# 44 A GRID-ENABLED SECURITY FRAMEWORK FOR COLLABORATIVE VIRTUAL ORGANISATIONS

Liviu Joita[1], Omer Rana[1], Pete Burnap[1], Jaspreet Singh Pahwa[1], Alex Gray[1], John Miles[2]
[1]*School of Computer Science, Cardiff University, Queen's Buildings, Newport Road, PO Box 916, Cardiff, CF24 3PX, Wales, UK*
[2]*CardiffSchool of Engineering, Cardiff University, Queen's Buildings, The Parade, PO Box 925, Cardiff, CF24 0YF, Wales, UK*
*E-mail: {L.Joita, O.F.Rana, P.Burnap, J.S.Pahwa, W.A.Gray}@cs.cardiff.ac.uk, MilesJC@cardiff.ac.uk*

*In the Architecture /Engineering / Construction (AEC) industry, large projects are tackled by consortia of companies and individuals who work collaboratively for the duration of the project. Planning, implementation and running of these AEC industry projects require the formation of secure Virtual Organisations (VOs) to enable collaboration between its members. The consortia are dynamic in nature and formed for the lifetime of the project. The paper emphasises the security issues of VOs in AEC industry. It describes the design and implementation of the Grid enabled security management service, based on Globus Security Infrastructure (GSI) [8] – a Globus toolkit component, of the Product Supplier Catalogue Database (PSCD) application, an ActivePlan Solutions Ltd. (APSL)[1] software supporting collaborative work in multiple consortia.*

## 1. INTRODUCTION

A typical AEC industry project involves many individuals and companies forming a consortium for the duration of a project. A consortium can be defined as a VO formed for the duration of the project. VOs are electronically networked organisations where IT and web based communication technology play an important role in coordinating various activities of these organisations [1], [5]. Such projects range in size from the design and construction of a single building, to the creation of a large national infrastructure such as: airports, dams, and highways. These projects are usually unique, very complex and involve many participants from a number of organizations acting collaboratively. The consortia include design teams, product

[1] ActivePlan Solutions Ltd – http://www.activeplan.co.uk

suppliers, contractors and inspection teams who must collaborate and conform to predefined scheduling constraints and standards. These participants also work concurrently, thus requiring real time collaboration between the geographically remote participants. A typical consortium member is often providing similar services to multiple projects simultaneously involving different partners. Web-based communication technology is beginning to play an increasingly important role in supporting collaboration in AEC projects particularly to enable a project management team to identify the current state of a project, its activities, and the constraints on these activities and their schedules. Members can participate in several consortia at the same time and can join or leave a consortium as the project evolves. Grid computing provides an important (vital) infrastructure to support such collaborations, as the interaction between participants within such projects involves resource and data sharing (often requiring high speed connectivity) [4], [5]. Security is also a significant concern in a commercial setting of this kind – and often a constraint not fully applicable to other uses of Grid infrastructure (such as scientific collaborations) [6], [7]. Role based access control has also been investigated in literature, and often is concerned with roles assigned to individuals (users) or organisations based on a workflow session. Each role is also assigned one or more tasks, and associated with these tasks can be access to data sources. A key theme in such work is determining how permissions on the underlying data sources (object-level permissions) can be mapped onto particular roles that exist in the system. Often, it is necessary to delegate permissions to use objects between roles. Park, Sandhu and Ahn [10] describe a role based access control system implemented via a Web server. They make use of cookies to maintain state (for recording user information in order to determine which user has visited a site before). Cookies are used in their system for transmitting authorisation information – to enable clients to present their authorised role(s) to the Web server. However, in most systems cookies are transmitted in text format, and therefore cannot be used for sensitive information. Park et al. make use of "secure" cookies – the user provides a user name and password, which are subsequently encrypted. The IP address of the user's machine (needed in IP_Cookie) is directly retrieved by the server. Shim and Park [11] use a slightly modified approach, whereby the user only presents authentication cookies to the Web server. If this is successful, then the server automatically generates a user name and password to the user – which must then be stored in the user's memory space (and not the users' hard disk). Authorised roles for the user are also retrieved. Subsequently, when the same user visits another Web server in the same domain, then the verification process does not need to be repeated. The same roles and role permissions are now granted to the user.

This paper describes the design, development and implementation of the Grid-enabled Security Management Service of the PSCD application – as part of the Collaborative Virtual TEams (COVITE) project [3], which brings together industry designers, suppliers and product manufacturers to work collaboratively in multiple consortia in a virtual environment. Secure access to information provided by suppliers and designers is a key theme addressed here. The system developed does not utilise cookies to record authorisation information, but makes use of X509 certificates [4], [6], [7]. Furthermore, the authorised users' roles and VOs they belong to are also taken into consideration when accessing the application [5]. Collaboration occurs between: (1) product suppliers and contractors for procurement

of supplies; (2) product specification designers for defining and building industry standards to describe available products; and (3) members of the consortia working on a particular construction project which require information on the products. In this paper we also describe our experience with Grid enabling the PSCD application using Globus and Java CoG toolkits. The PSCD application supports the collaboration described above using three functional modules: Security Management, User Management, and Data Management. As the scope of this paper is the security management service, based on the security and user management modules, details regarding the Data Management module can be found at Burnap, Joita and al. [2].

The paper is organised as follows: in Section 2 we discuss: (1) the PSCD application considerations, in regards to the need of supporting collaborative work from the point of view of the AEC industry, and (2) the PSCD security management service support considerations. Section 3 discusses security management service architecture, while section 4 describes user management support considerations respectively for the PSCD application. Conclusions and further work follow in Section 5.

## 2. THE PSCD APPLICATION CONSIDERATIONS

### 2.1 Collaborative Support Considerations

Collaboration in a construction engineering project can take place in various ways. Figure 1 gives a conceptual view of the PSCD application and the collaborative aspects mentioned in section 1. The suppliers and purchasers collaborate to procure supplies for a particular construction project of a particular VO by using the PSCD application. The application serves as a platform to bring together a large number of suppliers and contractors to negotiate and procure the necessary supplies for construction projects.

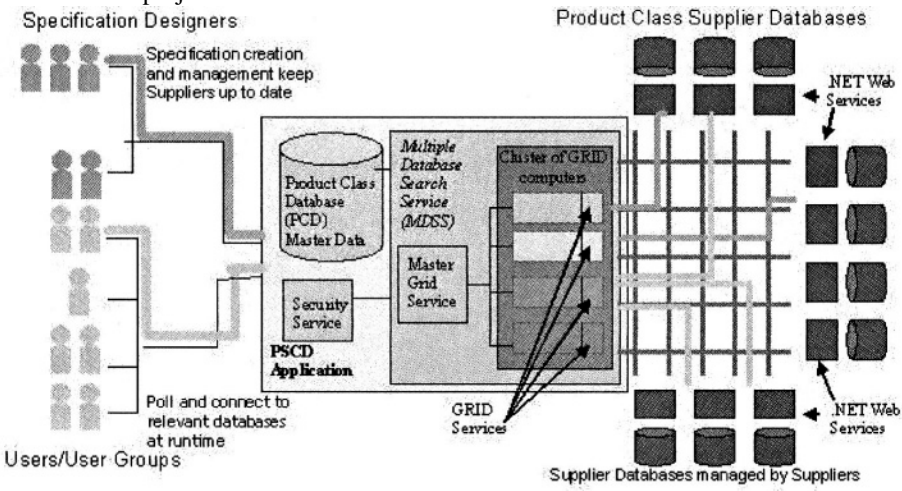


Figure 1 - Grid-enabled PSCD application diagram

The collaboration between Specification Designers is required to bring together product suppliers and contractors, so that contractors are aware of product availability. This is achieved by creating Product Classes and specification types for product suppliers in the collaboration environment. These Product Classes are at the heart of data procurement of the consortia. When a supplier wishes to advertise their products, they must use these classes. A Product Class can be defined as a template made up of a number of different specification types. Collaboration takes place when a number of Specification Designers come together and design a Product Class for a new product or when the product class is being peer reviewed.

Collaboration also takes place between members of consortia. This involves holding virtual meetings to discuss various issues over the lifetime of the project. Important issues could include construction designs, resource management and product selection, and procurement. Tackling these issues requires access to the needed information which is distributed across a large number of autonomously managed supplier databases. The Grid enabled Multiple Database Search Service (MDSS) [2] enables searching these supplier databases using a cluster of machines in a Grid network. When a search is made by the MDSS, the machines in the Grid network should collaborate to retrieve information on matching products to the consortium's requirements.

### 2.2 The PSCD Security Management Service Support Considerations

Security aspects rely on keeping important and sensitive information in the hands of authorized users. There are four important issues to deal with: authentication – being able to verify the identities of the parties involved; authorization – limiting access to resources to selected users or programs; confidentiality – ensuring that only the parties involved can understand the communication; integrity – being able to verify that the content of the communication is not changed during transmission [8].

Without a strong authentication, an unauthorized user, as a single user or as part of a VO, can access proprietary web resources containing information of other VOs. The Security Management Service is based on the GSI, a client-certificate authentication system, where users are identified by a globally unique name known as *Distinguished Name (DN).* A format example of a DN (also known as a *subject* name) is: *"C=UK, O=eScience, OU=Cardiff, L=WeSC, CN=firstname lastname"*.

Authentication with GSI is a matter of proving that a user is the entity identified by a DN. Resources then typically have a local configuration for mapping the DN to a local identity (e.g. a file containing DN and username pairs) [8].

The main issue in GSI authentication is the *certificate.* A GSI certificate, encoded in X509 certificate format, includes the following information [8]: (1) a *subject* name, identifying the person; (2) the public key belonging to the subject; (3) the identity of a Certificate Authority (CA), which has signed the certificate and certifies that the public key and the identity both belong to the subject; (4) the digital signature of the CA.

The authorization to access the resources is controlled by a mapping between the user's distinguished name and a local Unix username (identity) via a Grid-map file. The GSI uses the Secure Sockets Layer (SSL) for its mutual authentication protocol. The GSI enhances SSL by providing single sign-on capabilities for users; this is achieved by generating a proxy certificate. This proxy certificate is a lifetime limited

credential that acts on behalf of a user, and can be used to authenticate the user to the available Web resources. The advantage of this technology is that a user is not requested to enter a password every time he/she wants to access a Web resource, and he/she can use his/her proxy certificate for accessing resources.

## 3. SECURITY MANAGEMENT SERVICE ARCHITECTURE

Currently, Web browsers and Web servers do not support the concept of *delegation.* This means the creation of a lifetime limited private key and a certificate pair, known as a proxy, which can be used to authenticate to Web resources. As it was shown in section 2.2, the GSI provides the security mechanism for a user to delegate his/her credentials to the Web resources. This can be done using either Globus or Java CoG toolkits facilities. Whereas the focus of existing efforts in Web Service security (such as WS-Security) is to provide a transport layer mechanism for encoding SOAP messages, there is no clear agreement on how certificates should be obtained or verified. The challenge to build a secure access to PSCD web resources is to require the integration of the Security Management Service of the PSCD application into a single user-friendly service using the capabilities of GSI. Since the user accesses PSCD web resources remotely, it must be possible to establish the user's identity, the user's role and the VO the user belongs to with certainty. A Tomcat Web server is used to host the Security Management Service Module and to handle the connections to the PSCD application via the HTTPS protocol.

Figure 2 and 4 show the UML diagrams that describe the use cases, while Figure 3 and 5 show the architecture diagrams, of the security management service within the PSCD application. Modelling the context of the security management service (Figure 2) shows which actors lie outside of the module and interact with it. For example, in our security management system we provide login and validation cases inside the system. Similarly, users (Individual or Project Team Users), Specification Designers and Certificate Authorities exist outside the system. The things that live inside the system are responsible for carrying out the behaviour that those on the outside expect the system to provide. All those things on the outside that interact with the security management system constitute the system's context. This context therefore defines the environment in which our security management system operates.

Figures 2 and 3 also describe the security management service designed, deployed and integrated for the PSCD application, when a user provides a valid proxy certificate residing on his/her machine:

1. First, a user has to have a valid proxy certificate. The user submits his proxy certificate to the Tomcat Authentication Server (AS) via a Web interface using a JSP-Servlet interface.
2. Tomcat AS authenticates the certificate and obtains the local username for the PSCD application from the gridmap file.
3. Tomcat AS passes the local username, user role and VO to the IIS server that runs the PSCD system (which is a .NET web application environment). IIS then matches the username, the role and the VO to its local DB and creates a session for that user.

4. User preferences are applied to the 'index' page of the PSCD system and the user is presented with the home page of the application.

Modelling the requirement of the security management system (Figure 4) involves specifying what the system has to do (from the point of view of the outside of the system), independent of how the system should do it.

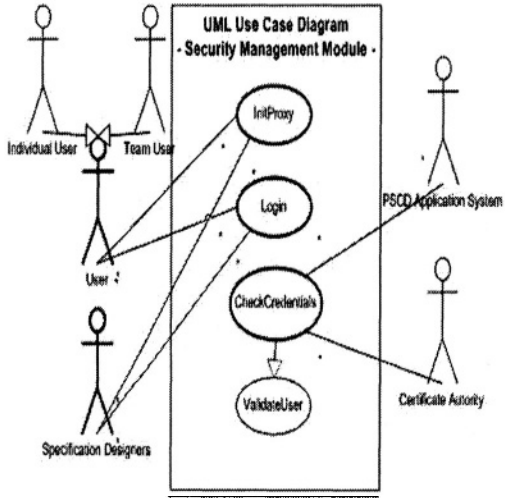


Figure 2 – UML Modeling the Context of the Security Management Service

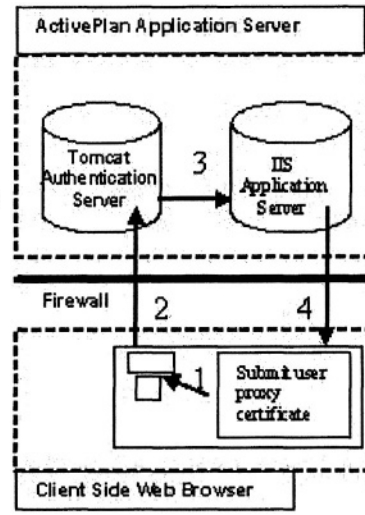


Figure 3 – ActivePlan Secure Login Architecture using a valid proxy certificate

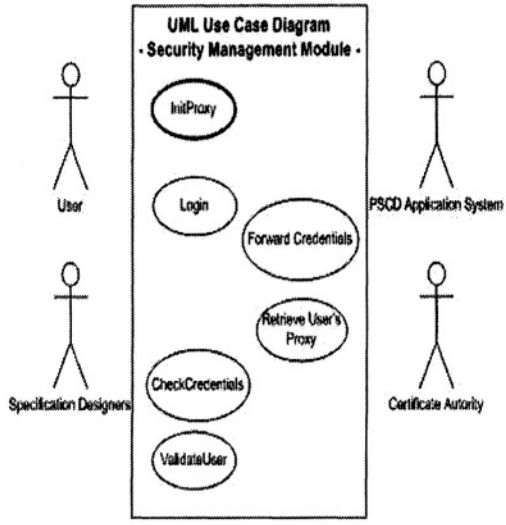


Figure 4 – UML Modeling the Requirement of the Security Management Service

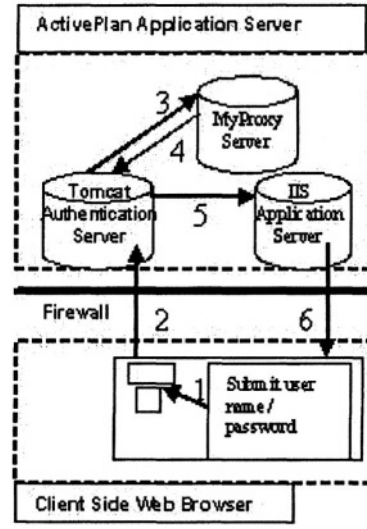


Figure 5 – ActivePlan Secure Login Architecture using username / password credentials

Figures 4 and 5 also describe the security management service designed, deployed and integrated for the PSCD application in the case that the user provides a username/password pair credentials which protect his/her proxy certificate that resides on the MyProxy credential repository [9]:

1. First, a user has to have a valid proxy certificate on the MyProxy Server machine.
2. The user submits his username/password pair credentials to the Tomcat Authentication Server (AS) via a web interface using JSP - servlet interface.
3. Tomcat AS uses the username/password pair to authenticate and authorize the user against his proxy certificate from MyProxy server
4. Tomcat AS authenticates the proxy certificate uploaded from the MyProxy server, and obtains the local username for the PSCD application from the Grid-map file.
5. Tomcat AS passes the local username, user role and VO to the IIS server that runs the PSCD system (which is a .NET web application environment). IIS then matches the user name to its local DB and creates a session for that user.
6. User preferences are applied to the 'index' page of the PSCD system and the user is presented with the home page of the application.

## 4. USER MANAGEMENT SUPPORT CONSIDERATIONS

Once the user has been authenticated (via a Globus proxy certificate [8] or a user name/password credentials) and authorised according to his/her user role and VO he/she belongs to, the PSCD system will dynamically determine which interface to display in the Web application front-end. There are several different versions of the menu written into die system, each of which contain links available to users depending on their role and VO they belong to. Figure 6 illustrates an example of such user login interface associated with the user role and VO.

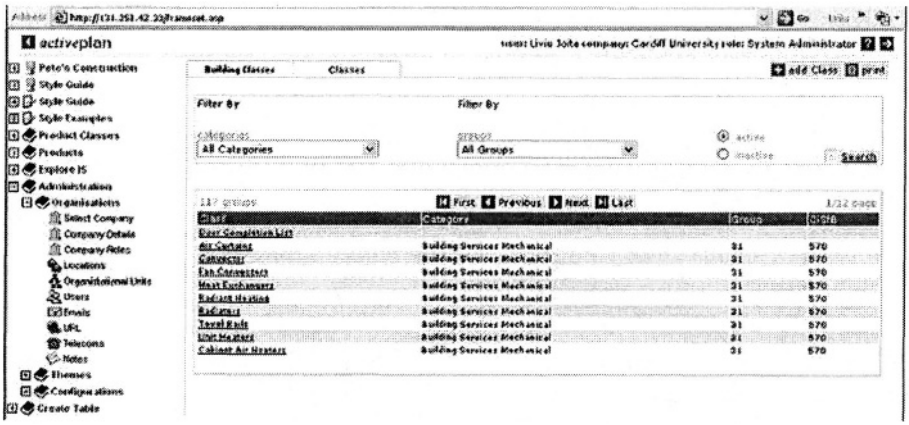


Figure 6 – User Interface

A user may be logged into the PSCD system, namely as a virtual organisation consisting of a single person user *or* as a member of single or possibly multiple

consortia - consortia could also feasibly be created within other consortia in an unlimited nested hierarchy. Changing virtual organisations would involve logging out and back in again.

## 5. CONCLUSIONS AND FURTHER WORK

The PSCD application includes a login interface using the security infrastructure based on GSI mechanism provided by the Grid middleware based on the Globus and Java CoG toolkits. Two scenarios have been developed: first, users use their local proxy certificate, and second, users use a username/password pair credentials in order to be authenticated and authorized to access the PSCD server resources. The login mechanism is implemented over a HTTPS connection. Further development will be done in regards to a secure integration within the PSCD .NET web development environment.

The user management system needs to incorporate logic to calculate discounts from manufacturers, either based on the identity of a user acting as a single user, or as a member of a consortia, namely VO. The storage location of this metadata must also be determined; this is an area that requires careful consideration. Should it reside on the central database or be stored by each supplier in the PSCD?

## 6. REFERENCES

1. Burn J., Marshall P, Wild M. Managing knowledge for strategic advantage in the virtual organisation, Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research, New Orleans, Louisiana, United States, ISBN 1-58113-063-5, pp. 19–26, 1999
2. Burnap P, Joita L, Pahwa JS, Gray A, Rana O, Miles J. Supporting Collaborative Working of Construction Industry Consortia via the Grid, in Proceedings of UK e-Science All Hands Meeting 2003, Nottingham, United Kingdom, 2-4 September 2003, Editor: Simon J Cox,© EPSRC September 2003, ISBN 1-904425-11-9, p. 87-94. http://www.nesc.ac.uk/events/ahm2003/AHMCD/pdf/018.pdf
3. COllaborative Virtual TEams (COVITE) project website: http://www.wesc.ac.uk/projectsite/covite/
4. Foster, I., Kesselman, C., Nick, J., Tuecke, S., The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration, Open Grid Service Infrastructure WG, Global Grid Forum, June 22,2002. http://www.globus.org/research/papers.html
5. Foster, I., Kesselman, C., Tuecke, S., The Anatomy of the Grid: Enabling Scalable Virtual Organizations, International J. Supercomputer Applications, 15(3), 2001. http://www.globus.org/research/papers.html
6. Foster, I., Kesselman, C., Tsudik, G., Tuecke, S., A Security Architecture for Computational Grids, Proc. 5th ACM Conference on Computer and Communications Security Conference, pp. 83-92, 1998. ftp://ftp.globus.org/pub/globus/papers/security.pdf
7. Foster, I., Karonis, N. T., Kesselman, C., Tuecke, S., Managing Security in High-Performance Distributed Computing, Cluster Computing, 1(1):95-107, 1998. ftp://ftp.globus.org/pub/globus/papers/cc-security.pdf
8. Grid Security Infrastructure, 2004. http://www-unix.globus.org/security/
9. MyProxy Online Credential Repository, 2004. http://grid.ncsa.uiuc.edu/myproxy/
10. Park, J.S., Sandhu, R., and Ahn, G.J., Role-based Access Control on the Web, ACM Transactions on Information and System Security, Vol. 4, No. 1,2001, pp 37—71
11. Shim, W. B. and Park, J. S., Implementing Web Access Control System for Multiple Web Servers in the Same Domain Using RBAC Concept, 8th International Conference on Parallel and Distributed Systems, 2001, pp 768—773