VO Intersection Trust in Ad hoc Grid Environment

Ladislav Huraj
Department of Informatics
Matthias Bel University
Tajovskeho 40, 97401 Ban. Bystrica, Slovakia
huraj@fpv.umb.sk

Helmut Reiser
MNM-Team
Leibniz Supercomputing Centre
Boltzmannstr. 1, 85748 Garching, Germany
reiser@lrz.de

Abstract

A secure environment is a top-priority for all the forms of grid computing. To establish trust, traditional grids use various methods, mostly centrally oriented ones, such as certification authorities, VO management servers or credential pools. An ad hoc grid environment is characterized by the absence of a central trusted authority; therefore collaborating entities must establish and maintain a trust relationship among themselves.

The paper presents an overview of ad hoc grids, the definitions as well as authorization mechanisms. A proposal for an authorization mechanism to support formation of VOs in ad hoc grids based on intersection of VOs is set out. The mechanism can facilitate the establishment of a trust relationship in cases when standard solutions have failed.

1. Introduction

Grids are used for their massive distributed computing and resource collaboration. Grids bring together users and resources across administrative and organizational domains. In order to utilize the computing resources from different providers, a trust model should be considered. To establish trust, traditional grids use various methods, mostly centrally oriented ones, such as certification authorities, VO management servers or credentials pools. Under the authority of these methods the Virtual Organization (VO) can be constructed and grid users are organized in these VOs. A user can be a member of any number of VOs.

The problem of access control to resources in grids, i.e. the authorization is conveniently simplified by adopting the schema based on VOs and resource owners. The relationship of the user with its VO, i.e. the claim of VO membership, is managed by the VO itself, while the resource owners evaluate locally the claims regarding their local policies and user characteristics. Typically, a user proves the membership to a particular VO, whose members are authorized to perform certain operations, by presenting a certificate.

In [1], [2] main phases of VO life-cycle are described: Identification, Formation, Operation, Evolution, and Dissolution. Trust values and policies are specified before starting the VO identification phase. In the VO identification phase, trust information could be taken into account when selecting potential VO members. The VO formation phase includes all the activities related to trust negotiation. During VO operation, trust values are computed and distributed among the VO members. On VO dissolution, trust information such as credentials and access rights are revoked.

In this article a proposal to support authorization mechanism based on intersection of VOs is presented. The mechanism can be used to build trust relationships during VO formation phase between grid entities in cases when standard solutions have failed. The method can be useful for trust management especially in an environment such as an ad hoc grid. The ad hoc grid environment, as described in detail in Section 2, binds together varied idle computational resources to form a one-off grid for a particular grid job. Once the job is completed, the grid is disbanded.

This paper is organized as follows. Section 2 presents an overview of the ad hoc grid. In Section 3, existing solutions for security mechanisms in traditional as well as in ad hoc grids are presented. Section 4 describes an implementation of the proposed mechanism into ad hoc grid environments. The paper concludes with a short summary.

2. Ad hoc grid environment

An ad hoc grid along with mobile grids and wireless grids belong to the category of accessible grids [3]. An accessible grid consists of a group of mobile or fixed devices with wired or wireless connectivity and predefined or ad hoc infrastructures.

The definition of ad hoc grid can be found in different authors. Friese, Smith and Freisleben [4] have defined an ad hoc grid as follows: *"The ad hoc grid is a spontaneous organization of cooperating heterogenous nodes into a logical community without a fixed infrastructure and with only minimal administrative requirements"*. In this definition, the ad hoc grid is providing computing resources for each member on demand. An informal definition of ad hoc grids is given by Amin, Laszewski and Mikler [5] as, *"a distributed computing architecture offering structure, technology-, and*

control-independent grid solutions that support sporadic and ad hoc use modalities."

Some authors [6], [7] define an ad hoc grid environment as *"a heterogeneous computing and communication system without a fixed infrastructure; all of its components are mobile."* Although the mobility of the devices must be regarded, in terms of the proposal set out in this article it is not relevant. The focus, as in the first two definitions, is on the grid structure, protocol, and control rather than the ad hoc mobility of devices.

The main characteristics of an ad hoc grid environment can be summed up as follows:

Dynamics: The main feature of an ad hoc grid is its highly dynamic nature, which results from the frequently changing structure of underlying networks and VOs due to grid members switching on and off, members entering and leaving, member mobility, and so on [3]. Traditional grid services like discovery, management, and security mechanisms are not appropriate to support such a grid architecture that is capable of handling sporadic and ad hoc communities and collaborations along with dynamically changing membership and access policies [5].

Resources: On the other side, ad hoc grids have more available resources (than for example MANETs or peer-to-peer networks), such as a synchronization system, higher communication and computational capacity, more stable connections, etc. [8]. In a peer-to-peer environment, there is no distinction between a resource user and a resource provider; each is commonly referred to as a "peer" [9]. In general, peer-to-peer systems are designed to fulfill a single task (e.g. file sharing), while grids are multi-purpose and offer greater flexibility for distributed design [10].

Independence: As mentioned in the previous definitions, ad hoc grids can be defined as a distributed computing infrastructure offering structure-, technology-, and control-independent grid solutions. Structural independence reflects the ability to self-organize among its participant members which means it is not possible to use centralized administrative services as in traditional grids. Each member in an ad hoc grid is responsible for itself. Technology independence reflects the ability to support multiple grid protocols and technologies. Control independence mirrors the ability to support administrative functionality without any central coordination [5]. Instead, an ad hoc grid has the control independence ability to manage its security and usage policies in the absence of a central controller [8].

As in the traditional grid, users can create virtual organizations or join existing VOs created by others in the ad hoc grid environment as well as share services, exchange data, and interactively communicate with other members within the same VO [5]. Note that VO members can be grid users as well as grid resources.

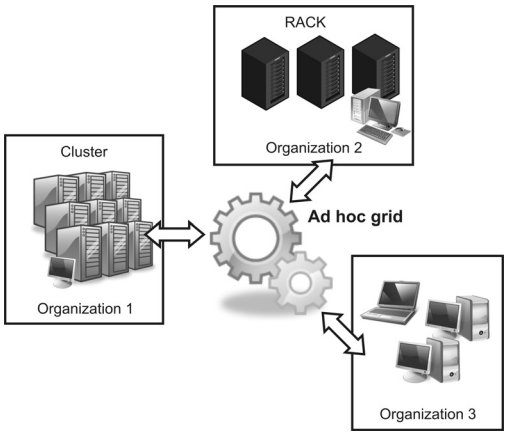

Figure 1. Ad hoc grid

3. Authorization and Trust

In traditional grid environments, there is usually a central administrative authority and the relationships between entities are pre-established and centrally monitored. The authority is trustworthy for all entities in the environment. Each entity possesses a credential or an identity certificate from this authority that qualifies the entity to collaborate with each other. Whole interactions are monitored and controlled by administrators which can respond when the behavior of an entity is not in accord with grid usage policy and terminate the trust relationship with the violating entity.

One of the first authorization mechanisms of the Globus Toolkit [11] in VOs was a simple mechanism called "grid mapfile" when the resource owner makes decisions based on this file. The grid mapfile is a list of all authorized grid users with their distinguished names mapped to local user accounts. This file can also serve as an access control list.

Virtual Organization Membership Service (VOMS) was developed by European DataGrid and DataTAG collaborations to manage authorization information in VO scope. Each VO has its own VOMS server and a separate database. VOMS is used to create an attribute certificate enabling the user to gain access to grid resources and including the information about a user's VO. VOMS can also be used to generate grid mapfiles [12].

The principle of Community Authorization Service (CAS), like VOMS, uses a CAS server for VO management. The CAS server issues a signed proxy credential to the user who has to contact the server and ask for permission to use the grid resource. The CAS server acts as a trusted authority between VO users and resource owners. In the CAS mechanism the grid mapfile needs to contain only the name of CAS server and not all the VO users [13].

PERMIS is an attribute-based access control infrastructure, which assigns both roles and attributes to users by multiple distributed attribute authorities. Both modes of

obtaining attribute assignments are possible: push mode where the user attribute assignments are sent to PERMIS by application or pull mode where PERMIS fetches the attribute assignments itself from LDAP repositories or SAML attribute authorities [14].

GridShib [16] is an integration of the federated identity management (FIM) infrastructure Shibboleth [15] with the Globus Toolkit grid technology [11] in order to provide attribute-based authorization for distributed scientific communities. A pair of software plugins are used; one for Globus Toolkit (using SAML to discover the attributes) and another for Shibboleth (to provide the attributes to the grid service provider). The plugins enable a GT grid service provider to securely request user attributes from a Shibboleth Identity Provider. Similar to PERMIS there are two main operations: the "push" of authorization-enabling attributes, where the client provides the attributes up front, obtaining and pushing those attributes to the grid service provider at the time of initial request, and the "pull" where the grid service provider requests attributes from the client's own administrative domain via a back-channel exchange.

Generally, the role of the VO in grid environment is to provide confirmation of VO membership and additional attributes. There are several forms of assertions. For example, a list of trusted subjects (e.g. grid mapfile), attribute certificates (e.g. VOMS, PERMIS), proxy credentials with authorization information included as an extension (e.g. CAS) or SAML reference statements (e.g. PERMIS, GridShib).

If situations or users require it, a combination of previous forms and mechanisms is possible for access management based upon VO membership in grids. For example, the IVOM project [17] of German Grid Initiative (D-Grid) [18] solves the interoperability between Shibboleth federations and VO management systems as well as between the three different Grid middlewares (gLite, GT and UNICORE) used by D-Grid communities.

3.1. Authorization and Trust in Ad hoc grid

In ad hoc grids, there is an absence of a globally trusted authority and participating entities must explicitly establish and maintain a trust relationship among themselves [5].

The authorization mechanisms for ad hoc grid environment in [10] are based on Globus Toolkit (GT) [11]. GT offers access control mechanisms to guarantee that only authorized users can call on grid services. The proposed approach has been divided into two parts. The first is a clear mechanism for authorization services in the ad hoc grid with a central authority granting or denying access which is trusted by all. But due to ad hoc grid independence, the central authority is not a suitable model. For the second approach, without a central authority, it is assumed that further security mechanisms are required to offer intra-node security. But their inter-service security model is oriented more towards control in the case of a malicious service being introduced into the grid rather than to authorization and trust decisions.

An ad hoc grid approach in [19] instead of one central certificate authority uses a set of trusted certificate authorities (CA), where a user identity is represented by an X.509 public-key certificate signed by a CA. Additionally, a user may choose to act as a CA generating identities for other users. The authentication system can be simply described as follows: every user has a set of trusted CAs; if there is a CA who issues a certificate to the first user and is trusted by the second user, and a CA who issues a certificate to the second user and is trusted by the first one, then mutually authenticated transaction is permitted between the users. Moreover, the question of trust is opened there: an authenticated user does not necessarily imply a trustworthy user. As in a traditional grid, a policy enforcement point (PEP) as well as a policy decision point (PDP) are used. But in ad hoc grid environments PDP and PEP are located on the same ad hoc grid peer, since in ad hoc grids each user is responsible for maintaining and securing itself. Rather than a single grid authorization policy, a distributed and fragmented grid policy is supported whereby each policy fragment is systematically controlled and enforced by different users participating in the ad hoc grid.

Kerschbaum et. al. [20] solve the question of trust and reputation for member selection in the VO formation phase. Relationships between users are a combination of previous performance and recommendation trust, i.e. the trust relationship between two participants is formed based on the past experience they had with each other. Each member must register with the Enterprise Network Infrastructure (EN) by presenting some credentials to obtain feedback ratings for other members with whom they experienced transactions. In the dissolution phase of each VO all members leave feedback ratings with the reputation server for the other members with whom they have completed transactions. The feedback ratings can be positive or negative. The system requires each transaction to be rated by the participants. But from the ad hoc grid point of view, the reputation service is centralized by the EN and, moreover, the solution is more peer-to-peer than grid oriented.

In [8] differences between ad hoc and traditional grid are summarized in a table, Table 1. For further security solutions it is necessary to study and to adapt techniques from MANETs and peer-to-peer networks to facilitate authentication for untrusted peers in ad hoc grids. On the other hand, it should be borne in mind that some techniques suitable for MANETs, such as identity-based authentication and symmetric-key-based authentication, are not suitable for ad hoc grids, since ad hoc grids are at a higher layer than MANETs.

Grid environments usually employ a delegation process

Table 1. Differences between ad hoc grids and traditional grids [8]

	Traditional Grids	**Ad Hoc Grids**
Administration	dedicated administrators	autonomous fashion
Members	dedicated members	frequently changing
Members' relationship	trust pre-established with CA	unknown to each other
Service availability	guaranteed with high availability	dynamically contributed by members

based on proxy certificates. In proxy delegation [21] a user generates a proxy certificate with a limited lifetime and delegates its rights to a grid job by assigning it the proxy certificate. The reason is a single sign-on: applications run by the user can authenticate themselves on behalf of the user using the proxy, and thus there is no need for the user to provide a password every time the application is run. The use of a proxy delegation model in ad hoc grids is for example shown in ad hoc grid security infrastructure in [19].

4. "Good society" VO trust model

In our proposal we focus more on the authorization problem rather than authentication problem. On the other hand, authorization is closely related to access control trust which is covered in the proposal.

An authorization situation occurs when a potential user requires resources from others. In an ad hoc grid, the decision regarding access is up to the resource owner. At first the resource owner tries to find the potential user within the grid mapfile. If the user is not included there, the resource owner asks for the user's attribute certificates. After that the resource owner checks if the user is member of the same VOs as the resource owner or if there are any trustworthy attribute authorities (Source Of Authorities, SOA) which have signed the certificates. If no use-conditions are found for potential user, the access to the resources is denied. We propose another possible way by which users can establish trust and build relationship under intersection of VOs when previously used methods were not successful.

All of the main characteristics i.e. *dynamics*, *resources* as well as *independence* of ad hoc grids mentioned in Section 2 were regarded during the design of the proposed approach. The good society trust model combines transitive trust with authorization certificates. Without loss of generality the attribute certificates were chosen as a general model of the VO membership assertion. Note that an attribute certificate is a data structure that binds information about the holder to the attributes that are assigned to them, digitally signed by the issuing attribute authority.

Since there is no direct trust to any VOs of a potential user from resource owner, the user tries to satisfy the owner to accept one of its VOs as a trustworthy VO and to allow access to the resources. The idea comes out from the human society. If a member wants to present the trustworthiness of its society/club, i.e. show that the society/club is a "good society", (s)he must list the reputable members of the society. In grid environment, the attribute certificates are used for this purpose. We look at attribute certificates more than trust certificates and less than authorization certificates. A new, indirect trust to a VO of potential user can be derived from these certificates.

The proposal requires two main conditions:
(i) storing of attribute certificates,
(ii) the trust is formed based on past authorized information, i.e. previous membership of the users.

The first condition (i) requires the storing of attribute certificates from previous transactions. Since there is no central database of the certificates, each user builds its own storage of its attribute certificates as well as of all attribute certificates of all known co-members of VOs. In this way, it can list its co-members in a VO as well as prove it with certificates. Building such storing space does not present a problem in a grid environment. A similar philosophy of storage in grid environment can be found for example in the authorization system Akenti [22]. Akenti caches all the certificates that it finds in order to reduce subsequent search time. It also caches the authorization decision as a capability certificate that contains the access rights of a user for a resource, so that subsequent requests for the same resource by the same user require no repeated decisions.

The second condition (ii) is based on previous authorization information. The trust decision of the resource owner is based on attribute certificates presented by a potential user. The potential user should substantiate the trustworthiness of its VO by presenting k co-members of its VO which are acceptable for the resource owner. The acceptance means that the co-members are also members of another VO that is trustworthy to the resource owner. The potential user proves this with their attribute certificates.

The trust for a potential user's VO is derived from the trust to trustworthy VOs. The intersection of potential user's VO and resource owner's VOs must be greater or equal to k where k is the number of members belonging to the intersection of the potential user's VO with the resource owner's VOs respectively. The value of the number k is based on resource owner policy. The higher k the higher the resulting trust, on the other side, the lower k the easier the feasibility of the authorization process. Moreover, the value k can differentiate the level of trust. The resource owner determines an interval of values of k; the values at the beginning of the interval mean low trust, i.e. the user

obtains some rights only particularly, and the values at the end of interval mean full trust and to obtain all the requested rights.

Note that such trust information is not in conflict with the independence of an ad hoc grid, the mechanism does not assume any strictly pre-definite structure of trust. On the other side, the idea of the mechanism is based on the fact that ad hoc grid participants have previous authorization relations and they have collaborated in previous grid or ad hoc grid projects based on attribute certificates.

For instance, in Figure 2, Alice is a member of VOa, Bob of VOb and VOc, and user Charlie is the member of VOc. The virtual organizations VOa, VOb and VOc are trustworthy for the resource owner. Moreover, the users Alice, Bob and Charlie belong together with the potential user to the virtual organization VOx that is not trustworthy for the resource owner. The potential user for the VOx acceptance should send k co-member certificates (k = 3) which belong to its VO as well as to the resource owner's VOs. In our case, these are the attribute certificates of the members Alice, Bob and Charlie. After that the resource owner can accept VOx and permit the access of the user to its grid resources. Note if k = 4, the condition is satisfied as well, because for user Bob there are two attribute certificates, one for VOb and one for VOc.

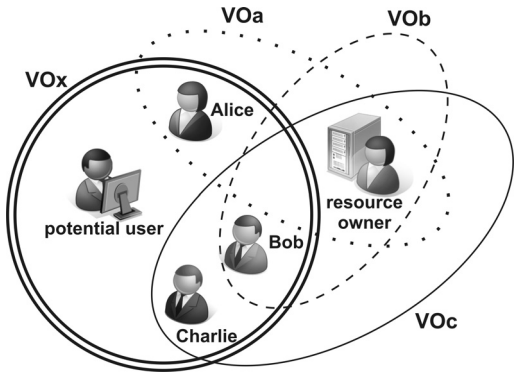

Figure 2. Intersection of VOs: VOa, VOb and VOc are trustworthy VOs for the resource owner. The trust for VOx is derived from them.

After the acceptance of a new VO, the attribute certificate of a potential user is regarded by the resource owner and the role as well as capability included in the certificate are used for achieving finer granularity of the trust.

Some aspects of the approach are further considered: the trustworthy VOs recognition, issuing of a new certificate and the absence of intersection of VOs.

Recognition of trustworthy VOs: For the acceptance of trust, the relevant attribute certificates must be shown to the resource owner. The method is based on the list of trustworthy VOs. The resource owner gives the list of all its trustworthy VOs as well as the minimal number k of co-members to the potential user. It is up to the user to search in its own certificate storage for relevant attribute certificates indirectly confirming the trustworthiness of its VO. If there are several combinations of VOs, the user chooses a VO in which its role is the closest to its requests for grid resources. After that the potential user sends the k attribute certificates to the resource owner. The resource owner proves the certificates and allows/denies the required resources and services. Although the resource owner in this approach must disclose the information about its trust VOs, it increases the facility of the authorization process in ad hoc grids. The searching burden is on the potential user requesting access to grid resources.

Issuing of a new certificate: After the acceptance of the potential users VO, the resource owner has two possibilities. It can add the user or the user's VO into its list of trustworthy users/VOs; or it can issue an attribute certificate with the set of rights for the user and so include the user into its VO. This certificate can be in the future used for further authorization decisions in the system as well.

Absence of attribute certificates: If appropriate attribute certificates for confirmation of VO trustworthiness cannot be found on the potential user's side, access to the resource is denied and other mechanisms of authorization and trust must be used. We must note that the position of our mechanism in an ad hoc grid environment is that of a support mechanism in the trust management and it should be combined with other authorization mechanisms. Implementation of the mechanism makes it possible to establish the trust relationships in the VO formation phase for ad hoc grids in cases when standard solutions failed.

The philosophy of the proposed mechanism corresponds with ad hoc grid characteristics. The mechanism does not expect any grid architecture and neither does it expect the availability of special services, which reflects the dynamics of the environment. Moreover, it is independent of any centralized service or coordination. On the other side, more available resources as well as multi-purposing and computational capacity from the grid environment are expected especially during the process of trustworthy subject searching and for storing of attribute certificates.

5. Conclusions

An ad hoc grid environment is an ad hoc organization of cooperating members without a fixed infrastructure and with only minimal administrative requirements. This paper has presented a short overview of this environment as well as of ad hoc grid authorization mechanisms.

We have designed support authorization mechanisms based on the intersection of VOs for an ad hoc grid. In the mechanism, the indirect trust for a VO is established based on the attribute certificates of k members which belong to trustworthy VOs. The mechanism can facilitate the building

of trust relationships for the phase of VO formation for ad hoc grid environments in cases when standard solutions have failed.

Further extension of the work involves the integration of the mechanism into existing grid middlewares like e.g. gLite or Globus Toolkit.

Acknowledgments. Parts of this work have been funded by the BMBF, the German Federal Ministry of Education and Research (FKZ 01IG07014D) and German Academic Exchange Service (DAAD).
The authors would like to thank the members of the Munich Network Management (MNM) Team for helpful discussions and valuable comments on earlier drafts of this paper. The MNM Team, directed by Prof. Dr. Heinz-Gerd Hegering, is a group of researchers at the Ludwig Maximilian University Munich, the Munich University of Technology, and the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences. *http://www.mnm-team.org*

References

[1] A. Arenas, M. Wilson, and B. Matthews, "On trust management in grids", In *Proceedings of the 1st international conference on Autonomic computing and communication systems*, ACM, October 2007, Brussels, Belgium.

[2] W. Hommel, and M. Schiffers, "Supporting Virtual Organization Life Cycle Management by Dynamic Federated User Provisioning," In *Proceedings of the 13th Workshop of the HP OpenView University Association (HPOVUA)*, Hewlett Packard Corporation, Nice, France, Mai 2006.

[3] H. Kurdi, M. Li, and H. Al-Raweshidy, "A Classification of Emerging and Traditional Grid Systems," In *IEEE Distributed Systems Online*, vol. 9, no. 3, March 2008.

[4] T. Friese, M. Smith, and B. Freisleben, "Hot Service Deployment in an Ad Hoc Grid Environment", In *Proceedings of the 2nd international conference on Service oriented computing*, ACM Press, New York, USA, 2004, pp. 75-83.

[5] K. Amin, G. von Laszewski, and A. R. Mikler, "Toward an Architecture for Ad Hoc Grids." In *Proceedings of the IEEE 12th International Conference on Advanced Computing and Communications (ADCOM 2004)*, Ahmedabad Gujarat, India, December 2004.

[6] D. C. Marinescu, G. M. Marinescu, Y. Ji, L. Blni, and H. J. Siegel, "Ad Hoc Grids: Communication and Computing in a Power Constrained Environment," In *Proceedings of the 22nd IEEE Int'l Performance, Computing and Communications Conf., (IPCCC)*, Phoenix, USA, IEEE Press. Los Alamitos, Ca, 2003, pp. 113-122.

[7] S. Shivle, H. Siegel, A. Maciejewski, et al., "Static Allocation of Resources to Communicating Subtasks in a Heterogeneous Ad Hoc Grid Environment," *Journal of Parallel and Distributed Computing*, vol. 66, no. 4, 2006, pp. 600-611.

[8] S. Zhao, A. Aggarwal, R. D. Kent, "PKI-Based Authentication Mechanisms in Grid Systems," In *IEEE Int. Conference on Networking, Architecture, and Storage*, 2007, pp.83-90.

[9] K. Amin, G. von Laszewski, and A. R. Mikler, "Grid Computing for the Masses: An Overview", In *Proceedings of the Grid Computing Conference (GCC 2003) (Lecture Notes in Computer Science, vol. 3033)*. Springer: Berlin, 2004; pp. 464-473.

[10] M. Smith, T. Friese, B. Freisleben, "Towards a Service-Oriented Ad Hoc Grid," In *Proceedings of the Third International Symposium on Parallel and Distributed Computing/Third International Workshop on Algorithms*, Models and Tools for Parallel Computing on Heterogeneous Networks (ISPDC/HeteroPar'04), Ireland, IEEE Press, 2004, pp. 201-208.

[11] "The Globus Toolkit," *http://www.globus.org/toolkit/*.

[12] R. Alfieri, R. Cecchini, V. Ciaschini, et al., "VOMS: an authorization system for virtual organizations," In *1st European across grids conference*, Spain, February 2003.

[13] L. Pearlman, V. Welch, I. Foster, et al., "A Community Authorization Service for Group Collaboration." In *the 3rd IEEE International Workshop for Policies on Distributed Systems and Networks*, 2002.

[14] Privilege and Role Management Infrastructure Standards Validation *http://www.permis.org/*

[15] Shibboleth *http://shibboleth.internet2.edu/*

[16] GridShib: A Policy Controlled Attribute Framework *http://gridshib.globus.org/*

[17] C. Grimm, R. Groeper, S. Makedanz, H. Pfeiffenberger, P. Gietz, M. Haase, M. Schiffers, and W. Ziegler, "Trust Issues in Shibboleth-Enabled Federated Grid Authentication and Authorization Infrastructures Supporting Multiple Grid Middleware," In *Third IEEE International Conference on e-Science and Grid Computing (e-Science 2007)*, Bangalore, India, December 2007, pp. 569-576.

[18] D-Grid Initiative *http://www.d-grid.de/*

[19] K. Amin, G. von Laszewski, M. Sosonkin, A.R. Mikler, and M. Hategan, "Ad Hoc Grid Security Infrastructure," In *6th IEEE/ACM International Workshop on Grid Computing (GRID'05)*, Seattle, USA, 2005, pp. 69-76.

[20] F. Kerschbaum, J. Haller, Y. Karabulut, and P. Robinson. "Pathtrust: A trust-based reputation service for virtual organization formation," In *iTrust2006, 4th International Conference on Trust Management*, Vol. 3986, Lecture Notes in Computer Science, pp. 193-205, Springer, 2006.

[21] S. Tuecke, V. Welch, D. Engert, L. Pearlman, and M. Thompson, "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile." *RFC 3820*, June 2004.

[22] M. R. Thompson, A. Essiari, and S. Mudumbai, "Certificate-based authorization policy in a PKI environment", In *ACM Transactions on Information and System Security (TISSEC)*, Volume 6, Issue 4, USA, November 2003, pp 566-588.