Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Security Focused Dynamic Virtual Organizations in the Grid based on Contracts

Bartosz KRYZA[1], Lukasz DUTKA[1], Renata SLOTA[2], Jacek KITOWSKI[1,2]
[1]*Academic Computer Centre CYFRONET-AGH, Nawojki 11, Krakow, 30-950, POLAND*
Email: bkryza@agh.edu.pl, dutka@agh.edu.pl
[2]*Institute of Computer Science AGH-UST, Mickiewicza 30, Krakow, POLAND*
Email: rena@agh.edu.pl, kito@agh.edu.pl

Abstract: In the paper our work in the area of supporting dynamic Virtual Organization creation and management with ontologies and contracts is presented. A framework called FiVO (Framework for Intelligent Virtual Organizations) is described, along with its overall application in a Grid setting, its architecture and sample use case.

1. Introduction

Virtual Organizations (VO) are the core concept of Grid computing which allows us to group users and resources into collaboration environments in order to share and use resources such as computing power and services based on proper rules. The main problem faced by Grid administrators and users is the burden of setting up a VO and managing its life-cycle, including inception, deployment, evolution and dissolution. In order to support creation of on-demand dynamic Virtual Organizations we propose a semantic based framework, called FiVO (Framework for Intelligent Virtual Organizations) [1,2]. This framework enables creating a particular VO based on a negotiated semantic contract, which defines the rules of resource sharing as well as SLA parameters that can be used by the monitoring infrastructure to enforce proper Quality of Service within the VO [3]. The framework is aimed at VO administrators and middleware service developers, in order to allow for semi-automatic configuration and deployment of the VO as well as further VO execution.

Current solutions related to contract based management of VO are mostly concerned with simple QoS parameters and SLA. However, we believe that contracts should include much more information, especially that related to the authorization statements which allow to state exact rules of sharing the resources within a VO in case of multiple parties. In order to support that scenario, the contract model must be abstract enough in order to handle various, often highly heterogeneous environments. Our vision is to provide a generic interface and contract model for the purpose of dynamic definition of Virtual Organization by means of contract statements and then properly deploy the VO depending on existing middleware, including security and monitoring components, in particular environment. This issue becomes of particular importance in case of modern large scale integration activities, for instance related to integration of multiple national Grid infrastructures (NGI's), where a need emerges to create Virtual Organizations spanning several infrastructures which often are based on incompatible middleware (e.g. Globus vs. Unicore) and use different models of Virtual Organizations. In that case availability of high level and middleware independent

VO management framework will allow to manage Virtual Organizations while limited the inherent burden on system administrators.

This paper describes a complex approach to addressing VO management issues in Grid environments. It describes the contract ontology we have developed with special focus on its security aspects, which make it possible to define during contract negotiation step of VO inception phase rules under which resources available within a VO can be shared by the participants of the VO and how it is used to configure underlying Grid authorization system used by a particular VO, e.g. PERMIS and VOMS. The framework is being evaluated within the framework of EU-IST project Gredia, on two commercial applications. First one is related to inter-banking solution for automatic credit-scoring of bank users credit requests. The second one is a media application oriented on providing a collaborative environment for nomadic journalists. The paper describes a sample case study based on a bank scenario where bank evaluates on-line requests for their clients, including information from third-party data sources which constitute the Virtual Organization.

2. Related Work

In [4] authors present an SLA negotiation and enforcement tool applicable to business settings based on GRIA middleware and evaluated within the EU-IST SIMDAT project. In the paper they present detailed mathematical model taking into account both resource usage reports as well as various SLA constraints. Authors of [5] present requirements for automating the contract management in a VO. They identify 3 kinds of contracts in a VO: business contract, ICT contract and ASP contract. In the context of the legality of a VO, it could be, in theory at least, registered as a legal entity or not. If it is not its contract is defined by bilateral agreements between the respective partners expressed in the form of contracts. The ICT contract involves the client and the participants of the VO. In [6] attempt was made to formalize a definition of contract-based multi-agent Virtual Organization. The authors define 4 key properties of VOs: Autonomy, Heterogeneity, Dynamism and Structure. They use terminology from agent-based systems, e.g. they refer to the VO itself as an agent. The contract is defined as a set of commitments, goals and agents in some context. The paper introduces a formal definition of a hierarchical VO with a set of agents (which can be VOs themselves), policies, goals and commitments. The VO is then a set of bilateral contracts between agents in a VO, and can be more easily defined in a distributed setting. For example for 3 partners and 2 contracts A<->B and B<->C, A and C don't event need to know about each other. Another example of contract based VO's is presented in [7]. The authors present web-Pilarcos J2EE based agent framework for managing contract based Virtual Organizations. The contract itself is an object (J2EE EntityBean) and can be in several states such as In-negotiation, Terminated etc. The proposed solution is not based on ontologies, and the metadata reasoning is mentioned briefly. The proposed architecture has many different components - which might make it hard for integration with custom systems - should rather provide a more unified interface based on easily adaptable standards. Paper discusses the basic requirements for a VO contract such as modeling of service behaviour, communication services and some non-functional properties such as QoS. It also discusses the operation of VOs, the need for monitoring of security and SLAs for ensuring proper QoS and the evolution of Vos. In [8] the authors propose an architecture of a system which maps Business Level Objectives to SLA and policies. The paper discusses the need to go from abstract SLA concepts understood differently by different parties to low-level configuration concepts - which they refer to Operational Level Agreement. The proposed system aims at supporting configuration of providers systems so that it can guarantee proper BLO and SLA. In [9] authors present a scheme for managing QoS based on SLA contracts with a focus on mobile devices, which functionality is split into two basic phases: discovery and reservation,

execution and monitoring. In [10] authors describe the approach to dynamic Virtual Organization of the TrustCOM project, where VO is defined as recursive set of organizations and other Virtual Organizations, which could be created on demand in reaction to a particular business need or market opportunity. The core issue was enabling of trust approach based on requestor experiences control of roles of a participant in a VO.

3. Methodology

The overall aim of the GREDIA is development of a Grid application platform, providing high level support for the implementation of Grid business applications concerned with users mobility. This platform is generic in order to combine both existing and arising Grid middleware, and facilitates the provision of business services, which mainly demand access and sharing of large quantities of distributed annotated numerical and multimedia content. One of the main GREDIA features is its focus on mobile users to exploit Grid technologies in seamless way by enabling mobile access and sharing of distributed content.

The potential results of the platform are being validated through two pilot applications, including media and banking. To handle complexity of allocating heterogeneous resources in the Grid and to make their usage possible with mobile devices, GREDIA strongly focuses on dynamic Virtual Organizations. A significant contribution of GREDIA is to hide the complexity of heterogeneous resources and support dynamic Virtual Organizations of business mobile entities through a special semantic framework.

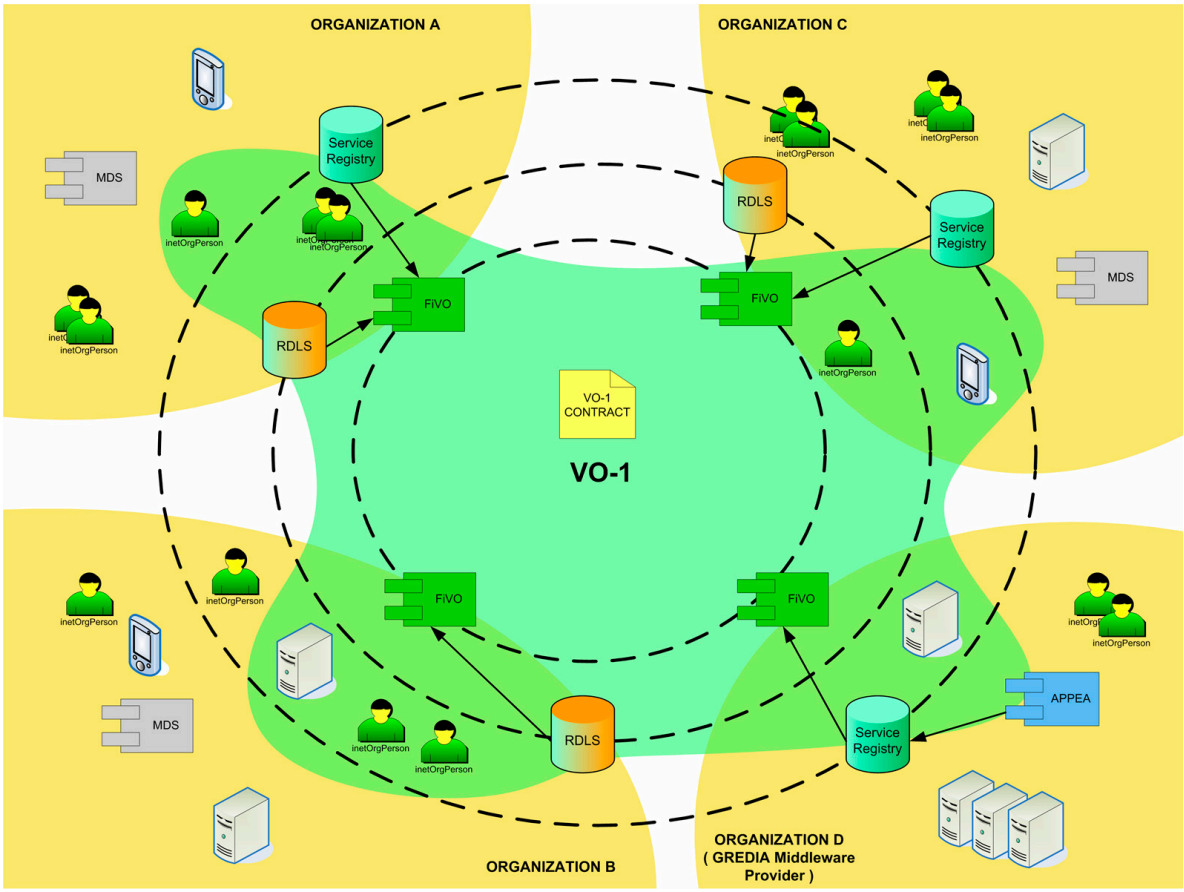

Figure 1. Sample deployment of FiVO in a Grid setting

Figure 1 presents example deployment of the FiVO framework in a distributed GREDIA environment. Four organizations are sharing their resources within the VO-1. FiVO component is deployed logically within each organization and is responsible for storing semantic descriptions of its contents (i.e. resources provided to other organizations). These

descriptions can include such aspects of organization as its structure and business logic described in proper ontology as well as hardware, data and service resources available and provide for sharing with other organizations.

The negotiation process is performed in a distributed and iterative manner, where responsible people from each participating organization state their requests and obligations using special Graphical User Interface which allows them to see the changes made by others and either accept or reject them. The user interface is based on Protege ontology editor, thus allowing users to directly have a semantic view over their resources as well as the current state of the contract negotiations (see Figure 2). The contract itself is defined using a special ontology.

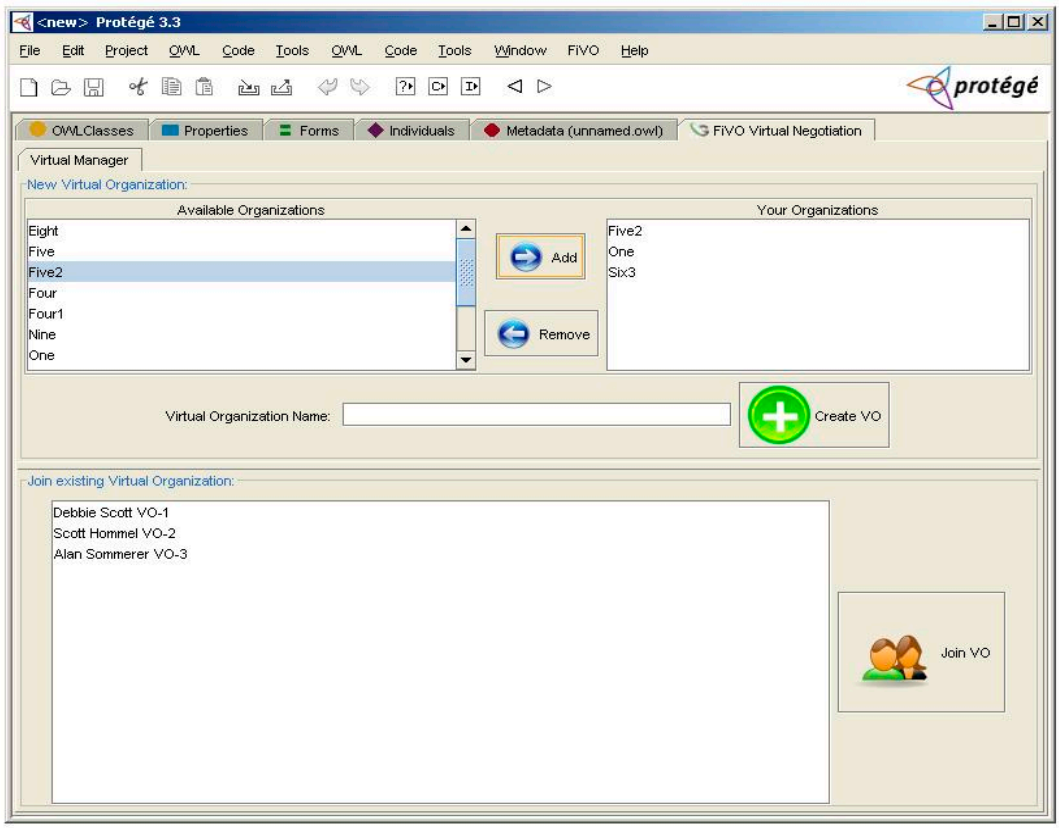

Figure 2. FiVO Graphical User Interface for contract negotiation

The Contract Ontology (see Figure 3) includes a set of ontologies, which allow to specify all issues necessary for the FiVO framework to configure and deploy the Virtual Organization. The main components of this ontology include generic model of Virtual Organization, Security Ontology which allows to defined abstract inter-domain security assertions on resource sharing, a QoS ontology which allows to state the required Quality of Service parameters for accessing resources in the VO and an ontology which describes the contract itself and formalizes the entire negotiation process. In order to reflect the domain specific aspects of the Virtual Organization several domain-level ontologies can be included in the contract ontology for a particular Virtual Organization in order to allow definition of rules for custom resources that will be available in the Virtual Organization.

After the contract between parties is negotiated, our framework configures semi-automatically all dependent Grid middleware such as authorization and monitoring systems in order for the Virtual Organization to be deployed. For instance the configuration of the PERMIS authorization layer is performed by setting up its LDAP certificate registries with proper policies specifying which roles can use which services and under what conditions Additionally the VOMS service is configure with proper attribute certificates specifying which users belong to which roles (see Figure 4).

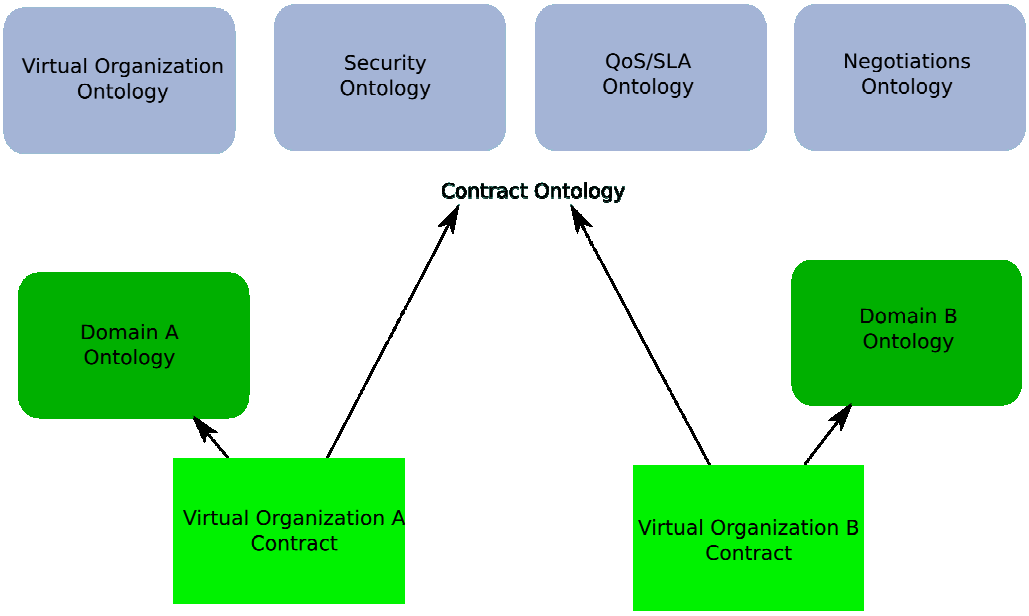

Figure 3. Overview of the contract ontology

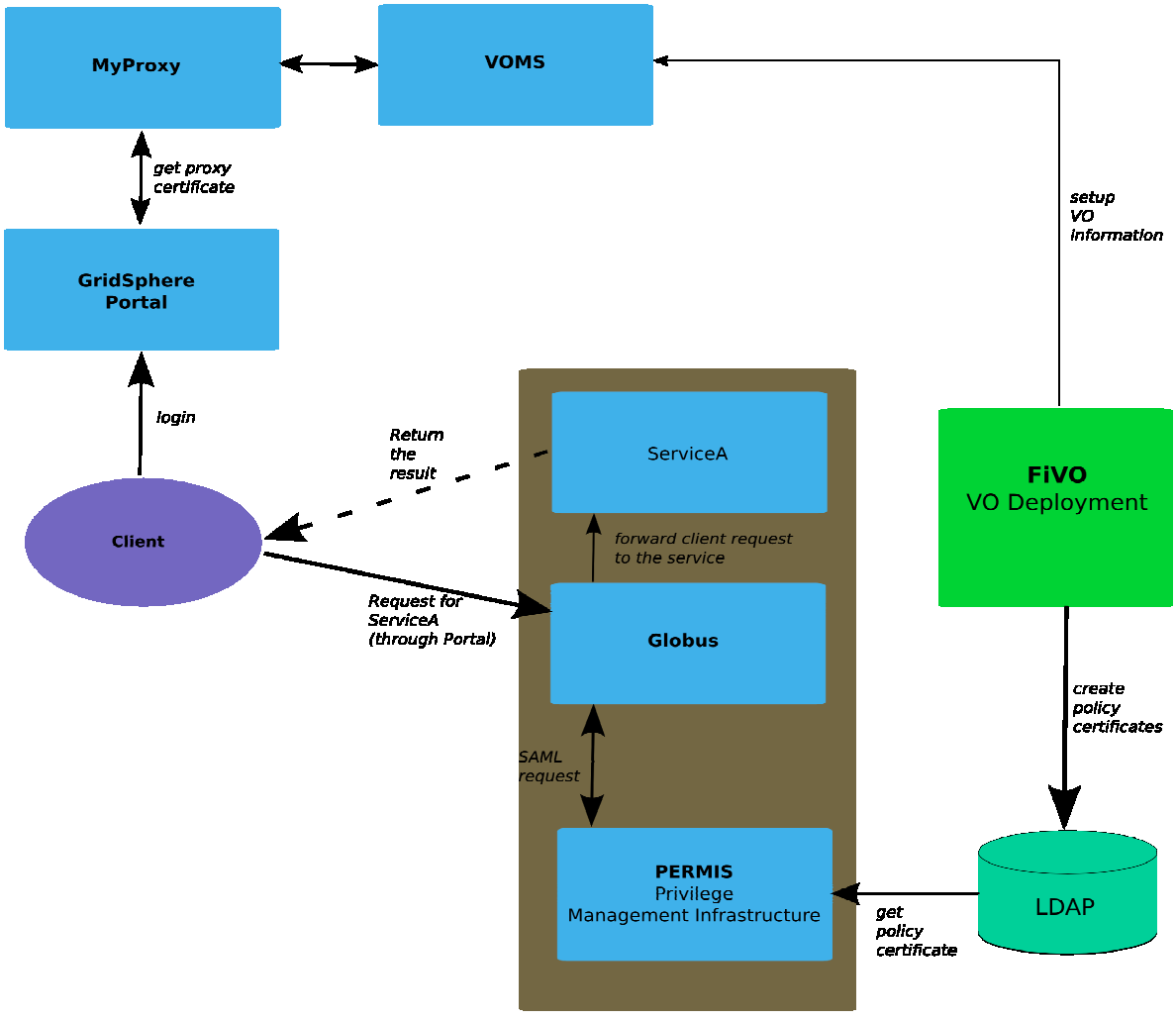

Figure 4. FiVO and authorization infrastructure in a typical Grid setting

The core of our framework is based on a Grid Organizational Memory (GOM) [11] semantic knowledge base, developed previously, which stores information about the contract and performs ontological reasoning in order to infer additional statements necessary to properly configure the middleware.

Of course our system is not dependent on any particular authorization or monitoring solution, as the Contract Ontology is abstract enough to allow generation of configuration in any available Grid middleware component, provided that proper plug-in is implemented in FiVO which can translate the ontology concepts to the configuration rules used by the underlying middleware.

4. Sample Use Case

Our system will be presented here based on a banking use case scenario where users apply for a loan using bank's website. The Virtual Organization for the bank has several requirements mostly relating to security and confidentiality of clients information. The bank's internal credit scoring services require additional information about the client during the loan evaluation process such as client credit history provided by a third-party, which must be a part of the Virtual Organization.

Within the bank itself, several users with various roles can be involved in the credit scoring process and according to their roles only certain operations can be performed on the clients data. Additional issue is assurance that the credit response will be generated in a given time frame, which imposes special requirements on the Quality of Service of the services used in the evaluation process.

Below is a part of the sample contract for this Virtual Organization rendered in Web Ontology Language:

```
<j.0:VirtualOrganization rdf:ID="EasyLoan">
 <j.0:name rdf:datatype="...">
       EasyLoan Application VO</j.0:name>
 <j.0:administeredBy rdf:resource="#Marco"/>
 <j.3:hasContract>
  <j.3:Contract rdf:ID="EasyLoanContract">
   <j.3:hasStatement>
    <j.3:Statement rdf:ID="StCreditCalculation">
     <j.3:hasAtom>
      <j.3:Atom rdf:ID="AtomCreditCalculationService">
       <j.3:hasActor rdf:ID="#Marco"/>
       <j.3:hasResource>
        <j.2:Service rdf:ID="CreditCalculationService">
         <j.0:isOwnedBy rdf:resource="#HappyBank"/>
         <j.0:belongsTo rdf:resource="#EasyLoan"/>
        </j.2:Service>
       </j.3:hasResource>
       <j.3:hasAction>
        <j.3:Action rdf:ID="ProvidesService"/>
       </j.3:hasAction>
       <j.3:hasParameter>
         <j.3:Parameter>
          <j.0:hasQoSAttribute>
           ---- j.5:QoSAttribute - #j.6:TimeToComplete
          </j.0:hasQoSAttribute>
          <j.6:hasValue>
            ---- { "15", #owlTime::unitMinute }
          </j.6:hasValue>
         </j.3:Parameter>
       </j.3:hasParameter>
       <j.3:hasParameter>
        <j.3:Parameter>
         <j.0:hasAuthorizationRestriction>
```

```
          ---- j.5:accessRole
         </j.0:hasAuthorizationRestriction>
        <j.6:hasValue>
         ---- { "#BankClerk" }
        </j.6:hasValue>
       </j.3:Parameter>
      </j.3:hasParameter>
      ---- more parameters ...
     </j.3:Atom>
    </j.3:hasAtom>
   </j.3:Statement>
  </j.3:hasStatement>
 </j.3:Contract>
</j.3:hasContract>
</j.0:VirtualOrganization>
```

This contract is used by FiVO to configure Grid middleware services such as VOMS, PERMIS or MDS in order to actually deploy the Virtual Organization in the Grid environment. This includes generation of for instance PERMIS policies as well as for instance WS-Agreement documents. Further enforcement of the contract statements is performed automatically by these services.

5. Conclusions

In this paper we have presented a framework for supporting dynamic Virtual Organizations inception and management in the Grid setting with a focus on both security of interaction within the VO as well as Quality of Service issues. The framework is currently being evaluated in two pilot applications, and we are still collecting relevant feedback from users that will be taken into account while finalizing the implementation of the system. Major achievements up to date include the definition of the Contract Ontology along with a formal negotiation model and development of the contract negotiation services and Graphical User Interface. The future work includes integration of the framework with most popular Grid middleware security and monitoring components for the purpose of scalable contract enforcement in large heterogeneous Virtual Organizations.

Acknowledgements

The authors want to acknowledge the support of the EU GREDIA Project (IST-FP6-034363) and AGH University of Science and Technology grants 11.11.120.777 and 500-08.

References

[1] Kryza, B., Dutka, L., Slota, R., and Kitowski, J., Supporting Knowledge-based Dynamic Virtual Organizations with Contracts, eChallenges 2007 Conference and Exhibition, The Hague, Netherlands, 24 - 26 October 2007. pp. 937–945. ,

[2] Kryza, B., Dutka, L., Slota, R., and Kitowski, J., Supporting Management of Dynamic Virtual Organizations in the Grid through Contracts, in: M. Bubak, M. Turala, K. Wiatr, Proceedings of Cracow'07 Grid Workshop, Oct 15-17 2007, Cracow, Poland. , ACC Cyfronet AGH, 2008, pp.140-147

[3] M. Zuzek, M. Talik, T. Swierczynski, C. Wisniewski, B. Kryza, L. Dutka, and J. Kitowski, Formal Model for Contract Negotiation in Knowledge-Based Virtual Organizations, in: M. Bubak, G. D. van Albada and J. Dongarra and P. M.A. Sloot (Eds.), Proceedings of Computational Science - ICCS 2008, 8th International Conference Krakow, Poland, June 2008, volume III, LNCS 5103, Springer, 2008, pp. 409-418

[4] Boniface, M., Phillips, S. and Surrige, M., Grid-Based Business Partnerships Using Service Level Agreements. In proc. of Cracow Grid Workshop 2006 (CGW'06), (Eds) Bubak, M., Turala, M., Wiatr, K., ACK-Cyfronet AGH, Krakow 2007, pp. 165–176

[5] M. Shelbourn, T. Hassan and C. Carter, Legal and contractual framework for the VO. In: L.M. Camarinha-Matos, H. Afsarmanesh and M. Ollus, (Eds), Virtual Organizations Systems and Practices. Springer, 2005, pp.167–176.

[6] Udupi, Y. B., and Singh, M. P. Contract enactment in virtual organizations: A commitment-based approach. In proc. of AAAI-06. AAAI Press. pp. 722–728
[7] Metso, J., and Kutvonen, L. Managing virtual organizations with contracts. In Workshop on Contract Architectures and Languages (CoALa2005) (2005). Enschede, The Netherlands, 2005.
[8] Hasselmeyer, P., Koller, B., Schubert, L., and Wieder, P. Towards SLA-supported resource management. in: M. Gerndt, D. Kranzlmuller (Eds.), Proc. of High Performance Computing and Communications, Second International Conference, HPCC 2006, Munich, Germany, September 2006, LNCS 4208, Springer 2006. pp. 743–752.
[9] Litke, A., Konstanteli, K., Andronikou, V., Chatzis, S., and Varvarigou, T., Execution Management and SLA Enforcement in Akogrimo. In proc. of Cracow Grid Workshop 2006 (CGW'06). (Eds) Bubak, M., Turala, M., and Wiatr, K. ACK-Cyfronet AGH, Krakow, 2007. pp. 154–164
[10] T Dimitrakos, G Laria, I Djordjevic, N Romano, F D'Andria, V Trpkovski, et al (6) Towards a Grid Platform Enabling Dynamic Virtual Organisations for Business Applications Proc. Trust Management, Third International Conference (iTrust 2005), Paris, France, 23-26 May 2005, LNCS 3477
[11] Kryza, B., Slota, R., Majewska, M., Pieczykolan, J., and Kitowski, J., Grid organizational memory: provision of a high-level Grid abstraction layer supported by ontology alignment, The International Journal of FGCS, Grid Computing: Theory, methods & Applications, vol. 23, issue 3, Mar 2007, Elsevier, 2007, pp. 348-358