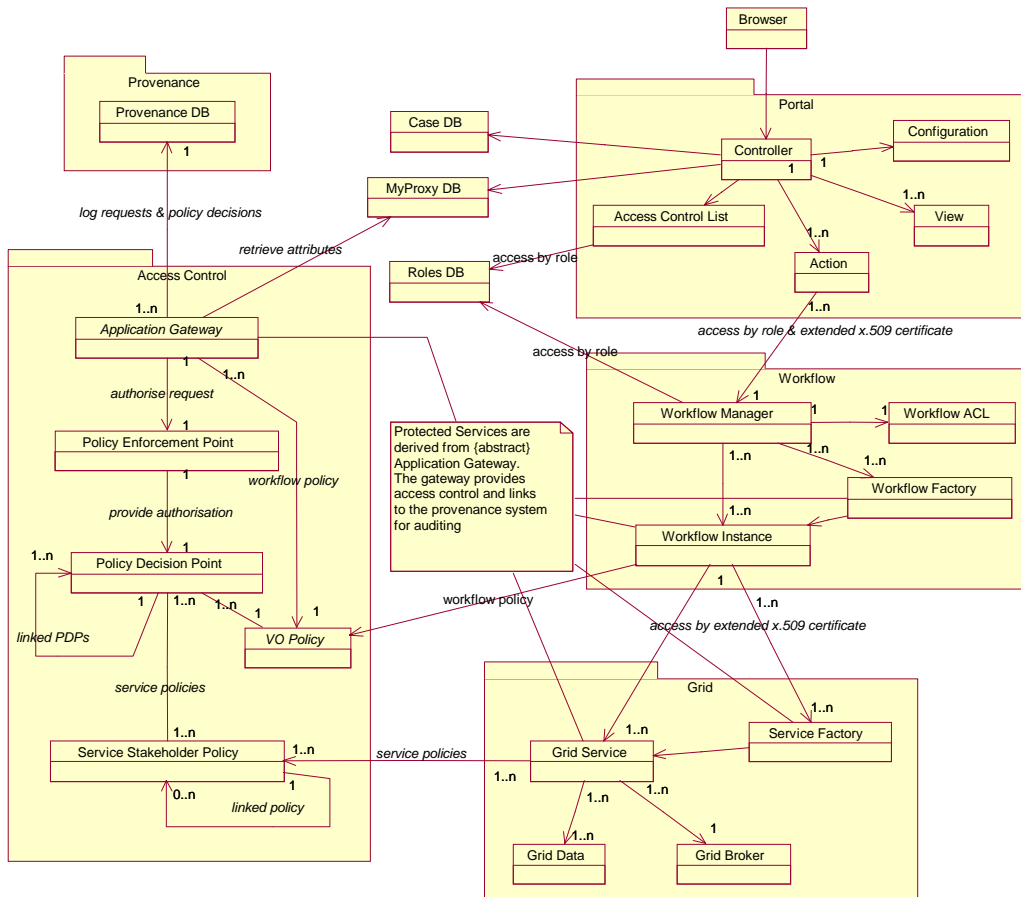


Figure 4 Proposed VO Access Control Architecture (analysis view)

- How the security mechanisms for distributed services support the policies of all stakeholders for a service creation and subsequent service access
- 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 concern how the VO policy is implemented and trade-offs in speed and manageability. For example, a single entity containing the VO policy for all services would be easy to manage and provide available visibility on the VO permissions but would have a speed impact on the authorisation of service requests. Conversely, if the VO policy were distributed, with each service having a local VO policy it would not impede policy decision time, 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; in this case, it is the workflow instance.

This research also proposes a system where authentication and authorisation services can be

dynamically added to services. The ‘Chain of Responsibility’ pattern [24] will be employed to create the dynamic list of services to provide assertions.

A role based policy and supporting mechanism would need to support models based on Bell-Lapadula [25] for privacy and protection of high-level data not for general use outside an organisation, and Biba’s integrity model [25]. The Bell-Lapadula policy is based on levels of access to sensitive data it controls the writing of information and ensures lower ranks cannot read sensitive data. Biba’s integrity model controls the writing of information at the expense of confidentiality, by using the users level of trust to modify data.

Workflow procedures may also have integrity constraints, such as Separation of Duty [26]. The workflow description would detail the roles required to complete a process, and in conjunction with the authentication mechanisms verify the users roles are sufficient to complete the task.

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 [27] running Globus Toolkit 3.2 [4]. The currently deployed demonstration of the DAME portal and diagnostics services has been deployed across the White Rose Grid (WRG) [28]. 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) Globus, The Globus Project, 2003. <http://www.globus.org>.
- (5) Della-Libera, G., et al., *Specification: Web Services Secure Conversation (WS-SecureConversation)*, IBM, 2002. <http://www-106.ibm.com/developerworks/library/ws-secon/>.
- (6) Foster, I. and C. Kesselman, Globus: A Metacomputing Infrastructure Toolkit. *International Journal of Supercomputer Applications*, 1998. **11**(2): p. 115-129.
- (7) 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.
- (8) Atkinson, B., et al., *Specification: Web Services Security (WS-Security)*, IBM, 2002. <http://www-106.ibm.com/developerworks/webservices/library/ws-secure>.
- (9) OASIS, *OASIS Security Services TC*, OASIS, 2003. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.
- (10) OASIS, *eXtensible Access Control Markup Language (XACML) Version 1.1*, OASIS, 2003. <http://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-1.1.pdf>.
- (11) Globus, *The WS-Resource Framework*, The Globus Alliance, 2004. <http://www.globus.org/wsrf/>.
- (12) Andrews, T., et al., *Business Process Execution Language for Web Services Version 1.1*, BEA, IBM, Microsoft, SAP AG and Siebel Systems, 2003. <http://www-106.ibm.com/developerworks/library/ws-bpel/>.
- (13) Foster, I., et al. A Security Architecture for Computational Grids. in *Proc. 5th ACM Conference on Computer and Communications Security Conference*. 1998.
- (14) Cannon, S., et al. Using CAS to Manage Role-Based VO Sub-Groups. in *CHEP 2003*. 2003. La Jolla, California.
- (15) Foster, I., et al. The Community Authorization Service: Status and future. in *CHEP 03*. 2003. La Jolla, California.
- (16) Foster, I., et al., *The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration*, 2002. <http://www.globus.org/research/papers/ogsa.pdf>
- (17) Alfieri, R., et al., *VOMS, an Authorization System for Virtual Organizations*, DataGrid Project, 2003. <http://grid-auth.infn.it/docs/VOMS-Santiago.pdf>.
- (18) 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.
- (19) Thompson, M., *Akenti: Distributed Access Control*, U.S. Dept. of Energy, 2003. <http://www-itg.lbl.gov/Akenti/>.
- (20) 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.
- (21) Erdos, M. and S. Cantor, *Shibboleth-Architecture DRAFT v05*, 2002. <http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf>.
- (22) Lepro, R., *Cardea: Dynamic Access Control in Distributed Systems*, NASA Advanced Supercomputing (NAS) Division, 2003. <http://www.nas.nasa.gov/Research/Reports/Techreports/2003/PDF/nas-03-020.pdf>.
- (23) The Apache Jakarta Project, *The Apache Struts Web Application Framework*, The Apache Software Foundation, 2004. <http://jakarta.apache.org/struts/>.
- (24) Gamma, E., *Design patterns : elements of reusable object-oriented software*. Addison-Wesley professional computing series. Reading, Mass.: Addison-Wesley. 1995, xv, 395.
- (25) Ferraiolo, D.F., D.R. Kuhn, and R. Chandramouli, *Access Control Policy, Models, and Mechanisms—Concepts and Examples*, in *Role-Based Access Control*. 2003, Artech House: Norwood, MA. p. 27-49.
- (26) Simon, R. and M. Zurko. Separation of duty in role-based environments. in *10th IEEE Computer Security Foundations Workshop*. 1997. Rockport, Mass.
- (27) The Apache Jakarta Project, *Apache Tomcat*, The Apache Software Foundation, 2004. <http://jakarta.apache.org/tomcat/>.
- (28) Dew, P.M., et al. The White Rose Grid: practice and experience. in *UK eScience - All Hands Meeting*. 2003. Nottingham, UK.